alert.category	alert.signature
Обнаружение успешных краж учетных данных	"ET PHISHING Successful Free Mobile (FR) Phish 2016-12-08", "ET PHISHING HTTP POST Contains Only Password (xyz) 2021-04-05", "ET PHISHING Successful RBC Royal Bank Phish M2 Aug 17 2017", "ET PHISHING Sendinblue Credential Phish Landing Page 2022-06-28", "ET PHISHING Successful Adobe Credential Phish 2022-06-21", "ET PHISHING Successful Barclays Phish M3 2016-09-09", "ET PHISHING Successful Generic Credential Phish Landing Page 2022-03-02", "ET PHISHING US Government Bid Credential Phish Landing Page 2022-12-28", "ET PHISHING Successful Singtel Phish 2016-06-22", "ET PHISHING Possible Successful COVID-19 Related Phish M2", "ET PHISHING Successful Generic Social Media Credential Phish 2022-03-31", "ET PHISHING Possible Successful Generic Phish (set) Dec 20 2016", "ET PHISHING Successful Squirrelmail Phishing 2015-11-20", "ET PHISHING Successful Google Drive Phish 2016-09-02", "ET PHISHING Possible Successful Generic Phish (set) 2017-12-20", "ET PHISHING Successful Generic Personalized Phish 2019-02-13", "ET PHISHING Successful Yahoo Phish 2016-10-27", "ET PHISHING Successful Hotmail Phish 2016-09-29", "ET PHISHING Successful Webmail Account Upgrade Phish 2016-12-27", "ET PHISHING Successful Canada Revenue Agency COVID-19 Assistance Eligability Phish 2020-04-01", "ET PHISHING Successful PayPal Phish Nov 24 2014", "ET PHISHING Successful Paypal Phish 2016-10-04", "ET PHISHING Successful Google Drive Phish M1 2016-09-01", "ET PHISHING Successful Office 365 Phish 2016-10-31", "ET PHISHING Successful Generic Phish 2022-07-29", "ET PHISHING Successful Bank of America Phish (set) M3 2016-10-14", "ET PHISHING Successful iCloud Phish 2015-12-02", "ET PHISHING Possible Successful Generic Phish (set) Jun 8 2016", "ET PHISHING Successful Docusign Phish 2016-11-17", "ET PHISHING Successful OWA Account Phish 2015-08-21", "ET PHISHING Successful Chase Phish M1 Aug 15 2017", "ET PHISHING Successful Paypal Phish M1 2016-01-19", "ET PHISHING Successful Microsoft Account Phish 2020-03-04", "ET PHISHING Successful Office 365 Phish 2022-07-19", "ET PHISHING Successful Google Drive Phish 2015-09-22", "ET PHISHING Successful Webmail Phish M1 2016-06-22", "ET PHISHING Successful Google Docs Phish M1 2016-10-19", "ET PHISHING Successful Paypal Phish M3 2016-10-26", "ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M4", "ET PHISHING Successful Paypal Phish 2015-12-05", "ET PHISHING Twitter Credential Phish Landing Page 2022-11-04", "ET POLICY Observed KnowBe4/Popcorn Training Simulated Phish Landing Page M3", "ET PHISHING Successful Bank of America Phish (set) M2 2016-10-14", "ET PHISHING Possible Successful Generic Phish (set) Oct 25 2016", "ET PHISHING Successful Adobe Phish 2016-09-14", "ET PHISHING Successful Santander Bank Phish 2016-10-28", "ET PHISHING Successful Paypal Phish M1 2016-12-05", "ET PHISHING Successful Generic Phish (set) 2020-08-07", "ET PHISHING Successful Tesco Phish (set) M4 Jul 18 2017", "ET PHISHING Successful Generic Phish (set) Oct 30 2017", "ET PHISHING HTTP POST Contains Only Password (gq) 2021-04-05", "ET PHISHING Successful Generic Credit Card Information Phish", "ET PHISHING Successful Webmail Account Upgrade Phish 2016-07-15", "ET PHISHING Observed DNS Query to ING Group Phishing Domain", "ET PHISHING Successful USAA Phish M1 2016-02-06", "ET PHISHING Successful Wells Fargo Phish M1 2016-11-18", "ET PHISHING Successful Adobe Phish Jun 17 2015", "ET PHISHING Successful Citibank Phish 2021-11-10", "ET PHISHING Successful Phishing Attempt via GetGoPhish Phishing Tool", "ET PHISHING Possible Successful TA422 Credential Phish 2022-03-17", "ET PHISHING Successful Generic Credential Phish 2022-07-08", "ET PHISHING Successful CenturyLink Phish 2016-10-12", "ET PHISHING Successful Paxful Cryptocurrency Wallet Phish Aug 30 2017", "ET PHISHING Successful Poste Italiane Phish Jun 08 2017", "ET PHISHING Possible Successful Generic Phish (set) Dec 13 2016", "ET PHISHING Facebook Credential Phish Landing Page M2 2022-06-01", "ET PHISHING Successful Docusign Phish M2 2016-08-17", "ET PHISHING Successful Paypal Phish 2015-12-24 M1", "ET PHISHING Possible Sucessful Generic Phish (set) 2020-08-04", "ET PHISHING Banca Monte dei Paschi di Siena Credential Phish Landing Page 2022-04-22", "ET PHISHING Successful Coinbase Phish 2022-07-18", "ET PHISHING Successful Yahoo Phish M1 2016-06-15", "ET PHISHING Facebook Credential Phish Landing Page 2022-06-08", "ET PHISHING Successful O2 Phish 2018-03-12", "ET PHISHING Successful Apple Phishing M1 2016-03-

	01", "ET PHISHING Successful Personalized Adobe PDF Online Phish 2016-10-26", "ET PHISHING Successful Yahoo Phish 2016-09-27", "ET PHISHING Successful Linkedin Phish 2016-10-12", "ET PHISHING Possible Successful Generic Phish 2016-06-22", "ET PHISHING Successful Excel Shared Document Phish 2016-06-02", "ET PHISHING Successful Personalized Phish (Multiple Brands) 2016-08-30", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mirohost .site in TLS SNI)", "ET PHISHING Successful Generic Phish 2022-03-11", "ET PHISHING Successful Google Drive Phish Dec 4 2015 M1", "ET PHISHING Successful DarkX Credential Phish 2022-12-19", "ET PHISHING Possible BulletProofLink Phishkit Activity - Redirect", "ET PHISHING Successful Sparkasse Credential Phish M1 2022-04-13", "ET PHISHING Successful Gmail Phish M1 2016-10-12", "ET PHISHING Generic Credential Phish Landing Page 2022-06-02", "ET PHISHING Successful RBFCU Credential Phish 2022-10-31", "ET PHISHING Successful iCloud Phish 2016-09-02", "ET PHISHING Successful Poste Italiane Phish 2016-12-23", "ET PHISHING Successful iTunes Connect Phish M3 2016-12-13", "ET PHISHING Successful Roundcube Credential Phish 2022-11-08", "ET PHISHING Phishing Landing Page - Excel Purchase Order Form", "ET PHISHING Successful Bank of America Phish 2016-12-05", "ET PHISHING Successful Microsoft Encrypted Email Phish M2 2016-06-23", "ET PHISHING Successful Intuit Phish 2016-07-21", "ET PHISHING Successful Fedex/DHL Phish 2018-10-22", "ET MALWARE Credit Card Scraper Domain in DNS Lookup (authorizen .net)", "ET PHISHING Possible Successful Generic Phish (set) Oct 26 2016", "ET PHISHING Successful Generic Phish (set) 2018-04-17", "ET PHISHING HTTP POST Contains Only Password (ga) 2021-04-05", "ET PHISHING Successful Paypal Phish 2016-08-31", "ET PHISHING Successful Generic Phish (set) 2018-10-16", "ET POLICY Observed KnowBe4/Popcorn Training Simulated Phish Landing Page M4", "ET PHISHING Successful Xoom Phishing 2015-11-24", "ET PHISHING Malicious SSL Certificate detected (Alibaba Phishing)", "ET PHISHING Client Cloaking Javascript Observed", "ET PHISHING Successful Facebook Phish 2016-05-18", "ET PHISHING lordspartner Phish Kit", "ET PHISHING Successful Personalized OWA Webmail Phish Oct 04 2016", "ET PHISHING Standard Bank Login Phish 2022-02-04", "ET PHISHING Successful mail .ru Credential Phish", "ET PHISHING Ulpian Credential Phish Landing Page 2022-11-22", "ET PHISHING Successful Craigslist (RO) Phish M2 Feb 24 2017", "ET PHISHING Successful Google Drive Phish Sept 1 M2 2015-09-02", "ET PHISHING Generic DarkX Phish 2022-01-22", "ET PHISHING Successful Bank of America Phish M2 2016-10-21", "ET PHISHING Successful Linkedin Phish 2016-12-09", "ET PHISHING Successful Credit Agricole Bank (FR) Phish M1 2016-10-19", "ET PHISHING Successful Generic Banking Phish 2016-10-28", "ET PHISHING Union Bank Credential Phish Landing Page 2022-08-29", "ET PHISHING Successful Paypal Phish 2016-09-09", "ET PHISHING Successful Generic Phish (set) Sep 28 2017", "ET PHISHING Successful Yahoo Mail Phish 2016-10-14", "ET PHISHING Successful Excel Phish 2016-08-19", "ET PHISHING Successful NAB Bank Phish M2 2016-10-19", "ET PHISHING Suspected TA445 Spearphishing Related Domain (meta-ua .space in TLS SNI)", "ET PHISHING Sucessful Alibaba Credential Phish 2022-06-29", "ET PHISHING Generic Credential Phish Landing Page M1 2022-09-28", "ET PHISHING Successful Google Drive Phish 2016-08-18", "ET PHISHING Successful Banco Itau (BR) Phish Jun 09 2017", "ET PHISHING Successful FreeMobile (FR) Phish M1 2016-10-31", "ET PHISHING Successful Survey Credential Phish M3 2022-04-04", "ET PHISHING Secure Email Portal Lure Landing Page", "ET PHISHING Successful Generic Phish (set) 2019-05-14", "ET MALWARE MSIL/PSW.Agent.RXP Checkin", "ET PHISHING Generic Credential Phish Landing Page 2022-10-26", "ET PHISHING Successful Maybank2u Phish 2016-06-17", "ET PHISHING Successful Excel Phish 2016-11-17", "ET PHISHING Possible Successful Outlook Web App Phish 2016-12-28", "ET PHISHING Successful USAA Phish 2015-10-20", "ET PHISHING Possible Successful Phish - Generic POST to myform.php Feb 01 2013", "ET PHISHING Successful NatWest Bank Phish 2015-11-03", "ET PHISHING Generic Phish Landing Page 2022-01-14", "ET PHISHING Successful DHL Phish 2016-11-15", "ET PHISHING Successful Workspace Phish 2016-01-26", "ET PHISHING Successful Spyus Phish (Multiple Brands) M1 2016-12-12", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (verify-mail .space)", "ET PHISHING Successful Paypal Phish Mar 22 2017", "ET PHISHING Successful PayPal Phish Nov 30

	2012", "ET PHISHING Successful Commonwealth Bank Phish Fake Error Page 2015-08-20", "ET HUNTING Suspicious HTTP POST Only Containing Password - Possible Phishing", "ET PHISHING Successful Manhattan College Credential Phish 2022-01-10", "ET PHISHING Successful Windows Live Phish 2016-12-23", "ET PHISHING Successful Phish Fake Document Loading Error 2015-07-27", "ET PHISHING Successful Bank of Oklahoma Phish M1 Jul 21 2016", "ET PHISHING Successful Bank of America Phish 2016-10-14", "ET PHISHING Successful Bank of America Phish 2015-10-02", "ET PHISHING Possible Successful USAA Phishing Domain Feb 02 2017", "ET PHISHING Successful Samsung Portal Phish 2015-10-13", "ET PHISHING L33bo Phishing Kit - Successful Credential Phish M4 2016-03-29", "ET PHISHING Successful Survey Credential Phish M6 2022-04-04", "ET PHISHING Successful Paypal Phish 2015-11-03 M3", "ET PHISHING Successful Wildblue Phishing M1 2015-11-24", "ET PHISHING Successful Banco de la Nacion Phish 2016-10-18", "ET PHISHING Successful Facebook Phish 2018-04-16", "ET PHISHING Successful Google Drive Phish 2016-10-12", "ET PHISHING Successful Wells Fargo Phish M1 2015-11-21", "ET PHISHING Possible Successful Generic Phish (set) 2017-12-04", "ET PHISHING Successful DHL Phish 2016-07-11", "ET PHISHING Successful Wells Fargo Phish 2016-11-28", "ET PHISHING L33bo Phishing Kit - Successful Credential Phish M1 2016-03-29", "ET PHISHING Successful Generic Phish 2022-08-01", "ET PHISHING Possible Successful Generic Phish Aug 31 2015", "ET PHISHING Generic Credential Phish Landing Page 2022-06-13", "ET PHISHING PerSwaysion JavaScript Response M1", "ET PHISHING Successful Webmail Phish M2 2016-06-22", "ET PHISHING Successful Barclays Phish M2 2016-10-06", "ET PHISHING Successful Generic Miarroba Phish 2019-07-11", "ET MALWARE MSIL/Spy.Agent.AES Zipped Exfil", "ET PHISHING Successful Amazon Phish 2015-11-07", "ET PHISHING Successful Emirates NBD Bank Credential Phish 2022-06-23", "ET PHISHING Successful Synchronize Email Account Phish 2016-06-15", "ET PHISHING Successful Christian Mingle Phish 2016-06-17", "ET PHISHING Successful 163.com Email Account Phish 2016-10-26", "ET PHISHING Successful Mailbox Deactivation Phish 2016-08-19", "ET PHISHING ING Credential Phish Landing Page 2022-05-27", "ET PHISHING Successful Navy Federal Phish 2016-06-16", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (weryfikacja-poczty .space)", "ET PHISHING Possible Successful Generic Phish (set) Nov 15 2016", "ET PHISHING Successful Amazon Account Phish 2015-08-21", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (kontrola-poczty .space)", "ET PHISHING PerSwaysion Landing Page M3", "ET PHISHING Possible Successful Generic Phish (set) Jul 10 2017", "ET PHISHING Successful NatWest Bank Phish M3 2016-10-19", "ET PHISHING Successful Wells Fargo Phish Loading Page 2016-01-07", "ET PHISHING Possible Cryptowallet Mining Pool Scam Landing Page", "ET PHISHING Successful Adobe Phish 2015-08-31", "ET PHISHING PerSwaysion Phishkit Javascript Config Variables", "ET PHISHING Successful Generic Credential Phish 2022-12-06", "ET PHISHING Successful Zimbra Account Phish 2015-10-23", "ET PHISHING Successful Paypal Phish M1 2016-11-17", "ET PHISHING Successful Dynamic Folder Phish M1 2016-11-22", "ET PHISHING Successful Personalized DHL Phish 2016-10-12", "ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (emails-circleci .com)", "ET PHISHING Possible Successful Generic Paypal Phish Jan 23 2016", "ET PHISHING Successful HMRC Phish Oct 18 2017", "ET PHISHING Possible Successful AirCanada Phish 2015-08-06", "ET PHISHING Successful Yahoo Phish 2016-10-25", "ET PHISHING Successful Danske Bank Phish (DA) 2016-10-27", "ET PHISHING Generic Credit Card Information in HTTP POST - Possible Successful Phish Jun 12 2017", "ET PHISHING Successful iTunes Phish Mar 21 2014", "ET PHISHING Successful Apple Phish (set) 2016-03-01", "ET PHISHING Successful Dynamic Folder Phish M1 2016-12-02", "ET PHISHING Successful Adobe Shared Document Phish 2016-09-29", "ET PHISHING Successful Google Drive Phish 2015-09-04", "ET PHISHING Apple Credential Phish Landing Page M1 2022-06-21", "ET PHISHING Possible Successful *.myjino. ru Phish 2016-12-16", "ET PHISHING Successful Dropbox Phish June 17 2015", "ET PHISHING Successful DHL Phish 2015-09-17", "ET PHISHING Successful UBS Phish 2016-10-21", "ET PHISHING iCloud Credential Phish Landing Page 2022-12-06", "ET PHISHING Successful Webmail Validator Phish M2 2016-09-02", "ET PHISHING Possible Successful Generic Phish (set)

	2020-11-19", "ET PHISHING Successful Banco Itau (BR) Phish M2 2016-12-08", "ET PHISHING Possible Successful Generic Phish (set) 2021-03-18", "ET PHISHING Successful LCL Bank Phish 2015-11-05", "ET PHISHING Successful Supplier Portal Phish 2016-10-07", "ET PHISHING Successful Facebook Phish M2 2016-09-30", "ET PHISHING Successful Chase Phish M2 2016-10-17", "ET PHISHING Successful US Bank Phish M2 2015-12-22", "ET PHISHING Successful Alibaba Phish 2016-09-29", "ET PHISHING Possible Successful Generic Phish (set) Nov 20 2017", "ET PHISHING Possible Successful Ebay Phishing Domain Feb 02 2017", "ET PHISHING Successful Raiffeisen Phish Nov 03 2017", "ET PHISHING Successful Google Docs Phish M2 2016-10-19", "ET PHISHING Successful Bank of America Phish M1 Oct 01 2012", "ET PHISHING Successful Airbnb COVID-19 Phish 2020-03-26", "ET PHISHING Successful Webmail Validator Phish M1 2016-09-02", "ET PHISHING Successful Chase Phish 2016-09-02", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mod-mil .site in TLS SNI)", "ET PHISHING Successful Barclays Phish M1 2016-10-06", "ET PHISHING Successful Apple Phish M1 2016-09-29", "ET PHISHING Successful Outlook Phish 2016-10-03", "ET PHISHING Successful SeniorPeopleMeet Phish M1 2016-09-14", "ET PHISHING Successful Chase Phish M1 2016-08-26", "ET PHISHING Successful Dynamic Folder Phishing Oct 06 2016", "ET PHISHING Successful IRS Phish 2016-01-23", "ET PHISHING Successful Trust Wallet Phish 2022-10-11", "ET PHISHING Possible Successful Generic Phish (set) 2021-03-08", "ET PHISHING Successful EC21 B2B Phish 2016-10-21", "ET PHISHING Possible Successful Yahoo Phish Nov 21 2012", "ET PHISHING Possible Successful Generic Phish (set) 2018-06-14", "ET PHISHING Successful Google Drive Phish 2016-09-27", "ET PHISHING Possible Successful Google Drive Phish M1 2015-07-28", "ET PHISHING Successful Generic Credential Phish M1 2022-06-08", "ET PHISHING Successful Bank of America Phish 2016-10-03", "ET PHISHING Possible Successful Craigslist Phishing Domain Feb 07 2017", "ET PHISHING Successful Adobe Shared Document Phish 2016-08-10", "ET PHISHING Successful Airbnb COVID-19 Phish 2020-03-25", "ET PHISHING Possible Successful Paypal Phishing Domain (IT) Oct 10 2017", "ET PHISHING Successful Generic Phish (set) 2019-05-21", "ET PHISHING Suspected TA445 Spearphishing Related Domain (bigmir .space in TLS SNI)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (ua-passport .space)", "ET PHISHING Possible Successful Banking Phish (BR) 2016-09-29", "ET PHISHING Successful Generic Phish (set) 2018-10-18", "ET PHISHING Successful Dropbox Phish 2016-08-31", "ET PHISHING Successful Paypal Phish Oct 16 2017", "ET PHISHING L33bo Phishing Kit - Successful Credential Phish M3 2016-03-29", "ET PHISHING Generic Successful Phish 2022-10-11", "ET PHISHING Successful SeniorPeopleMeet Phish M2 2016-09-14", "ET PHISHING Possible Successful COVID-19 Related Phish M1", "ET PHISHING Observed DNS Query to OWA Phishing Domain", "ET PHISHING Successful Paypal Account Phish Oct 30", "ET PHISHING Successful Bradesco Bank Phish M1 Jan 05 2017", "ET PHISHING Possible Successful Hotmail Phish Nov 21 2012", "ET PHISHING Possible Successful Phish (Google/Dropbox/Netflix) 2015-07-11", "ET PHISHING Successful Paypal Phish 2016-10-21", "ET PHISHING Successful Ebay Phish M2 2016-12-29", "ET PHISHING Emirates NBD Bank Credential Phish Landing Page 2022-06-23", "ET PHISHING Successful Dropbox Phish 2016-05-16", "ET PHISHING Suspected TA445 Spearphishing Related Domain (weryfikacja-konta .space in TLS SNI)", "ET PHISHING Successful Generic Credential Phish 2022-10-11", "ET PHISHING Possible Successful Generic Phish (set) Jun 08 2017", "ET PHISHING BulletProofLink Phishkit Activity (GET)", "ET PHISHING Successful Apple ID Phish 2015-08-18", "ET PHISHING Successful Email System Manager Phish 2016-04-13", "ET PHISHING Successful Coinbase Credential Phish 2023-01-09", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mod-mil .site)", "ET PHISHING Successful Generic .EDU.TW Phish (Legit Set)", "ET PHISHING Successful Google Drive/Dropbox Phish Nov 20 2016", "ET PHISHING Successful DHL Phish 2016-10-07", "ET PHISHING Successful Facebook Phish 2019-08-29", "ET PHISHING Successful FR Gmail Phish M1 2016-03-15", "ET PHISHING Successful USAA Phish M2 2016-02-06", "ET PHISHING Successful Apple Store Phish M4 2016-12-29", "ET PHISHING Successful Paypal Account Phish 2015-10-30 3", "ET PHISHING Successful Colleagues Quarantined with COVID-19 Phish 2020-03-25", "ET PHISHING Possible

	Successful Generic Phish (set) 2019-01-30", "ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21", "ET PHISHING Successful US Bank Phish 2016-06-09 M1", "ET PHISHING Possible Successful Verified by Visa Phish Jan 30 2014", "ET PHISHING Successful Bank of America Phish M2 2016-10-27", "ET PHISHING Successful Windows Live Account Phish 2016-10-26", "ET PHISHING Successful Paypal Phish M1 2016-10-17", "ET PHISHING Successful HM Revenue & Customs Phish M2 Apr 07 2017", "ET PHISHING Successful Generic Phish - Observed in Apple/Bank of America/Amazon 2016-10-26", "ET PHISHING Successful Ameli.fr Phish M1 2016-10-26", "ET PHISHING Successful Bank of America Phish M1 2016-10-27", "ET PHISHING Successful Instagram Phish Mar 14 2017", "ET PHISHING Successful Paypal Phish M2 2016-10-06", "ET PHISHING Successful Wells Fargo Phish M1 2016-09-30", "ET PHISHING Successful Gmail Account Update Phish 2016-05-10", "ET PHISHING Successful IRS Phish 2018-05-07", "ET PHISHING Successful Adobe Shared Document Phish 2016-10-03", "ET PHISHING Possible Successful Generic Phish 2016-05-26", "ET PHISHING Successful Phish to Compromised Wordpress Site 2016-03-23", "ET PHISHING Possible Successful Generic Phish (set) Jan 03 2017", "ET PHISHING Successful Generic Phish 2020-01-29 (set)", "ET PHISHING Generic Credential Phish Landing Page 2022-05-27", "ET PHISHING Successful Microsoft Outlook Credential Phish 2022-10-03", "ET PHISHING Successful Veridian Credit Union Credential Phish 2022-11-08", "ET PHISHING Successful Adobe Phish 2022-01-12", "ET PHISHING Successful XBOOMBER Paypal Phish Nov 28 2016", "ET PHISHING Successful Office 365 Phish 2016-08-24", "ET PHISHING Successful Ziraat Bankasi (TK) Phish M2 Oct 12 2017", "ET PHISHING Successful Generic L33bo Phish - URI Contents (set)", "ET PHISHING Axie Infinity Credential Phish Landing Page M2 2022-05-18", "ET PHISHING Successful Generic Phish to zap-webspace.com Webhost 2018-10-25", "ET PHISHING Possible Successful Generic Phish (set) 2017-12-03", "ET PHISHING Successful Paypal Phish M2 Aug 14 2017", "ET PHISHING Possible Successful Generic Phish (set) 2018-05-31", "ET PHISHING Successful Google Drive Phish M1 2016-12-02", "ET PHISHING Possible DarkX Credential Phishing Landing Page 2022-12-19", "ET PHISHING Successful Telstra Phish M1 2015-09-05", "ET PHISHING Successful Anonisma Phish 2015-12-01", "ET PHISHING Successful Zoom.us Phish 2021-10-25", "ET PHISHING GCash Credential Phish 2022-06-17", "ET PHISHING Successful Generic Phish 2018-06-27 (set)", "ET PHISHING Successful PayPal Phish Dec 19 2012", "ET PHISHING Successful BECU Phish 2022-09-08", "ET PHISHING Successful Gmail Phish 2016-08-18", "ET PHISHING Successful Gmail Phish M1 2016-08-12", "ET PHISHING Successful Facebook Phish 2018-01-26", "ET PHISHING Successful Adobe Online Phish 2015-09-30", "ET PHISHING Successful Generic Phish M2 2016-10-27", "ET PHISHING Nourblog1 Phish Kit", "ET PHISHING Successful Sparkasse Credential Phish M2 2022-04-13", "ET PHISHING Successful Protected PDF (Excel Template) Phish 2016-12-28", "ET PHISHING Successful Generic Cryptowallet Credential Phish 2022-05-12", "ET PHISHING Successful Generic Phish (set) 2018-03-12", "ET PHISHING Successful Generic Credit Card Information Phish 2020-01-27", "ET PHISHING 401TRG Successful Multi-Email Phish - Observed in Docusign/Dropbox/Onedrive/Gdrive Nov 02 2017", "ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .xyz) 2021-04-15", "ET PHISHING Successful Google Drive Phish M2 2016-08-25", "ET PHISHING Successful Apple Store Phish M1 2016-12-29", "ET PHISHING Successful Apple Phish 2016-06-15", "ET PHISHING Successful Orange Credential Phish 2022-07-07", "ET PHISHING Successful CSIS Credential Phish", "ET PHISHING Successful Alibaba Phish 2016-12-20", "ET PHISHING Successful Generic Credential Phish - Loading Messages 2015-08-12", "ET PHISHING Successful Microsoft Office Phish 2020-02-26", "ET PHISHING Generic Credential Phish Landing Page 2022-02-25", "ET PHISHING Successful Sparkasse (DE) Phish 2016-12-22", "ET PHISHING Successful Yahoo Password Strength Phish M2 2016-08-24", "ET PHISHING Successful Mailbox Renew Phish 2015-08-14", "ET PHISHING Successful Dubai Islamic Internet Bank Phish 2016-12-20", "ET PHISHING TA398 Phishing Kit URI Pattern M1", "ET PHISHING Successful Fake Webmail Quota Phish 2015-09-10", "ET PHISHING Successful GNCU Credential Phish 2022-11-14", "ET PHISHING Possible Successful Generic Phish (set) 2018-06-11", "ET PHISHING Successful Generic Credit Card Information Phish 2019-06-04", "ET PHISHING Monzo Credential

	Phish Landing Page 2022-02-17", "ET PHISHING Midea Credential Phish Landing Page 2022-07-12", "ET PHISHING Successful EDF Account Phish 2015-09-01", "ET PHISHING Successful Adobe Phish 2016-04-29", "ET PHISHING Successful Excel Phish Aug 15 2016", "ET PHISHING Successful US Bank Phish M1 2015-12-22", "ET PHISHING Successful Google Docs Phish 2016-09-01", "ET PHISHING Successful Generic Credential Phish M2 2022-06-08", "ET PHISHING Successful US Bank Phish 2016-09-20", "ET PHISHING Generic Credential Phish Landing Page 2022-10-03", "ET PHISHING Successful USAA Phish 2015-09-05", "ET PHISHING Caixa Credential Phish Landing Page 2022-07-05", "ET PHISHING Possible Successful Generic Phish Jan 14 2016", "ET PHISHING Successful Banco do Brasil Phish M2 Sep 29 2017", "ET PHISHING Successful iCloud Phish Oct 10 2016", "ET PHISHING Successful Netflix Credential Phish 2022-12-27", "ET PHISHING PerSwaysion JavaScript Response M2", "ET PHISHING Successful OWA Phish Apr 25 2017", "ET PHISHING Successful Generic Phish - JS Redirect to PDF 2016-08-24", "ET PHISHING PyPI Successful Credential Harvesting Attempt", "ET PHISHING Possible Successful Linkedin Phishing Domain Feb 02 2017", "ET PHISHING Possible Successful Generic Phish (set) May 24 2017", "ET PHISHING Successful PHOEN!X Apple Phish M1 2015-12-29", "ET PHISHING Successful Zimbra Phish 2015-11-03", "ET PHISHING DHL Credential Phish Landing Page 2022-10-07", "ET PHISHING Successful Dropbox Phish 2015-11-04", "ET PHISHING Successful Banco de la Repblica Oriental del Uruguay Phish 2022-11-30", "ET PHISHING Successful Generic Phish (set) 2019-04-12", "ET PHISHING Successful Paypal Phish M2 Sep 15 2017", "ET PHISHING Successful Citizenbank Phish 2016-05-24 M2", "ET PHISHING DHL Credential Phish Landing Page 2022-06-09", "ET PHISHING Successful Microsoft Account Phish 2019-01-29", "ET PHISHING Successful Dropbox Phish 2015-12-10", "ET PHISHING Successful Ebay Phish M1 2016-12-29", "ET PHISHING Successful My ADP Phish (set) 2017-02-16", "ET PHISHING IRS Payment Credential Phish Debit Card or Check Data Exfil", "ET PHISHING Successful DHL Phish 2016-02-09", "ET PHISHING Successful Generic Phish (set) Aug 21 2017", "ET PHISHING Facebook Credential Phish Landing Page 2022-06-21", "ET PHISHING DAWN Comment in Phish Landing Page 2022-02-01", "ET PHISHING Facebook Credential Phish Landing Page 2022-08-22", "ET PHISHING Successful US Government Bid Credential Phish 2022-12-28", "ET PHISHING Successful Scotiabank Phish M1 May 24 2017", "ET PHISHING Successful Apple Phish M1 2015-12-02", "ET PHISHING Successful Banco Itau (BR) Phish M1 2016-12-08", "ET PHISHING Successful Generic Phish (set) 2018-09-21", "ET PHISHING Successful Paypal Phish M2 2016-10-05", "ET PHISHING Successful Apple Phish M1 2016-09-14", "ET PHISHING Possible Successful Generic Phish (set) 2018-02-13", "ET PHISHING Successful Excel Online Phish 2015-12-08", "ET PHISHING Generic Phishing DNS Lookup (xn--sapeaunoticias-kjb .com .br)", "ET PHISHING Successful UK Tax Phishing M1 2016-02-01", "ET PHISHING Successful Apple Store Transaction Cancellation Phish 2016-08-30", "ET PHISHING Successful Generic Phish 2018-05-08 (set)", "ET PHISHING Successful Bradesco Bank Phish M2 Jan 05 2017", "ET PHISHING Generic Credential Phish Landing Page 2022-10-12", "ET PHISHING Successful Generic Phish 2016-09-08", "ET PHISHING Suspected TA445 Spearphishing Related Domain (kontrola-poczty .site in TLS SNI)", "ET PHISHING Generic Credential Phish 2020-07-27 (set)", "ET PHISHING Successful Gmail Phish M2 2016-10-12", "ET PHISHING Successful o365 Credential Phish 2022-12-19", "ET PHISHING Successful Generic Phish (Meta HTTP-Equiv Refresh) Dec 29 2016", "ET PHISHING Successful Shared Adobe PDF Phish 2016-11-17", "ET PHISHING Successful Google Drive Phish 2016-10-06", "ET PHISHING Suspected TA445 Spearphishing Related Domain (walidacja-uzytkownika .space in TLS SNI)", "ET PHISHING Successful Citizenbank Phish 2016-05-24 M1", "ET PHISHING Successful WhatsApp Payment Phish 2016-09-01", "ET PHISHING Successful Spyus Phish (Multiple Brands) M2 2016-12-12", "ET PHISHING Successful Email Login Phish 2016-06-02", "ET PHISHING Successful Citibank Phish Landing Page", "ET PHISHING Successful Chase Phish 2016-10-18", "ET PHISHING Successful Commonwealth Bank Phish 2015-08-20", "ET PHISHING FancyBear/APT28 Related Phish Landing Page 2022-03-08", "ET PHISHING Successful DHL Phish 2016-09-16", "ET PHISHING Successful Paypal Phish M5 2016-12-13", "ET PHISHING Successful Microsoft Live Email Account Phish 2016-09-08", "ET PHISHING Possible Successful Generic Phish (set) 2020-09-29", "ET PHISHING

	Successful FreeMobile (FR) Phish M1 2016-10-06", "ET PHISHING Successful Credential Phish (Multiple Brands) 2016-11-18", "ET PHISHING Successful Key Bank Phish M1 2015-08-20", "ET PHISHING Successful Outlook Phish 2015-08-18", "ET PHISHING Successful Bank of America Phish M2 2015-10-02", "ET PHISHING Successful Account Update Phish 2015-09-01", "ET PHISHING Successful Google Docs Phish 2015-12-09", "ET PHISHING Successful Halkbank Phish M1 2018-04-16", "ET PHISHING BT Group Credential Phish Landing Page 2022-07-01", "ET PHISHING Generic Credential Phish Landing Page 2022-12-07", "ET PHISHING ING Banking Credential Phish Landing Page 2022-12-12", "ET PHISHING Successful Santander Phish M2 Oct 04 2017", "ET PHISHING HTTP POST Contains Only Password (cf) 2021-04-05", "ET PHISHING Successful Earthlink Phish 2016-10-21", "ET PHISHING Generic Credential Phish Landing Page 2022-05-24", "ET PHISHING Successful Monzo Credential Phish M3 2022-02-17", "ET PHISHING Successful Square Phish 2016-06-15", "ET PHISHING Possible Successful SWF/XML Phish 2016-05-02", "ET PHISHING Successful BB&T Bank Phish 2016-12-15", "ET PHISHING Successful Fedex/DHL Phish (set) 2018-10-22", "ET PHISHING Successful America First CU Credential Phish 2022-12-14", "ET PHISHING Successful Generic Personalized Phish 2018-09-27 M2", "ET PHISHING Successful Apple Account Phish Feb 17 2017", "ET PHISHING Successful DHL Phish 2015-09-14", "ET PHISHING Successful Dropbox Phish M2 2015-12-10", "ET PHISHING Successful Phish OWA Credentials 2016-08-16", "ET PHISHING TA398 Phishing Kit URI Pattern M2", "ET PHISHING Possible Successful Generic Phish to .ma Domain 2020-07-15", "ET PHISHING Successful Adobe Phish M1 2016-07-11", "ET PHISHING Successful ABSA Phish 2016-10-26", "ET PHISHING Successful Generic Phish 2016-10-27", "ET PHISHING Successful Google Drive Phish 2016-11-18", "ET PHISHING Successful Key Bank Phish M2 2015-08-20", "ET PHISHING Successful Impots.gouv.fr Phish M1 2015-08-21", "ET PHISHING Successful Adobe Online Account Phish 2015-08-21", "ET PHISHING Successful Adobe Shared Document Phishing 2015-11-20", "ET PHISHING Successful Google Account Phish Dec 04 2012", "ET PHISHING Successful Microsoft Live Email Account Phish 2016-11-29", "ET PHISHING ghayt_Zone Phishing Kit", "ET PHISHING Successful Chase Phish 2020-10-14", "ET PHISHING Possible BulletProofLink Phishkit Activity - Retrieving Images", "ET PHISHING Successful Bank of America Phish 2015-11-21", "ET PHISHING Successful Natwest Bank Phish 2015-11-21", "ET PHISHING IRS Payment Credential Phish Form", "ET PHISHING Successful Chase Phish M3 2016-08-26", "ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (circle-ci .com)", "ET PHISHING Successful Apple Phish M1 Mar 15 2017", "ET PHISHING Successful Shipping Document Phish 2015-09-29", "ET PHISHING PerSwaysion Phishkit Message Variables", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mil-gov .space in TLS SNI)", "ET POLICY Observed KnowBe4/Popcorn Training Simulated Phish Landing Page M5", "ET PHISHING Possible Successful Fedex Phish 2015-07-28", "ET PHISHING Successful AOL/PayPal Phish Nov 24 2014", "ET PHISHING PerSwaysion Phishkit Javascript - Observed Repetitive Custom JS Components", "ET PHISHING Possible Successful Generic Phish (set) Nov 16 2016", "ET PHISHING Successful Alibaba Credential Phish 2015-10-05", "ET PHISHING Successful Facebook Payment Phish M1 2016-09-29", "ET PHISHING Successful PostBank Credential Phish 2022-12-12", "ET PHISHING Successful Banamex Bank Phish 2016-12-29", "ET PHISHING Successful Generic Credit Card Information Phish 2019-11-04", "ET PHISHING Successful Banco do Brasil Phish M2 2016-10-25", "ET PHISHING Possible Successful Generic Phish (set) 2017-12-19", "ET PHISHING Successful NAB Bank Phish M1 2016-10-19", "ET PHISHING Successful Paypal (DE) Phish 2016-10-04", "ET PHISHING Successful Generic .EDU Phish Aug 17 2017", "ET PHISHING Successful Generic Credential Phish 2022-11-22", "ET PHISHING Successful Excel Online Phish 2016-10-05", "ET PHISHING Possible Successful Remax Phish - Hotmail Creds Nov 25 2013", "ET PHISHING Successful Paxful Cryptocurrency Wallet Phish 2020-08-17", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (walidacja-uzytkownika .space)", "ET PHISHING Successful Banco Itau (BR) Mobile Phish Feb 17 2017", "ET PHISHING Successful Mailbox Shutdown Phish M1 2016-05-16", "ET PHISHING Successful BankAustria Phish Nov 03 2017", "ET PHISHING Generic Credential Phish Landing Page 2022-09-14", "ET PHISHING Successful Facebook

	Phish 2022-07-18", "ET PHISHING Successful Dynamic Folder Phish 2016-10-26", "ET PHISHING Successful WeTransfer Phish Oct 04 2016", "ET PHISHING Facebook Credential Phish Landing Page M1 2022-06-01", "ET PHISHING Successful Facebook Credential Phish 2022-07-05", "ET PHISHING Possible Successful Generic Phish (set) Nov 22 2016", "ET PHISHING Axie Infinity Credential Phish Landing Page M3 2022-05-18", "ET PHISHING Successful WhatsApp Payment Phish M1 2016-11-15", "ET PHISHING Successful Survey Credential Phish M2 2022-04-04", "ET PHISHING Successful HealthEquity Phish 2016-09-01", "ET PHISHING Generic Credential Phish Landing Page 2022-06-21", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirohost .site)", "ET PHISHING Successful PDF Online Phish 2016-12-19", "ET PHISHING Successful Outlook Webmail Phishing 2015-11-21", "ET PHISHING Successful Survey Credential Phish 2015-08-12", "ET PHISHING Successful Chase Phish 2015-09-23", "ET PHISHING Successful Facebook Phish 2016-10-12", "ET PHISHING Successful BT GROUP Credential Phish 2022-11-23", "ET PHISHING Successful Amazon Phish 2016-10-27", "ET HUNTING Possible Fake 404 Credential Phish Landing Page", "ET PHISHING Successful PHOEN!X Apple Phish M2 2015-12-29", "ET PHISHING Successful IRS Credential Phish 2022-04-25", "ET PHISHING Successful Credit Agricole Bank (FR) Phish M3 2016-10-19", "ET PHISHING Successful Mailbox Upgrade Phish 2016-06-27 M2", "ET PHISHING Successful Yahoo Password Strength Phish M1 2016-08-24", "ET PHISHING Possible Successful Phish to .tk domain Aug 26 2016", "ET PHISHING Successful Generic Phish (set) 2018-06-29", "ET PHISHING HTTP POST to Free Webhost - Possible Successful Phish (site40 . net) Jul 18 2017", "ET PHISHING Successful Zimbra Phish 2015-10-30", "ET PHISHING Successful Trademe Phish M3 2015-11-26", "ET PHISHING Possible Successful Generic Phish (set) Sep 19 2017", "ET PHISHING Successful Sparkasse Phish Nov 03 2017", "ET PHISHING Successful Survey Credential Phish M4 2022-04-04", "ET HUNTING Suspicious POST to Wordpress Folder - Possible Successful Banking Phish", "ET PHISHING Successful Commerce Bank Phish 2022-07-30", "ET PHISHING Successful Personalized DHL Phish 2016-10-20", "ET PHISHING Observed Possible Phishing Landing Page 2021-06-29", "ET PHISHING Successful Chase Phish 2016-12-13", "ET PHISHING Successful Stripe Phish 2016-12-09", "ET PHISHING Successful Generic .EDU Phish (Legit Set)", "ET PHISHING Possible Successful Generic Phish (set) Jul 06 2017", "ET PHISHING Generic Credential Phish Landing Page M2 2022-09-28", "ET PHISHING Successful Generic Phish (set) 2018-09-24", "ET PHISHING Successful Blockchain Account Phish Aug 19 2016", "ET PHISHING IRS Credential Phish Direct Deposit Payment Data Exfil", "ET PHISHING Successful Paypal Phish 2016-09-06", "ET PHISHING Successful Generic Phish - Phone Number 2015-09-02", "ET PHISHING Successful USAA Phish 2016-08-30", "ET PHISHING Possible Successful Generic Phish to .ml Domain 2018-10-23", "ET PHISHING Successful Outlook WebApp Phish 2016-09-02", "ET PHISHING Microsoft Excel Credential Phish Landing Page 2022-10-03", "ET PHISHING Successful Paypal Phish M1 2016-10-05", "ET PHISHING Successful Yobit Cryptocurrency Exchange Phish 2017-12-28", "ET PHISHING Successful Paypal Phish Jan 23 2017", "ET PHISHING Successful Tesco Phish (set) M3 Jul 18 2017", "ET PHISHING Successful Paypal Phish 2015-10-28 3", "ET PHISHING Successful Bank of America Phish M1 2016-08-31", "ET PHISHING Successful Yahoo Phish M1 2016-09-08", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mil-gov .space)", "ET PHISHING GOV UK Possible COVID-19 Phish 2020-04-06", "ET PHISHING Suspected TA445 Spearphishing Related Domain (verify-mail .space in TLS SNI)", "ET PHISHING Apple Credential Phish Landing Page M2 2022-06-21", "ET PHISHING Possible Successful Generic Phish to .gq Domain 2018-10-23", "ET PHISHING Successful Paypal Phish Nov 24 2014", "ET PHISHING Successful ANZ Internet Banking Phish 2022-06-23", "ET PHISHING Successful Gmail Phish 2016-09-30", "ET PHISHING Possible Successful Yahoo Phish Jun 23 2015", "ET PHISHING Successful Apple Phish M2 2016-09-29", "ET PHISHING Generic Credential Phish Landing Page M2 2022-04-05", "ET PHISHING Possible Successful Generic Phish (set) 2021-04-08", "ET PHISHING Successful Generic Phish (set) 2019-07-09", "ET PHISHING Successful Adobe Shared PDF Phish 2016-12-13", "ET PHISHING Successful Mailbox Update Phish 2016-02-17", "ET PHISHING Successful Outlook Phish 2016-08-31", "ET PHISHING Suspected TA445 Spearphishing

	Related Domain in DNS Lookup (meta-ua .space)", "ET PHISHING Successful Generic Phish (set) 2018-08-01", "ET PHISHING Successful Dropbox Phish 2016-10-25", "ET PHISHING Successful TeamIPwned Phish 2016-08-30", "ET MALWARE MSIL/PSW.Agent.SUD Zipped Data Exfil", "ET PHISHING Successful Google Drive Phish 2016-12-22", "ET PHISHING Successful Microsoft Phish 2022-07-10", "ET PHISHING Successful Telstra Credential Phish 2022-08-26", "ET PHISHING Possible Successful AOL Phish Nov 21 2012", "ET PHISHING Successful Mailbox Shutdown Phish M2 2016-05-16", "ET PHISHING Successful Webmail Phish M3 2016-06-22", "ET PHISHING Successful Mailbox Upgrade Phish 2016-06-27 M1", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M7", "ET PHISHING Successful Gmail Phish 2016-12-06", "ET PHISHING Successful Tectite Web Form Submission - Possible Phishing", "ET PHISHING Successful Made In China Phish 2016-09-28", "ET PHISHING Successful Telstra Credential Phish 2022-08-29", "ET PHISHING Possible Successful Generic Phish (set) 2019-02-13", "ET PHISHING Successful View Invoice Phish M2 2016-10-05", "ET PHISHING Successful Dynamic Folder Phish 2016-11-28", "ET PHISHING Successful Generic Banking Phish 2022-01-11", "ET PHISHING Successful Generic Webmail Phish 2016-12-02", "ET PHISHING Successful Team IPwned Phish 2016-08-24", "ET PHISHING Possible Successful Hostinger Generic Phish Jun 09 2017", "ET PHISHING Successful Exmo Cryptocurrency Exchange Phish Aug 28 2017", "ET PHISHING Successful Generic Credential Phish 2022-10-20", "ET PHISHING Successful Generic OWA Phish 2016-10-04", "ET PHISHING Successful Blackboard Account Phish 2015-10-08", "ET PHISHING Successful Dynamic Folder Phishing M1 2016-09-26", "ET PHISHING Successful UK Tax Phishing M2 2016-02-01", "ET PHISHING Possible Successful Cartasi Phishing Domain Feb 02 2017", "ET PHISHING Successful Generic Phish 2018-02-26 (set)", "ET PHISHING Successful Tradekey Phish 2015-11-19", "ET PHISHING Facebook Credential Phish Landing Page M1 2022-08-01", "ET PHISHING Successful Mailbox Renewal Phish 2016-08-19", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M2", "ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M1", "ET PHISHING Successful Alibaba Phish 2016-09-28", "ET PHISHING Successful Etisalat Phish 2016-12-20", "ET PHISHING Successful Adobe Shared Document Phish 2015-11-14", "ET PHISHING Successful Adobe Personalized Phish 2016-10-04", "ET PHISHING Successful OWA Phish 2022-06-23", "ET PHISHING Successful Chase Phish Dec 29 2016", "ET PHISHING Successful Dynamic Folder Phish M3 2016-11-22", "ET PHISHING PlayerUnknown's Battlegrounds Credential Phish Landing Page M2 2022-07-05", "ET PHISHING Successful Apple Phish M1 2016-10-07", "ET PHISHING Possible Successful Chase Phish Feb 02 2017", "ET PHISHING Successful Paypal Phish 2016-01-15 M2", "ET PHISHING BulletProofLink Phishkit Password-Processing URL", "ET PHISHING Successful Apple Phishing 2016-03-03", "ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (email-circleci .com)", "ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (circle-cl .com)", "ET PHISHING Successful Outlook Webmail Account Phish 2015-09-02", "ET PHISHING Possible Successful Generic Phish (set) Jan 17 2017", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain", "ET PHISHING Successful Bank of America Phish (set) 2016-02-27", "ET PHISHING Successful Dropbox Phish 2016-09-29", "ET PHISHING Successful Apple Phish M1 2016-02-23", "ET PHISHING Successful Generic Credential Phish Landing Page 2022-07-26", "ET PHISHING Successful Carribean International Bank Account Phish 2015-08-25", "ET PHISHING Successful Bank of America Phish M4 2016-10-27", "ET PHISHING Successful WhatsApp Phish M2 2016-12-07", "ET PHISHING Possible Successful Yahoo Phish Nov 25 2013", "ET PHISHING Successful Generic Credential Phish 2022-09-26", "ET PHISHING Successful Generic Phish 2018-05-16 (set)", "ET PHISHING Successful Webmail Account Phish 2015-09-02", "ET PHISHING Possible Successful Credential Phish Oct 1 2015", "ET PHISHING Possible Successful Apple Phish 2015-07-27", "ET PHISHING Successful Generic Phish (302) 2016-12-16", "ET PHISHING Successful Personalized Email Phish 2016-07-22", "ET PHISHING Possible Successful Citibank Phish M2 2016-08-22", "ET PHISHING TA398/Sidewinder Credential Phish Landing Page M3 2022-11-18", "ET PHISHING Possible Successful Phish - Generic Form Names 2016-09-16", "ET PHISHING Successful Intuit Phish 2016-08-01", "ET

	PHISHING Successful Paypal Phish M2 2016-10-17", "ET PHISHING Successful Facebook Mobile Phish 2017-08-15", "ET PHISHING Successful DHL Phish 2015-09-30", "ET PHISHING Possible Successful Generic Phish Nov 09 2017 (set)", "ET PHISHING Successful Generic AES Phish M2 Oct 24 2017", "ET PHISHING Successful Generic Phish 2019-04-30 (set)", "ET PHISHING Successful Generic Phish (set) 2019-12-12", "ET PHISHING Successful ING Banking Credential Phish 2022-12-12", "ET PHISHING Successful Chase Phish 2016-06-15", "ET PHISHING Successful OX App Suite Phish 2017-10-12", "ET PHISHING Radobank Phishing Landing Page 2022-07-05", "ET PHISHING Successful Postbank Online Banking Phish M1 2016-09-30", "ET PHISHING Possible Successful Apple Phish 2015-07-30", "ET PHISHING Successful Adobe Shared Document Phish 2016-08-11", "ET PHISHING Successful DrSpam Phish 2016-06-08 M2", "ET PHISHING L33bo Phishing Kit - Successful Credential Phish M2 2016-03-29", "ET PHISHING AlaskaUSA FCU Phish 2022-07-24", "ET PHISHING Facebook Credential Phish Landing Page 2022-12-27", "ET PHISHING Successful Paypal Phish M1 2016-11-29", "ET PHISHING Possible Successful Generic Phish (set) Oct 26 2017", "ET PHISHING Generic Credential Phish Landing Page 2022-10-28", "ET PHISHING Successful SFR Account Phish 2015-09-01", "ET PHISHING Successful Barclays Phish M2 2016-09-09", "ET PHISHING Successful Apple Phish M3 Feb 06 2016", "ET PHISHING Successful France Ministry of Action and Public Accounts Phish 2019-07-04", "ET PHISHING Successful Banco do Brasil Phish Mar 30 2017", "ET PHISHING Generic Credential Phish Landing Page 2022-03-01", "ET PHISHING Successful TA422 Credential Phish 2022-03-17 M1", "ET PHISHING Suspected TA445 Spearphishing Related Domain (creditals-mirohost .space in TLS SNI)", "ET PHISHING Possible Successful Generic Phish (set) 2019-03-06", "ET PHISHING Successful Sign PDF Phish 2016-05-18", "ET PHISHING Possible Successful Discover Phish Feb 02 2017", "ET PHISHING Successful Personalized Phish 2016-09-14", "ET PHISHING Successful Generic Credential Phish 2022-06-13", "ET PHISHING Generic Credential Phish Redirection 2022-03-14", "ET PHISHING Successful Telstra Refund Phish 2016-12-13", "ET PHISHING Successful Paypal Phish M4 2016-10-06", "ET PHISHING Successful Emirate Phish 2016-09-29", "ET PHISHING Successful Chase Phish 2016-10-07", "ET PHISHING Suspected TA445 Spearphishing Related Domain (walidacja-poczty .space in TLS SNI)", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mirohost .online in TLS SNI)", "ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .live) 2021-04-15", "ET PHISHING Facebook Phishing Domain in DNS Lookup", "ET PHISHING Successful Paypal Phish M2 2016-11-17", "ET PHISHING Successful H&M Revenue Phish M2 2016-06-22", "ET PHISHING Generic Credential Phish Landing Page 2022-10-20", "ET PHISHING Successful Poloniex Cryptocurrency Exchange Phish Aug 28 2017", "ET PHISHING Successful PNC Bank Phish M2 2016-10-14", "ET PHISHING Possible Successful Generic Phish (set) 2019-11-06", "ET PHISHING Successful Wells Fargo/CIBC Bank Phish M1 2015-08-25", "ET PHISHING Successful Discover Phish M2 2016-12-14", "ET PHISHING Successful Craigslist Phish 2016-07-11", "ET PHISHING Successful Paypal Phish 2016-10-31", "ET PHISHING Successful View Samples Phish 2016-09-09", "ET PHISHING Successful RBC Royal Bank Phish M1 Aug 17 2017", "ET PHISHING Successful Paypal Phish 2016-06-15", "ET PHISHING Successful Ourtime.com Phish 2016-11-28", "ET PHISHING Successful Outlook Phish 2016-10-25", "ET PHISHING Generic Credential Phish Landing Page 2022-12-02", "ET PHISHING Possible Successful Phish to Hostinger Domains M3 2016-04-04", "ET PHISHING Successful Monzo Credential Phish M2 2022-02-17", "ET PHISHING Successful Wells Fargo Phish M2 2016-09-16", "ET PHISHING Successful Apple Store Phish M3 2016-12-29", "ET HUNTING Possible Phishing - Form submitted to submit-form Form Hosting", "ET PHISHING PUBG Credential Phish Landing Page 2022-08-22", "ET PHISHING Successful PNC Bank Phish M1 2016-10-14", "ET PHISHING Successful Tesco Bank Phish M1 Phish 2016-12-15", "ET PHISHING Possible Successful Gmail Phish Nov 25 2013", "ET PHISHING Successful Luno Credential Phish 2022-10-20", "ET PHISHING Successful HitBTC Cryptocurrency Exchange Phish 2017-12-28", "ET PHISHING Spox Phish Kit Landing Page 2022-07-05", "ET POLICY Observed KnowBe4/Popcorn Training Simulated Phish Landing Page M1", "ET PHISHING Successful Chase Phishing 2016-12-12", "ET PHISHING Successful Wells Fargo Phish 2016-10-21", "ET PHISHING Successful

	Facebook Phish 2020-01-10", "ET PHISHING Successful Generic Phish - Fake Loading Page 2017-08-03", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M3", "ET PHISHING Successful Generic Credential Phish 2022-03-18", "ET PHISHING Successful Made in China Credential Phish 2022-12-14", "ET PHISHING Successful Earthlink Phish 2016-07-19", "ET PHISHING Successful Australian Government Credential Phish 2022-07-06", "ET PHISHING Metawallet Phish Landing Page 2022-01-13", "ET PHISHING Successful Adobe Shared Document Phish 2016-08-19", "ET PHISHING Successful Onedrive Credential Phish 2022-06-22", "ET PHISHING Successful OWA Phish 2022-08-17", "ET PHISHING Successful Apple Phishing 2016-03-01 M5", "ET PHISHING Possible Successful Generic Phish 2015-07-31", "ET PHISHING Successful Paypal Phish 2016-12-09", "ET PHISHING Possible Successful Phish - Verify Email Error Message M1 Aug 14 2017", "ET PHISHING Successful Chase Phish 2015-12-22", "ET PHISHING Successful HBL Bank Phish M1 2016-10-12", "ET PHISHING Microsoft Account Credential Phish Landing Page 2022-04-26", "ET PHISHING Successful Personalized Webmail Phish 2016-10-05", "ET PHISHING Successful Paypal (DE) Phish 2016-12-19", "ET PHISHING Successful Discover Phish M3 2016-12-14", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing", "ET PHISHING Successful Halkbank Phish M2 2018-04-16", "ET PHISHING Successful Dynamic Folder Phishing 2016-01-08", "ET PHISHING Successful Apple Phish M2 2016-10-07", "ET PHISHING IRS Credential Phish Credit Card Payment Data Exfil", "ET PHISHING Successful Santander Phish M1 Oct 04 2017", "ET PHISHING Successful Midea Credential Phish 2022-07-12", "ET PHISHING Successful IRS Phish (set) 2016-01-23", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (verify-email .space)", "ET PHISHING Successful Royal Bank of Canada Credential Phish 2022-03-02", "ET PHISHING Successful Outlook Password Update Phish M3 2016-09-01", "ET PHISHING GCash Credential Phish Landing Page 2022-06-17", "ET PHISHING Tectite Web Form Submission - Possible Successful Phish", "ET PHISHING Successful EDU Phish 2017-12-04", "ET PHISHING Possible Successful Generic Phish (set) Feb 26 2016", "ET PHISHING Successful World Health Organization COVID-19 Phish 2020-03-23", "ET PHISHING Successful BoA Credential Phish 2022-10-24", "ET PHISHING Successful HBL Bank Phish M2 2016-10-12", "ET PHISHING [eSentire] Successful 163 Webmail Phish 2018-07-25", "ET PHISHING Successful Paypal Phish M2 2016-11-29", "ET PHISHING Successful Generic Phish (set) 2018-09-26", "ET PHISHING Successful Citizens Bank Credential Phish 2022-10-24", "ET PHISHING Successful Paypal Phish 2016-01-15 M3", "ET PHISHING Sparkasse Credential Phish Landing Page M2 2022-04-13", "ET PHISHING Successful Bank of America Phish M3 2016-10-27", "ET PHISHING Successful Impots.gouv.fr Phish 2016-10-31", "ET PHISHING Successful Bank of America Phish M1 2016-11-23", "ET PHISHING Possible Successful Generic Phish to .ga Domain 2018-10-23", "ET PHISHING Successful Tesco Phish (set) M2 Jul 18 2017", "ET PHISHING Possible Successful Generic Windows.net Hosted Phish 2020-10-14", "ET PHISHING Successful Craigslist (RO) Phish M1 Feb 24 2017", "ET PHISHING Generic Phish Landing Page 2022-03-29", "ET PHISHING Successful Generic Epass Phish 2016-09-01", "ET PHISHING Successful Facebook Phish M1 2016-09-30", "ET PHISHING Successful Wells Fargo Phish 2016-10-06", "ET PHISHING Possible Successful Websocket Credential Phish Sep 15 2017", "ET PHISHING Successful Google Docs Phish 2016-09-28", "ET PHISHING Suspected TA445 Spearphishing Related Domain (verify-email .space in TLS SNI)", "ET PHISHING Binance Credential Phish Landing Page 2022-10-07", "ET PHISHING Successful Metawallet Phish 2022-01-13", "ET PHISHING Successful Alibaba Phish 2016-10-28", "ET PHISHING Successful Chase Phish 2015-11-03", "ET PHISHING Generic Credential Phish 2022-10-12", "ET PHISHING Successful Binance Credential Phish 2022-10-07", "ET PHISHING Generic Credential Phish Landing Page 2022-12-27", "ET PHISHING Successful DenizBank Phish 2018-04-16", "ET PHISHING Successful Adobe Shared Document Phish 2016-05-04", "ET PHISHING Successful ViewDocsOnline Phish 2015-09-15", "ET PHISHING Successful Chase Phish 2016-10-31", "ET PHISHING Successful Office 365 Phish Oct 10 2017 (set)", "ET PHISHING Successful Square Phish Nov 16 2015", "ET PHISHING Possible Successful Phish - Other Credentials Nov 25 2013", "ET PHISHING Successful Adobe Phish 2016-07-21", "ET PHISHING Successful PNC Bank Phish 2016-01-

	09", "ET PHISHING Successful Bank of America Phish (set) M1 2016-10-14", "ET PHISHING Successful Bank of Scotland Phish M1 2015-11-05", "ET PHISHING Generic Credential Phish Landing Page M3 2022-04-05", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (creditals-email .space)", "ET PHISHING Successful Docusign/O365 Phish 2016-07-15", "ET PHISHING Possible Successful Ebay Phish Jan 30 2017", "ET PHISHING Successful LCL Banque et Assurance (FR) Phish 2016-10-22", "ET PHISHING Possible Successful Generic Phish (set) Dec 07 2016", "ET PHISHING Fifth Third Banking Credential Phish Landing Page 2022-12-07", "ET PHISHING Possible Phishing Landing Page 2021-05-18", "ET PHISHING PlayerUnknown's Battlegrounds Credential Phish Landing Page M1 2022-07-05", "ET PHISHING Successful Apple ID Phish M1 2016-10-04", "ET PHISHING Successful Generic Credential Phish 2022-10-10", "ET PHISHING Successful Google Drive Phish M2 2016-06-11", "ET PHISHING Successful Wells Fargo Phish 2016-10-05", "ET PHISHING PerSwaysion Phishkit Javascript Checks if New Visitor", "ET PHISHING Successful Adobe Online Document Phish 2016-04-25", "ET PHISHING Successful HM Revenue & Customs Phish M1 Apr 07 2017", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (bigmir .space)", "ET PHISHING Successful Chase Phish M4 2016-08-26", "ET PHISHING Successful Generic Phish (set) 2018-07-19", "ET PHISHING Generic Credential Phish Landing Page 2022-08-23", "ET PHISHING Successful Paypal Phish 2015-11-03 M4", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (kontrola-poczty .site)", "ET PHISHING Possible Successful Generic Phish 2016-08-19", "ET PHISHING Possible Successful Apple Phishing Domain Feb 02 2017", "ET PHISHING Successful Apple Suspended Account Phish M2 Aug 09 2016", "ET PHISHING Successful Generic Credential Phish 2022-08-26", "ET PHISHING Successful Chase Phish M1 2016-10-17", "ET PHISHING Generic Cryptowallet Credential Phish Landing Page 2022-06-03", "ET PHISHING Facebook Credential Phish Landing Page 2022-07-18", "ET PHISHING Successful Wildblue/CenturyLink Phish 2015-12-08", "ET PHISHING Possible Successful Google Drive Phish 2015-07-28", "ET PHISHING Successful Paypal Phish M2 2016-12-13", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirrohost .space)", "ET PHISHING Successful Paypal Phish 2016-05-26", "ET PHISHING Successful View Invoice Phish M1 2016-10-05", "ET PHISHING e-Orico Credential Phish Landing Page 2022-12-12", "ET PHISHING Successful Craigslist Phish 2016-04-25", "ET PHISHING Successful Yahoo Credential Phish 2015-10-03", "ET PHISHING Successful Ebay Phish 2016-12-12", "ET PHISHING Successful Dynamic Folder Phishing 2016-09-12", "ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M2", "ET PHISHING Successful Yahoo Phish M2 2016-06-15", "ET PHISHING Generic Credential Phish Landing Page 2022-07-26", "ET PHISHING Successful Apple Phish M1 Feb 06 2016", "ET PHISHING Successful Personalized Adobe Online PDF Phish 2016-11-28", "ET PHISHING Successful Banco do Brasil Phish M1 Sep 29 2017", "ET PHISHING Successful Paypal Phish 2015-10-29", "ET PHISHING Successful Gmail Phish 2015-11-05", "ET PHISHING PerSwaysion Phishkit Javascript - Observed Repetitive Custom CSS Components", "ET PHISHING Successful Battle.net Phish 2015-09-22", "ET PHISHING Generic Credential Phish Landing Page 2022-09-26", "ET PHISHING Successful Apple Phish M2 Mar 15 2017", "ET PHISHING Possible Successful Citibank Phish M1 2016-08-22", "ET PHISHING Successful Adobe Phish 2016-03-10", "ET PHISHING Possible Successful Generic Phish (set) 2018-01-02", "ET PHISHING Successful Credit Agricole Credential Phish 2022-11-23", "ET PHISHING Successful Outlook Password Update Phish M2 2016-09-01", "ET PHISHING Successful Generic Phish (set) 2018-10-22", "ET PHISHING Successful IBC Bank Phish 2015-10-29", "ET PHISHING Successful WhatsApp Phish M1 2016-12-07", "ET PHISHING Successful Survey Credential Phish M1 2022-04-04", "ET PHISHING Successful Paypal Phish M1 2016-10-06", "ET PHISHING Successful OWA Credential Phish 2022-07-13", "ET PHISHING Successful ING Group Phish 2022-06-24", "ET PHISHING Successful Outlook Phish 2016-10-26", "ET PHISHING Successful Navy Federal Credit Union Phish 2016-02-01", "ET PHISHING Successful Generic Webmail Account Phish 2016-07-15", "ET PHISHING Successful OWA Phish 2022-07-11", "ET PHISHING Successful Banco do Brasil Phish M3 Sep 29 2017", "ET PHISHING Possible Successful Remax Phish - AOL Creds Jun 23 2015", "ET PHISHING Successful Ziraat

	Bankasi (TK) Phish M1 Oct 12 2017", "ET PHISHING Successful LocalBitcoins Cryptocurrency Exchange Phish Aug 30 2017", "ET PHISHING Successful Paypal Phish M3 2016-10-06", "ET PHISHING Successful Tesco Bank Phish (set) Jul 17 2017", "ET PHISHING Successful DHL Account Phish 2015-11-03", "ET PHISHING Successful Docusign Phish 2015-10-28", "ET PHISHING Possible Successful Generic Phish to .gqn Domain 2018-10-23", "ET PHISHING Possible Successful Generic Phish (set) May 25 2017", "ET PHISHING Generic Landing Page 2022-02-04", "ET PHISHING Successful Outlook Password Update Phish M1 2016-09-01", "ET PHISHING Successful Paypal Phish M3 2016-10-05", "ET PHISHING [eSentire] Successful Generic Phish 2018-06-15", "ET PHISHING Successful Office 365 Phish 2016-11-18", "ET PHISHING Possible Successful Generic Phish 2016-10-07", "ET PHISHING Successful Canada Revenue Agency Phish 2015-08-18", "ET PHISHING Possible Successful Phish to Hostinger Domains M5 2016-04-04", "ET PHISHING Successful Hinet Phish 2015-11-19", "ET PHISHING Successful Axie Infinity Credential Phish M1 2022-05-18", "ET PHISHING Tripod/Lycos Form Submission - Possible Successful Phish", "ET PHISHING Successful DHL Credential Phish M1 2022-06-09", "ET PHISHING Successful iTunes Connect Phish M2 2016-12-13", "ET PHISHING Successful Chase Phish 2016-12-01", "ET PHISHING Successful UPS Phish 2015-11-05", "ET POLICY Observed KnowBe4/Popcorn Training Simulated Phish Landing Page M2", "ET PHISHING Successful DHL Phish 2016-08-11", "ET PHISHING Successful Generic Credential Phish 2022-09-14", "ET PHISHING Successful Generic Personalized Phish 2019-03-11", "ET PHISHING Successful Tata Communications Phish 2016-08-19", "ET PHISHING Successful Email Settings Error Phish 2016-11-17", "ET PHISHING Successful USAA Phish 2016-11-22", "ET PHISHING Successful Dynamic Folder Phishing 2016-02-23", "ET PHISHING Possible Successful Google Drive Phishing Domain Feb 02 2017", "ET PHISHING Successful Facebook (TR) Phish 2016-12-08", "ET PHISHING Suspected TA445 Spearphishing Related Domain (weryfikacja-poczty .space in TLS SNI)", "ET PHISHING Generic Credential Phish Landing Page 2022-06-29", "ET PHISHING Successful Mailbox Update Phish 2016-02-17 M2", "ET PHISHING Generic Credential Phish Landing Page M1 2022-10-11", "ET PHISHING Generic Webmail Phishing Landing", "ET PHISHING Possible Successful Generic Phish (set) Jul 13 2016", "ET PHISHING Successful Postbank Online Banking Phish M2 2016-09-30", "ET PHISHING Successful Alibaba Phish 2016-10-18", "ET PHISHING BulletProofLink Phishkit Template", "ET PHISHING Successful Paypal Phish M1 2016-09-29", "ET PHISHING Generic Credential Phish 2022-03-18", "ET PHISHING Successful MetaMask Pass Phrase Phish 2022-12-27", "ET PHISHING Successful Dropbox/Docusign Phish 2016-10-28", "ET PHISHING Successful Phish Gmail Recovery Information 2015-10-01", "ET PHISHING Successful Halifax Bank Phish M1 2015-12-10", "ET PHISHING Successful Generic Credential OTP Phish 2022-11-22", "ET PHISHING Possible Successful Generic Phish - Credit Card", "ET PHISHING Sparkasse Credential Phish Landing Page M4 2022-04-13", "ET PHISHING Successful Excel Online Phish 2016-01-06", "ET PHISHING Successful Gmail Phish M2 2016-09-29", "ET PHISHING Successful Ameli.fr Phish M2 Oct 26 2016-10-26", "ET PHISHING Generic Credential Phish Activity POST", "ET PHISHING Successful Intuit Phish 2022-02-03", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M6", "ET PHISHING Successful TA422 Credential Phish 2022-03-17 M2", "ET PHISHING Successful Lucy Server Phish", "ET PHISHING Successful National Bank Phish Jan 05 2017", "ET PHISHING Successful Outlook Phish 2022-10-06", "ET PHISHING Successful RoundCube Phish 2022-07-18", "ET PHISHING Successful Chase Phish 2016-10-25", "ET PHISHING Successful Facebook Phish 2019-04-26", "ET PHISHING Successful AOL Phish M3 2016-07-14", "ET PHISHING Successful DHL Phish 2016-10-18", "ET PHISHING Successful Credential Phish (Multiple Brands) 2016-12-22", "ET PHISHING PerSwaysion Landing Page M1", "ET PHISHING Faebook Credential Phish Landing Page M1 2022-05-27", "ET PHISHING Successful Telstra Phish M2 2015-09-05", "ET PHISHING Successful SFR Phishing 2015-11-24", "ET PHISHING Successful American Express Phish M2 2016-10-31", "ET PHISHING Successful Phish Outlook Credentials Oct 01 2015", "ET PHISHING Possible Interac Phish Aug 18 2017", "ET PHISHING Successful Apple Phish 2016-03-09", "ET PHISHING Successful Earthlink Phish 2016-06-16", "ET PHISHING Successful Webmail Phish 2015-08-27", "ET PHISHING Generic Phishing Domain in DNS

	Lookup (info-getting-eu. com)", "ET PHISHING Successful Generic Credential Phish 2022-10-26", "ET PHISHING Successful Amazon Phish M2 2016-10-05", "ET PHISHING Successful Apple Store Phish M2 2016-12-29", "ET PHISHING Possible Successful Generic Phish to .icu Domain 2019-02-06", "ET PHISHING Generic Credential Phish Landing Page 2022-10-10", "ET PHISHING Successful Idaho Central Credit Union Credential Phish", "ET PHISHING Successful Caixa Credential Phish 2022-07-05", "ET PHISHING Successful Generic .EDU.CO Phish (Legit Set)", "ET PHISHING Successful Netflix Payment Phish M1 Jan 04 2017", "ET PHISHING Successful Apple Phish 2016-10-05", "ET PHISHING Successful Paypal Phish 2016-08-30", "ET PHISHING Successful Facebook Phish 2019-04-12", "ET PHISHING Successful Wells Fargo Phish M2 2016-11-18", "ET PHISHING Successful Generic Credential Phish 2022-06-14", "ET PHISHING Facebook Credential Phish Landing Page M2 2022-08-01", "ET PHISHING America First CU Account Recovery 2022-10-27", "ET PHISHING Successful Adobe Phish M3 2016-07-11", "ET PHISHING Successful Facebook Phish 2016-09-02", "ET PHISHING Possible Successful CDC Coronavirus Related Phish 2020-04-07", "ET PHISHING Microsoft Credential Phish 2022-03-14", "ET PHISHING Successful Apple Phish 2015-10-23", "ET PHISHING Successful Apple Phish (FR) M2 2016-10-07", "ET PHISHING Possible Successful Apple Phish 2015-07-31", "ET PHISHING HTTP POST Contains Only Password (ml) 2021-04-05", "ET PHISHING Successful Blocked Email Account Phish M1 2016-08-23", "ET PHISHING Successful FreeMobile (FR) Phish M3 2016-10-06", "ET PHISHING Successful NHS Webmail Phish 2020-03-23", "ET PHISHING Possible Successful Bank of America Phishing Domain Feb 02 2017", "ET PHISHING Possible Successful Gmail Phish Nov 21 2012", "ET PHISHING Successful Generic AES Phish M1 Oct 24 2017", "ET PHISHING Successful RBC Royal Bank Phish Jan 30 2017", "ET PHISHING Successful Apple Phish M3 2016-09-14", "ET PHISHING Successful Paypal Phish M4 2016-12-13", "ET PHISHING America First CU Successful Phish 2022-10-27", "ET PHISHING Successful Generic Mailbox Phish 2019-03-07", "ET PHISHING Successful Cryptocurrency Exchange Phish (set) 2018-10-25", "ET PHISHING Successful Microsoft Credential Phish 2022-06-28", "ET PHISHING Possible Successful Phish - Generic Status Messages Sept 11 2015", "ET PHISHING Facebook Credential Phish Landing Page M2 2022-05-27", "ET PHISHING Successful Navy Federal Phish 2022-10-11", "ET PHISHING Successful CIBC Phish 2016-08-30", "ET PHISHING Successful Monzo Credential Phish M1 2022-02-17", "ET PHISHING Successful Docusign/Outlook Phish 2016-08-17", "ET PHISHING Axie Infinity Credential Phish Landing Page M1 2022-05-18", "ET PHISHING Successful Amazon Phish M1 2016-10-05", "ET PHISHING Successful Generic Wembail Phish M2 2016-11-18", "ET PHISHING Successful Wells Fargo Phish M1 2016-12-29", "ET PHISHING Successful Outlook Webmail Phishing M2 2015-11-21", "ET PHISHING Successful OWA Phish 2022-07-15", "ET PHISHING Successful Woodforest Bank Phish M1 2015-08-31", "ET PHISHING Successful Generic PII Phish", "ET PHISHING Successful Survey Credential Phish M5 2022-04-04", "ET PHISHING Successful DHL Phish (Meta HTTP-Equiv Refresh) 2017-02-08", "ET PHISHING Successful Apple Phish M3 2016-09-29", "ET PHISHING Successful Webmail Mailbox Quota Phish 2016-09-02", "ET PHISHING Successful FR Carte Bleue / BCP Phish 2016-09-06", "ET PHISHING Successful Paypal Phish Mar 14 2017", "ET PHISHING Successful Mailbox Shutdown Phish M3 2016-05-16", "ET PHISHING Successful Linkedin Phish 2016-11-17", "ET PHISHING Survey Credential Phish Landing Page 2022-04-04", "ET PHISHING Successful Yahoo Phish 2016-10-14", "ET PHISHING Successful Horde Webmail Phish 2015-08-21", "ET PHISHING Successful Generic .EDU.BR Phish (Legit Set)", "ET PHISHING Generic Phishing domain observed in TLS SNI (info-getting-eu. com)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (konto-verify .space)", "ET PHISHING Successful Paypal Phish 2015-10-23", "ET PHISHING Successful Paypal (FR) Phish Oct 16 2017", "ET PHISHING Possible Successful Generic Phish (set) Sept 02 2016", "ET PHISHING Successful Generic Phish 2020-09-21", "ET PHISHING Successful Dynamic Folder Phish 2016-10-10", "ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M4", "ET PHISHING Successful Wildblue Phishing M2 2015-11-24", "ET PHISHING Successful Apple Phish Oct 31 2016", "ET PHISHING Successful Paypal Phish 2015-10-28", "ET PHISHING Successful Docusign Phish M1 2016-08-17", "ET PHISHING Successful Generic

	Email Account Phish 2019-12-10", "ET PHISHING Successful Dropbox Phish 2016-09-14", "ET PHISHING Successful Wells Fargo Phish M1 2016-09-16", "ET PHISHING Successful Generic Credit Card Information Phish 2020-02-25", "ET PHISHING Successful Generic Credential Phish 2022-05-24", "ET PHISHING Successful Paypal Phish M1 Dec 8 2015", "ET PHISHING Successful Bank of America Phish 2015-10-29", "ET PHISHING Successful Dynamic Folder FreeMobile (FR) Phishing 2016-10-06", "ET PHISHING Successful Hotmail Phish 2016-07-14", "ET PHISHING Successful Google Drive Phish 2016-10-11", "ET PHISHING Successful WhatsApp Payment Phish M2 2016-11-15", "ET PHISHING Successful Western Union/Paypal Phish 2016-09-26", "ET PHISHING Successful Credit Agricole Bank (FR) Phish M2 2016-10-19", "ET PHISHING Successful PlayerUnknown's Battlegrounds Credential Phish 2022-07-05", "ET PHISHING Successful Email Termination Phish 2016-06-22", "ET PHISHING Successful Generic Multi-Account Phish 2018-02-16", "ET PHISHING Successful Paypal Phish M1 Sep 15 2017", "ET PHISHING Successful Paypal Phish M1 2016-12-13", "ET PHISHING Possible Successful Generic Phish (set) Dec 27 2016", "ET PHISHING Successful Amazon Account Phish M3 2015-08-21", "ET PHISHING Possible Successful Tripod.com Phish 2016-03-31", "ET PHISHING Possible Successful Generic Phish (set) 2018-07-19", "ET PHISHING Successful Western Union Phish 2016-09-27", "ET PHISHING Generic Phish 2022-02-04", "ET PHISHING Successful Outlook Web App Phish 2015-10-15", "ET PHISHING Successful Apple Phish M2 Feb 06 2016", "ET PHISHING Successful Netflix Phish 2016-10-12", "ET HUNTING Suspicious HTTP POST Only Containing Pass - Possible Phishing", "ET PHISHING Successful Microsoft Account Phish 2019-11-06", "ET PHISHING Successful Apple Phish 2016-09-27", "ET PHISHING Successful Generic Credential Phish 2022-06-17", "ET PHISHING Successful Vmware/Zimbra Phish 2015-09-28", "ET PHISHING Successful Wells Fargo Account Phish 2015-08-18", "ET PHISHING Successful Generic Phish 2021-11-10", "ET PHISHING Successful Banco do Brasil Phish May 25 2017", "ET PHISHING Successful Apple ID Phish 2016-10-25", "ET PHISHING Successful Generic Phish (set) 2018-03-13", "ET PHISHING Successful Orange (FR) Phish 2016-10-06", "ET PHISHING Successful Paypal Phish M2 2015-11-03", "ET PHISHING Successful Webmail Update Phish 2015-10-08", "ET PHISHING Successful Australian Government myGov Credential Phish 2022-12-14", "ET PHISHING Successful DHL Credential Phish M2 2022-06-09", "ET PHISHING Successful Email Credential Phish 2015-08-12", "ET PHISHING Possible Successful Remax Phish - Other Creds Jun 23 2015", "ET PHISHING Successful Banque Populaire (FR) Phish 2016-12-12", "ET PHISHING Successful Adobe Shared Document Phish 2016-11-15", "ET PHISHING Generic Credential Phish Landing Page M2 2022-10-11", "ET PHISHING Possible Successful Generic Phish - Three Security Questions", "ET PHISHING Successful Outlook Phish 2016-10-18", "ET PHISHING Suspected TA445 Spearphishing Related Domain (ua-passport .space in TLS SNI)", "ET PHISHING Successful Adobe Shared Document Phish 2016-08-26", "ET PHISHING Successful US Bank Phish 2016-06-09 M2", "ET MALWARE BluStealer - SysInfo Exfil via Telegram M2", "ET PHISHING Successful Orderlink (IN) Phish Feb 24 2017", "ET PHISHING Successful iTunes Connect Phish M1 2016-12-13", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirohost .online)", "ET PHISHING TMOBILE Successful Credential Phish 2022-11-01", "ET PHISHING Successful Google Drive Phish June 17 2015", "ET PHISHING Possible Successful Generic Phish (set) Aug 31 2017", "ET PHISHING Successful LinkedIn Phish 2015-09-17", "ET PHISHING Successful Chase Phish M2 2016-12-07", "ET PHISHING Successful Linkedin Phish 2016-11-18", "ET PHISHING Successful American Express Phish M1 2016-10-31", "ET PHISHING Successful AOL Phish M1 2016-07-14", "ET PHISHING Possible Successful Generic Phish to .cf Domain 2018-10-23", "ET PHISHING Successful FedEx Phish 2022-07-20", "ET PHISHING Possible Successful Generic SSN Phish", "ET PHISHING Successful Mailbox Update Credential Phish 2015-10-02", "ET PHISHING Successful Outlook Phish 2016-07-14", "ET PHISHING Suspicious Generic Login - Possible Successful Phish 2019-01-02", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (creditals-mirohost .space)", "ET PHISHING Successful Survey Credential Phish M7 2022-04-04", "ET PHISHING Successful Generic Credential Phish 2022-10-12", "ET PHISHING Successful Sparkasse (DE) Phish 2016-11-28", "ET PHISHING HTTP POST Contains Only Password

	(tk) 2021-04-05", "ET PHISHING Successful Banca Monte dei Paschi di Siena Credential Phish 2022-04-22", "ET PHISHING Successful RBC Royal Bank Phish Mar 27 2017", "ET PHISHING Successful Paypal Account Phish 2015-10-30 2", "ET PHISHING Successful AOL Phish 2015-10-09", "ET PHISHING Successful Bank of America Phish M2 2016-10-10", "ET PHISHING Successful Generic Redeye Phish 2020-07-24", "ET PHISHING Successful Password Protected AMEX Phish 2016-12-09", "ET PHISHING Successful Excel Phish 2016-09-26", "ET PHISHING Successful Three Step Gmail Phish (3 of 3) 2016-12-02", "ET PHISHING Possible Successful Phish - Password Submitted to *.000webhostapp.com", "ET PHISHING Successful Caixa Credential Phish 2022-06-29", "ET PHISHING Successful Three Step Gmail Phish (1 of 3) 2016-12-02", "ET PHISHING Successful DHL Phish 2016-12-08", "ET PHISHING Successful Yahoo Phish 2016-12-08", "ET PHISHING Generic Credential Phish Landing Page 2022-09-23", "ET PHISHING Successful Onedrive Phish 2016-05-16", "ET PHISHING Successful Universal Webmail Phish 2016-08-19", "ET PHISHING Successful Paypal Account Phish 2015-10-16", "ET PHISHING Generic Banking Phish Landing Page 2022-01-11", "ET PHISHING Successful Barclays Phish M1 2016-11-23", "ET PHISHING Successful Keybank Phish 2016-09-29", "ET PHISHING Successful Paypal Phish M3 2016-09-29", "ET PHISHING Successful Formbuddy Credential Phish Submission 2016-01-15", "ET PHISHING Successful Google Drive Phish 2016-01-12", "ET PHISHING Successful Apple Phish M1 2016-11-15", "ET PHISHING Successful Generic Phish (set) 2018-03-08", "ET PHISHING Successful Generic Webmail Phish M1 2016-11-18", "ET PHISHING Successful WZ-REKLAMA Phish 2016-01-08", "ET PHISHING Suncoast Credit Union Credential Phish Landing Page 2022-12-19", "ET PHISHING Possible Successful Generic Phish (set) May 31 2017", "ET PHISHING Successful Paypal Phish 2015-12-08 M3", "ET PHISHING Possible Successful AOL Phish Nov 25 2013", "ET PHISHING Successful Axie Infinity Credential Phish M2 2022-05-18", "ET PHISHING PerSwaysion Landing Page M2", "ET PHISHING Successful Wells Fargo Phish 2016-08-31", "ET PHISHING Successful Blocked Email Account Phish M2 2016-08-23", "ET PHISHING Successful Generic Adobe Phish 2019-07-29", "ET PHISHING Observed Possible Phishing Landing Page 2021-06-25", "ET PHISHING Successful Ebay Phish 2016-06-14", "ET PHISHING Successful Generic Webmail Phish 2016-10-21", "ET PHISHING Successful Adobe Credential Phish 2022-07-08", "ET PHISHING Successful National Bank Phish Mar 13 2017", "ET PHISHING Successful Generic Brand Phish 2016-12-01", "ET PHISHING Successful Generic Credential Phish 2022-06-01", "ET PHISHING Successful Paypal Phish M3 2016-12-13", "ET PHISHING Successful Comcast Phish 2016-08-18", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mirrohost .space in TLS SNI)", "ET PHISHING Successful Amazon Phish 2015-09-22", "ET PHISHING Successful Wells Fargo Phish 2016-05-26", "ET PHISHING Successful Apple ID Phish M2 2016-10-04", "ET MALWARE Possible Magecart Credit Card Information JS Script", "ET PHISHING Generic Korean Bank Credential Theft 2023-01-09", "ET PHISHING Possible Successful Generic Phish (set) Jan 12 2017", "ET PHISHING Successful Generic Phish (Redirect to Download PDF) 2016-02-08", "ET PHISHING Successful DHL Phish 2019-10-18", "ET PHISHING Possible Successful Phish to Hostinger Domains M1 2016-04-04", "ET PHISHING Suspected TA445 Spearphishing Related Domain (creditals-email .space in TLS SNI)", "ET PHISHING Successful Facebook Credential Phish 2022-08-01", "ET PHISHING Successful National Australia Bank Phish 2016-12-02", "ET PHISHING Successful Generic Credit Card Information Phish 2019-08-02", "ET PHISHING Successful USAA Phish 2016-06-15", "ET PHISHING Possible Successful Generic Phish (set) Aug 25 2017", "ET PHISHING Successful Linkedin Phish 2016-09-27", "ET INFO Observed testcookie-nginx-module", "ET PHISHING Successful Microsoft Account Credential Phish 2022-04-26", "ET PHISHING Successful Xfinity/Comcast Phish 2016-06-17", "ET PHISHING Successful AOL Phish 2016-10-24", "ET PHISHING Successful Standard Bank Phish 2016-06-23", "ET PHISHING Generic Phishkit Landing Page M2", "ET PHISHING Generic Credential Phish Activity GET", "ET PHISHING Successful Alibaba Phish 2016-10-26", "ET PHISHING Successful Wells Fargo Phish M2 2015-11-21", "ET PHISHING Successful Apple Phish (FR) M1 2016-10-07", "ET PHISHING Successful Bank of Oklahoma Phish M2 Jul 21 2016", "ET PHISHING [eSentire] Successful Personalized Phish 2018-06-15", "ET PHISHING Possible Successful Generic Web.App Hosted Phish

	2020-10-14", "ET PHISHING Successful Generic 000webhostapp.com Phish 2017-10-27", "ET PHISHING Successful DHL Phish 2015-11-14", "ET PHISHING TodayZoo Phishing Kit GET M2", "ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M2", "ET PHISHING Sucessful Global Sources Credential Phish 2022-06-29", "ET PHISHING Successful Excel Online Phish 2015-11-26", "ET PHISHING Successful Generic Phish 2022-03-28", "ET PHISHING PerSwaysion Phishkit Landing Page", "ET PHISHING Successful Google Credential Phish 2016-02-17", "ET PHISHING Successful Sparkasse Phish 2016-10-03", "ET PHISHING Successful Wells Fargo Phish 2018-03-12", "ET PHISHING Successful Apple Phish M2 2016-11-15", "ET PHISHING Successful Bank of America Phish 2015-11-06", "ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M1", "ET PHISHING Successful Google Drive Phish M2 2016-12-02", "ET PHISHING Successful Impots.gouv.fr Phish M2 2015-08-21", "ET PHISHING Possible Successful Phish - Generic Credential POST to Ngrok.io", "ET PHISHING Successful Maersk Phishing 2016-02-25", "ET PHISHING Successful Generic Phish (set) 2020-06-10", "ET PHISHING Successful Google Drive Phish M1 2016-06-11", "ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M3", "ET PHISHING Successful Account Update Phish 2016-09-06", "ET PHISHING LinkedIn Phish Landing Page 2022-01-31", "ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M3", "ET PHISHING Successful Bank of America Phish M2 2016-08-31", "ET PHISHING Successful Clydesdale Bank Phish 2020-12-30", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (weryfikacja-konta .space)", "ET PHISHING Successful PlayerUnknown's Battlegrounds Phish 2021-11-10", "ET PHISHING Navy Federal Credit Union Credential Phish Landing Page 2022-07-05", "ET MALWARE MSIL/PSW.Agent.SUD Zipped Data Exfil (set)", "ET PHISHING Successful Canada Revenue Agency Phish 2016-08-30", "ET PHISHING Successful Impots.gouv.fr Phish 2016-10-24", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mod-mil .online)", "ET PHISHING Successful Generic Credential Phish 2015-10-03", "ET PHISHING Successful Chase Phish 2016-12-16", "ET PHISHING Successful Generic Credit Card Information Phish Oct 10 2017", "ET PHISHING Suspected TA445 Spearphishing Related Domain (mod-mil .online in TLS SNI)", "ET PHISHING Successful Paypal Phish M2 2016-09-29", "ET PHISHING Successful Facebook Phish 2016-10-06", "ET PHISHING Australian Government Credential Phish Landing Page 2022-07-06", "ET PHISHING Successful Generic Phish (set) 2019-08-23", "ET PHISHING Socios Credential Phish Landing Page 2022-12-22", "ET PHISHING Successful Three Step Gmail Phish (2 of 3) Phish 2016-12-02", "ET PHISHING Successful FreeMobile (FR) Phish M2 2016-10-06", "ET PHISHING Possible Successful Generic Phish (set) Aug 22 2017", "ET PHISHING Successful Mailbox Deactivation Phish 2016-12-15", "ET PHISHING Possible Successful Paypal Phishing Domain Feb 02 2017", "ET PHISHING Successful Bank of America Phish M2 2016-11-23", "ET PHISHING Successful Amazon (UK) Phish 2016-10-17", "ET PHISHING Successful Chase Phish M2 2015-12-01", "ET PHISHING TA398/Sidewinder Credential Phish Landing Page M1 2022-11-18", "ET PHISHING Successful Paypal Phish M2 2016-12-05", "ET PHISHING Suspected TA445 Spearphishing Related Domain (kontrola-poczty .space in TLS SNI)", "ET PHISHING Successful Chase Phish 2015-09-24", "ET PHISHING Successful Anonisma Paypal Phish 2015-12-29", "ET PHISHING Successful Microsoft Live Email Account Phish 2016-10-18", "ET PHISHING TodayZoo Phishing Kit GET M1", "ET PHISHING BulletProofLink Phishkit Activity (POST)", "ET PHISHING Successful Microsoft Phish 2016-12-08", "ET PHISHING Generic Phishkit Activity (GET)", "ET PHISHING Successful Google Drive Phish 2016-10-14", "ET PHISHING Sparkasse Credential Phish Landing Page M3 2022-04-13", "ET PHISHING Successful Free.fr Phish 2016-03-10", "ET PHISHING Possible BulletProofLink Phishkit Activity - Retrieving Resources", "ET PHISHING Possible Successful Generic Phish (set) 2018-05-02", "ET PHISHING Successful Facebook Credential Phish 2021-11-16", "ET PHISHING Successful Apple Phish M2 2015-12-02", "ET PHISHING Successful Amazon.com Phish M1 2016-06-27", "ET PHISHING Suspicious Form with Action Value Equal to bit .ly", "ET PHISHING Successful Idaho Central CU Phish 2022-07-24", "ET PHISHING Successful Wells Fargo Account Phish 2015-08-14", "ET PHISHING Successful HM Revenue Phish 2016-11-23", "ET PHISHING Successful DrSpam Phish 2016-06-08 M1", "ET PHISHING Successful Barclays Phish M1

	2016-09-09", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (walidacja-poczty .space)", "ET PHISHING Successful Webmail Account Upgrade Phish 2016-07-21", "ET PHISHING Successful Dynamic Folder Phish M2 2016-12-02", "ET PHISHING Adobe Phish Landing Page 2022-01-12", "ET PHISHING Successful Tesco Phish (set) M1 Jul 18 2017", "ET PHISHING Successful Westpac Bank Phish 2016-08-31", "ET PHISHING Successful Apple Phishing 2016-03-01 M3", "ET PHISHING ING Group Credential Phish Landing Page 2022-12-02", "ET PHISHING Successful BBVA Compass Account Phish 2015-08-21", "ET PHISHING Successful Personalized Email Update Phish 2016-11-17", "ET PHISHING Successful Liqui Cryptocurrency Exchange Phish 2017-12-28", "ET PHISHING Possible Successful TSB Bank Phish 2018-05-07", "ET PHISHING Sparkasse Credential Phish Landing Page M1 2022-04-13", "ET PHISHING Possible Successful Docusign Phish 2015-07-27", "ET PHISHING Successful Google Drive Phish 2016-12-07", "ET PHISHING Successful Personalized Outlook Phish 2016-10-26", "ET PHISHING Successful Apple Phish 2019-12-18", "ET PHISHING Coinbase Credential Phish Landing Page 2022-11-29", "ET PHISHING Successful Netflix Phish 2016-11-15", "ET PHISHING Possible Successful Generic Phish (set) Jul 11 2017", "ET PHISHING Possible Successful Phish - Other Credentials Nov 21 2012", "ET PHISHING Successful HM Revenue Phish 2016-10-06", "ET PHISHING Coinbase Credential Phish Landing Page 2022-12-02", "ET PHISHING Ping Identity Landing Page 2022-03-14", "ET PHISHING Successful Generic Credential Phish 2022-05-27", "ET PHISHING Successful Apple Phish M2 2016-09-14", "ET PHISHING Possible Successful Phish - Saved Website Comment Observed", "ET PHISHING Successful Wells Fargo Phish 2021-03-16", "ET PHISHING Suspected TA445 Spearphishing Related Domain (konto-verify .space in TLS SNI)", "ET PHISHING Successful Canada Revenue Agency COVID-19 Assistance Eligability (FR) Phish 2020-04-01", "ET PHISHING Successful Dynamic Folder Phish 2016-11-15", "ET PHISHING Successful Generic Credential Phish 2022-03-02", "ET PHISHING Successful Facebook Phish 2015-08-27", "ET PHISHING Successful Dropbox Phish 2016-10-14", "ET PHISHING Successful Email Settings Phish 2016-10-28", "ET PHISHING Facebook Credential Phish Landing Page 2022-07-29", "ET PHISHING Successful Generic Credential Phish Activity POST", "ET PHISHING Successful Dropbox Business Phish 2016-11-17", "ET PHISHING Manhattan College Phish Landing Page 2022-01-10", "ET PHISHING Sparkasse Credential Phish Landing Page 2022-06-10", "ET PHISHING Successful iTunes Connect Phish M1 2016-10-21", "ET PHISHING PerSwaysion Phishkit Javascript Variable", "ET PHISHING Successful Yahoo Phish 2016-07-11", "ET PHISHING TA398/Sidewinder Credential Phish Landing Page M2 2022-11-18", "ET PHISHING Possible Successful Phish to Hostinger Domains M2 2016-04-04", "ET PHISHING TMOBILE Credential Phish Landing Page 2022-11-01", "ET PHISHING Successful FreeMobile (FR) Phish 2016-09-28", "ET PHISHING Successful FR Gmail Phish M2 2016-03-15", "ET PHISHING Successful Dynamic Folder Phish Oct 07 2016", "ET PHISHING Successful Alibaba Credential Phish 2022-11-30", "ET PHISHING Successful Generic Phish Phish 2018-08-21", "ET PHISHING Possible Successful Phish to Hostinger Domains Apr 4 M4", "ET PHISHING Generic Credential Phish Landing Page M1 2022-04-05", "ET PHISHING Successful Nordea Netbank Credential Phish 2022-11-04", "ET PHISHING Possible Successful Generic Phish (set) Oct 13 2016", "ET PHISHING Generic Phishkit Landing Page M3"
Попытки получения системных файлов	"ET POLICY IP Check Domain (whatismyip in HTTP Host)", "ET SCAN Modified Sipvicious Sundayddr Scanner (sipsscuser)", "ET SCAN Toata Scanner User-Agent Detected", "GPL NETBIOS NT NULL session", "GPL DNS named authors attempt", "ET SCAN Httprint Web Server Fingerprint Scan", "ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Enumeration Activity M2", "ET SCAN Sqlmap SQL Injection Scan", "ET SCAN NMAP SIP Version Detection Script Activity", "ET USER_AGENTS FOCA User-Agent", "GPL SNMP public access udp", "ET SCAN Metasploit WMAP GET len 0 and type", "ET POLICY Inbound /uploadify.php Access", "ET SCAN SQL Power Injector SQL Injection User Agent Detected", "ET WEB_SERVER Outbound PHP User-Agent", "ET SCAN Acunetix Version 6 (Free Edition) Scan Detected", "ET EXPLOIT NEC SL2100 - Session Enumeration Attempt", "ET SCAN SQLNinja MSSQL Authentication Mode Scan", "ET VOIP Modified Sipvicious Asterisk PBX User-Agent", "ET EXPLOIT Netgear DGN Remote Command

	Execution", "ET POLICY Java Url Lib User Agent Web Crawl", "ET SCAN Springenwerk XSS Scanner User-Agent Detected", "ET SCAN Hikvision IP Camera 5.4.0 Information Disclosure", "ET SCAN Xenu Link Sleuth Scanner Outbound", "GPL SNMP SNMP NT UserList", "ET EXPLOIT Linksys Smart WiFi Information Disclosure Attempt Inbound", "ET SCAN Internet Scanning Project HTTP scan", "ET WEB_SERVER Muieblackcat scanner", "ET WEB_SPECIFIC_APPS Solr DataImport Handler Disclose Config URL", "ET EXPLOIT Xiongmai/HiSilicon DVR - OpenTelnet Inbound - Possilbe CVE-2020-22253 Attempt", "ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Probe", "ET WEB_SERVER PHP Easteregg Information-Disclosure (zend-logo)", "ET SCAN Laravel Debug Mode Information Disclosure Probe Inbound", "GPL WEB_SERVER .htaccess access", "ET VOIP Possible Modified Sipvicious OPTIONS Scan", "ET SCAN Nessus FTP Scan detected (ftp_writeable_directories.nasl)", "ET SCAN Automated Injection Tool User-Agent (AutoGetColumn)", "ET SCAN Netsparker Default User-Agent", "ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Vulnerable Response", "ET SCAN HP Enterprise VAN SDN Controller", "ET WEB_SERVER Brutus Scan Inbound", "ET POLICY Cisco Data Center Network Manager - Vulnerable Version Detected 10.4", "GPL SCAN ssh-research-scanner", "ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt", "ET SCAN Vega Web Application Scan", "ET SCAN Apache mod_proxy Reverse Proxy Exposure 1", "ET POLICY IP Check Domain (showip in HTTP Host)", "ET SCAN DavTest WebDav Vulnerability Scanner Default User Agent Detected", "ET WEB_SPECIFIC_APPS Joomla Full Path Disclosure -- content.php", "ET SCAN WITOOL SQL Injection Scan", "ET POLICY python.urllib User Agent Web Crawl", "ET INFO Pulse Secure VPN Version Disclosure Attempt", "ET SCAN Skipfish Web Application Scan Detected (2)", "ET SCAN HZZP Scan in Progress calc in Headers", "GPL SMTP expn decode", "ET SCAN FHScan core User-Agent Detect", "ET SCAN SFTP/FTP Password Exposure via sftp-config.json", "ET SCAN Potential SSH Scan", "ET SCAN Sivus VOIP Vulnerability Scanner SIP Components Scan", "ET POLICY libwww-perl User-Agent", "ET SCAN External to Internal UPnP Request tcp port 2555", "ET SCAN WhatWeb Web Application Fingerprint Scanner Default User-Agent Detected", "ET WEB_SERVER Automated Site Scanning for backupdata", "GPL SCAN nessus 2.x 404 probe", "GPL SMTP expn root", "ET POLICY POSSIBLE Web Crawl using Curl", "GPL DNS named version attempt", "ET SCAN Geutebrueck re_porter 7.8.974.20 Information Disclosure", "ET POLICY HTTPie User-Agent Outbound", "ET SCAN FTPSync Settings Disclosure Attempt", "ET WEB_SERVER PyCurl Suspicious User Agent Inbound", "ET WEB_SPECIFIC_APPS Possible Oracle GlassFish Server Administration Console Authentication Bypass Attempt", "ET SCAN NMAP OS Detection Probe", "ET WEB_SERVER Inbound PHP User-Agent", "ET SCAN Arachni Scanner Web Scan", "ET SCAN Mini MySqlatOr SQL Injection Scanner", "ET SCAN RatProxy in-use", "ET SCAN Inspathx Path Disclosure Scanner User-Agent Detected", "ET WEB_CLIENT Google Chrome Credential Stealing via SCF file Reflected Request", "ET SCAN Acunetix Accept HTTP Header detected scan in progress", "ET POLICY POSSIBLE Crawl using Fetch", "ET SCAN Cisco Torch IOS HTTP Scan", "GPL RPC xdmcp info query", "ET USER_AGENTS pxyscand/ Suspicious User Agent Outbound", "ET EXPLOIT AVTECH Authenticated Command Injection in PwdGrp.cgi", "ET SCAN FOCA uri", "ET SCAN Watchfire AppScan Web App Vulnerability Scanner", "ET SCAN Acunetix Version 6 Crawl/Scan Detected", "GPL SMTP vrfy root", "GPL SNMP SNMP trap Format String detected", "ET SCAN Skipfish Web Application Scan Detected", "GPL NETBIOS SMB startup folder access", "ET SCAN Nmap NSE Heartbleed Response", "GPL SCAN ISS Pinger", "ET USER_AGENTS SAP CVE-2020-6287 PoC UA Observed", "ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Enumeration Activity M1", "ET WEB_SERVER PHP Easteregg Information-Disclosure (phpinfo)", "GPL WEB_SERVER perl command attempt", "ET SCAN Hmap Webserver Fingerprint Scan", "ET SCAN Voiper Toolkit Torturer Scan", "ET SCAN Nessus FTP Scan detected (ftp_anonymous.nasl)", "GPL SCAN webtrends scanner", "ET POLICY Cisco Data Center Network Manager - Vulnerable Version Detected 11.1", "ET SCAN Grendel Web Scan - Default User Agent Detected", "ET USER_AGENTS PyCurl Suspicious User Agent Outbound", "ET WEB_SERVER DD-WRT Information Disclosure Attempt", "ET USER_AGENTS Binget PHP Library User Agent

	Outbound", "ET SCAN Amap TCP Service Scan Detected", "ET WEB_SPECIFIC_APPS Solr DataImport Handler Disclose Admin Cores", "ET POLICY IP Check Domain (showmyip in HTTP Host)", "ET SCAN Httprecon Web Server Fingerprint Scan", "ET SCAN Grendel-Scan Web Application Security Scan Detected", "ET EXPLOIT TerraMaster TOS Information Leak Inbound (CVE-2022-24990)", "ET SCAN DirBuster Scan in Progress", "ET SCAN DotDotPwn User-Agent", "ET EXPLOIT Possible Cisco Data Center Network Manager - Log Retrieval (CVE-2019-1622)", "ET SCAN Sipvicious Scan", "ET SCAN Sipvicious User-Agent Detected (friendly-scanner)", "ET SCAN Internal to Internal UPnP Request tcp port 2555", "ET SCAN Nmap NSE Heartbleed Request", "ET SCAN Port Unreachable Response to Xprobe2 OS Fingerprint Scan", "ET SCAN SipCLI VOIP Scan - TCP", "ET SCAN OpenVAS User-Agent Inbound", "ET WEB_SERVER Automated Site Scanning for backup_data", "ET WEB_SPECIFIC_APPS Joomla Full Path Disclosure -- php5x.php", "ET WEB_SERVER Possible Successful Juniper NetScreen ScreenOS Firmware Version Disclosure Attempt", "GPL WEB_SERVER /~root access", "ET EXPLOIT D-Link 850L Password Extract Attempt", "ET SCAN Potential VNC Scan 5800-5820", "ET WEB_SERVER pxyscand Suspicious User Agent Inbound", "ET SCAN Suspicious User-Agent Containing SQL Inject/ion Likely SQL Injection Scanner", "ET POLICY IP Check Domain (icanhazip. com in HTTP Host)", "ET WEB_SERVER Recon-ng User-Agent", "ET SCAN Grabber.py Web Scan Detected", "ET SCAN Non-Allowed Host Tried to Connect to MySQL Server", "ET SCAN WebShag Web Application Scan Detected", "ET SCAN External to Internal UPnP Request udp port 1900", "GPL NETBIOS SMB CD...", "ET SCAN IBM NSA User Agent", "ET EXPLOIT Attempted Directory Traversal via HTTP Cookie (CVE-2020-9484)", "ET SCAN w3af User-Agent 2", "ET POLICY IP Check Domain (cmyip.com in HTTP Host)", "GPL WEB_SERVER Tomcat server snoop access", "ET WEB_SPECIFIC_APPS WordPress DB XML dump attempted access", "ET WEB_SPECIFIC_APPS Netgear WNR2000v5 Possible Serial Number Leak", "ET USER_AGENTS Atomic_Email_Hunter User-Agent Inbound", "GPL SNMP private access udp", "ET POLICY Cisco Data Center Network Manager Version Check Inbound (flowbit set)", "ET EXPLOIT AVTECH Authenticated Command Injection in CloudSetup.cgi (Outbound)", "ET INFO Vulnerable SAP NetWeaver Path Observed - Information Disclosure (CVE-2016-2388)", "ET POLICY Possible Web Crawl - libwww-perl User Agent", "ET SCAN SQLNinja MSSQL XPCmdShell Scan", "ET EXPLOIT AVTECH Authenticated Command Injection in CloudSetup.cgi", "ET POLICY IP Check whatismyip.com Automation Page", "ET SCAN Positive Technologies XSpider Security Scanner User-Agent (PTX)", "ET SCAN Pavuk User Agent Detected - Website Mirroring Tool for Off-line Analysis", "ET SCAN WSFuzzer Web Application Fuzzing", "ET SCAN libwww-perl GET to // with specific HTTP header ordering without libwww-perl User-Agent", "ET SCAN Medusa User-Agent", "ET SCAN Inspathx Path Disclosure Scan", "ET SCAN Cisco Torch TFTP Scan", "GPL DNS zone transfer UDP", "ET SCAN Suspicious User-Agent Containing Web Scan/er Likely Web Scanner", "ET SCAN Apache mod_proxy Reverse Proxy Exposure 2", "ET POLICY Peach C++ Library User Agent Inbound", "ET POLICY MOBILE Apple device leaking UDID from SpringBoard via GET", "GPL SMTP vrfy decode", "ET SCAN SIP erase_registrations/add registrations attempt", "ET SCAN Netsparker Scan in Progress", "ET SCAN Wikto Scan", "ET SCAN Brutus Scan Outbound", "ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt", "ET SCAN McAfee/Foundstone Scanner Web Scan", "ET SCAN w3af User Agent", "GPL NETBIOS RFParalyze Attempt", "ET SCAN DEBUG Method Request with Command", "ET SCAN Absinthe SQL Injection Tool HTTP Header Detected", "ET SCAN Paros Proxy Scanner Detected", "ET EXPLOIT Possible Vacron NVR Remote Command Execution", "ET SCAN Sivus VOIP Vulnerability Scanner SIP Scan", "ET WEB_SERVER PHP Easteregg Information-Disclosure (funny-logo)", "ET SCAN Amap UDP Service Scan Detected", "ET SCAN Asp-Audit Web Scan Detected", "ET EXPLOIT AVTECH Unauthenticated Command Injection in DVR Devices", "ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt", "ET SCAN Possible DavTest WebDav Vulnerability Scanner Initial Check Detected", "ET SCAN Voiper Fuzzing Scan", "GPL MISC ident version request", "ET SCAN SQLNinja MSSQL Database User Rights Scan", "ET WEB_SPECIFIC_APPS Online Trade - Information Disclosure", "ET SCAN Possible SQLMAP Scan", "ET

	WEB_SPECIFIC_APPS Solr DataImport Handler Disclose Config", "ET WEB_SERVER Wordpress Login Bruteforcing Detected", "ET EXPLOIT AVTECH Authenticated Command Injection in adcommand.cgi", "ET SCAN Possible WafWoof Web Application Firewall Detection Scan", "ET SCAN Hello Peppa! Scan Activity", "ET SCAN MS Terminal Server Traffic on Non-standard Port", "ET SCAN SQLBrute SQL Scan Detected", "ET WEB_SPECIFIC_APPS XML External Entity Information Disclosure", "ET SCAN Sipsak SIP scan", "ET USER_AGENTS EmailSiphon Suspicious User-Agent Inbound", "ET SCAN Suspicious User-Agent Containing Security Scan/ner Likely Scan", "ET EXPLOIT D-Link DIR601 2.02 Credential Disclosure", "ET SCAN Wikto Backend Data Miner Scan", "ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt", "ET SCAN SQLNinja MSSQL Version Scan", "ET EXPLOIT Possible Jira User Enumeration Attempts (CVE-2020-14181)", "ET SCAN Modified Sipvicious User-Agent Detected (sundayddr)", "GPL NETBIOS SMB CD..", "ET EXPLOIT SSL excessive fatal alerts (possible POODLE attack against server)", "ET SCAN Hydra User-Agent", "ET USER_AGENTS EmailSiphon Suspicious User-Agent Outbound", "ET VOIP Possible Inbound VOIP Scan/Misuse With User-Agent Zoiper", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Default Credentials", "ET POLICY Possible Web Crawl using Wget", "GPL SCAN superscan echo", "ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND", "ET SCAN Tomcat Web Application Manager scanning", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Configuration Download", "ET SCAN Possible Fast-Track Tool Spidering User-Agent Detected", "ET USER_AGENTS Atomic_Email_Hunter User-Agent Outbound", "ET SCAN Potential VNC Scan 5900-5920", "ET SCAN SipCLI VOIP Scan", "ET POLICY ApacheBenchmark Tool User-Agent Detected", "ET SCAN Goatzapszu Header from unknown Scanning Tool", "ET SCAN sipscan probe", "ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt", "ET SCAN Possible Mysqloit Operating System Fingerprint/SQL Injection Test Scan Detected", "ET WEB_SERVER PHP Easteregg Information-Disclosure (php-logo)", "ET SCAN NMAP SIP Version Detect OPTIONS Scan", "ET SCAN Enumiax Inter-Asterisk Exchange Protocol Username Scan", "GPL SNMP public access tcp", "ET WEB_SERVER /etc/shadow Detected in URI", "ET WEB_SERVER DFind w00tw00t GET-Requests", "ET SCAN Nessus User Agent", "GPL NETBIOS SMB startup folder unicode access", "ET SCAN ntop-ng Authentication Bypass via Session ID Guessing", "ET SCAN UPnP SUBSCRIBE Inbound - Possible CallStranger Scan (CVE-2020-12695)", "ET SCAN Wapiti Web Server Vulnerability Scan", "GPL DNS named iquery attempt", "ET SCAN Smap VOIP Device Scan", "ET POLICY Peach C++ Library User Agent Outbound", "ET SCAN w3af Scan In Progress ARGENTINA Req Method", "ET SCAN Observed Suspicious UA (Callstranger Vulnerability Checker)", "ET SCAN HID VertX and Edge door controllers discover", "ET SCAN Sipp SIP Stress Test Detected", "ET SCAN Chroot-apache0day Unknown Web Scanner User Agent", "ET SCAN Default Mysqloit User Agent Detected - Mysql Injection Takover Tool", "ET WEB_SPECIFIC_APPS Joomla Full Path Disclosure -- ldap.php", "ET WEB_SERVER Binget PHP Library User Agent Inbound", "ET SCAN Stompy Web Application Session Scan", "ET SCAN SQLix SQL Injection Vector Scan", "ET EXPLOIT Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution", "ET SCAN SQLNinja MSSQL User Scan", "ET SCAN Nessus Netbios Scanning", "GPL SNMP private access tcp"
Попытки получения привилегий пользователя	"GPL SQL dbms_repcat.comment_on_repgroup buffer overflow attempt", "ET WEB_SPECIFIC_APPS Dicoogle PACS 2.5.0 - Directory Traversal", "ET SCADA Sunway ForceControl Activex Control Vulnerability", "GPL SQL cancel_statistics ordered sname/oname buffer overflow attempt", "ET EXPLOIT Possible SharePoint XSS (CVE-2017-8514) Inbound", "GPL SQL dbms_repcat.drop_priority_date buffer overflow attempt", "ET WEB_CLIENT QuickTime Remote Exploit (exploit specific)", "GPL SQL user name buffer overflow attempt", "ET WEB_SERVER WebShell - Generic - c99shell based POST structure", "ET EXPLOIT SonicWall Global Management System - XMLRPC set_time_zone Command Injection (CVE-2018-9866)", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdSave Method Access Buffer Overflow", "ET MALWARE Possible STEADYPULSE Webshell Accessed M2", "ET WEB_CLIENT Adobe Audition

	Malformed Session File Buffer Overflow Attempt", "ET EXPLOIT Netgear R7000 Command Injection Exploit", "ET WEB_SERVER WebShell - JSP File Admin - POST Structure - dir", "ET ACTIVEX Possible Autodesk MapGuide Viewer ActiveX LayersViewWidth Method Access Denial of Service 2", "ET EXPLOIT Possible Inbound Flash Exploit with Stack-Based wininet", "ET WEB_SPECIFIC_APPS Fortify Software Security Center XML External Entity Injection 2", "ET ACTIVEX 2X Client for RDP ClientSystem Class ActiveX Control InstallClient Function Call Attempt", "GPL SQL drop_master_repobject ordered type buffer overflow attempt", "ET RPC DCERPC SVCCTL - Remote Service Control Manager Access", "GPL SQL dbms_repcat.alter_master_propagation buffer overflow attempt", "GPL SQL dbms_repcat_utl.drop_an_object buffer overflow attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Response)", "GPL SQL instantiate_online ordered refresh_template_name buffer overflow attempt", "ET WEB_SPECIFIC_APPS Cacti Superlinks Plugin SQL Injection", "ET EXPLOIT MS-Officecmd Remote Code Execution Attempt", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 6", "ET ACTIVEX Possible Windows Live Writer ActiveX BlogThisLink Method Access Denail of Service Attack 2", "GPL MISC rlogin bin", "ET WEB_SPECIFIC_APPS Kibana Attempted LFI Exploitation (CVE-2018-17246)", "ET WEB_CLIENT Microsoft Application Crash Report Indicates Potential VGX Memory Corruption", "ET ATTACK_RESPONSE Possible BeEF HTTP Headers Inbound", "ET EXPLOIT Possible Redirect to SMB exploit attempt - 302", "ET ACTIVEX Microsoft Internet Explorer Tabular DataURL ActiveX Control Memory Corruption Attempt", "ET ACTIVEX TeeChart Professional ActiveX Control integer overflow Vulnerability 3", "ET ACTIVEX TeeChart Professional ActiveX Control integer overflow Vulnerability 5", "ET EXPLOIT Generic ADSL Router DNS Change POST Request", "ET ACTIVEX dBpowerAMP Audio Player 2 FileExists Method ActiveX Buffer Overflow", "GPL SQL dbms_repcat_rgt.instantiate_offline buffer overflow attempt", "ET EXPLOIT CVE-2016-0189 Common Construct M1", "ET SCADA SEIG Modbus 3.4 - Remote Code Execution", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Service Enable", "ET EXPLOIT Jitsi Meet Plugin XSS Attempt (CVE-2021-26812)", "ET WEB_SPECIFIC_APPS Symantec Messaging Gateway 9.5.3-3 - Arbitrary file download 2", "ET EXPLOIT Possible Linksys E1500/E2500 apply.cgi RCE Attempt", "ET EXPLOIT SQL sp_configure attempt", "GPL SQL dbms_repcat.drop_snapshot_repobject buffer overflow attempt", "ET EXPLOIT php script double base64 encoded Remote Code Execution 1", "ET WEB_SERVER SQL sp_start_job attempt", "ET ACTIVEX Possible IBM Tivoli Provisioning Manager Express Isig.isigCtl.1 ActiveX RunAndUploadFile Method Overflow 2", "ET WEB_SERVER WebShell - Generic - c99shell based POST structure w/multipart", "ET ACTIVEX Adobe browser document ActiveX DoS Attempt", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 2", "ET EXPLOIT Possible CVE-2018-4407 - Apple ICMP DoS PoC", "ET FTP Possible FTP Daemon Username INSERT INTO SQL Injection Attempt", "GPL SQL dbms_repcat.drop_delete_resolution buffer overflow attempt", "ET EXPLOIT Possible CVE-2016-0777 Client Sent Roaming Resume Request", "ET EXPLOIT Nagios XI Remote Code Execution", "ET WEB_SPECIFIC_APPS Blind Server-Side Request Forgery", "ET EXPLOIT Nagios XI Remote Code Execution 2", "ET EXPLOIT xdebug OS Command Execution", "ET ACTIVEX AVTECH Software ActiveX Snapshot Method Buffer Overflow Attempt", "ET EXPLOIT Nagios XI Set DB User Root", "ET WEB_CLIENT Possible Internet Explorer VBscript CVE-2014-6332 multiple redim preserve", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 1", "ET WEB_CLIENT Microsoft Rich Text File .RTF File download with invalid listoverridecount", "ET WEB_CLIENT Adobe Authplay.dll NewClass Memory Corruption Attempt", "ET ACTIVEX Possible Cyme ChartFX client server ActiveX Control ShowPropertiesDialog arbitrary code execution", "ET EXPLOIT Linksys Router Unauthenticated Remote Code Execution", "GPL SQL dbms_offline_og.begin_instantiation buffer overflow attempt", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 UTF-8 Inbound Web Servers Likely Command Execution 7", "ET WEB_SPECIFIC_APPS Hadoop YARN ResourceManager Unauthenticated Command Execution", "GPL SQL

	sys.dbms_repcat_mas.create_master_repgroup buffer overflow attempt", "ET ACTIVEX Oracle AutoVue Activex Insecure method (ExportEdaBom)", "ET ACTIVEX Tracker Software pdfSaver ActiveX StoreInRegistry Method Access Potential Buffer Overflow", "ET SCADA PROMOTIC ActiveX Control Insecure method (SaveCfg)", "ET SCADA PROMOTIC ActiveX Control Insecure method (AddTrend)", "ET WEB_SERVER WebShell - PHPShell - PHPKonsole URI", "ET EXPLOIT Generic ADSL Router DNS Change Request", "ET WEB_SPECIFIC_APPS OGNL Expression Injection (CVE-2017-9791)", "ET ACTIVEX ASUS Net4Switch ActiveX CxDbgPrint Format String Function Call Attempt", "GPL SQL dbms_repcat.create_mview_repgroup buffer overflow attempt", "ET ACTIVEX Possible CA BrightStor ARCserve Backup ActiveX AddColumn Method Access Buffer Overflow", "ET EXPLOIT Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution Windows", "ET WEB_CLIENT Foxit PDF Reader Title Stack Overflow", "ET EXPLOIT SUSPICIOUS DTLS Pre 1.0 Fragmented Client Hello Possible CVE-2014-0195", "ET EXPLOIT Possible Realtek SDK - formRebootCheck/formWsc Stack Buffer Overflow Inbound (CVE-2021-35392)", "GPL SQL dbms_repcat_admin.register_user_repgroup buffer overflow attempt", "ET ACTIVEX Possible IBM Lotus Quickr for Domino ActiveX control Import_Times Method Access buffer overflow Attempt", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct (Reversed)", "ET EXPLOIT php script double base64 encoded Remote Code Execution 2", "ET WEB_SPECIFIC_APPS Apache CouchDB Remote Code Execution 2", "GPL SQL dbms_repcat.alter_priority_nvarchar2 buffer overflow attempt", "ET ACTIVEX Possible AOL SuperBuddy ActiveX Control Remote Code Execution Attempt", "ET ACTIVEX Microsoft DirectX 9 ActiveX Control Format String Function Call", "ET WEB_CLIENT Spectre Exploit Javascript", "ET WEB_CLIENT Possible CVE-2014-4113 Exploit Download", "ET ACTIVEX Possible CommuniCrypt Mail SMTP ActiveX AddAttachments Method Access Stack Buffer Overflow", "GPL SQL dbms_repcat.set_local_flavor buffer overflow attempt", "GPL SQL dbms_repcat.alter_site_priority buffer overflow attempt", "ET ACTIVEX Viscom Movie Player Pro SDK ActiveX DrawText method Buffer Overflow Function Call", "ET ACTIVEX Quest vWorkspace Broker Client ActiveX Control SaveMiniLaunchFile Remote File Creation/Overwrite 2", "ET FTP Possible FTP Daemon Username UPDATE SET SQL Injection Attempt", "ET EXPLOIT Nagios XI SQL Injection", "GPL SQL dbms_repcat.purge_master_log buffer overflow attempt", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Reboot Router)", "ET WEB_CLIENT EMET Detection Via XMLDOM", "ET WEB_SPECIFIC_APPS Nagios XI Network Monitor - OS Command Injection", "ET WEB_SPECIFIC_APPS Attempted Symantec Secure Web Gateway RCE", "ET ACTIVEX Possible McAfee Virtual Technician MVT.MVTControl.6300 ActiveX Control GetObject method Remote Code Execution 2", "GPL SQL dbms_repcat_instantiate.drop_site_instantiation buffer overflow attempt", "ET ACTIVEX Tracker Software pdfSaver ActiveX StoreInRegistry Method Access Potential Buffer Overflow 2", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 3", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 3", "ET WEB_SERVER Coldfusion cfcexplorer Directory Traversal", "ET ACTIVEX Possible Honeywell Tema Remote Installer ActiveX DownloadFromURL method Remote Code Execution", "ET WEB_SERVER WebShell - PHPShell - Comment", "GPL SQL sp_password password change", "ET ACTIVEX Oracle Document Capture File Overwrite or Buffer Overflow Attempt", "ET EXPLOIT Possible CVE-2015-7547 A/AAAA Record Lookup Possible Forced FallBack(fb set)", "ET ACTIVEX Possible Advantech Studio ISSymbol ActiveX Control Multiple Buffer Overflow Attempt", "ET ACTIVEX EdrawSoft Office Viewer Component ActiveX FtpUploadFile Stack Buffer Overflow", "ET ACTIVEX Possible NET-i viewer ActiveX Control BackupToAvi Method Access Buffer Overflow", "ET EXPLOIT Zollard PHP Exploit Telnet Outbound", "ET WEB_CLIENT Adobe Acrobat Reader FlateDecode Stream Predictor Exploit Attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request)", "GPL SQL alter file buffer overflow attempt", "GPL SQL dbms_repcat.generate_snapshot_support buffer overflow attempt", "ET ACTIVEX Quest Explain Plan Display ActiveX Control SaveToFile Insecure Method Access", "GPL SQL dbms_repcat.add_object_to_flavor buffer overflow attempt", "ET EXPLOIT Apache

	Struts 2 REST Plugin ysoserial Usage (B64) 2", "ET ACTIVEX Possible Chilkat Software FTP2 ActiveX Component GetFile Access Remote Code Execution", "GPL SQL dbms_repcat.add_columns_to_flavor buffer overflow attempt", "ET ACTIVEX Possible NET-i viewer ActiveX Control ConnectDDNS Method Access Code Execution Vulnerability", "ET WEB_CLIENT PolarisOffice Insecure Library Loading", "GPL SQL dbms_repcat_sna_utl.register_flavor_change buffer overflow attempt", "ET EXPLOIT Apache Struts Possible OGNL Java WriteFile in URI", "ET WEB_SPECIFIC_APPS JcomBand toolbar ActiveX Control isRegistered Property Buffer Overflow Attempt", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M2", "GPL SQL dbms_repcat.generate_replication_package buffer overflow attempt", "ET EXPLOIT CVE-2018-8174 Common Construct B64 M1", "ET ACTIVEX Possible Crystal Reports Viewer Activex Control ServerResourceVersion Insecure Method Access", "GPL SQL dbms_repcat.alter_priority_nchar buffer overflow attempt", "ET WEB_SPECIFIC_APPS CMS Made Simple Remote Code Execution", "GPL SQL dbms_repcat.comment_on_mview_repsites buffer overflow attempt", "ET WEB_CLIENT Adobe Acrobat newfunction Remote Code Execution Attempt", "ET WEB_CLIENT Possible Microsoft Edge Remote Command Execution PoC (CVE-2018-8495)", "GPL SQL dbms_repcat.alter_priority_raw buffer overflow attempt", "ET EXPLOIT Apache Struts Possible OGNL AllowStaticMethodAccess in client body", "ET EXPLOIT Unknown Command Injection Attempt Inbound (Possible Mirai Activity)", "ET EXPLOIT Realtek SDK - Command Injection Inbound (CVE-2021-35395)", "ET ACTIVEX Dell Webcam CrazyTalk ActiveX Control BackImage Access Potential Buffer Overflow Attempt", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M1", "ET ACTIVEX Possible Electronic Arts SnoopyCtrl ActiveX Control Buffer Overflow 2", "ET EXPLOIT bin bash base64 encoded Remote Code Execution 1", "GPL SQL dbms_repcat.alter_priority_date buffer overflow attempt", "ET WEB_CLIENT Microsoft Application Crash Report Indicates Potential VGX Memory Corruption 2", "ET ACTIVEX Possible Sony PC Companion Admin_RemoveDirectory Stack-based Unicode Buffer Overload SEH", "ET EXPLOIT Apache Struts Possible OGNL Java ProcessBuilder URI", "GPL SQL repcat_import_check ordered gowner/gname buffer overflow attempt", "ET EXPLOIT Nagios XI SQL Injection 2", "ET ACTIVEX Possible Camera Stream Client Possible ActiveX Control SetDirectory Method Access Buffer Overflow 2", "ET ATTACK_RESPONSE WSO - WebShell Activity - POST structure", "ET WEB_CLIENT Spectre Kernel Memory Leakage JavaScript", "ET EXPLOIT Apache Struts 2 REST Plugin (B64) 5", "ET EXPLOIT Zimbra <8.8.11 - XML External Entity Injection/SSRF Attempt (CVE-2019-9621)", "ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ExportSettings Remote File Overwrite Attempt", "ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 2", "ET EXPLOIT Possible Zyxel Authentication Bypass Inbound (CVE-2021-3297)", "ET EXPLOIT Ghostscript illegal read undefinedfilename attempt", "ET ACTIVEX Possible IBM Lotus iNotes Upload Module possible ActiveX Control Attachment_Times Method Access Buffer Overflow Attempt", "GPL SQL sys.dbms_repcat_conf.alter_site_priority_site buffer overflow attempt", "ET WEB_SPECIFIC_APPS MicroFocus Secure Messaging Gateway SQL Injection", "GPL SQL drop_site_instantiate ordered refresh_template_name buffer overflow attempt", "ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Function Name", "ET EXPLOIT AnyDesk UDP Discovery Format String (CVE-2020-13160)", "ET ACTIVEX Possible Edraw Diagram Component 5 ActiveX LicenseName Access Potential buffer overflow DOS", "ET WEB_CLIENT Possible Internet Explorer srcElement Memory Corruption Attempt", "ET WEB_SPECIFIC_APPS Apache CouchDB Remote Code Execution 3", "GPL SQL dbms_repcat.define_column_group buffer overflow attempt", "ET EXPLOIT Ghostscript invalidcheck escape attempt", "ET WEB_SERVER Possible Cookie Based BackDoor Used in Drupal Attacks", "ET WEB_SERVER WebShell - Generic - c99shell based header w/colons", "ET WEB_CLIENT Firefox Plugin Parameter EnsureCachedAttrParamArrays Remote Code Execution Attempt", "ET EXPLOIT ZTE Cable Modem RCE Attempt (CVE-2014-2321)", "ET WEB_SPECIFIC_APPS Wordpress Arbitrary File Deletion 2", "GPL SQL instantiate_offline ordered refresh_template_name buffer overflow attempt", "ET

	WEB_CLIENT Mozilla Firefox nsTreeSelection Element invalidateSelection Remote Code Execution Attempt", "ET EXPLOIT Ghostscript LockDistillerParams type confusion attempt", "ET INFO Plaintext SSH Authentication Identified (Encryption set to None)", "ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6077)", "ET WEB_SPECIFIC_APPS Cisco BBSM Captive Portal AccesCodeStart.asp Cross-Site Scripting Attempt", "ET EXPLOIT IE Scripting Engine Memory Corruption Vulnerability M2 (CVE-2019-0752)", "ET ACTIVEX Possible Dell IT Assistant detectIESettingsForITA.ocx ActiveX Control readRegVal Remote Registry Dump Vulnerability 2", "ET WEB_CLIENT Apple Quicktime RTSP Content-Type overflow attempt", "GPL SQL dbms_repcat.add_update_resolution buffer overflow attempt", "ET SCADA PcVue Activex Control Insecure method (LoadObject)", "GPL SQL dbms_repcat.alter_priority_char buffer overflow attempt", "ET ACTIVEX Oracle AutoVue Activex Insecure method (Export3DBom) Format String Function Call", "GPL SQL dbms_repcat.add_site_priority_site buffer overflow attempt", "ET ACTIVEX Oracle AutoVue Activex Insecure method (SaveViewStateToFile)", "GPL SQL dbms_repcat.comment_on_repobject buffer overflow attempt", "ET MALWARE Possible STEADYPULSE Webshell Accessed M1", "ET ACTIVEX Possible BarCodeWiz (BARCODEWIZLib.BarCodeWiz) ActiveX Control Buffer Overflow", "ET EXPLOIT Wscript Shell Run Attempt - Likely Hostile", "ET WEB_SERVER Possible WebShell Access Inbound [exec] M1 (CISA AA21-259A)", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct HEX", "ET EXPLOIT Possible Redirect to SMB exploit attempt - 307", "ET WEB_CLIENT HTA File containing Wscript.Shell Call - Potential CVE-2017-0199", "ET WEB_CLIENT Possible Adobe Acrobat Reader Newclass Invalid Pointer Remote Code Execution Attempt", "ET EXPLOIT Possible CVE-2015-7547 Long Response to AAAA lookup", "ET EXPLOIT Possible Realtek SDK - Stack Buffer Overflow via UPnP SUBSCRIBE Callback Header Inbound (CVE-2021-35393)", "GPL SQL dbms_rectifier_diff.rectify buffer overflow attempt", "ET EXPLOIT Possible Internet Explorer Memory Corruption Vulnerability (CVE-2015-2444)", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 1", "ET EXPLOIT HP Enterprise VAN SDN Controller Upload Backdoor", "ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6334)", "ET WEB_CLIENT GENERIC VB ShellExecute Function Inside of VBSCRIPT tag", "ET ACTIVEX Possible IBM Tivoli Provisioning Manager Express Isig.isigCtl.1 ActiveX RunAndUploadFile Method Overflow", "ET ACTIVEX Possible Quest vWorkspace Broker Client ActiveX Control SaveMiniLaunchFile Remote File Creation/Overwrite", "ET ACTIVEX Possible BarCodeWiz BarcodeWiz.dll ActiveX Control Barcode Method Remote Buffer Overflow Attempt", "GPL SQL dbms_repcat.specify_new_masters buffer overflow attempt", "ET EXPLOIT php script double base64 encoded Remote Code Execution 9", "ET EXPLOIT Apache Struts 2 REST Plugin Vulnerability (CVE-2017-9805)", "ET EXPLOIT VMware NSX SD-WAN Command Injection 2", "ET MALWARE Kryptik Check-in", "ET HUNTING PDF Containing Subform with JavaScript", "ET EXPLOIT Apache Struts 2 REST Plugin (B64) 4", "ET NETBIOS PolarisOffice Insecure Library Loading - SMB Unicode", "ET WEB_CLIENT PDF With Adobe Audition Session File Handling Memory Corruption Attempt", "ET WEB_SPECIFIC_APPS cmd powershell base64 encoded to Web Server 3", "ET WEB_SPECIFIC_APPS Jenkins Script Console Usage (Can be Used to Spawn Shell)", "ET WEB_SERVER WebShell - Generic - c99shell based header", "ET ACTIVEX Softek Barcode Reader Toolkit ActiveX Control Format String Function Call", "GPL SQL mdsys.md2.validate_geom buffer overflow attempt", "GPL SQL dbms_repcat.add_priority_raw buffer overflow attempt", "ET EXPLOIT Cisco Adaptive Security Appliance - Path Traversal", "ET ACTIVEX Possible LEADTOOLS ActiveX Raster Twain AppName Method Access Buffer Overflow", "ET EXPLOIT Apache Struts RCE CVE-2018-11776 POC M1", "ET WEB_CLIENT Malicious iframe guessing router password 1", "ET ACTIVEX Possible Camera Stream Client Possible ActiveX Control SetDirectory Method Access Buffer Overflow", "ET EXPLOIT Possible Realtek SDK - formStaticDHCP Stack Buffer Overflow Inbound (CVE-2021-35393)", "ET EXPLOIT Ruckus vRIoT Command Injection Attempt Inbound (CVE-2020-26878)", "GPL SQL dbms_repcat.relocate_masterdef buffer overflow attempt", "ET ACTIVEX Possible Microsoft WMI Administration Tools WEBSingleView.ocx ActiveX Buffer Overflow

	Attempt Function Call", "ET ACTIVEX AVTECH Software ActiveX Buffer Overflow Function Call", "GPL SQL dbms_repcat.drop_column_group buffer overflow attempt", "ET EXPLOIT Apache Struts RCE CVE-2018-11776 POC M2", "ET EXPLOIT Ghostscript LockDistillerParams type confusion attempt (SMTP)", "ET WEB_SPECIFIC_APPS Jenkins Script Console Usage (Metasploit Windows CMD Shell)", "ET ACTIVEX Possible Oracle Hyperion Financial Management TList6 ActiveX Control Remote Code Execution", "ET ACTIVEX Gesytec ElonFmt ActiveX Component Format String Function Call", "ET EXPLOIT Generic ADSL Router DNS Change GET Request", "ET WEB_SPECIFIC_APPS cmd powershell base64 encoded to Web Server 1", "ET EXPLOIT FTPShell client Stack Buffer Overflow", "ET EXPLOIT Apache Struts 2 REST Plugin (B64) 6", "ET WEB_CLIENT Possible Adobe Reader 9.4 this.printSeps Memory Corruption Attempt", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct DECC", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 UTF-8 Inbound Web Servers Likely Command Execution 6", "ET WEB_CLIENT Adobe Shockwave Director tSAC Chunk memory corruption Attempt", "ET EXPLOIT Possible WePresent WIPG1000 File Inclusion", "ET WEB_CLIENT Possible Adobe Reader and Acrobat Forms Data Format Remote Security Bypass Attempt", "ET EXPLOIT php script base64 encoded Remote Code Execution 1", "ET ACTIVEX Possible Samsung Kies ActiveX PrepareSync method Buffer overflow", "ET ACTIVEX Possible WinZip FileView ActiveX CreateNewFolderFromName Method Access Buffer Overflow", "ET SCADA DATAC RealWin SCADA Server Buffer Overflow", "GPL SQL dbms_repcat.obsolete_flavor_definition buffer overflow attempt", "GPL SQL TO_CHAR buffer overflow attempt", "ET EXPLOIT Possible CVE-2015-7547 Malformed Server Response A/AAAA", "ET WEB_CLIENT Apple Safari UXSS (CVE-2017-7089)", "ET ACTIVEX Dell Webcam CrazyTalk ActiveX Control BackImage Access Potential Buffer Overflow Attempt 2", "GPL SQL dbms_repcat.define_priority_group buffer overflow attempt", "ET ACTIVEX Avaya CallPilot Unified Messaging ActiveX Function Call", "ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed CWS", "ET EXPLOIT SAP NetWeaver AS Directory Traversal Attempt Inbound (CVE-2020-6286)", "GPL SQL dbms_repcat.switch_snapshot_master buffer overflow attempt", "GPL SQL create file buffer overflow attempt", "ET WEB_CLIENT Adobe Acrobat Util.printf Buffer Overflow Attempt", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M3", "ET ACTIVEX TeeChart Professional ActiveX Control integer overflow Vulnerability 2", "GPL SQL dbms_repcat.comment_on_column_group buffer overflow attempt", "ET ACTIVEX Possible SonicWALL SSL-VPN End-Point Interrogator/Installer ActiveX Control Install3rdPartyComponent Method Buffer Overflow", "ET FTP Possible FTP Daemon Username UNION SELECT SQL Injection Attempt", "GPL SQL dbms_repcat_rgt.drop_site_instantiation buffer overflow attempt", "ET EXPLOIT Oracle Weblogic Server Deserialization Remote Command Execution", "ET EXPLOIT Cisco Catalyst Remote Code Execution (CVE-2017-3881)", "ET WEB_CLIENT Possible Microsoft Internet Explorer URI Validation Remote Code Execution Attempt", "ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ImportSettings Remote File Overwrite Attempt", "ET EXPLOIT Possible ZTE ZXV10 H108L Router Root RCE Attempt", "ET WEB_CLIENT Firefox Proxy Prototype RCE Attempt (CVE-2014-8636)", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 6", "ET EXPLOIT SugarCRM PHP Shell Upload Attempt", "ET EXPLOIT Possible Cisco IKEv1 Information Disclosure Vulnerability CVE-2016-6415", "ET EXPLOIT php script base64 encoded Remote Code Execution 3", "ET ACTIVEX Possible Oracle Hyperion Financial Management TList6 ActiveX Control Remote Code Execution 2", "GPL EXPLOIT xp_sprintf possible buffer overflow", "GPL SQL dbms_repcat.comment_on_repsites buffer overflow attempt", "GPL SQL dbms_repcat.comment_on_site_priority buffer overflow attempt", "ET FTP Possible FTP Daemon Username INTO OUTFILE SQL Injection Attempt", "GPL IMAP login buffer overflow attempt", "ET ACTIVEX J-Integra ActiveX SetIdentity Buffer Overflow", "ET WEB_SPECIFIC_APPS Jenkins Script Console Usage (Metasploit Unix Shell)", "ET ACTIVEX Possible beSTORM ActiveX (WinGraphviz.dll) Remote Heap Overflow", "ET EXPLOIT xp_enumerrorlogs access", "ET WEB_SERVER Apache Continuum Arbitrary Command Execution", "GPL SQL dbms_repcat.drop_snapshot_repgroup buffer overflow attempt", "ET WEB_SERVER

	Microsoft IIS Remote Code Execution (CVE-2017-7269)", "GPL SQL dbms_repcat.set_columns buffer overflow attempt", "ET EXPLOIT MS16-009 IE MSHTML Form Element Type Confusion (CVE-2016-0061)", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 1", "ET WEB_CLIENT Malicious SCF File Inbound", "ET EXPLOIT Apache Struts Possible OGNL Java WriteFile in client_body", "ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M1", "ET EXPLOIT php script double base64 encoded Remote Code Execution 5", "ET WEB_CLIENT BeEF Cookie (BEEFHOOK)", "ET ACTIVEX Possible KeyHelp ActiveX LaunchTriPane Remote Code Execution Vulnerability 2", "GPL SQL drop_master_repgroup ordered gname buffer overflow attempt", "ET ACTIVEX Possible Autodesk MapGuide Viewer ActiveX LayersViewWidth Method Access Denial of Service", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdOpen Method Access Buffer Overflow 2", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 2", "ET WEB_CLIENT Microsoft Windows Media component specific exploit", "ET EXPLOIT Zollard PHP Exploit Telnet Inbound", "ET ACTIVEX AVTECH Software ActiveX Login Method Buffer Oveflow Attempt", "GPL SQL dbms_repcat.send_old_values buffer overflow attempt", "ET WEB_CLIENT Internet Explorer CTableRowCellsCollectionCacheItem.GetNext Memory Use-After-Free Attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Disable Firewall", "GPL SQL create_mview_repgroup ordered fname buffer overflow attempt", "GPL SQL dbms_offline_og.begin_flavor_change buffer overflow attempt", "GPL SQL og.begin_load ordered gname buffer overflow attempt", "ET WEB_CLIENT Possible IE10 Use After Free CVE-2014-0322", "ET ACTIVEX Possible NET-i viewer ActiveX Control BackupToAvi Method Access Buffer Overflow 2", "ET EXPLOIT Ghostscript illegal read undefinedfilename attempt (SMTP)", "ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ExportSettings Function Call Attempt", "ET WEB_CLIENT Microsoft Office Visio DXF File Processing Remote Code Execution", "ET WEB_CLIENT Firefox Interleaving document.write and appendChild Overflow (POC SPECIFIC)", "ET ACTIVEX Oracle AutoVue Activex Insecure method (ExportEdaBom) Format String Function Call", "ET EXPLOIT Possible Realtek SDK - formWlanMultipleAP Stack Buffer Overflow Inbound (CVE-2021-35393)", "GPL SQL dbms_repcat.drop_priority_nvarchar2 buffer overflow attempt", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 4", "GPL SQL dbms_repcat.alter_mview_propagation buffer overflow attempt", "GPL SQL dbms_repcat.cancel_statistics buffer overflow attempt", "ET EXPLOIT Possible ZyXEL P660HN-T v1 RCE (CVE-2017-18368)", "ET ACTIVEX Possible IBM Rational ClearQuest Activex Control RegisterSchemaRepoFromFileByDbSet Insecure Method Access", "ET WEB_CLIENT Malicious iframe guessing router password 2", "GPL SQL dbms_repcat.drop_unique_resolution buffer overflow attempt", "ET ACTIVEX Axis Media Controller ActiveX SetImage Method Remote Code Execution Attempt", "GPL SQL dbms_repcat.alter_priority_number buffer overflow attempt", "ET EXPLOIT Possible Linksys WAP54Gv3 Remote Debug Root Shell Exploitation Attempt", "GPL SQL dbms_rectifier_diff.differences buffer overflow attempt", "ET WEB_SPECIFIC_APPS TimThumb Remote Command Execution", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Enable Guest Network)", "ET EXPLOIT Possible Firefox PDF.js Same-Origin-Bypass CVE-2015-4495 M2", "ET EXPLOIT Possible Redirect to SMB exploit attempt - 301", "ET WEB_SERVER WebShell - JSP File Admin", "ET ACTIVEX TeeChart Professional ActiveX Control integer overflow Vulnerability 1", "ET ACTIVEX Possible KeyHelp ActiveX LaunchTriPane Remote Code Execution Vulnerability", "ET ACTIVEX ASUS Net4Switch ipswcom.dll ActiveX Stack Buffer Overflow", "ET EXPLOIT php script double base64 encoded Remote Code Execution 4", "ET EXPLOIT MySQL Server for Windows Remote SYSTEM Level Exploit (Stuxnet Technique)", "GPL SQL dbms_repcat.add_priority_char buffer overflow attempt", "GPL SQL dbms_repcat_admin.unregister_user_repgroup buffer overflow attempt", "ET WEB_CLIENT BeEF Cookie Outbound", "ET WEB_SERVER Possible Cisco Adaptive Security Appliance Web VPN FTP or CIFS Authentication Form Phishing Attempt", "ET FTP Possible FTP Daemon Username SELECT FROM SQL Injection Attempt", "GPL SQL

	dbms_repcat.create_master_repgroup buffer overflow attempt", "ET WEB_CLIENT PowerShell call in script 1", "GPL SQL xp_printstatements possible buffer overflow", "ET WEB_SPECIFIC_APPS XML External Entity Remote Code Execution", "ET WEB_SERVER Adobe Flash Player Rosetta Flash compressed CWS in URI", "ET WEB_CLIENT Potential MSXML2.FreeThreadedDOMDocument Uninitialized Memory Corruption Attempt", "GPL SQL dbms_repcat.alter_site_priority_site buffer overflow attempt", "GPL SQL sp_password - password change", "ET WEB_CLIENT Possible MacOSX HelpViewer 10.12.1 XSS Arbitrary File Execution and Arbitrary File Read (CVE-2017-2361)", "GPL SQL dbms_repcat.remove_master_databases buffer overflow attempt", "ET WEB_CLIENT Possible BeEF Default SSL Cert", "ET NETBIOS SMB Trans2 Query_Fs_Attribute_Info SrvSmbQueryFsInformation Pool Buffer Overflow", "GPL SQL dbms_repcat.add_priority_varchar2 buffer overflow attempt", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct HEXC", "ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 2", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 4", "ET ACTIVEX FathFTP 1.8 EnumFiles Method ActiveX Buffer Overflow", "ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Construct", "ET EXPLOIT Apache Struts Possible OGNL Java Exec In URI", "GPL SQL refresh_mview_repgroup ordered gowner buffer overflow attempt", "ET ACTIVEX AVTECH Software ActiveX _DownloadPBClose Method Buffer Overflow Attempt", "ET WEB_CLIENT Possible CVE-2013-1710/CVE-2012-3993 Firefox Exploit Attempt", "ET ACTIVEX SoftArtisans XFile FileManager ActiveX GetDriveName method stack overflow Attempt", "ET ACTIVEX AVTECH Software ActiveX SendCommand Method Buffer Overflow Attempt", "GPL SQL dbms_repcat.register_snapshot_repgroup buffer overflow attempt", "ET WEB_SERVER WebShell - zecmd - Form", "ET MALWARE Possible Linux/Cdorked.A Incoming Command", "ET ACTIVEX AVTECH Software ActiveX _DownloadPBControl Method Buffer Overflow Attempt", "ET WEB_CLIENT [TW] WEBDAV UA", "ET ACTIVEX Possible AOL ICQ ActiveX Control DownloadAgent Method Access Arbitrary File Download and Execute", "GPL SQL service_name buffer overflow attempt", "GPL SQL dbms_repcat.register_mview_repgroup buffer overflow attempt", "ET ATTACK_RESPONSE Possible Lateral Movement - File Creation Request in Remote System32 Directory (T1105)", "GPL SQL dbms_repcat.make_column_group buffer overflow attempt", "ET ACTIVEX Possible Sony PC Companion Load method Stack-based Unicode Buffer Overload SEH", "ET EXPLOIT Possible Redirect to SMB exploit attempt - 303", "ET ACTIVEX AVTECH Software ActiveX _DownloadPBOpen Method Buffer Overflow Attempt", "ET ACTIVEX Possible McAfee Virtual Technician MVT.MVTControl.6300 ActiveX Control GetObject method Remote Code Execution", "ET EXPLOIT Gitlab Login Attempt with hard-coded password (CVE-2022-1162)", "ET WEB_SPECIFIC_APPS WordPress Plugin Job Manager Stored Cross-Site Scripting", "ET ACTIVEX Trend Micro Internet Security Pro 2010 ActiveX extSetOwner Remote Code Execution Attempt", "ET EXPLOIT SQL sp_configure - configuration change", "ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M3", "ET SCADA SEIG SYSTEM 9 - Remote Code Execution", "ET EXPLOIT Ghostscript invalidcheck escape attempt (SMTP)", "ET WEB_SPECIFIC_APPS ELF file magic encoded ASCII Inbound Web Servers Likely Command Execution 4", "ET WEB_CLIENT [Volex] Possible ColdFusion Unauthenticated Upload Attempt (CVE-2018-15961)", "ET ACTIVEX Possible NOS Microsystems Adobe Reader/Acrobat getPlus Get_atlcomHelper ActiveX Control Multiple Stack Overflows Remote Code Execution Attempt", "ET ACTIVEX TRENDnet TV-IP121WN UltraMJCam ActiveX Control OpenFileDlg Access Potential Remote Stack Buffer Overflow 2", "ET WEB_CLIENT Adobe Reader and Acrobat U3D File Invalid Array Index Remote Code Execution Attempt", "GPL SQL sp_adduser - database user creation", "ET WEB_SERVER SQL sp_delete_alert attempt", "ET WEB_SPECIFIC_APPS ELF file magic plain Inbound Web Servers Likely Command Execution 11", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 Hex Escape Inbound Web Servers Likely Command Execution 8", "ET WEB_CLIENT Internet Explorer execCommand function Use after free Vulnerability 0day Metasploit 2", "GPL SQL dbms_repcat.drop_site_priority buffer overflow attempt", "ET EXPLOIT Possible

	ShuttleTech 915WM DNS Change Attempt", "GPL SQL dbms_repcat.create_master_repobject buffer overflow attempt", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdOpen Method Access Buffer Overflow", "GPL SQL dbms_repcat_auth.revoke_surrogate_repcat buffer overflow attempt", "ET ACTIVEX Oracle AutoVue Activex Insecure method (Export3DBom)", "ET ACTIVEX HP Easy Printer Care Software XMLCacheMgr ActiveX Control Remote Code Execution Attempt", "GPL SQL dbms_repcat.unregister_mview_repgroup buffer overflow attempt", "GPL SQL dbms_repcat.drop_column_group_from_flavor buffer overflow attempt", "GPL SQL dbms_repcat.drop_priority buffer overflow attempt", "ET ACTIVEX Possible Windows Live Writer ActiveX BlogThisLink Method Access Denail of Service Attack", "ET WEB_CLIENT PWNJS JS Constructs", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 3", "ET SCAN struts-pwn User-Agent", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 2", "GPL SQL dbms_repcat.add_unique_resolution buffer overflow attempt", "GPL SQL dbms_repcat.add_delete_resolution buffer overflow attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Add Admin Passwd", "ET EXPLOIT IBM QRadar SIEM Unauthenticated Remote Code Execution", "ET ACTIVEX Possible HP Easy Printer Care XMLCacheMgr Class ActiveX Control Remote Code Execution", "ET ACTIVEX SoftArtisans XFile FileManager ActiveX Buildpath method stack overflow Attempt", "GPL SQL dbms_offline_snapshot.end_load buffer overflow attempt", "GPL SQL dbms_repcat.drop_priority_number buffer overflow attempt", "ET WEB_SERVER Possible WebShell Access Inbound [upload] M1 (CISA AA21-259A)", "ET EXPLOIT php script double base64 encoded Remote Code Execution 3", "ET WEB_SERVER ASP.NET Forms Authentication Bypass", "ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - ROP", "ET EXPLOIT Possible Linksys WRT100/110 RCE Attempt (CVE-2013-3568)", "GPL SQL dbms_repcat.refresh_mview_repgroup buffer overflow attempt", "ET EXPLOIT SUSPICIOUS Possible CVE-2017-0199 IE7/NoCookie/Referer HTA dl", "ET WEB_CLIENT VLC Media Player .ass File Buffer Overflow Attempt", "GPL SQL dbms_repcat.alter_priority buffer overflow attempt", "ET ACTIVEX Possible SkinCrafter ActiveX Control InitLicenKeys Method Access Buffer Overflow 2", "GPL SQL dbms_repcat.add_priority_nvarchar2 buffer overflow attempt", "GPL SQL dbms_offline_og.end_flavor_change buffer overflow attempt", "ET WEB_SPECIFIC_APPS Apache CouchDB Remote Code Execution 1", "ET EXPLOIT Possible Inbound Flash Exploit (CVE-2018-15982)", "ET EXPLOIT SUSPICIOUS DTLS 1.2 Fragmented Client Hello Possible CVE-2014-0195", "ET WEB_CLIENT Possible BeEF Module in use", "GPL EXPLOIT xp_cmdshell program execution 445", "GPL SQL dbms_repcat.alter_priority_varchar2 buffer overflow attempt", "GPL SQL dbms_repcat.drop_master_repobject buffer overflow attempt", "ET EXPLOIT Ghostscript setpattern type confusion attempt (SMTP)", "ET WEB_CLIENT Possible Foxit/Adobe PDF Reader Launch Action Remote Code Execution Attempt", "ET EXPLOIT Possible CVE-2015-7547 Long Response to A lookup", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct DECCS", "GPL EXPLOIT rsh bin", "ET WEB_SPECIFIC_APPS cmd powershell base64 encoded to Web Server 2", "ET EXPLOIT Apache Struts Possible OGNL Java Exec In URI M2", "ET ACTIVEX SoftArtisans XFile FileManager ActiveX DriveExists method stack overflow Attempt", "GPL SQL dbms_offline_og.resume_subset_of_masters buffer overflow attempt", "ET ACTIVEX WMITools ActiveX Remote Code Execution", "ET EXPLOIT php script double base64 encoded Remote Code Execution 7", "ET ACTIVEX Quest InTrust Annotation Objects ActiveX Control Add Access Potential Remote Code Execution", "ET EXPLOIT Adobe Coldfusion BlazeDS Java Object Deserialization Remote Code Execution", "GPL SQL dbms_repcat.drop_object_from_flavor buffer overflow attempt", "ET WEB_CLIENT Possible Android RCE via XSS and Play Store XFO", "ET NETBIOS Microsoft Windows RRAS SMB Remote Code Execution", "ET WEB_SPECIFIC_APPS Yahoo CD Player ActiveX Open Stack Overflow Attempt", "GPL SQL dbms_repcat.create_mview_repobject buffer overflow attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Startup Script", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 2", "ET WEB_SERVER PHP Crawler", "GPL SQL

	ctx_output.start_log buffer overflow attempt", "ET EXPLOIT bin bash base64 encoded Remote Code Execution 3", "ET WEB_CLIENT [TW] CAB From Possible WebDAV Share Possible DiagCab Abuse Attempt", "ET ACTIVEX EdrawSoft Office Viewer Component ActiveX FtpUploadFile Format String Function Call Attempt", "GPL SQL register_user_repgroup ordered privilege_type buffer overflow attempt", "ET EXPLOIT Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution Unix", "GPL MISC rsh echo + +", "GPL EXPLOIT sp_start_job - program execution", "GPL SQL dbms_repcat.alter_snapshot_propagation buffer overflow attempt", "ET WEB_CLIENT Possible Adobe Multimedia Doc.media.newPlayer Memory Corruption Attempt", "ET WEB_CLIENT VBscript UAF (CVE-2018-8373)", "ET WEB_CLIENT Mozilla Firefox mChannel Object Dangling Pointer Use-After-Free Memory Corruption Attempt", "ET ACTIVEX Possible Sony PC Companion CheckCompatibility method Stack-based Unicode Buffer Overload", "GPL SQL dbms_repcat.resume_master_activity buffer overflow attempt", "ET EXPLOIT Apache Struts 2 REST Plugin XStream RCE (ProcessBuilder)", "ET ACTIVEX Possible Electronic Arts SnoopyCtrl ActiveX Control Buffer Overflow", "GPL SQL dbms_repcat_instantiate.instantiate_offline buffer overflow attempt", "GPL EXPLOIT xp_cmdshell - program execution", "ET WEB_CLIENT Possible Adobe Acrobat and Reader Pushstring Memory Corruption Attempt", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdImport Method Access Buffer Overflow", "ET WEB_CLIENT Google Chrome XSS (CVE-2017-5124)", "ET ACTIVEX Possible AOL ICQ ActiveX Control DownloadAgent Method Access Arbitrary File Download and Execute 2", "ET ACTIVEX Quest InTrust Annotation Objects ActiveX Control Add Access Potential Remote Code Execution 2", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 4", "ET EXPLOIT D-Link DSL-2750B - OS Command Injection", "ET WEB_CLIENT [TW] WEBDAV Requesting Startup Dir", "ET EXPLOIT php script double base64 encoded Remote Code Execution 6", "GPL SQL dbms_repcat.alter_master_repobject buffer overflow attempt", "ET WEB_SPECIFIC_APPS Cisco Adaptive Security Appliance WebVPN Cross Site Scripting Attempt", "GPL SQL dbms_repcat.send_and_compare_old_values buffer overflow attempt", "ET ACTIVEX Quest Explain Plan Display ActiveX Control SaveToFile Insecure Method Access 2", "ET ACTIVEX Possible Kazaa Altnet Download Manager ActiveX Control Install Method Access Buffer Overflow", "GPL SQL dbms_repcat.purge_flavor_definition buffer overflow attempt", "ET EXPLOIT Apache Struts 2 REST Plugin (ProcessBuilder)", "ET ACTIVEX SoftArtisans XFile FileManager ActiveX stack overfow Function call Attempt", "ET EXPLOIT MS-SQL SQL Injection closing string plus line comment", "ET EXPLOIT Possible Belkin N600DB Wireless Router Request Forgery Attempt", "ET WEB_SPECIFIC_APPS Geutebrueck re_porter 16 - Cross-Site Scripting 5", "ET SCADA PcVue Activex Control Insecure method (GetExtendedColor)", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Crontab", "GPL SQL dbms_repcat.purge_statistics buffer overflow attempt", "ET EXPLOIT xp_enumdsn access", "ET ACTIVEX Possible Symantec AppStream LaunchObj ActiveX Control Arbitrary File Download and Execute", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (GET conf.bin)", "ET WEB_SPECIFIC_APPS SaschArt SasCam Webcam Server ActiveX Buffer Overflow Function Call", "ET WEB_SERVER Aribitrary File Upload Vulnerability in WP Mobile Detector", "GPL SQL dbms_repcat.execute_ddl buffer overflow attempt", "ET ACTIVEX SoftArtisans XFile FileManager ActiveX DeleteFile method stack overflow Attempt", "ET ACTIVEX Possible CA BrightStor ARCserve Backup ActiveX AddColumn Method Access Buffer Overflow 2", "ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Construct Hex Encode", "GPL SQL dbms_repcat.drop_site_priority_site buffer overflow attempt", "ET WEB_SPECIFIC_APPS Fortify Software Security Center XML External Entity Injection 3", "GPL SQL dbms_offline_og.begin_load buffer overflow attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Start the Microhard Sh (msshc) service", "ET WEB_SPECIFIC_APPS Oracle WebLogic RCE Shell Inbound M2 (CVE-2020-14882)", "GPL SQL dbms_repcat.validate_for_local_flavor buffer overflow attempt", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command

	Inbound via HTTP M1", "ET EXPLOIT Apache Struts 2 REST Plugin (Runtime.Exec)", "ET ACTIVEX Possible Ecava IntegraXor save method Remote ActiveX Buffer Overflow", "GPL SQL dbms_repcat.drop_mview_repgroup buffer overflow attempt", "ET ACTIVEX Multiple Altiris Products AeXNSConsoleUtilities.dll ActiveX Control BrowseAndSaveFile Method Buffer Overflow Attempt Function Call", "ET WEB_CLIENT Oracle Java 6 Object Tag launchjnlp docbase Parameters Buffer Overflow", "ET WEB_CLIENT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Percent Hex Encode", "ET WEB_CLIENT GENERIC Possible IE Memory Corruption CollectGarbage with DOM Reset", "ET EXPLOIT Possible CVE-2015-7547 Large Response to A/AAAA query", "GPL SQL dbms_repcat.unregister_snapshot_repgroup buffer overflow attempt", "ET ACTIVEX Possible HP ALM XGO.ocx ActiveX Control SetShapeNodeType method Remote Code Execution", "ET WEB_CLIENT Hostile Microsoft Rich Text File (RTF) with corrupted listoverride", "ET WEB_CLIENT Possible Internet Explorer VBscript failure to handle error case information disclosure obfuscated CVE-2014-6332", "GPL SQL sys.dbms_repcat_conf.add_priority_char buffer overflow attempt", "ET EXPLOIT JavaX Toolkit Posting Plugin-Detect Data", "ET SCADA PcVue Activex Control Insecure method (DeletePage)", "GPL SQL time_zone buffer overflow attempt", "ET WEB_SPECIFIC_APPS Possible Jenkins CLI RCE (CVE-2017-1000353)", "ET EXPLOIT Ghostscript illegal delete bindnow attempt", "GPL SQL dbms_repcat.add_priority_date buffer overflow attempt", "ET EXPLOIT bin bash base64 encoded Remote Code Execution 2", "GPL SQL mdsys.md2.sdo_code_size buffer overflow attempt", "ET WEB_SERVER Possible WebLogic Operator Login With Default Creds", "ET WEB_CLIENT DLL or EXE File From Possible WebDAV Share Possible DLL Preloading Exploit Attempt", "ET ACTIVEX Possible NET-i viewer ActiveX Control ConnectDDNS Method Access Code Execution Vulnerability 2", "ET ACTIVEX Possible Chilkat Software FTP2 ActiveX Component GetFile Access Remote Code Execution 2", "ET WEB_CLIENT VLC Media Player smb URI Handling Remote Buffer Overflow Attempt", "ET ACTIVEX Oracle AutoVue Activex Insecure method (SaveViewStateToFile) Format String Function Call", "ET ACTIVEX Magneto ICMP ActiveX ICMPSendEchoRequest Remote Code Execution Attempt", "ET ACTIVEX Possible HP Easy Printer Care XMLCacheMgr Class ActiveX Control Remote Code Execution 2", "GPL SQL dbms_repcat.comment_on_unique_resolution buffer overflow attempt", "GPL SQL dbms_repcat.generate_replication_trigger buffer overflow attempt", "ET EXPLOIT php script double base64 encoded Remote Code Execution 8", "ET ACTIVEX TRENDnet TV-IP121WN UltraMJCam ActiveX Control OpenFileDlg Access Potential Remote Stack Buffer Overflow", "ET WEB_SERVER Possible WebLogic Monitor Login With Default Creds", "ET WEB_CLIENT Possible Embedded NTLM Hash Theft Code", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 UTF-8 Inbound Web Servers Likely Command Execution 5", "ET EXPLOIT Metasploit js_property_spray sprayHeap", "GPL SQL dbms_repcat.repcat_import_check buffer overflow attempt", "ET WEB_CLIENT Microsoft Rich Text File download - SET", "ET EXPLOIT Metasploit mstime_malloc no-spray", "ET ACTIVEX 2X Client for RDP ClientSystem Class ActiveX Control InstallClient Download and Execute", "ET WEB_SERVER SQL sp_password attempt", "ET SCADA Sunway ForceControl Activex Control Remote Code Execution Vulnerability 2", "ET ACTIVEX Possible WebEx UCF atucfobj.dll ActiveX NewObject Method Buffer Overflow", "ET ACTIVEX Novell iPrint ActiveX GetDriverSettings Remote Code Execution Attempt", "GPL SQL drop_mview_repgroup ordered gowner/gname buffer overflow attempt", "ET INFO DoSWF Flash Encryption Banner", "ET ACTIVEX Cisco AnyConnect VPN Secure Mobility Client Cisco.AnyConnect.VPNWeb.1 Arbitrary Program Execution Attempt", "GPL SQL dbms_offline_og.end_instantiation buffer overflow attempt", "ET EXPLOIT Metasploit Various Java Exploit Common Class name", "ET ATTACK_RESPONSE WSO - WebShell Activity - WSO Title", "ET EXPLOIT Tomcat File Upload Payload Request (CVE-2017-12615)", "ET WEB_CLIENT Spectre Kernel Memory Leakage JavaScript (POC Based)", "ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ImportSettings Function Call Attempt", "GPL SQL dbms_repcat.comment_on_priority_group buffer overflow attempt", "ET WEB_CLIENT BeEF Style Request (GET)", "GPL SQL sa login failed", "ET WEB_SERVER WebShell - JSP

	RAT", "ET ACTIVEX CygniCon CyViewer ActiveX Control SaveData Insecure Method Vulnerability", "ET WEB_CLIENT Microsoft IE CSS Clip Attribute Memory Corruption (POC SPECIFIC)", "GPL SQL dbms_repcat.define_site_priority buffer overflow attempt", "ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed FWS", "ET EXPLOIT Possible 2015-7547 PoC Server Response", "GPL NETBIOS xp_reg* registry access", "GPL SQL dbms_repcat.rename_shadow_column_group buffer overflow attempt", "GPL SQL dbms_repcat.register_statistics buffer overflow attempt", "ET EXPLOIT Nagios XI Adding Administrative User", "ET WEB_SPECIFIC_APPS Fortify Software Security Center XML External Entity Injection 4", "GPL SQL sys.dbms_repcat_conf.drop_priority_varchar2 buffer overflow attempt", "ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 1", "ET ACTIVEX IDrive Online Backup ActiveX control SaveToFile Insecure Method", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 5", "ET ACTIVEX Chilkat Crypt ActiveX Control SaveDecrypted Insecure Method Vulnerability", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct HEXCS", "ET EXPLOIT Possible Realtek SDK - formWlSiteSurvey Stack Buffer Overflow Inbound (CVE-2021-35393)", "ET WEB_CLIENT Possible CVE-2014-4113 Exploit Download with Hurricane Panda IOC", "GPL SQL dbms_repcat_rgt.instantiate_online buffer overflow attempt", "ET WEB_CLIENT Microsoft Visio 2003 mfc71enu.dll DLL Loading Arbitrary Code Execution Attempt", "ET WEB_SERVER WebShell - PHPShell - Haxplorer URI", "ET ACTIVEX Possible Aloaha PDF Crypter activex SaveToFile method arbitrary file overwrite", "GPL SQL dbms_repcat.drop_priority_char buffer overflow attempt", "ET EXPLOIT Possible Internet Explorer CVE-2014-6332 Common Construct URLENCODE", "GPL SQL dbms_repcat.add_column_group_to_flavor buffer overflow attempt", "ET EXPLOIT VMware NSX SD-WAN Command Injection", "GPL SQL dbms_repcat.drop_mview_repobject buffer overflow attempt", "ET ACTIVEX Tracker Software pdfSaver ActiveX InitFromRegistry Method Access Potential Buffer Overflow", "ET ACTIVEX Possible Crystal Reports Viewer Activex Control ServerResourceVersion Insecure Method Access 2", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Add Port Forwarding)", "GPL SQL dbms_repcat.comment_on_update_resolution buffer overflow attempt", "ET EXPLOIT xp_readerrorlogs access", "ET ACTIVEX Ubisoft CoGSManager ActiveX RunCore method Buffer Overflow Vulnerability", "ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 1", "ET WEB_SPECIFIC_APPS Wordpress Arbitrary File Deletion 1", "ET ACTIVEX Possible CA eTrust PestPatrol ActiveX Control Buffer Overflow", "GPL SQL dbms_repcat.create_snapshot_repgroup buffer overflow attempt", "ET WEB_CLIENT RealPlayer FLV Parsing Integer Overflow Attempt", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdExport Method Access Buffer Overflow 2", "ET EXPLOIT Geutebruck Remote Command Execution", "ET ACTIVEX Possible SkinCrafter ActiveX Control InitLicenKeys Method Access Buffer Overflow", "ET WEB_CLIENT Microsoft Windows MPEG Layer-3 Audio Decoder Buffer Overflow", "GPL SQL dbms_repcat.abort_flavor_definition buffer overflow attempt", "ET WEB_CLIENT BeEF Framework Comment In Response", "ET WEB_CLIENT Opera Window.Open document.cloneNode Null Pointer Deference Attempt", "ET EXPLOIT Nagios XI Remote Code Execution 3", "GPL SQL mdsys.sdo_admin.sdo_code_size buffer overflow attempt", "ET EXPLOIT php script base64 encoded Remote Code Execution 2", "ET WEB_CLIENT Internet Explorer Memory Corruption Vulnerability (CVE-2015-2444)", "GPL SQL dbms_repcat.suspend_master_activity buffer overflow attempt", "GPL SQL rectifier_diff ordered sname1 buffer overflow attempt", "ET EXPLOIT Oracle WebLogic JNDI Injection RCE Attempt (CVE-2021-2109)", "ET WEB_SPECIFIC_APPS ManageEngine Exchange Reporter Plus Remote Code Execution", "ET EXPLOIT TrendMicro node.js HTTP RCE Exploit Inbound (showSB)", "GPL SQL dbms_offline_og.end_load buffer overflow attempt", "ET MALWARE Possible Backdoor.Adwind Download", "ET EXPLOIT Exim Internet Mailer Remote Code Execution", "ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 3", "ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35395)", "ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361", "ET ACTIVEX Possible WinZip

	FileView (WZFILEVIEW.FileViewCtrl.61) ActiveX Buffer Overflow 2", "ET EXPLOIT Redfish API User Enumeration Attempt (CVE-2022-2827)", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard Low Port)", "GPL SQL dbms_repcat.publish_flavor_definition buffer overflow attempt", "ET SCADA PcVue Activex Control Insecure method (SaveObject)", "GPL SQL dbms_repcat.comment_on_delete_resolution buffer overflow attempt", "ET EXPLOIT Apache Struts Possible OGNL Java ProcessBuilder in client body", "ET WEB_SPECIFIC_APPS WordPress Plugin Advanced Custom Fields Remote File Inclusion", "ET WEB_CLIENT Adobe Acrobat PDF Reader use after free JavaScript engine (CVE-2017-16393)", "ET EXPLOIT D-LINK DIR-615 Cross-Site Request Forgery (CVE-2017-7398)", "ET EXPLOIT Apache Struts 2 REST Plugin XStream RCE (Runtime.Exec)", "ET WEB_SPECIFIC_APPS Elektronischer Leitz-Ordner 10 - SQL Injection", "ET WEB_SPECIFIC_APPS Airties AIR5444TT - Cross-Site Scripting", "GPL SQL sp_start_job - program execution", "ET WEB_CLIENT Microsoft Excel file download - SET 1", "GPL SQL dbms_repcat.drop_priority_nchar buffer overflow attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Auto-enable the Microhard Sh (msshc) service", "GPL SQL dbms_repcat.compare_old_values buffer overflow attempt", "ET EXPLOIT Apache Struts Possible OGNL AllowStaticMethodAccess in URI", "GPL SQL dbms_repcat.add_grouped_column buffer overflow attempt", "ET WEB_SPECIFIC_APPS MicroFocus Secure Messaging Gateway Remote Code Execution", "ET EXPLOIT PHP-CGI Query String Parameter Vuln Inbound (CVE-2012-2311)", "GPL SQL dbms_repcat_instantiate.instantiate_online buffer overflow attempt", "ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 3", "ET ACTIVEX TeeChart Professional ActiveX Control integer overflow Vulnerability 4", "ET EXPLOIT Possible Zoom Client Auto-Join (CVE-2019-13450)", "GPL SQL sys.dbms_repcat_conf.drop_priority_raw buffer overflow attempt", "GPL SQL dbms_repcat.add_priority_nchar buffer overflow attempt", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (DMZ enable and Disable)", "GPL SQL dbms_repcat.drop_priority_varchar2 buffer overflow attempt", "ET EXPLOIT HID VertX and Edge door controllers command_blink_on Remote Command Execution", "ET EXPLOIT Atlassian Bitbucket CVE-2022-36804 Exploit Attempt", "ET ACTIVEX Tom Sawyer Possible Memory Corruption Attempt Format String Function Call", "GPL SQL dbms_repcat.drop_update_resolution buffer overflow attempt", "ET EXPLOIT HP Smart Storage Administrator Remote Command Injection", "GPL SQL dbms_repcat_sna_utl.create_snapshot_repgroup buffer overflow attempt", "GPL SQL sp_delete_alert log file deletion", "GPL SQL dbms_repcat.validate_flavor_definition buffer overflow attempt", "ET EXPLOIT HP Enterprise VAN SDN Controller Install Backdoor", "ET ACTIVEX Advanced File Vault Activex Heap Spray Attempt", "ET WEB_CLIENT Android Webkit removeChild Use-After-Free Remote Code Execution Attempt", "ET WEB_SPECIFIC_APPS ELF file magic plain Inbound Web Servers Likely Command Execution 12", "ET WEB_CLIENT BeEF HTTP Get Outbound", "ET MOBILE_MALWARE Possible Android CVE-2014-6041", "ET NETBIOS Microsoft Windows SMB Client Race Condition Remote Code Execution", "ET WEB_SPECIFIC_APPS GitList Argument Injection", "ET EXPLOIT Possible WINS Server Remote Memory Corruption Vulnerability", "GPL SQL snapshot.end_load ordered gname buffer overflow attempt", "ET EXPLOIT MySQL Server for Windows Remote SYSTEM Level Exploit (Stuxnet Techique DUMP INTO executable)", "ET ACTIVEX Possible NVIDIA Install Application ActiveX Control AddPackages Unicode Buffer Overflow", "ET SCADA ICONICS WebHMI ActiveX Stack Overflow", "ET ACTIVEX LEADTOOLS Imaging LEADSmtp ActiveX SaveMessage Method Vulnerability", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 1", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 Hex Escape Inbound Web Servers Likely Command Execution 9", "ET EXPLOIT IBM WebSphere - RCE Java Deserialization", "GPL SQL dbms_repcat.generate_mview_support buffer overflow attempt", "GPL SQL from_tz buffer overflow attempt", "GPL SQL dbms_offline_snapshot.begin_load buffer overflow attempt", "ET WEB_SPECIFIC_APPS ELF file magic encoded Base64 Hex Escape Inbound Web Servers Likely Command

	Execution 10", "ET ACTIVEX Possible AdminStudio Activex Control LaunchProcess Method Access Arbitrary Code Execution", "ET WEB_SERVER Generic PHP Remote File Include", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdImport Method Access Buffer Overflow 2", "ET EXPLOIT Ghostscript illegal delete bindnow attempt (SMTP)", "GPL SQL unregister_user_repgroup ordered privilege_type buffer overflow attempt", "ET ACTIVEX Avaya CallPilot Unified Messaging ActiveX InstallFrom Method Access Attempt", "ET WEB_SERVER Possible Wordpress Super Cache Plugin PHP Injection mclude", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command Inbound via HTTP M3", "ET ATTACK_RESPONSE Windows SCM DLL Hijack Command Inbound via HTTP M2", "ET EXPLOIT SUSPICIOUS DTLS 1.0 Fragmented Client Hello Possible CVE-2014-0195", "GPL SQL sys.dbms_repcat_fla_mas.publish_flavor_definition buffer overflow attempt", "ET WEB_SPECIFIC_APPS Fortify Software Security Center XML External Entity Injection 1", "ET ACTIVEX Possible Dell IT Assistant detectIESettingsForITA.ocx ActiveX Control readRegVal Remote Registry Dump Vulnerability", "ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns", "GPL SQL dbms_repcat.begin_flavor_definition buffer overflow attempt", "ET WEB_SERVER WSO WebShell Activity POST structure 2", "ET EXPLOIT Nanopool Claymore Dual Miner Remote Code Execution Linux", "ET SCADA CitectSCADA ODBC Overflow Attempt", "ET WEB_SERVER Possible Wordpress Super Cache Plugin PHP Injection mfunc", "ET FTP Possible FTP Daemon Username DELETE FROM SQL Injection Attempt", "ET EXPLOIT Possible 2015-7547 Malformed Server response", "ET EXPLOIT CVE-2018-8174 Common Construct B64 M2", "ET WEB_SERVER Possible Apache Struts OGNL in Dynamic Action", "GPL SQL dbms_repcat.refresh_snapshot_repgroup buffer overflow attempt", "ET WEB_SERVER Possible Wordpress Super Cache Plugin PHP Injection dynamic-cached-content", "ET ACTIVEX Possible IBM Lotus Quickr for Domino ActiveX control Attachment_Times Method Access buffer overflow Attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Service start", "ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed ZWS", "ET INFO NetSSH SSH Version String Hardcoded in Metasploit", "ET WEB_SERVER Image Content-Type with Obfuscated PHP (Seen with C99 Shell)", "ET EXPLOIT CVE-2016-0189 Common Construct M2", "ET EXPLOIT HP Enterprise VAN SDN Controller Exec Backdoor", "ET WEB_CLIENT Type Confusion Microsoft Edge (CVE-2017-11873)", "GPL SQL numtoyminterval buffer overflow attempt", "ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 5", "ET EXPLOIT Ghostscript setpattern type confusion attempt", "GPL SQL dbms_repcat.do_deferred_repcat_admin buffer overflow attempt", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Change Admin Passwd", "GPL SQL dbms_repcat.drop_master_repgroup buffer overflow attempt", "GPL SQL dbms_repcat.generate_replication_support buffer overflow attempt", "ET ACTIVEX Possible LEADTOOLS ActiveX Raster Twain AppName Method Access Buffer Overflow 2", "ET ACTIVEX Possible Edraw Diagram Component 5 ActiveX LicenseName Access Potential buffer overflow DOS 2", "ET WEB_CLIENT PowerShell call in script 2", "ET WEB_SPECIFIC_APPS GitStack - Unsanitized Argument Remote Code Execution", "GPL SQL dbms_repcat.switch_mview_master buffer overflow attempt", "ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 6", "ET WEB_CLIENT Possible Chrome WebEx Extension RCE Attempt", "ET EXPLOIT Possible CVE-2016-0777 Server Advertises Suspicious Roaming Support", "ET EXPLOIT Possible CVE-2016-10033 PHPMailer RCE Attempt", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdExport Method Access Buffer Overflow", "ET ACTIVEX Potential ThreeDify Designer ActiveX Control cmdSave Method Access Buffer Overflow 2", "ET EXPLOIT CVE-2018-8174 Common Construct B64 M3", "ET EXPLOIT Apache Struts 2 REST Plugin ysoserial Usage (B64) 3", "GPL SQL grant_surrogate_repcat ordered userid buffer overflow attempt", "ET WEB_CLIENT Adobe Flash Player Button Remote Code Execution Attempt", "ET SCADA PcVue Activex Control Insecure method (AddPage)", "ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - Shell", "ET ACTIVEX Possible Oracle AutoVue ActiveX SetMarkupMode Method Access Remote Code Execution", "ET EXPLOIT Apache Struts 2 REST Plugin ysoserial Usage (B64) 1", "GPL SQL dbms_repcat.drop_priority_raw buffer overflow attempt", "ET EXPLOIT

	Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)", "GPL SQL xp_cmdshell program execution", "GPL SQL dbms_repcat_rgt.check_ddl_text buffer overflow attempt", "ET ACTIVEX Ubisoft CoGSManager ActiveX Initialize method Buffer Overflow Vulnerability", "GPL SQL add_grouped_column ordered sname/oname buffer overflow attempt", "ET EXPLOIT Possible dlink-DSL2640B DNS Change Attempt", "ET WEB_CLIENT IE Double Free (CVE-2018-8460)", "GPL SQL alter_mview_propagation ordered gname buffer overflow attempt", "ET ACTIVEX Possible WebEx UCF atucfobj.dll ActiveX NewObject Method Buffer Overflow 2", "ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M2", "GPL NETBIOS xp_reg* - registry access", "ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - STSC", "ET WEB_SERVER Cisco BBSM Captive Portal AccesCodeStart.asp Cross-Site Scripting Attempt", "ET WEB_SERVER Joomla Upload File Filter Bypass", "ET WEB_SPECIFIC_APPS Drupal RCE (CVE-2018-7602)", "ET EXPLOIT SAP NetWeaver AS JAVA CRM - Log injection Remote Command Execution", "ET EXPLOIT ThinkPHP Attempted Bypass and Payload Retrieval", "ET WEB_SPECIFIC_APPS Apache CouchDB Remote Code Execution 4", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Add Root Htpasswd", "ET EXPLOIT Possible Firefox PDF.js Same-Origin-Bypass CVE-2015-4495 M1", "ET NETBIOS PolarisOffice Insecure Library Loading - SMB ASCII", "GPL SQL dbms_repcat.drop_columns_from_flavor buffer overflow attempt", "ET EXPLOIT TrendMicro node.js HTTP RCE Exploit Inbound (openUrlInDefaultBrowser)", "ET ACTIVEX Adobe browser document ActiveX DoS Function call Attempt", "GPL SQL shellcode attempt", "ET EXPLOIT Nanopool Claymore Dual Miner Remote Code Execution Windows", "GPL SQL comment_on_repobject ordered type buffer overflow attempt", "GPL SQL dbms_repcat.create_snapshot_repobject buffer overflow attempt", "ET ACTIVEX Easewe FTP OCX ActiveX Control EaseWeFtp.ocx Remote Code Execution Attempt", "ET EXPLOIT Apache Struts Possible OGNL Java Exec in client body"
Потенциально опасный трафик	"ET EXPLOIT Suspicious FTP RETR to .hta file possible exploit (CVE-2017-0199)", "ET INFO DYNAMIC_DNS Query to a *.mynetav .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lessmiths .com Domain", "ET INFO DYNAMIC_DNS Query to a *.syntereo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddns.name Domain", "ET INFO DYNAMIC_DNS Query to a *.thomastech .net Domain", "ET INFO DYNAMIC_DNS Query to a *.anal-slavery .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.privatizehealthinsurance .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zeleznock .net Domain", "ET POLICY DNS Query to DynDNS Domain *.servepics .com", "ET POLICY Vulnerable Java Version 16.0.x Detected", "ET INFO DYNAMIC_DNS Query to a *.is-a-painter .com Domain", "ET INFO DYNAMIC_DNS Query to a *.autoprin .com Domain", "ET INFO DYNAMIC_DNS Query to a *.normaweese .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.darriondemelo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.linkin .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fridg .com Domain", "ET INFO DYNAMIC_DNS Query to a *.smelly .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.deaftone.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.argusdenshi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.v6 .rocks Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.what2no .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.groks-the .info Domain", "ET INFO DYNAMIC_DNS Query to a *.simplecharity .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ntdll .top Domain", "ET HUNTING Observed Lets Encrypt Certificate - Possible COVID-19 Related M1", "ET INFO DYNAMIC_DNS Query to a *.be .sexy Domain", "ET INFO DYNAMIC_DNS Query to a *.shit .vc Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsdyn .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sourcekeeper .com Domain", "ET POLICY DNS Query to .onion proxy Domain (vtorchike.com)", "ET INFO DYNAMIC_DNS Query to a *.is-a-nascarfan .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.pirate)", "ET INFO ET INFO URL Shortening Service Domain in DNS Lookup (s59 .site)", "ET INFO DYNAMIC_DNS Query to a *.kyrgyzstan .kg Domain", "ET HUNTING Request for .bin with BITS/ User-Agent", "ET INFO DYNAMIC_DNS HTTP Request to a *.jnrcs .org Domain", "ET POLICY Apache HTTP Server 2.4.49 Observed - Vulnerable to CVE-2021-

	41773", "ET INFO Lockbit Ransomware Related Domain in DNS Lookup (decoding .at)", "ET INFO DYNAMIC_DNS HTTP Request to a *.servemp3 .com Domain", "ET INFO DYNAMIC_DNS Query to a *.pedie .info Domain", "ET POLICY DNS Query to DynDNS Domain *.ddnsking .com", "ET INFO DYNAMIC_DNS Query to a *.ideaustry .sg Domain", "ET INFO DYNAMIC_DNS Query to a *.dyn .ch Domain", "ET INFO Onion/TOR Successful Proxy Request Response (Inbound)", "ET INFO DYNAMIC_DNS HTTP Request to a *.tien-shan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynv6 .net Domain", "ET INFO HTTP Request to a *.cz.tf domain", "ET POLICY SMB NT Create AndX Request For a .sys File - Possible Lateral Movement", "ET POLICY DNS Query to DynDNS Domain *.ddns .net", "ET HUNTING SUSPICIOUS Reassigned Eval Function 3", "ET INFO DYNAMIC_DNS Query to a *.suroot.com Domain", "ET INFO DYNAMIC_DNS Query to a *.chesta .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bellywings .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.robinhud .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bridge-club-hannover .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.g33k .com .ve Domain", "ET INFO DYNAMIC_DNS Query to a *.merseine .org Domain", "ET INFO DYNAMIC_DNS Query to a *.happyrobotics .com Domain", "ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .com filename inside", "ET INFO DYNAMIC_DNS Query to a *.webhop .info Domain", "ET HUNTING Request for EXE via WinHTTP M1", "ET INFO DYNAMIC_DNS Query to a *.is-a-therapist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.scay .net Domain", "ET INFO DYNAMIC_DNS Query to a *.hobby-site .org Domain", "ET INFO DYNAMIC_DNS Query to a *.barrell-of-knowledge .info Domain", "ET INFO Shared File Retrieved (roamresearch .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.embeddedonline .org Domain", "ET INFO DYNAMIC_DNS Query to a *.parquecidades-eim .pt Domain", "ET INFO DYNAMIC_DNS Query to a *.darriondemelo .com Domain", "ET MALWARE ETag HTTP Header Observed at CNCERT Sinkhole", "ET INFO DYNAMIC_DNS HTTP Request to a *.est-mon-blogueur .com Domain", "ET INFO DNS Query for a Suspicious Malware Related Numerical .in Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynalias .net Domain", "ET HUNTING Suspicious svchost.exe in URI - Possible Process Dump/Trojan Download", "ET INFO DYNAMIC_DNS HTTP Request to a *.hitremixes .com Domain", "ET INFO DYNAMIC_DNS Query to a *.stoupin .ru Domain", "ET POLICY SMB NT Create AndX Request For a .bat File", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Hex Encoded Class file", "ET USER_AGENTS Observed Suspicious UA (xPCAP)", "ET INFO Obfuscated Split String (Single Q) 4", "ET INFO DYNAMIC_DNS Query to a *.robot-armies .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torsanctions.com)", "ET SCAN OpenVASVT RCE Test String in HTTP Request Inbound", "ET INFO DYNAMIC_DNS Query to a *.blinklab .com Domain", "ET INFO DYNAMIC_DNS Query to a *.onapon .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homeunix .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webs .vc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.moabphoto .com Domain", "ET INFO DYNAMIC_DNS Query to a *.0x .no Domain", "ET INFO Query for Suspicious .xe.cx Domain", "ET INFO DYNAMIC_DNS Query to a *.gotdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jlengineering .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.anpmech .com Domain", "ET INFO DYNAMIC_DNS Query to a *.igotwasted .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.it-share .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.efrati .org Domain", "ET DNS Query for .cc TLD", "ET INFO DYNAMIC_DNS Query to a *.themoosebarn .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zaibar .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.artisnotcrime .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bgdsupport .com Domain", "ET POLICY DNS Query to DynDNS Domain *.mypsx .net", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-financialadvisor .com Domain", "ET PHISHING Browser Plugin Detect - Observed in Apple Phishing", "ET INFO DYNAMIC_DNS Query to a *.handfolding .com Domain", "ET INFO DYNAMIC_DNS Query to a *.larakaras .com Domain", "ET INFO Query for Suspicious .eu.tf Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iugaming .com Domain", "ET INFO DYNAMIC_DNS Query to a *.etowns.net Domain",

	"ET INFO DYNAMIC_DNS HTTP Request to a *.photogenic .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webhop .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.sosfuvos .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-blogger .com Domain", "ET INFO DYNAMIC_DNS Query to a *.operationbim .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.anime-stars .com Domain", "ET WEB_CLIENT Possible Malvertising FlashPost - POST to *.stats", "ET INFO Observed Commonly Abused Domain (blogattach .naver .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.garmanage .com Domain", "ET INFO HTTP Request to Suspicious *.okinawa Domain", "ET INFO DYNAMIC_DNS Query to a *.thompent .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bine .me Domain", "ET INFO DYNAMIC_DNS Query to a *.civvic .ro Domain", "ET INFO DYNAMIC_DNS Query to a *.selfip .net Domain", "ET INFO DYNAMIC_DNS Query to a *.cashit .info Domain", "ET INFO DYNAMIC_DNS Query to a *.game-server .cc Domain", "ET WEB_CLIENT Hex Obfuscation of unescape % Encoding", "ET SCAN Open-Proxy ScannerBot (webcollage-UA)", "ET INFO DYNAMIC_DNS Query to a *.vxe6 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.swds .com .au Domain", "ET INFO DYNAMIC_DNS Query to a *.geobattery .com Domain", "ET INFO DYNAMIC_DNS Query to a *.saucedchicago .com Domain", "ET INFO DYNAMIC_DNS Query to a *.for-better .biz Domain", "ET WEB_CLIENT Possible %u UTF-8 Encoded Iframe Tag", "ET INFO DYNAMIC_DNS HTTP Request to a *.glengall .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsapi .info Domain", "ET INFO DYNAMIC_DNS Query to a *.patelmortgage .com Domain", "ET INFO Inveigh Proxy Powershell Script Retrieval (Inbound)", "ET INFO DYNAMIC_DNS Query to a *.anime-stars .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing glassfish external statistics impl", "ET HUNTING File Sharing Related Domain in DNS Lookup (download .mediafire .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.authorizeddns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jaytex .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.nullexistence .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cechire .com Domain", "ET INFO DYNAMIC_DNS Query to a *.robonauts .net Domain", "ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .com filename inside", "ET INFO DYNAMIC_DNS HTTP Request to a *.cylone .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynserv .org Domain", "ET INFO DYNAMIC_DNS Query to *lookin.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.vicinanza .org Domain", "ET HUNTING Downloaded Powershell Script Detects AV Product", "ET INFO DYNAMIC_DNS Query to a *.dynalias .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.x443 .pw Domain", "ET INFO DYNAMIC_DNS Query to a *.antiphone .net Domain", "ET INFO Observed Public Cloud Domain (cld .pt in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.vicinanza .org Domain", "ET INFO DYNAMIC_DNS Query to a *.effers.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.voyez .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myeffect .net Domain", "ET INFO DYNAMIC_DNS Query to a *.zipper-maker .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dontexist .com Domain", "ET POLICY HTTP Request to a *.tk domain", "ET USER_AGENTS Suspicious User-Agent (VB OpenUrl)", "ET INFO Unix/Linux Processhider Source Being Downloaded", "ET INFO DYNAMIC_DNS Query to a *.seburn .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-knight .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nj .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dubya .us Domain", "ET INFO DYNAMIC_DNS Query to a *.barbaforte .org Domain", "ET INFO Observed Abused Redirect Service SSL Cert (svc .dynamics .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-very-nice .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.now-dns .top Domain", "ET INFO DYNAMIC_DNS Query to a *.koellreutter .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pushitlive .net Domain", "ET INFO DYNAMIC_DNS Query to a *.from-wa .com Domain", "ET DNS Query to a *.top domain - Likely Hostile", "ET EXPLOIT Malformed HeartBeat Request method 2", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-entertainer .com Domain", "ET HUNTING Observed POST to xsph .ru Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oast .pro)", "ET INFO DYNAMIC_DNS HTTP Request to a *.southern .com .my

	Domain", "ET INFO DYNAMIC_DNS Query to a *.tallison .com Domain", "ET INFO Query for Suspicious .edu.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.groups .id Domain", "ET INFO DYNAMIC_DNS Query to a *.freetruthordare .com Domain", "ET INFO DYNAMIC_DNS Query to a *.intercop .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.propertyshots .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.authorizeddns .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pegle .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.youramys .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-bruinsfan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.bureaua .net Domain", "ET INFO DYNAMIC_DNS Query to a *.americanunfinished .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ix .tc Domain", "ET INFO DYNAMIC_DNS Query to a *.servebbs .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (nZva2UtQ29tbW) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.heroinewarrior .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nm .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.17ping .cn Domain", "ET INFO DYNAMIC_DNS Query to a *.drm .hk Domain", "ET INFO Observed DNS Query to DDNS Domain .dns1 .us", "ET INFO DYNAMIC_DNS Query to a *.trickip .org Domain", "ET INFO DYNAMIC_DNS Query to a *.macrofox .org Domain", "ET INFO DYNAMIC_DNS Query to a *.castleman .net Domain", "ET INFO DYNAMIC_DNS Query to a *.knowsitall .info Domain", "ET INFO DYNAMIC_DNS Query to a *.lilyspadd .com Domain", "ET INFO DYNAMIC_DNS Query to a *.32-b .it Domain", "ET INFO DYNAMIC_DNS Query to a *.epicgamer .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.teamradicus .com Domain", "ET JA3 HASH - Possible Cobalt Strike Server", "ET INFO SUSPICIOUS Java Request to ChangeIP Dynamic DNS Domain", "ET INFO DYNAMIC_DNS Query to a *.ivi .pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.x24hr .com Domain", "ET INFO DYNAMIC_DNS Query to a *.peeinthesnow .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.koellreutter .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.b0ne.com Domain", "ET INFO DYNAMIC_DNS Query to a *.it-share .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.scrapper-site .net Domain", "ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .scr filename inside", "ET INFO External File Sharing Service Domain (api .anonfile .com in TLS SNI)", "ET INFO Noction IRP Probe", "ET INFO DYNAMIC_DNS HTTP Request to a *.cloudbusinessportal .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-financialadvisor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-me .org Domain", "ET USER_AGENTS Observed Suspicious UA (Mozilla 6.0)", "ET INFO DYNAMIC_DNS Query to a *.icemail .me .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.ftpaccess .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jkub .com Domain", "ET INFO DYNAMIC_DNS Query to a *.vhfdental .com Domain", "ET INFO DYNAMIC_DNS Query to a *.pii .at Domain", "ET POLICY Powershell Command With Hidden Window Argument Over SMB - Likely Lateral Movement", "ET WEB_CLIENT Obfuscated Javascript // ptth (escaped)", "ET INFO DYNAMIC_DNS HTTP Request to a *.swhill .co .uk Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (requestbin .net)", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (Zva2UtUmVzdE1ld) in DNS TXT Reponse", "ET ADWARE_PUP Socelars Related Domain in DNS Lookup", "ET INFO DYNAMIC_DNS HTTP Request to a *.requitas .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.duta .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.btarena .com Domain", "ET INFO DYNAMIC_DNS Query to a *.alfa145 .com Domain", "ET INFO DYNAMIC_DNS Query to a *.puffballofevil .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.effers.com Domain", "ET INFO Minimal HTTP GET Request to cl .ly", "ET INFO DYNAMIC_DNS HTTP Request to a *.ugego .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.office-on-the .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.internet-slackers .us Domain", "ET INFO DYNAMIC_DNS Query to a *.partybag .com Domain", "ET INFO DYNAMIC_DNS Query to a *.x3mfly .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.battlecore .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.sellsyourhome .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.suroot.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.jpleventos .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.scrapitsoftware .com Domain", "ET HUNTING Inbound Powershell Creating .hta File", "ET INFO DYNAMIC_DNS HTTP Request to a *.networkoutpost .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ntdll .top Domain", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncEnumPrinterDrivers", "ET INFO DYNAMIC_DNS HTTP Request to a *.misecure .com Domain", "ET HUNTING Generic IOT Downloader Malware in POST (Outbound)", "ET INFO DYNAMIC_DNS HTTP Request to a *.onedumb .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-very-nice .org Domain", "ET INFO DYNAMIC_DNS Query to a *.iiiii .info Domain", "ET INFO DYNAMIC_DNS Query to a *.x443 .pw Domain", "ET WEB_SERVER WebShell - Generic - c99shell based header", "ET INFO DYNAMIC_DNS Query to a *.jaytex .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.verbateam .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tinyrealm .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yiannamarie .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vankin .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kyrgyzstan .kg Domain", "ET DNS Excessive DNS Responses with 1 or more RR's (100+ in 10 seconds) to google.com.br possible Cache Poisoning Attempt", "ET INFO DYNAMIC_DNS Query to a *.privatedns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.oviivory .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ms .com Domain", "ET INFO DYNAMIC_DNS Query to a *.palvelin .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-patsfan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ame-life .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wo5m .net Domain", "ET INFO DYNAMIC_DNS Query to a *.hobby-site .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.d-n-s .org .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.theoceanforest .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sandmeiers .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.getmyip .com Domain", "ET MALWARE BluStealer Related Domain in DNS Lookup (premium12 .web-hosting .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.twilightparadox .com Domain", "ET INFO DYNAMIC_DNS Query to a *.barrel-of-knowledge .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-md .com Domain", "ET INFO DYNAMIC_DNS Query to a *.64-b .it Domain", "ET INFO Commonly Abused Domain Service Domain in DNS Lookup (temp .swtest .ru)", "ET INFO DYNAMIC_DNS Query to a *.homenode .ca Domain", "ET JA3 HASH - DeimosC2 Agent Activity (set)", "ET INFO DYNAMIC_DNS HTTP Request to a *.florafamily .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cissp .or .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.remotecam .nu Domain", "ET WEB_CLIENT Hex Obfuscation of document.write # Encoding", "ET INFO Obfuscated Split String (Single Q) 6", "ET INFO Observed DNS Query to .desi TLD", "ET INFO DYNAMIC_DNS HTTP Request to a *.2to1agri .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cityofgreen .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vpnx .nl Domain", "ET INFO DYNAMIC_DNS Query to a *.verbateam .net Domain", "ET INFO DYNAMIC_DNS Query to a *.automotive .si Domain", "ET INFO DYNAMIC_DNS Query to a *.mp3real .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.1337 .cx Domain", "ET INFO DYNAMIC_DNS Query to a *.mrgshrimp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.issmarterthanyou .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sly .io Domain", "ET INFO DYNAMIC_DNS Query to a *.montyconsulting .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dream .org .il Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.railpage .org Domain", "ET INFO 404 Response with Javascript Variable in Page", "ET INFO DYNAMIC_DNS HTTP Request to a *.linuxd1 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.widlund .fi Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.edns .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.artitech .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.leonardocastano .com .ar Domain", "ET POLICY Unserialized Java Payload via RMI Response", "ET INFO DYNAMIC_DNS Query to a *.ospachat .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-chef .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ciscofreak .com Domain", "ET POLICY Vulnerable Java Version 17.0.x Detected", "ET

	INFO DYNAMIC_DNS HTTP Request to a *.moneyhome .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.derekcturner .net Domain", "ET MALWARE ETag HTTP Header Observed at JPCERT Sinkhole", "ET INFO DYNAMIC_DNS Query to a *.gw .lt Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mysecondarydns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.chery .co .il Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hopto .me Domain", "ET INFO DYNAMIC_DNS Query to a *.kir22 .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ryanbauman .com Domain", "ET POLICY DNS Query to DynDNS Domain *.servegame .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.bgdsupport .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.biometrika .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.thenest .org Domain", "ET POLICY DNS Query to DynDNS Domain *.mymediapc .net", "ET INFO DYNAMIC_DNS Query to a *.svmblocker .com Domain", "ET MALWARE Java Download non Jar file", "ET INFO DYNAMIC_DNS HTTP Request to a *.isageek .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ripservers .com Domain", "ET INFO DYNAMIC_DNS Query to *bestdeals.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.proxydns .com Domain", "ET INFO Observed DNS Query to Dynamic DNS Service (giize .com)", "ET INFO DYNAMIC_DNS Query to a *.queerline .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bureaua .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lutzenheiser .com Domain", "ET INFO DYNAMIC_DNS Query to a *.inovasi .co .id Domain", "ET INFO DYNAMIC_DNS Query to a *.iz .rs Domain", "ET EXPLOIT TLS HeartBeat Request (Server Initiated) fb set", "ET INFO DYNAMIC_DNS HTTP Request to a *.mtrshop .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mascarenhas .inf .br Domain", "ET INFO DYNAMIC_DNS Query to a *.htpc .cl Domain", "ET ATTACK_RESPONSE Nishang Invoke-PowerShellTcp Shell Prompt Outbound", "ET INFO BrowseTor .onion Proxy Service SSL Cert", "ET INFO DYNAMIC_DNS Query to a *.fivepals .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ayasophia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myddns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.abc92 .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsapi .info Domain", "ET POLICY DNS Query to .onion proxy Domain (totortoweb.com)", "ET INFO DNS Query for Suspicious .icu Domain", "ET INFO DYNAMIC_DNS Query to a *.is-into-games .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.n4t .co Domain", "ET INFO DYNAMIC_DNS Query to a *.iamallama .com Domain", "ET INFO DYNAMIC_DNS Query to a *.qlbv .vn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-rockstar .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-la .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveminecraft .net Domain", "ET INFO Query for Suspicious .ca.tf Domain", "ET INFO ARM7 File Download Request from IP Address", "ET POLICY Serialized Java Object returned via LDAPv3 Response", "ET INFO DYNAMIC_DNS Query to a *.dontexist .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.truewan .co .za Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-linux-user .org Domain", "ET INFO HTTP Request to a *.dtdns.net domain", "ET INFO DYNAMIC_DNS Query to a *.ikoona .com Domain", "ET INFO DYNAMIC_DNS Query to a *.chatnook.com Domain", "ET INFO DYNAMIC_DNS Query to a *.astrabus .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.fin-tech .com Domain", "ET INFO DYNAMIC_DNS Query to a *.unix .id .lv Domain", "ET INFO DYNAMIC_DNS Query to a *.thehomeserver .net Domain", "ET INFO DYNAMIC_DNS Query to a *.spottt .com Domain", "ET INFO DYNAMIC_DNS Query to a *.eimertvink .nl Domain", "ET PHISHING Observed CloudFlare Interstitial Phishing Page", "ET HUNTING Suspicious Domain Request for Possible COVID-19 Domain M1", "ET INFO Observed URL Shortening Service Domain (gg-l .xyz in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.slumbo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lutzenheiser .com Domain", "ET INFO DYNAMIC_DNS Query to a *.splinteredlightbooks .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.birdriver .org Domain", "ET INFO DYNAMIC_DNS Query to a *.est-a-la-masion .com Domain", "ET INFO DYNAMIC_DNS Query to freemyip .com Domain", "ET INFO DYNAMIC_DNS Query to a *.rebol .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.https443 .net Domain", "ET POLICY DNS Query to .onion proxy Domain

	(door2tor.org)", "ET INFO DYNAMIC_DNS Query to a *.dx .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.salty72 .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.selfip .com Domain", "ET ATTACK_RESPONSE UTF8 base64 wide string /This Program/ in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.veriler .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torpaycash.com)", "ET INFO DYNAMIC_DNS Query to a *.webhop .org Domain", "ET HUNTING Request to .CF Domain with Minimal Headers", "ET INFO DYNAMIC_DNS HTTP Request to a *.serverpit .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.publicvm .com Domain", "ET POLICY Vulnerable Java Version 12.0.x Detected", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypsx .net Domain", "ET INFO DYNAMIC_DNS Query to a *.ubeagle .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.monitoryourinternet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.trickip .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-landscaper .com Domain", "ET INFO HTTP POST Request to Suspicious *.gq domain", "ET POLICY DNS Query to DynDNS Domain *.ditchyourip .com", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.parody)", "ET INFO HTTP Request to a *.nl.ai domain", "ET INFO DYNAMIC_DNS Query to a *.sexidude .com Domain", "ET HUNTING RedditSharp UA in POST (POST)", "ET INFO DYNAMIC_DNS HTTP Request to a *.yhkrubber .com .my Domain", "ET INFO DYNAMIC_DNS Query to a *.ugego .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.qhigh .com Domain", "ET INFO Query for Suspicious .de.tf Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.susangilmore .com Domain", "ET HUNTING Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)", "ET INFO DYNAMIC_DNS Query to a *.ind .st Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alexandravlad .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wiki .gd Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.punkassgamers .com Domain", "ET POLICY Seetrol Software Download (GET)", "ET INFO DYNAMIC_DNS HTTP Request to a *.klodia .ru Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (dm9rZS1XbWlNZXR) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.davidmcorn .com Domain", "ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.host2go .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.spacegas .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyn .mk Domain", "ET POLICY DNS Query to .onion proxy Domain (walterwtor.com)", "ET INFO DYNAMIC_DNS Query to a *.btbtrading .it Domain", "ET INFO DYNAMIC_DNS Query to a *.3vm .cl Domain", "ET INFO Self-Hosted Git Service Domain in DNS Lookup (gitea .com)", "ET INFO DYNAMIC_DNS Query to a *.addns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mymom .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.esmtp .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.uitgavepatroon .nl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsfor .me Domain", "ET POLICY DNS Query to DynDNS Domain *.hosthampster .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.yiamuc .com Domain", "ET NETBIOS DCERPC DCOM ExecuteShellCommand Call - Likely Lateral Movement", "ET INFO DYNAMIC_DNS HTTP Request to a *.myftp.biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.keybusinessconnection .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-tx .com Domain", "ET INFO DYNAMIC_DNS Query to a *.navigogroup .cl Domain", "ET HUNTING Request for EXE via WinHTTP M2", "ET INFO DYNAMIC_DNS Query to a *.fr .to Domain", "ET POLICY DNS Query to .onion proxy Domain (enter2tor.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.aispilot .com Domain", "ET INFO DYNAMIC_DNS Query to a *.vlad .md Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.qpoe .com Domain", "ET POLICY SMB NT Create AndX Request For an Executable File", "ET INFO DYNAMIC_DNS Query to a *.wiki .gd Domain", "ET INFO Observed URL Shortening Service Domain (t .ly in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.info .gf Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.0x .no Domain", "ET INFO DYNAMIC_DNS Query to a *.ayso795 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hmsolucoes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hpc .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sceniconline .com Domain", "ET SMTP EXE - ZIP file

	with .pif filename inside", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (Zva2UtQ29) in DNS TXT Reponse", "ET INFO DNS Query for Suspicious .ch.vu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ivi .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.info .gf Domain", "ET INFO DYNAMIC_DNS Query to a *.orienta .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.kickto .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.4pu .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ez-dns.com Domain", "ET INFO DYNAMIC_DNS Query to a *.serveris .id .lv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.patelmortgage .com Domain", "ET INFO URL Shortening Service Domain in DNS Lookup (t .ly)", "ET INFO DYNAMIC_DNS Query to a *.nowddns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-lost .org Domain", "ET POLICY DNS Query to DynDNS Domain *.point2this .com", "ET INFO DYNAMIC_DNS Query to a *.bizzapp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hackquest .com Domain", "ET INFO HTTP Request to a *.cam domain", "ET INFO DYNAMIC_DNS Query to a *.4040 .idv .tw Domain", "ET INFO DYNAMIC_DNS Query to a *.monobasin .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-very-sweet .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gparente .net .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.selfip .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.gatesweb .info Domain", "ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer", "ET INFO DYNAMIC_DNS Query to a *.soapclient .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.my .to Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-libertarian .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.multiverso .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.instanthq .com Domain", "ET WEB_SERVER SQL Errors in HTTP 500 Response (error in your SQL syntax)", "ET INFO HTTP Request to a *.xe.cx domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gigaportal .pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.imexsac .com Domain", "ET POLICY DNS Query to DynDNS Domain *.ufcfan .org", "ET WEB_CLIENT Hex Obfuscation of replace Javascript Function % Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.sequoiapartners .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveftp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.misecure .com Domain", "ET INFO DYNAMIC_DNS Query to a *.vizvaz .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wayner .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.computersforpeace .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.img .com .ar Domain", "ET WEB_CLIENT Possible PDF Launch Function Remote Code Execution Attempt with Name Representation Obfuscation", "ET INFO DYNAMIC_DNS HTTP Request to a *.pixelfucker .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dfdl .com Domain", "ET INFO DYNAMIC_DNS Query to a *.servebbs .net Domain", "ET INFO DYNAMIC_DNS Query to a *.youdontcare .com Domain", "ET INFO DYNAMIC_DNS Query to a *.fuettertdasnetz .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.forumz .info Domain", "ET INFO DYNAMIC_DNS Query to a *.jkub .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chimmychurry .com Domain", "ET HUNTING Suspicious Request to iplogger .org Contains Period", "ET INFO DYNAMIC_DNS Query to a *.3d-game.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tru .io Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bucu .pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.moot .es Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.z0d .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.est-a-la-maison .com Domain", "ET POLICY Nslookup Command in SMB Traffic - Possible Lateral Movement", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-al .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-vt .com Domain", "ET INFO DYNAMIC_DNS Query to a *.southquay .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-home .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hepcats .net Domain", "ET INFO DYNAMIC_DNS Query to a *.jasems .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dvrcam .info Domain", "ET SCAN Suspicious inbound to MSSQL port 1433", "ET INFO DYNAMIC_DNS HTTP Request to a *.tafca .co .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-hi .com Domain", "ET POLICY Query to a *.opengw.net Open VPN Relay Domain", "ET POLICY DNS Query to

	DynDNS Domain *.damnserver .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.wild1 .net Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.cf)", "ET INFO DYNAMIC_DNS Query to a *.tdkare .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.linuxd1 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.themoosebarn .com Domain", "ET INFO DYNAMIC_DNS Query to a *.echoparklake .com Domain", "ET INFO DYNAMIC_DNS Query to a *.fearpenguins .com Domain", "ET INFO DYNAMIC_DNS Query to a *.iii .cl Domain", "ET POLICY DNS Query to .onion proxy Domain (tor2web)", "ET INFO DYNAMIC_DNS HTTP Request to a dns-stuff.com Domain *.dns-stuff.com", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-patsfan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ezua .com Domain", "ET SCAN MySQL Malicious Scanning 3", "ET INFO DYNAMIC_DNS HTTP Request to a *.astrabus .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.16-b .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gr8domain .biz Domain", "ET WEB_CLIENT Hex Obfuscation of eval %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.kfco .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dorthel .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homelinuxserver .org Domain", "ET INFO DYNAMIC_DNS Query to a *.slumbo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.selfip .info Domain", "ET WEB_CLIENT Possible % Encoded Iframe Tag", "ET INFO DYNAMIC_DNS HTTP Request to a *.jetos .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tx2600 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.selfip .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.eating-organic .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.changeip .co Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.libre)", "ET INFO DYNAMIC_DNS HTTP Request to a *.chocolatespicacho .com Domain", "ET POLICY DNS Query to DynDNS Domain *.nhlfan .net", "ET INFO DYNAMIC_DNS Query to a *.dynu .com Domain", "ET HUNTING Possible Bot CnC Beacon (GET)", "ET INFO Observed DNS Query to .okinawa TLD", "ET INFO Query for Suspicious .us.tf Domain", "ET INFO Query for Suspicious .at.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.scrapping .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.serveftp .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ishevchenko .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mine .tk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fantasyleague .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.keystoneuniformcap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.4pu .com Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.pw)", "ET INFO Observed Pastebin Style Domain (pastetext .net in TLS SNI)", "ET INFO Observed DNS Query to .fit TLD", "ET INFO DYNAMIC_DNS Query to a *.ohbah .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-tn .com Domain", "ET POLICY Possible Powershell .ps1 Script Use Over SMB", "ET INFO DYNAMIC_DNS Query to a *.usajusaj .org Domain", "ET INFO DYNAMIC_DNS Query to a *.homaxcorp .com Domain", "ET MALWARE Observed DNS Query to bablosoft Domain (downloads .bablosoft .com)", "ET INFO DYNAMIC_DNS Query to a *.03c8 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.moot .es Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.est-a-la-maison .com Domain", "ET USER_AGENTS Observed Suspicious UA (zwt)", "ET INFO DYNAMIC_DNS Query to a *.gotgeeks.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.keystoneuniformcap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dcmusic .ca Domain", "ET HUNTING Request for EXE via WinHTTP M3", "ET INFO DYNAMIC_DNS Query to a *.voles35 .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.intranetwifi .it Domain", "ET INFO URL Shortening/Redirect Service Domain in DNS Lookup (clik .rip)", "ET INFO DYNAMIC_DNS HTTP Request to a *.theriens .com Domain", "ET INFO DYNAMIC_DNS Query to a *.chimmychurry .com Domain", "ET INFO DYNAMIC_DNS Query to a *.extramindcorp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeunix .com Domain", "ET USER_AGENTS Observed Suspicious UA (Chrome)", "ET INFO DYNAMIC_DNS HTTP Request to a *.isa-geek .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ndra .biz Domain", "ET USER_AGENTS Suspicious User-Agent (kath)", "ET WEB_CLIENT Hex Obfuscation of charCodeAt %u UTF-16 Encoding", "ET INFO Observed Self-Hosted Git Service Domain (gitea .com in TLS SNI)",

	"ET INFO DYNAMIC_DNS HTTP Request to a *.bizzapp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.itsaol .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hin .tw Domain", "ET INFO External IP Lookup Domain DNS Lookup (my-ip .io)", "ET INFO Possible Chrome Plugin install", "ET INFO Dotted Quad Host RTF Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.sarah-lai .com Domain", "ET INFO Observed DNS Query to DDNS Domain .otzo .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.soapclient .com Domain", "ET INFO DYNAMIC_DNS Query to a *.a4t .in Domain", "ET INFO DYNAMIC_DNS Query to a *.madhacker .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.robbieb .me .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.uk .ms Domain", "ET INFO DYNAMIC_DNS Query to a *.artisnotcrime .com Domain", "ET INFO DYNAMIC_DNS Query to a *.18t .biz Domain", "ET HUNTING Possibly Suspicious Request for Putty.exe from Non-Standard Download Location", "ET INFO DYNAMIC_DNS HTTP Request to a *.servecounterstrike .com Domain", "ET POLICY DNS Query to DynDNS Domain *.homesecuritypc .com", "ET INFO DYNAMIC_DNS Query to a *.xxxy .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.keecha .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dleon .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.soussa-csc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ldtp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.rebatesrule .net Domain", "ET USER_AGENTS Suspicious User-Agent (boostsoftware-urlexists)", "ET INFO DYNAMIC_DNS HTTP Request to a *.gotdns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.diyplans .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dynalias .net Domain", "ET SCAN MySQL Malicious Scanning 1", "ET HUNTING Suspicious smss.exe in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.dvrdns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.soon .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-very-bad .org Domain", "ET INFO DYNAMIC_DNS Query to a *.xst .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.melakaboy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xxxxx .tw Domain", "ET HUNTING Suspicious Windows Commands in POST Body (nltest)", "ET INFO DYNAMIC_DNS HTTP Request to a *.seasol .net Domain", "ET INFO DYNAMIC_DNS Query to a *.pbohara .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-caterer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-student .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servepics .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.normaweese .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-techie .com Domain", "ET INFO DYNAMIC_DNS Query to a *.autoroutedemorges .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dockl .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blacknapkins .org Domain", "ET INFO DYNAMIC_DNS Query to a *.bkpsports .com Domain", "ET INFO DYNAMIC_DNS Query to a *.contem .bz Domain", "ET INFO DYNAMIC_DNS Query to a *.theoceanforest .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.deusexmachina .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mediatriumph .com Domain", "ET INFO DYNAMIC_DNS Query to a *.myddns .biz Domain", "ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)", "ET INFO DYNAMIC_DNS Query to a *.mkahowes .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dubya .net Domain", "ET POLICY Command Shell Activity Over SMB - Possible Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.monkeywerks .net Domain", "ET WEB_SERVER - EXE File Uploaded - Hex Encoded", "ET INFO DYNAMIC_DNS Query to a *.serveftp .org Domain", "ET USER_AGENTS Suspicious User-Agent (HaxerMen)", "ET INFO DYNAMIC_DNS Query to a *.gracesiefer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.whyboner .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hackquest .com Domain", "ET INFO DYNAMIC_DNS Query to a *.packeting .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.csproject .org Domain", "ET INFO DYNAMIC_DNS Query to a *.buyshouses .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.champagnewishesandrvdreams .com Domain", "ET HUNTING Kaspov Related Hex In HTTP Accept Header", "ET INFO Base64 Encoded powershell.exe in HTTP Response M1", "ET INFO DYNAMIC_DNS HTTP Request to a *.logntw .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cohens .org .il Domain", "ET INFO DYNAMIC_DNS HTTP

	Request to a *.is-a-soxfan .org Domain", "ET WEB_CLIENT PDF Name Representation Obfuscation of Pages", "ET INFO DYNAMIC_DNS Query to a *.mooo .info Domain", "ET INFO DYNAMIC_DNS Query to a *.adagio .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.adepoju .org Domain", "ET DNS Query to a .tk domain - Likely Hostile", "ET INFO DYNAMIC_DNS Query to a *.sixth .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.livewave .ru Domain", "ET INFO Collaboration/File Sharing Platform Domain in DNS Lookup (notion .so)", "ET INFO X86_64 File Download Request from IP Address", "ET INFO DYNAMIC_DNS HTTP Request to a *.sundby .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dark-byte .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ind .st Domain", "ET INFO DYNAMIC_DNS Query to a *.ishevchenko .net Domain", "ET INFO DYNAMIC_DNS Query to a *.photogenic .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.roig .com Domain", "ET WEB_CLIENT Hex Obfuscation of parseInt % Encoding", "ET USER_AGENTS Suspicious User-Agent (aaaa)", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (XctT2JqZW) in DNS TXT Reponse", "ET WEB_SERVER .PHP being served from WP 1-flash-gallery Upload DIR (likely malicious)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mine .bz Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (52b2tlLVdtaU1ldG) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.mtrshop .com Domain", "ET INFO Obfuscated Split String (Double Q) 5", "ET INFO DYNAMIC_DNS Query to a *.darktech.org Domain", "ET HUNTING HTTP Request for OpenNIC API GeoIP Request", "ET INFO DYNAMIC_DNS Query to a *.dnsrd .com Domain", "ET INFO DYNAMIC_DNS Query to a *.firstimage .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fivepals .com Domain", "ET INFO DYNAMIC_DNS Query to a *.contactme .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dateeasily .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-found .org Domain", "ET POLICY HTTP Request to a *.qc.cx domain", "ET HUNTING Suspicious Quotation Mark Usage in FTP Username", "ET HUNTING Suspicious GET To gate.php with no Referer", "ET INFO Lockbit Ransomware Related Domain in DNS Lookup (lockbit-decryptor .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.anondns .net Domain", "ET HUNTING Generic IOT Downloader Malware in POST (Inbound)", "ET INFO DYNAMIC_DNS Query to a *.monopolecorp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hectorhector .com Domain", "ET INFO DYNAMIC_DNS Query to a *.novohorizonte .pt Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sells-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nard .ca Domain", "ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.ladatap .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-bulls-fan .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.aintno .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.flazzard .com Domain", "ET HUNTING 7-zip Executable Requested (GET)", "ET INFO DYNAMIC_DNS Query to a *.from-ks .com Domain", "ET INFO SMTP PDF Attachment Flowbit Set", "ET INFO DYNAMIC_DNS HTTP Request to a *.in-the-band .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lovethosetrains .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrcork .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lflink .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-az .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-free .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lamivolts .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsget .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-remote .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dubya .biz Domain", "ET POLICY Powershell Command With No Profile Argument Over SMB - Likely Lateral Movement", "ET POLICY HTTP Request to a *.cw.cm domain", "ET POLICY SMB Remote AT Scheduled Job Create Request - Possible Lateral Movement", "ET INFO DYNAMIC_DNS HTTP Request to a *.nux .co .za Domain", "ET INFO DYNAMIC_DNS Query to a *.lebtimnetz .de Domain", "ET INFO DYNAMIC_DNS Query to a *.from-id .com Domain", "ET POLICY DNS Query to DynDNS Domain *.serveirc .com", "ET WEB_SERVER WebShell Generic - *.tar.gz in POST body", "ET INFO DYNAMIC_DNS Query to a *.ftp1 .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.unix .id .lv Domain", "ET INFO DYNAMIC_DNS HTTP

	Request to a *.myftp .biz Domain", "ET INFO SPARC File Download Request from IP Address", "ET INFO DYNAMIC_DNS Query to a *.deusexmachina .org Domain", "ET POLICY Packity Proxy Connection", "ET INFO DYNAMIC_DNS HTTP Request to a *.freedynamicdns .net Domain", "ET INFO DYNAMIC_DNS Query to a *.antexknitting .com Domain", "ET INFO DYNAMIC_DNS Query to a *.xinit .se Domain", "ET POLICY MAZE Ransomware Victim Publishing Site DNS Lookup (mazenews .top)", "ET INFO Observed Commonly Abused Domain in DNS Lookup (blogattach .naver .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.vizvaz .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.galecsy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.buys .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.enemyterritory .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.heatmypool .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.generi .cc Domain", "ET PHISHING Possible Phish - Saved Website Comment Observed", "ET INFO DYNAMIC_DNS Query to a *.office-on-the .net Domain", "ET WEB_CLIENT Hex Obfuscation of String.fromCharCode %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS Query to a *.gotdns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bmvl .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cardias .adv .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.almostmy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.4irc.com Domain", "ET INFO DYNAMIC_DNS Query to a *.cuetara .name Domain", "ET POLICY SMB2 Remote AT Scheduled Job Create Request", "ET INFO DYNAMIC_DNS Query to a *.is-very-evil .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsup .net Domain", "ET INFO DYNAMIC_DNS Query to a *.spacetechnology .net Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.ga)", "ET INFO DYNAMIC_DNS Query to a *.is-an-actor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-found .org Domain", "ET INFO DYNAMIC_DNS Query to a *.podzone .net Domain", "ET INFO Observed Blockchain Domain (api .blockcypher .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypop3 .net Domain", "ET INFO Observed DNS Query to .ryukyu TLD", "ET INFO DYNAMIC_DNS Query to a *.kicks-ass .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tcp4 .me Domain", "ET INFO Observed File Sharing Service Domain (link .storjshare .io in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.v0id .nl Domain", "ET INFO DYNAMIC_DNS Query to a *.uitgavepatroon .nl Domain", "ET INFO DYNAMIC_DNS Query to a *.wanip .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.offbitch .com Domain", "ET POLICY Nessus Server SSL certificate detected", "ET INFO DYNAMIC_DNS HTTP Request to a *.mystakidis .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns-report .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.reasonman .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.seasol .org Domain", "ET INFO DYNAMIC_DNS Query to a *.8bit .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wooloo .net Domain", "ET INFO DYNAMIC_DNS Query to *onthenetas.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.cobra200 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.flink .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.afphila .com Domain", "ET INFO DYNAMIC_DNS Query to a *.blogdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bizis .si Domain", "ET INFO DYNAMIC_DNS Query to a *.x24hr .com Domain", "ET INFO DYNAMIC_DNS Query to a *.barratella .com Domain", "ET HUNTING Suspicious GET Request for .mspl File", "ET INFO Obfuscated Split String (Double Q) 1", "ET INFO DYNAMIC_DNS HTTP Request to a *.kik .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mefound .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.3vm .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.isa-geek .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.monopolecorp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.freewww .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nflfan .org Domain", "ET INFO Dotted Quad Host DLL Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.thejordaans .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns-stuff .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsrd .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing tracing Provider Factory", "ET INFO DYNAMIC_DNS Query to a *.qc .to Domain", "ET INFO DYNAMIC_DNS Query to a *.webs .vc Domain",

	"ET INFO DYNAMIC_DNS Query to a *.auraria .org Domain", "ET HUNTING DNS Lookup for 8+ hexadecimal only duckdns domain", "ET HUNTING Suspicious Registrar Nameservers in DNS Response (carbon2u)", "ET INFO DYNAMIC_DNS HTTP Request to a *.qualitypoolsboulder .com Domain", "ET POLICY DNS Query to DynDNS Domain *.nflfan .org", "ET INFO HTTP Request to a *.ga domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.changeip .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.packeting .eu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.easefun .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.0000000000000000000 .com Domain", "ET INFO DYNAMIC_DNS Query to a *.neoneptune .com Domain", "ET INFO DYNAMIC_DNS Query to a *.newsofmaricopa .com Domain", "ET INFO PSSC Powershell File Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveusers .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mylogisoft .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-into-cartoons .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.erke .biz .tr Domain", "ET INFO Obfuscated Split String (Single Q) 7", "ET POLICY DNS Query to DynDNS Domain *.myvnc .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns2 .us Domain", "ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.toadfishmonastery .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.quicksytes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.georgiagun .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.doomdns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.boldlygoingnowhere .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.folklandmanagement .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bellasclown .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-slick .com Domain", "ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware", "ET INFO DYNAMIC_DNS Query to a *.for-some .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tworiverssoftware .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zverovich .net Domain", "ET INFO DYNAMIC_DNS Query to a *.entergod .com Domain", "ET WEB_CLIENT Hex Obfuscation of unescape %u UTF-8 Encoding", "ET SCAN Generic IDBTE4M Exploit Scanner (Inbound)", "ET INFO WinUpack Modified PE Header Inbound", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-geek .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.windmillstravel .com Domain", "ET INFO DYNAMIC_DNS Query to a *.yhoccotruyen .org Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (mssql_query)", "ET INFO DYNAMIC_DNS Query to a *.from-de .com Domain", "ET INFO DYNAMIC_DNS Query to a *.de-a .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-office .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ssitech .bg Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.taco-land .net Domain", "ET INFO DYNAMIC_DNS Query to a *.euasazic .ro Domain", "ET INFO HTTP Request to a *.tw domain", "ET INFO DYNAMIC_DNS Query to a *.pakasak .com Domain", "ET INFO DYNAMIC_DNS Query to a *.milk .is Domain", "ET INFO URL Shortening Service Domain in DNS Lookup (webz .cc)", "ET INFO DYNAMIC_DNS Query to a *.hicam .net Domain", "ET INFO DYNAMIC_DNS Query to a *.clienturl .net Domain", "ET USER_AGENTS Suspicious User Agent (reqwest/)", "ET INFO DYNAMIC_DNS Query to a *.is-very-good .org Domain", "ET INFO DYNAMIC_DNS Query to a *.line .pm Domain", "ET INFO DYNAMIC_DNS Query to a *.painefieldcap .org Domain", "ET INFO HTTP Request to a *.gq domain", "ET INFO DYNAMIC_DNS Query to a *.proxydns .co .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.starscene .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.inkcat .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lehoozeher .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.saves-the-whales .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.reg .my .id Domain", "ET POLICY HTTP Request to a *.gv.vg domain", "ET HUNTING Suspicious csrss.exe in URI", "ET INFO DYNAMIC_DNS Query to a *.airlinemeals .net Domain", "ET WEB_CLIENT Possible Microsoft Internet Explorer CSS Cross-Origin Theft Attempt", "ET INFO DYNAMIC_DNS HTTP Request to a *.ljhb .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.csproject .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ga .com Domain", "ET MALWARE Observed DNS Query to Known Knotweed/SubZero Domain", "ET INFO

	DYNAMIC_DNS Query to a *.688 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.handfolding .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-liberal .com Domain", "ET INFO DYNAMIC_DNS Query to a *.celebsplay .com Domain", "ET INFO Observed File Sharing Service Download Domain (files .catbox .moe in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.misconfused .org Domain", "GPL FTP CWD ~root attempt", "ET INFO DYNAMIC_DNS Query to a *.lain .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.readmyblog .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nx .tc Domain", "ET INFO DNS Query for Suspicious .co.be Domain", "ET INFO DYNAMIC_DNS Query to a *.jundy .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ks .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddns .cam Domain", "ET POLICY DNS Query to DynDNS Domain *.eating-organic .net", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-or .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dtdns .org Domain", "ET POLICY SMB Executable File Transfer", "ET INFO DYNAMIC_DNS Query to a *.mefound .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.smh .com .my Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Prgrm.txt)", "ET INFO DYNAMIC_DNS Query to a *.triki .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.remotecam .nu Domain", "ET POLICY HTTP OPTIONS invalid method case outbound", "ET INFO CDXML Powershell File Request", "ET INFO DYNAMIC_DNS Query to a *.authorizeddns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bearfacts .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cascadesterling .com Domain", "ET INFO DNS Query for a Suspicious *.be.ma domain", "ET INFO DYNAMIC_DNS Query to a *.writesthisblog .com Domain", "ET INFO DYNAMIC_DNS Query to a *.qualitypoolsboulder .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns1 .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gerastar .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.ycare .de Domain", "ET INFO DYNAMIC_DNS Query to a *.mobile-node .net Domain", "ET INFO DYNAMIC_DNS Query to a *.fatdiary .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.adagio .tw Domain", "ET INFO HTTP POST Request to Suspicious *.gdn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dailyview .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dpo .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rebatesrule .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddnslive .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.squirly .info Domain", "ET INFO DYNAMIC_DNS Query to a *.showmyhomes .com Domain", "ET INFO DYNAMIC_DNS Query to a *.yurigoron .com Domain", "ET INFO HTTP Request to a *.top domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.id .web .id Domain", "ET INFO Obfuscated Split String (Single Q) 9", "ET INFO Query for Suspicious .bg.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.fartit .com Domain", "ET INFO DYNAMIC_DNS Query to a *.clarkstock .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hatenboer .org Domain", "ET INFO DYNAMIC_DNS Query to a *.prettyweak .com Domain", "ET INFO DYNAMIC_DNS Query to a *.htclink .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mutluay .com Domain", "ET INFO DYNAMIC_DNS Query to a *.podzone .org Domain", "ET HUNTING SUSPICIOUS *.pdf.exe in HTTP URL", "ET INFO DYNAMIC_DNS HTTP Request to a *.play .ai Domain", "ET INFO DYNAMIC_DNS Query to a *.sandhofner .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.360technologies .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myphotos .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.undo .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gurdit .com Domain", "ET INFO HTTP Request to a *.ru.tf domain", "ET INFO Dotted Quad Host PS Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-dc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-socialist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeftp .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-by .us Domain", "ET INFO DYNAMIC_DNS Query to a *.dougtreadwell .com Domain", "ET INFO DYNAMIC_DNS Query to a *.now-dns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.homeplex .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tzafrir .org .il Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servehumour .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mmafan .biz Domain", "ET

	INFO DYNAMIC_DNS Query to a *.dixiesewing .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rwbcode .com Domain", "ET INFO DYNAMIC_DNS Query to a *.minecraftr .us Domain", "ET POLICY DNS Query to .onion proxy Domain (onion.to)", "ET INFO DYNAMIC_DNS HTTP Request to a *.shitcunt .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rpz .su Domain", "ET HUNTING Powershell Downloader with Start-Process Inbound M1", "ET INFO DYNAMIC_DNS HTTP Request to a *.game-host .org Domain", "ET INFO Unconfigured nginx Access", "ET POLICY DNS Query to DynDNS Domain *.cable-modem .org", "ET INFO DYNAMIC_DNS Query to a *.gerastar .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.station .moe Domain", "ET MALWARE Large DNS Query possible covert channel", "ET INFO DYNAMIC_DNS Query to a *.b0ne.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.beerprojects .com Domain", "ET INFO DYNAMIC_DNS Query to a *.skies .tw Domain", "ET POLICY DNS Query to DynDNS Domain *.couchpotatofries .org", "ET INFO DYNAMIC_DNS HTTP Request to a *.novohorizonte .pt Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webhop .me Domain", "ET HUNTING SUSPICIOUS Possible automated connectivity check (www.msn.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.kawa-kun .com Domain", "ET INFO DYNAMIC_DNS Query to a *.wwwhost .us Domain", "ET POLICY Vulnerable Java Version 10.0.x Detected", "ET INFO DYNAMIC_DNS Query to a *.is-a-bulls-fan .com Domain", "ET POLICY Possible Mobile Malware POST of IMSI International Mobile Subscriber Identity in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.logic .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.from-mo .com Domain", "ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.birdsofnorthamerica .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.crabdance .com Domain", "ET INFO Serialized Data request", "ET HUNTING Suspicious TLS SNI Request for Root", "ET INFO DYNAMIC_DNS Query to a *.awiki .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.guild-site .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fiid .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myjamesonline .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ecosys .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.ssmailer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.studiovk .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mypets .ws Domain", "ET INFO DYNAMIC_DNS Query to a *.ripservers .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-work .com Domain", "ET INFO DYNAMIC_DNS Query to a *.forgot .his .name Domain", "ET INFO DYNAMIC_DNS Query to a *.jomblo .asia Domain", "ET POLICY DNS Query to DynDNS Domain *.pointto .us", "ET INFO DYNAMIC_DNS Query to *isgre.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.tscng .org Domain", "ET INFO DYNAMIC_DNS Query to a *.endoftheinternet .org Domain", "ET POLICY Powershell Command With Encoded Argument Over SMB - Likely Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.itemdb .com Domain", "ET INFO DYNAMIC_DNS Query to a *.trickip .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.djbomba .one .pl Domain", "ET INFO Dotted Quad Host GZ Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.qlbv .vn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ryanjlowe .us Domain", "ET INFO DYNAMIC_DNS Query to a *.limetropy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bounceme .net Domain", "ET WEB_SERVER Possible bash shell piped to dev udp Inbound to WebServer", "ET INFO DYNAMIC_DNS Query to a *.zzux .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sundby .com Domain", "ET INFO DNS Query to a Suspicious *.vv.cc domain", "ET INFO SUPERH File Download Request from IP Address", "ET POLICY Vulnerable Java Version 1.6.x Detected", "ET INFO DYNAMIC_DNS Query to a *.uk .ms Domain", "ET INFO DYNAMIC_DNS Query to a *.fragmentary .info Domain", "ET INFO DYNAMIC_DNS Query to a *.endofinternet .org Domain", "ET POLICY DNS Query for try2check.me Carder Tool", "ET INFO DYNAMIC_DNS Query to *athersite.com Domain (Sitelutions)", "ET HUNTING Office Doc Retrieving Shortened URL (bit .do)", "ET INFO DYNAMIC_DNS HTTP Request to a *.voles35 .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-socialist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fmg .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.seprotec .net .br Domain", "ET

	POLICY Ipconfig Command in SMB Traffic - Possible Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.byte4byte .com Domain", "ET INFO DYNAMIC_DNS Query to a *.baikabibai .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.youdontcare .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tinosmarble .com Domain", "ET HUNTING Suspicious POST Request with Possible COVID-19 Domain M1", "ET INFO DYNAMIC_DNS Query to a *.themcleans .us Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-server .com Domain", "GPL RPC rlogin LinuxNIS", "ET USER_AGENTS Observed DPRK Related APT User-Agent (dafom)", "ET WEB_SERVER PHP REQUEST SuperGlobal in URI", "ET INFO DYNAMIC_DNS Query to a *.cloudwatch .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.limetropy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sixth .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.scottexteriors .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-chef .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.groups .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.okay .com .tr Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.changeip .us Domain", "ET INFO DYNAMIC_DNS Query to a *.cw03 .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.unusualperson .com Domain", "ET INFO DYNAMIC_DNS Query to a *.now-dns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.4irc.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ideaustry .sg Domain", "ET INFO Observed Anonymous File Sharing Service in SSL Cert (fromsmash .co)", "ET INFO DYNAMIC_DNS Query to a *.squirly .info Domain", "ET INFO DYNAMIC_DNS Query to a *.nufszone .com Domain", "ET POLICY DNS Query to .onion proxy Domain (onion.gq)", "ET INFO Obfuscated Split String (Double Q) 13", "ET INFO DYNAMIC_DNS Query to a *.ssl443 .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ryanjlowe .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mchini .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrbonus .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dob .jp Domain", "ET INFO DYNAMIC_DNS Query to a *.webhop .biz Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (dm9rZS1Db21) in DNS TXT Reponse", "GPL FTP SITE EXEC attempt", "ET INFO DYNAMIC_DNS Query to a *.myftp .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nokedli .org Domain", "ET INFO DYNAMIC_DNS Query to a *.oops .wtf Domain", "ET INFO DYNAMIC_DNS Query to a *.voyez .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.ssitech .bg Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.make .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dabhome .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ikwb .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.afphila .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lostgumball .com Domain", "ET INFO DYNAMIC_DNS Query to a *.v0id .nl Domain", "ET INFO URL Shortner Domain in DNS Lookup (urlz .fr)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-green .com Domain", "ET MALWARE DNS query for Morto RDP worm related domain qfsl.net", "ET INFO DYNAMIC_DNS Query to a *.from-hi .com Domain", "GPL MISC rlogin echo++", "ET INFO DYNAMIC_DNS HTTP Request to a *.pitam .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fuettertdasnetz .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bedwell .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dogdammit .com Domain", "ET POLICY DNS Query to DynDNS Domain *.net-freaks .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.academic .org .il Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-cpa .com Domain", "ET INFO Observed URL Shortening Service Domain (webz .cc in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.gentile .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.leonisbg .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.echoparklake .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-chef .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tehlab .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ocry .com Domain", "ET INFO DYNAMIC_DNS Query to a *.superizeme .com Domain", "ET INFO DYNAMIC_DNS Query to a *.soussa-csc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.barrell-of-knowledge .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.assexyas.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.andreymorozov .ru Domain", "ET

	INFO DYNAMIC_DNS Query to a *.etowns.org Domain", "ET INFO Java Request to DynDNS Pro Dynamic DNS Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tth .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sjschroeder .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ve3 .info Domain", "ET INFO Observed URL Shortening Service Domain (vtaurl .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.b33r .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tecnova .com .br Domain", "ET INFO Dotted Quad Host M5 (noalert)", "ET INFO DYNAMIC_DNS Query to a *.dnset .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.port25 .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.robonauts .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chekanov .net Domain", "ET INFO Observed External IP Lookup Domain (ipbase .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.is-a-guru .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ctx .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.clienturl .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fin-tech .com Domain", "ET EXPLOIT Malformed HeartBeat Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.brasilia .me Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.collegefan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-mt .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mysecuritycamera .org Domain", "ET INFO DYNAMIC_DNS Query to a *.d-n-s .org .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-player .com Domain", "ET INFO DYNAMIC_DNS Query to a *.wooloo .net Domain", "ET INFO DYNAMIC_DNS Query to a *.chicago360factor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.2fine .de Domain", "ET INFO DYNAMIC_DNS Query to a *.koakh .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dubya .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.space-to-rent .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (dm9rZS1Db21tYW) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.iliensale .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.happyminecraft .org Domain", "ET POLICY HTTP traffic on port 443 (HEAD)", "ET INFO DYNAMIC_DNS HTTP Request to a *.linuxstart .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kickto .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsdojo .net Domain", "ET POLICY DNS Query to DynDNS Domain *.bounceme .net", "ET INFO DYNAMIC_DNS Query to a *.elliotshoe .com Domain", "ET HUNTING Possible COVID-19 Domain in SSL Certificate M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.podzone .net Domain", "ET MALWARE DNS query for Morto RDP worm related domain jaifr.net", "ET INFO DYNAMIC_DNS HTTP Request to a *.alte .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jomblo .asia Domain", "ET POLICY DNS Query to .onion proxy Domain (onion. pw)", "ET INFO DYNAMIC_DNS Query to a *.okzk .com Domain", "ET POLICY SMB2 NT Create AndX Request For a .bat File", "ET INFO DYNAMIC_DNS HTTP Request to a *.xinit .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isa-geek .com Domain", "ET EXPLOIT_KIT Suspicious VBS Encoding Observed in BottleEK", "ET INFO DYNAMIC_DNS Query to a *.youramys .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-celticsfan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.intercop .de Domain", "ET HUNTING Suspicious winlogin.exe in URI", "ET INFO DYNAMIC_DNS Query to a *.wo5m .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mywww .biz Domain", "ET HUNTING Suspicious GET Request with Possible COVID-19 Domain M1", "ET INFO DYNAMIC_DNS Query to a *.dnet .hu Domain", "ET INFO DYNAMIC_DNS Query to a *.creery .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lojadebikini .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.elliotshoe .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alimentoshen .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.abatek .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sleeperkidsworld .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zhanwenhan .com Domain", "ET POLICY DNS Query to DynDNS Domain *.mysecuritycamera .org", "ET INFO DYNAMIC_DNS Query to a *.nard .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dansted .org Domain", "ET USER_AGENTS Observed Suspicious User-Agent (altera forma)", "ET INFO DYNAMIC_DNS Query to a *.malam .or .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nullexistence

	.net Domain", "ET INFO DYNAMIC_DNS Query to a *.dynet .com Domain", "ET INFO DYNAMIC_DNS Query to a *.galitec .es Domain", "ET INFO DYNAMIC_DNS Query to a *.bad .mn Domain", "ET INFO DYNAMIC_DNS Query to a *.servebbs .org Domain", "ET INFO DYNAMIC_DNS Query to a *.does-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.k22 .su Domain", "ET INFO DYNAMIC_DNS Query to a *.tinyrealm .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alsupnet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.norushcharge .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-geek .net Domain", "ET INFO DYNAMIC_DNS Query for Suspicious .dyndns-at-home.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.broke-it .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dumb1 .com Domain", "ET INFO DYNAMIC_DNS Query to a *.thejordaans .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isasecret .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blogdns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-into-anime .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torsona.com)", "ET INFO DYNAMIC_DNS Query to a *.dnslive .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iownyour .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.sovich .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servegame .org Domain", "ET WEB_SERVER PHP POST SuperGlobal in POST", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-llama .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.superizeme .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mypi .co Domain", "ET HUNTING Suspicious Terse Request for .pif", "ET POLICY DNS Query to .onion proxy Domain (onion2web.com)", "ET POLICY DNS Query to .onion proxy Domain (torpayeur.com)", "ET INFO DYNAMIC_DNS Query to a *.dynalias .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsalias .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-fl .com Domain", "ET INFO DYNAMIC_DNS Query to a *.toadfishmonastery .org Domain", "ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M1", "ET INFO DYNAMIC_DNS HTTP Request to a *.networkguru .com Domain", "ET INFO DYNAMIC_DNS Query to a *.abk .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnet .hu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tombu .net Domain", "ET INFO Observed URL Shortening Service Domain (dik .si in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.geekhardware .com Domain", "ET INFO DYNAMIC_DNS Query to a *.nodnor .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nn-foto .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeunix .org Domain", "ET INFO DYNAMIC_DNS Query to a *.clickip .de Domain", "ET INFO DYNAMIC_DNS Query to a *.sheepindonesia .org Domain", "ET INFO DYNAMIC_DNS Query to a *.socalfishkillaz .com Domain", "ET INFO DYNAMIC_DNS Query to a *.undo .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.devwonders .com Domain", "ET POLICY DNS Query to DynDNS Domain *.dnsiskinky .com", "ET HUNTING Zero Content-Length HTTP POST with data (outbound)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-mail .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.progressivecongressnews .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ny .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.off .li Domain", "ET INFO DYNAMIC_DNS Query to a *.barvennon .com Domain", "ET POLICY DNS Query to DynDNS Domain *.mysecuritycamera .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.essexregional .org Domain", "ET HUNTING Observed Suspicious Reversed String Inbound (Winmgmts)", "ET INFO DYNAMIC_DNS Query to a *.24x7 .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.letz .dev Domain", "ET INFO DYNAMIC_DNS Query to a *.chekanov .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dade .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mutsuura .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mandhplum .net Domain", "ET INFO WinUpack Modified PE Header Outbound", "ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrface .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.baselinux .net Domain", "ET WEB_CLIENT Hex Obfuscation of replace Javascript Function %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.lamivolts .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bien .se Domain", "ET WEB_CLIENT Likely

	Malicious PDF Containing StrReverse", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ne .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rtmuller .net Domain", "ET INFO DYNAMIC_DNS Query to a *.play .ai Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.niigeo .ru Domain", "ET INFO Query for a Suspicious *.noc.su domain", "ET INFO DYNAMIC_DNS Query to a *.blogdns .net Domain", "ET EXPLOIT TLS HeartBeat Request (Client Initiated) fb set", "ET INFO Query for Suspicious .ch.tf Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bgg .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.instanthq .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsalias .org Domain", "ET INFO DYNAMIC_DNS Query to a *.n-e-t .name Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kaohsiung .tv Domain", "ET INFO DYNAMIC_DNS Query to a *.onmypc .us Domain", "ET INFO DYNAMIC_DNS Query to a *.dsmtp .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cable-modem .org Domain", "ET WEB_CLIENT PDF Containing Windows Commands Downloaded", "ET INFO Suspicious Outbound SIG DNS Query", "ET INFO DYNAMIC_DNS HTTP Request to a *.privatedns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.qthome .org Domain", "ET HUNTING Suspicious Windows Commands in POST Body (ipconfig)", "ET INFO DYNAMIC_DNS HTTP Request to a *.1337 .cx Domain", "ET INFO DYNAMIC_DNS Query to a *.doomdns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.crafting .xyz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sne .jp Domain", "ET HUNTING Suspicious Terse HTTP Request to textbin", "ET INFO DYNAMIC_DNS Query to a *.primavera .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.home .dyndns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.homelinux .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cspcorp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.yourvaluedhomes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.crossharbour .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-pics .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ak .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blogsyte .com Domain", "ET WEB_SERVER WebShell - JSPCMD - Form", "ET INFO DYNAMIC_DNS Query to a *.sino .tw Domain", "ET INFO DYNAMIC_DNS Query to a *.lojadebikini .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.auraria .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hackerzinc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.l5 .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mankenskiold .se Domain", "ET INFO DYNAMIC_DNS Query to a *.misconfused .org Domain", "ET INFO Doc Requesting Remote Template (.dotm)", "ET INFO DYNAMIC_DNS HTTP Request to a *.yourspecialtee .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyn .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.port0 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sitaci .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bot .nu Domain", "ET INFO DYNAMIC_DNS Query to a *.mydad .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.soon .it Domain", "ET USER_AGENTS Suspicious User-Agent (Microsoft-ATL-Native/9.00)", "ET INFO DYNAMIC_DNS HTTP Request to a *.cloudwatch .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fido .be Domain", "ET HUNTING EXE Using Suspicious IAT ZwUnmapViewOfSection Possible Malware Process Hollowing", "ET INFO Anonymous File Sharing Domain in DNS Lookup (fromsmash .com)", "ET WEB_CLIENT Hex Obfuscation of String.fromCharCode % Encoding", "ET INFO DYNAMIC_DNS Query to a *.doomdns .org Domain", "ET INFO Observed Temporary File Sharing Service Domain (litter .catbox .moe in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.swe .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.for-some .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.arrowtechnical .co .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.blue-jade .net Domain", "ET ATTACK_RESPONSE UTF16-LE base64 wide string /This Program/ in DNS TXT Reponse", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (leHQuRW5jb2) in DNS TXT Reponse", "ET HUNTING Suspicious services.exe in URI", "ET HUNTING Generic Powershell DownloadString Command", "ET INFO DYNAMIC_DNS Query to a *.ayasophia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsking .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.gilead .org .il Domain", "ET INFO DYNAMIC_DNS Query to a *.dontexist .com Domain", "ET JA3 HASH - Possible Rclone Client Response (Mega Storage)", "ET INFO DYNAMIC_DNS Query to a *.fintech-llc .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing Classes used in awt exploits", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddj .co .za Domain", "ET INFO DYNAMIC_DNS Query to a *.ionexusa .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bouncers4rent .com Domain", "ET INFO DYNAMIC_DNS Query to a *.parikh .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.automotive .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyn-o-saur .com Domain", "ET INFO DNS Query for a Suspicious *.co.tv domain", "ET INFO HTTP Request to Suspicious *.world Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.borkar .in Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tedfullwood .com Domain", "ET INFO Wget Request for Executable", "ET INFO DYNAMIC_DNS Query to a *.moochurch .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sexmistrz .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.louis-ip .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.answersbot .com Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (mysql_query)", "ET INFO DYNAMIC_DNS HTTP Request to a *.prettyweak .com Domain", "ET POLICY HTTP Request to a *.cu.cc domain", "ET INFO DYNAMIC_DNS Query to a *.lehoozeher .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homaxcorp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.securitytactics .com Domain", "ET SMTP Incoming SMTP Message with Possibly Malicious MIME Epilogue 2016-05-13 (BadEpilogue)", "ET INFO DYNAMIC_DNS HTTP Request to a *.zverovich .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.project .li Domain", "ET INFO DYNAMIC_DNS Query to a *.possessed .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.de-a .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.flnet.org Domain", "ET INFO DYNAMIC_DNS Query to a *.lflinkup .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.geobattery .com Domain", "ET INFO HTTP Request to a *.edu.tf domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zelslonik .info Domain", "ET USER_AGENTS Suspicious Custom Firefox UA Observed (Firefox...)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-not-certified .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ubeagle .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ame-life .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-pr .com Domain", "ET INFO Observed URL Shortening Service Domain (www .temporary-url .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.good-newz .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.est-le-patron .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-uberleet .com Domain", "ET POLICY DNS Query to .onion proxy Domain (bortor.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-musician .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.memoryguide .org Domain", "ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-in .com Domain", "ET HUNTING File Sharing Related Domain (www .mediafire .com) in DNS Lookup", "ET INFO Query for Suspicious .pl.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.dob .jp Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jasems .com Domain", "ET HUNTING Microsoft Office User-Agent Requesting An Excel File", "ET INFO DYNAMIC_DNS HTTP Request to a *.d-n-s .name Domain", "ET INFO DYNAMIC_DNS Query to a *.authorizeddns .net Domain", "ET INFO DYNAMIC_DNS Query to a *.coreytech .com Domain", "ET INFO DYNAMIC_DNS Query to a *.amurt .org .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.starnerd .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.castleman .net Domain", "ET INFO DYNAMIC_DNS Query to a *.ezwebsites .com Domain", "ET USER_AGENTS Observed Suspicious UA (.NET Framework Client)", "ET INFO DYNAMIC_DNS HTTP Request to a *.notici .as Domain", "ET POLICY DNS Query to DynDNS Domain *.read-books .org", "ET POLICY Vulnerable Java Version 11.0.x Detected", "ET POLICY DNS Query to .onion proxy Domain (torpayusd.com)", "ET INFO DYNAMIC_DNS Query to a *.mcsoft .org Domain", "ET WEB_SERVER PHP COOKIE SuperGlobal in URI", "ET POLICY DNS Query to DynDNS Domain *.dynns .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.davidmcorn .com Domain", "ET INFO

	DYNAMIC_DNS HTTP Request to a *.ddns .me Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.myfw.us Domain (Sitelutions)", "ET INFO Pastebin-style Service (textbin .net in TLS SNI)", "ET INFO Obfuscated Split String (Double Q) 2", "ET POLICY SMB NT Create AndX Request For an Executable File In a Temp Directory", "ET INFO DYNAMIC_DNS Query to a *.yiannamarie .com Domain", "ET INFO DYNAMIC_DNS Query to a *.morganisageek .org Domain", "ET INFO DYNAMIC_DNS Query to a *.mypop3 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.linkpc .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nethub .fi Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chicago360factor .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shen .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.pegle .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ownip .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-by .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-into-cars .com Domain", "ET MALWARE DNS Query Sinkhole Domain Various Families (Possible Infected Host)", "ET INFO DYNAMIC_DNS Query to a *.dnsdojo .com Domain", "ET INFO Psiphon VPN Related Activity (POST)", "ET INFO DYNAMIC_DNS HTTP Request to a *.stuff-4-sale .us Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.myftp.biz Domain", "ET INFO DYNAMIC_DNS Query to a *.is-leet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.minetest .land Domain", "ET INFO DYNAMIC_DNS Query to a *.kicks-ass .net Domain", "ET INFO DYNAMIC_DNS Query to a *.freeddns .us Domain", "ET INFO DYNAMIC_DNS Query to a *.ducklog .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dockl .com Domain", "ET INFO DYNAMIC_DNS Query to a *.happyminecraft .org Domain", "ET USER_AGENTS Observed Malicious User-Agent (Brute Force Attacks)", "ET INFO DYNAMIC_DNS Query to a *.vankin .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-leet .com Domain", "ET INFO DYNAMIC_DNS Query to a *.midjava .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (52b2tlLUNvbW1hbm) in DNS TXT Reponse", "ET HUNTING Possible NOBELIUM CnC Traffic (Observed UA)", "ET INFO Dotted Quad Host ZIP Request", "ET INFO DYNAMIC_DNS Query to a *.id .web .id Domain", "ET INFO DYNAMIC_DNS Query to a *.from-sd .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.galitec .es Domain", "ET INFO DYNAMIC_DNS Query to a *.vr .lt Domain", "ET INFO DYNAMIC_DNS Query to a *.khabbaby .com Domain", "ET POLICY DNS Query to DynDNS Domain *.workisboring .com", "ET POLICY Observed DNS Query to DynDNS Domain (publicvm .com)", "ET POLICY DNS Query to DynDNS Domain *.hopto .org", "ET INFO DYNAMIC_DNS HTTP Request to a *.pce-cihazlari .com .tr Domain", "ET INFO DYNAMIC_DNS Query to a *.homedns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.yhkrubber .com .my Domain", "ET INFO DYNAMIC_DNS Query to a *.cascadesterling .com Domain", "ET INFO DYNAMIC_DNS Query to a *.webhop .net Domain", "ET INFO Microsoft Netconnection Domain in DNS Lookup", "ET POLICY DNS Query to DynDNS Domain *.collegefan .org", "ET INFO DYNAMIC_DNS HTTP Request to *.passinggas.net Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.skc .su Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.minecraft .pe Domain", "ET INFO DYNAMIC_DNS Query to a *.duta .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.xcv .cx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.evs .net .br Domain", "ET INFO DYNAMIC_DNS Query to a *.recyclesolutionsllc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.expedicionesytrekking .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-into-games .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vaizer .cl Domain", "ET POLICY DNS Query to DynDNS Domain *.homesecuritymac .com", "ET INFO DYNAMIC_DNS Query to a *.is-a-anarchist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thehomeserver .net Domain", "ET HUNTING SUSPICIOUS Reassigned Eval Function 1", "ET POLICY HTTP Request to a *.co.tv domain", "ET INFO DYNAMIC_DNS Query to a *.computersforpeace .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lczipper .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jolleybeef .com Domain", "ET HUNTING Suspicious Domain (laurentprotector .com) in TLS SNI", "ET INFO DYNAMIC_DNS HTTP Request to a *.energysemi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.rude .li Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sellsyourhome .org Domain",

	"ET INFO DYNAMIC_DNS Query to a *.unids .com Domain", "ET INFO Pastebin Style Domain in DNS Lookup (pastetext .net)", "ET INFO DYNAMIC_DNS HTTP Request to a *.antexknitting .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.autoroutedemorges .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hosthampster .com Domain", "ET INFO DYNAMIC_DNS Query to a *.osclabs .ro Domain", "ET WEB_SERVER SQL Errors in HTTP 500 Response (mssql_query)", "ET HUNTING Screenshot Uploaded to Discord", "ET INFO DYNAMIC_DNS Query to a *.from-il .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.diyplans .org Domain", "ET INFO SUSPICIOUS UA starting with Mozilla/0", "ET INFO DYNAMIC_DNS HTTP Request to a *.bellywings .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.e-m-a-i-l .org Domain", "ET INFO DYNAMIC_DNS Query to a *.usjepor .com Domain", "ET JA3 HASH - Possible Nessus Client", "ET INFO DYNAMIC_DNS HTTP Request to a *.splinteredlightbooks .com Domain", "ET HUNTING Suspicious Office Template Style Request (GET)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mikata .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myhousesetup .com Domain", "ET INFO POST to Double Slash in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-saved .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sazhenec .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.etowns.org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hunnur .com Domain", "ET WEB_CLIENT Hex Obfuscation of replace Javascript Function %u UTF-16 Encoding", "ET POLICY DNS Query to DynDNS Domain *.dnsfor .me", "ET INFO DYNAMIC_DNS HTTP Request to a *.minecraftnoob .com Domain", "ET INFO DYNAMIC_DNS Query to a *.yourtrap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.keine-panik .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-ip .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-geek .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ycare .de Domain", "ET INFO DYNAMIC_DNS Query to a *.hackerzinc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.nelsonshack .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zyix .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bmrresources .com Domain", "ET INFO DYNAMIC_DNS Query to a *.salford-hall .co .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.k .vu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-sd .com Domain", "ET WEB_SERVER WebShell - D.K - Title", "ET INFO DYNAMIC_DNS HTTP Request to a *.franchisecandidates .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tountas .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ma .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xst .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.dhcp .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fairuse .org Domain", "ET INFO DYNAMIC_DNS Query to a *.chebicon .ru Domain", "ET INFO Online File Storage Domain in DNS Lookup (gofile .io)", "ET INFO DYNAMIC_DNS Query to a *.vpnx .nl Domain", "ET POLICY HSRP Active Router Changed", "ET INFO DYNAMIC_DNS HTTP Request to a *.3n .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.freeddns .uk Domain", "ET WEB_CLIENT PDF With Hidden Embedded File", "ET INFO DYNAMIC_DNS HTTP Request to a *.simplecharity .com Domain", "ET INFO DYNAMIC_DNS Query to a *.imexsac .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cspcorp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ecosys .eu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wileymetal .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cuetara .name Domain", "ET INFO DYNAMIC_DNS Query to a *.porngo .at Domain", "ET HUNTING Suspicious Redirect to Download EXE from Bitbucket", "ET INFO DYNAMIC_DNS Query to a *.nunc .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jesus .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.stoupin .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gets-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chery .co .il Domain", "ET INFO DYNAMIC_DNS Query to a *.compucase .com Domain", "ET USER_AGENTS Observed Suspicious UA (NSIS_Inetc (Mozilla))", "ET INFO DYNAMIC_DNS HTTP Request to a *.ohbah .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.oz)", "ET INFO DYNAMIC_DNS Query to a *.leitungsen .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.motoretta .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.masplene .com Domain", "ET INFO DYNAMIC_DNS

	HTTP Request to a *.2fine .de Domain", "ET USER_AGENTS Observed Suspicious UA (Absent)", "ET INFO DYNAMIC_DNS HTTP Request to a *.4dq .com Domain", "ET INFO DYNAMIC_DNS Query to a *.webmdee .com Domain", "ET INFO DYNAMIC_DNS Query to a *.youpc .ro Domain", "ET EXPLOIT Fortinet FortiWeb OS Command Injection Inbound M2 (CVE-2021-22123)", "ET HUNTING Microsoft Office User-Agent Requesting A Doc File", "ET INFO DYNAMIC_DNS Query to a *.humorvisite .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.pwm .hu Domain", "ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M1", "ET INFO DYNAMIC_DNS Query to a *.iantaylor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.wiab-service .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.usakoi .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torexplorer.com)", "ET USER_AGENTS Suspicious User-Agent (Windows 8)", "ET INFO DYNAMIC_DNS Query to a *.alimentoshen .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.line .pm Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-teacher .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns .navy Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.solfa .org Domain", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (ZXh0LkVuY29k) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.off .li Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zhanwenhan .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cardias .adv .br Domain", "ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M3", "ET INFO DYNAMIC_DNS Query to a Suspicious dynapoint.pw Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.top)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dropfiles .net Domain", "ET HUNTING Suspicious Percentage Symbol Usage in FTP Username", "ET INFO DYNAMIC_DNS HTTP Request to a *.teleconomiser .com Domain", "ET HUNTING Request to .TK Domain with Minimal Headers", "ET INFO DYNAMIC_DNS HTTP Request to a *.amurt .org .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.javahound .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thainewasia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.endoftheinternet .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dns .army Domain", "ET INFO DYNAMIC_DNS Query to dns-stuff.com Domain *.dns-stuff.com", "ET INFO DYNAMIC_DNS HTTP Request to a *.now-dns .net Domain", "ET POLICY DNS Query to DynDNS Domain *.mlbfan .org", "ET INFO DYNAMIC_DNS Query to a *.a-quo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.monopolepower .com Domain", "ET USER_AGENTS Suspicious User-Agent (Collection Info)", "ET INFO DYNAMIC_DNS HTTP Request to a *.gw .lt Domain", "ET SCAN Generic IDBTE4M Exploit Scanner (Outbound)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mylftv .com Domain", "ET INFO Observed DNS Query to DDNS Domain .zyns .com", "ET INFO DYNAMIC_DNS Query to a *.fedea .com .ar Domain", "ET WEB_SERVER SQL Errors in HTTP 500 Response (pgsql_query)", "ET HUNTING File Sharing Related Domain in DNS Lookup (filesend .jp)", "ET INFO DYNAMIC_DNS HTTP Request to a *.lflink .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsalias .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.roig .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.toshibanetcam .com Domain", "ET SHELLCODE Possible Backslash Escaped UTF-8 0c0c Heap Spray", "ET INFO DYNAMIC_DNS Query to a *.port25 .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.alexandravlad .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lflinkup .net Domain", "ET WEB_CLIENT Hex Obfuscation of arguments.callee %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.alltransportme .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alphasoft .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wiab-service .se Domain", "ET USER_AGENTS Observed Suspicious UA (CODE)", "ET INFO Query for Suspicious .ru.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.logic .com .br Domain", "ET INFO Observed URL Shortening Service Domain (prourl .in in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.donhoo .com Domain", "ET INFO Observed SyncroMSP Remote Management Software Domain (kabutoservices .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.leonardocastano .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mindhackers .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.priamaakcia .sk Domain", "ET INFO DYNAMIC_DNS

	Query to a *.aen .su Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isyour .guru Domain", "ET INFO DYNAMIC_DNS Query to a *.xcportugal .org Domain", "ET HUNTING Observed Lets Encrypt Certificate - Possible COVID-19 Related M2", "ET INFO Potential Common Malicious JavaScript Loop", "ET INFO Applet Tag In Edwards Packed JavaScript", "ET INFO DYNAMIC_DNS HTTP Request to a *.64-b .it Domain", "ET POLICY HTTP Request to a *.ce.ms domain", "ET USER_AGENTS Suspicious User-Agent Mozilla/3.0", "ET INFO External File Sharing Domain in DNS Lookup (anonfile .com)", "ET INFO DYNAMIC_DNS Query to a *.dprdsulsel .go .id Domain", "ET WEB_SERVER PHP SERVER SuperGlobal in POST", "ET INFO DYNAMIC_DNS Query to a *.swhydro .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-painter .com Domain", "ET INFO DYNAMIC_DNS Query to a *.theriens .com Domain", "ET INFO DYNAMIC_DNS Query to a *.marieblazek .com Domain", "ET INFO DYNAMIC_DNS Query to a *.nokedli .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.32-b .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.a-quo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.epicgamer .org Domain", "ET INFO Dotted Quad Host XLSX Request", "ET WEB_SERVER Non-Standard HTML page in Joomla /com_content/ dir", "ET HUNTING Suspicious Windows Commands in POST Body (net view)", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing management MBeanServer", "ET INFO DYNAMIC_DNS HTTP Request to a *.chrismac .org Domain", "ET INFO SUSPICIOUS UA starting with Mozilla/9", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.ga)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mathewparkin .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nelsonshack .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.usrsrc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.birdriver .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kompaniet .nu Domain", "ET INFO DYNAMIC_DNS Query to a *.psybnc .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dabhome .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dyn-o-saur .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.joeliriano .com Domain", "ET HUNTING Suspicious GET Request for .spc File", "ET INFO DYNAMIC_DNS HTTP Request to a *.mlbfan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nodnor .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.leitud .ee Domain", "ET INFO DYNAMIC_DNS Query to a *.okay .com .tr Domain", "ET INFO DYNAMIC_DNS Query to a *.dvrdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kbgz .com .my Domain", "ET POLICY DNS Query to .onion proxy Domain (torminater.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.igotwasted .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ia .com Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oast .fun)", "ET INFO DYNAMIC_DNS Query to a *.is-slick .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mydad .info Domain", "ET INFO DYNAMIC_DNS Query to a *.guild-site .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.euasazic .ro Domain", "ET POLICY DNS Query to DynDNS Domain *.myftp .org", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-cpa .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jmstudios .com Domain", "ET INFO DYNAMIC_DNS Query to a *.k4w411 .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.for-our .info Domain", "ET INFO DYNAMIC_DNS Query to a *.oljka .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (dy1PYmplY3) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.dfdl .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ourhobby .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.oops .wtf Domain", "ET INFO DYNAMIC_DNS Query to a *.qpoe .com Domain", "ET INFO DYNAMIC_DNS Query to a *.https443 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.koakh .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-oh .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypi .co Domain", "ET INFO DYNAMIC_DNS Query to a *.ddns .cam Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.teaches-yoga .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tantrum .org Domain", "ET INFO DYNAMIC_DNS Query to a *.softwarefinesse .com Domain", "ET INFO DYNAMIC_DNS Query to a *.widlund .fi Domain", "ET INFO DYNAMIC_DNS Query to a *.xxxy .info Domain", "ET POLICY DNS Query to DynDNS Domain *.blogsyte .com", "ET INFO DYNAMIC_DNS

	Query to a *.is-a-chef .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-republican .com Domain", "ET POLICY WinRM wsman Access - Possible Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.joeliriano .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hansa-tmp .cn Domain", "ET INFO DYNAMIC_DNS Query to a *.beerprojects .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vhfdental .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.calvaryduncan .com Domain", "ET DOS DNS Amplification Attack Possible Inbound Windows Non-Recursive Root Hint Reserved Port", "ET INFO DYNAMIC_DNS Query to a *.weixservice .com Domain", "ET INFO DYNAMIC_DNS Query to a *.changeip .us Domain", "ET INFO DYNAMIC_DNS Query to a *.abatek .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.australia .ai Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hicam .net Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing mbeanserver Introspector", "ET INFO DYNAMIC_DNS Query to a *.changeip .co Domain", "ET INFO DYNAMIC_DNS Query to a *.americajhon .com .pe Domain", "ET INFO DYNAMIC_DNS Query to a *.swhill .co .uk Domain", "ET USER_AGENTS Suspicious User-Agent (adlib)", "ET INFO DYNAMIC_DNS Query to a *.spelar .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.technopagans .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zza .pl Domain", "ET INFO DNS Query Domain .bit", "ET INFO DYNAMIC_DNS Query to a *.qhigh .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cloudranger .net Domain", "ET INFO HTTP POST Request to Suspicious *.ga Domain", "ET INFO Public Cloud Domain in DNS Lookup (cld .pt)", "ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M1", "ET INFO DYNAMIC_DNS HTTP Request to a *.120v .ac Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynathome .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-gone .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-in .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsiskinky .com Domain", "ET POLICY DNS Query to DynDNS Domain *.ddns .me", "ET INFO DYNAMIC_DNS Query to a *.tomahawkchurch .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.daev .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ninth .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kicks-ass .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ucvradio .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnslive .net Domain", "ET POLICY Vulnerable Java Version 13.0.x Detected", "ET INFO DYNAMIC_DNS Query to a *.wolf-tec .net Domain", "ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 2", "ET INFO DYNAMIC_DNS HTTP Request to a *.gnutella2 .info Domain", "ET HUNTING SUSPICIOUS *.doc.exe in HTTP HEADER", "ET INFO HTTP Request to a *.de.ms domain", "ET INFO Observed DNS Query to DynDNS Domain (linkpc .net)", "ET USER_AGENTS Suspicious User-Agent Simple Bot", "ET INFO DYNAMIC_DNS HTTP Request to a *.raspberryip .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cnstefancelmare .ro Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.cyb)", "ET INFO DYNAMIC_DNS Query to a *.root .sx Domain", "ET INFO DYNAMIC_DNS Query to a *.drupalpixels .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dailyholycrap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-mi .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.datacommunicationsinc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.localghost .org Domain", "ET INFO DYNAMIC_DNS Query to a *.teamradicus .com Domain", "ET INFO DYNAMIC_DNS Query to a *.taco-land .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ut .com Domain", "ET WEB_CLIENT Possible Javascript obfuscation using app.setTimeOut in PDF in Order to Run Code", "ET INFO DYNAMIC_DNS Query to a *.cleansite .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.technopagans .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homelinuxserver .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ct .com Domain", "ET WEB_CLIENT Hex Obfuscation of Script Tag %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blizzie .net Domain", "ET INFO DYNAMIC_DNS Query to a *.inkcat .net Domain", "ET POLICY HTTP traffic on port 443 (TRACE)", "ET INFO DYNAMIC_DNS Query to a *.rundis .com Domain", "ET POLICY Vulnerable Java Version 1.5.x Detected", "ET INFO DYNAMIC_DNS Query to a *.shadir

	.com Domain", "ET INFO DYNAMIC_DNS Query to a *.4dq .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cleansite .biz Domain", "ET INFO Observed Anonymous File Sharing Service Domain (send .vis .ee in TLS SNI)", "ET POLICY DNS Query to DynDNS Domain *.freedynamicdns .net", "ET INFO File Sharing Domain in DNS Lookup (drive .protonmail .com)", "ET INFO DYNAMIC_DNS Query to a *.keriss .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.usajusaj .org Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.gdn)", "ET HUNTING Observed DNS Query for EmerDNS TLD (.emc)", "ET INFO DYNAMIC_DNS HTTP Request to a *.abc92 .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.thetrist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.orienta .com .br Domain", "ET INFO ZeroTier Related Activity (udp)", "ET INFO DYNAMIC_DNS HTTP Request to a *.pointto .us Domain", "ET WEB_SERVER HTTP Request to a *.33db9538.com domain - Anuna Checkin - Compromised PHP Site", "ET USER_AGENTS Observed Suspicious UA (Client)", "ET INFO DYNAMIC_DNS Query to a *.bien .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.synoserver .com Domain", "ET INFO DYNAMIC_DNS Query to a *.adepoju .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-wiki .com Domain", "ET USER_AGENTS User-Agent (Internet Explorer)", "ET INFO Obfuscated Split String (Single Q) 12", "ET INFO Commonly Abused File Sharing Domain in DNS Lookup (ftpupload .net)", "ET INFO DYNAMIC_DNS Query to a *.essexregional .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pogramkran .net Domain", "ET INFO DYNAMIC_DNS Query to a *.raspberryip .com Domain", "ET HUNTING Suspicious GET Request for .i686 File", "ET INFO DYNAMIC_DNS Query to a *.baselinux .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-at-home .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mrbonus .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.justdied .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeunix .net Domain", "ET WEB_CLIENT Hex Obfuscation of charCodeAt %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.jmstudios .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.autoprin .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.syntereo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bizis .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.verymad .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jonward .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.suns .si Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-green .com Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.dnsalias.ru Domain", "ET INFO DYNAMIC_DNS Query to a *.17ping .cn Domain", "ET INFO DYNAMIC_DNS Query to a *.fairuse .org Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class B64 encoded class", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ok .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (V3LU9iam) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.ruok .org Domain", "ET INFO SUSPICIOUS Java Request to Afraid.org Top 100 Dynamic DNS Domain", "ET INFO DYNAMIC_DNS Query to a *.from-nv .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tobuy .us Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies/Firefox_)", "ET INFO DYNAMIC_DNS Query to a *.aeroantenna .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webqi .org Domain", "ET INFO DYNAMIC_DNS Query to a *.is-certified .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-player .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-nascarfan .com Domain", "ET WEB_CLIENT Hex Obfuscation of Script Tag % Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-teacher .com Domain", "ET POLICY NSecSoft Remote Monitoring Update/Download Activity M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.smlsoft .com Domain", "ET HUNTING SUSPICIOUS OVH Shared Host SSL Certificate (Observed In Use by Some Trojans)", "ET WEB_SERVER SQL Errors in HTTP 500 Response (mysql_query)", "ET INFO DYNAMIC_DNS HTTP Request to a *.worse-than .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myz .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-doctor .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.baikabibai .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.scrapping .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.doomdns .org Domain", "ET HUNTING Suspicious

	User-Agent (Mozilla/5.0_)", "ET INFO DYNAMIC_DNS Query to a *.iwantthisjunk .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.recyclesolutionsllc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zsh .jp Domain", "ET INFO DYNAMIC_DNS Query to a *.free-pic .org Domain", "ET INFO Dotted Quad Host M4 (noalert)", "ET INFO DYNAMIC_DNS Query to a *.horng-bin .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.senaputra .com Domain", "ET POLICY DNS Query to DynDNS Domain *.mysecuritycamera .net", "ET INFO DYNAMIC_DNS Query to a *.mypicture .info Domain", "ET POLICY SMB Remote AT Scheduled Job Pipe Creation", "ET INFO DYNAMIC_DNS Query to a *.tworiverssoftware .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.soundcast .me Domain", "ET POLICY SMB NT Create AndX Request For a Powershell .ps1 File", "ET INFO DYNAMIC_DNS HTTP Request to *.athersite.com Domain (Sitelutions)", "ET JA3 HASH - Possible RustyBuer Client Activity", "ET INFO DYNAMIC_DNS Query to a *.3dxtras .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iiiii .info Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (YXJ0LVByb2N) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.mikata .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.majoitus .ee Domain", "ET POLICY SMB NT Create AndX Request For a DLL File", "ET INFO DYNAMIC_DNS Query to a *.motoretta .ca Domain", "ET INFO Embedded Executable File in PDF - This Program Cannot Be Run in DOS Mode", "ET INFO DYNAMIC_DNS Query to a *.gets-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsdojo .com Domain", "ET INFO Dotted Quad Host XLS Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.ssott .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dns-free.ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onthewifi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lettersandscience .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-cubicle-slave .com Domain", "ET USER_AGENTS Observed Suspicious UA (DxD)", "ET HUNTING .exec in HTTP URI Inbound - Possible Exploit Activity", "ET INFO DYNAMIC_DNS Query to a *.issmarterthanyou .com Domain", "ET INFO DYNAMIC_DNS Query to a *.daev .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.ozziesworld .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homelinux .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ilovecollege .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.happyrobotics .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ygto .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.galipan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.faqserv .com Domain", "ET HUNTING Possible REvil 0day Exploitation Activity Inbound", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrbasic.com Domain", "ET INFO DYNAMIC_DNS Query to a *.franchisecandidates .com Domain", "ET HUNTING Observed Suspicious Reversed String Inbound (Powershell)", "ET INFO DYNAMIC_DNS Query to a *.sceniconline .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mobile-node .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blogdns .com Domain", "ET POLICY DNS Query to .onion proxy Domain (bonytor.com)", "ET POLICY DNS Query to .onion proxy Domain (jamator.com)", "ET INFO SUSPCIOUS Non-standard base64 charset used for encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.oviivory .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sbinfo .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.chan)", "ET HUNTING Suspicious Windows Commands in POST Body (net config)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ttkacz .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rundis .com Domain", "ET INFO DYNAMIC_DNS Query to a *.freetcp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zyix .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.null)", "ET INFO Suspicious Domain (*.gq) in TLS SNI", "ET INFO DYNAMIC_DNS Query to a *.appswiss .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isa-geek .net Domain", "ET INFO DYNAMIC_DNS Query to a *.triviem .cl Domain", "GPL ATTACK_RESPONSE id check returned apache", "ET INFO DYNAMIC_DNS Query to a *.antrak .org .tr Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onmypc .info Domain", "ET INFO DYNAMIC_DNS Query to a *.ralphs .com .au Domain", "ET INFO DYNAMIC_DNS Query to a *.bnene .com Domain", "ET HUNTING SUSPICIOUS Possible

	automated connectivity check (www.bing.com)", "ET INFO DYNAMIC_DNS Query to a *.buys .ru Domain", "ET POLICY Possible HTA Application Download", "ET HUNTING Generic IOT Downloader Malware in GET (Inbound)", "ET INFO DYNAMIC_DNS HTTP Request to a *.annaffiare .org Domain", "ET POLICY Suspicious File Sharing Domain in DNS Lookup (drive .cloudplus .one)", "ET INFO DNS Query for Suspicious .cz.cc Domain", "ET POLICY DNS Query to .onion proxy Domain (onion. sx)", "ET HUNTING NOP Sled in HTTP URI Inbound - Possible Exploit Activity", "ET INFO SUSPICIOUS UA starting with Mozilla/7", "ET INFO DYNAMIC_DNS HTTP Request to a *.evils .in Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lflinkup .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.francemacau .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.work .gd Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.networkindia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-anarchist .com Domain", "ET WEB_CLIENT Obfuscated Javascript // ptth", "ET INFO DYNAMIC_DNS Query to a *.forss .to Domain", "ET INFO DYNAMIC_DNS Query to a *.toh .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.freeddns .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alfa145 .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Accessing Importing glassfish", "ET INFO DYNAMIC_DNS Query to a *.unibutton .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tombu .net Domain", "ET INFO DYNAMIC_DNS Query to a *.yiff .fi Domain", "ET POLICY DNS Query to DynDNS Domain *.servep2p .com", "ET INFO DYNAMIC_DNS Query to a *.strangled .net Domain", "ET POLICY DNS Query to DynDNS Domain *.zapto .org", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-work .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jetos .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.endofinternet .net Domain", "ET INFO DYNAMIC_DNS Query to a *.bigmoney .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.eolicatalinay .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.24x7 .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homelinux .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypets .ws Domain", "ET INFO DYNAMIC_DNS Query to a *.tenspot .net Domain", "ET INFO URL Shortening/Redirect Service Domain (clik .rip in TLS SNI)", "ET POLICY DNS Query to .onion proxy Domain (torforlove.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.strangled .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sheepindonesia .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.otzo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.klipp .su Domain", "ET INFO DYNAMIC_DNS Query to a *.from-nc .com Domain", "ET INFO External IP Lookup Domain in DNS Lookup (ipwho .is)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dubya .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.us .to Domain", "ET HUNTING Base64 Encoded Server Response (success)", "ET INFO DYNAMIC_DNS HTTP Request to a *.krnc .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.mrcork .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-wy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.railpage .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blinklab .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ryanandjen .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.erotikload .at Domain", "ET INFO DYNAMIC_DNS Query to a *.onedumb .com Domain", "ET INFO DYNAMIC_DNS Query to a *.gally .jp Domain", "ET INFO DYNAMIC_DNS Query to a *.tehlab .org Domain", "ET INFO DYNAMIC_DNS Query to a *.mudchute .com Domain", "ET WEB_SERVER Possible SQLi xp_cmdshell POST body", "ET DNS DNS Lookup for localhost.DOMAIN.TLD", "ET INFO Observed Anonymous File Sharing Service (fromsmash .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.motorwisemechanical .com .au Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.03c8 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.is-not-certified .com Domain", "ET SCAN StarDotStar HELO, suspected AUTH LOGIN botnet", "ET INFO DYNAMIC_DNS Query to a *.lessmiths .com Domain", "ET INFO DYNAMIC_DNS Query to a *.boldlygoingnowhere .org Domain", "ET INFO DNS Query for Suspicious .gq Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.contem .bz Domain", "ET INFO DYNAMIC_DNS Query to a *.anpmech .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.stufftoread .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.from-co .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.huepfler .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iii .cl Domain", "ET POLICY DNS Query to DynDNS Domain *.quicksytes .com", "ET INFO DYNAMIC_DNS Query to a *.actsministries .org Domain", "ET INFO Dotted Quad Host DOCX Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveblog .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.skc .su Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-blogger .com Domain", "ET INFO DYNAMIC_DNS Query to a *.firesidegrillandbar .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jade-hamburg .de Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-landscaper .com Domain", "ET INFO DYNAMIC_DNS Query to ath .cx Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xevna .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sosfuvos .net Domain", "ET POLICY DNS Query to DynDNS Domain *.myactivedirectory .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.root .sx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kreider .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sells-for-u .com Domain", "ET INFO DYNAMIC_DNS Query to a *.getamonkey .com Domain", "ET USER_AGENTS Suspicious User-Agent (Installed OK)", "ET INFO DYNAMIC_DNS Query to a *.trumpetx .net Domain", "ET MALWARE DNS query for Morto RDP worm related domain jaifr.com", "ET INFO DYNAMIC_DNS Query to a *.ham .gd Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servebbs .org Domain", "ET INFO DYNAMIC_DNS Query to a *.alanbrothers .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveris .id .lv Domain", "ET INFO HTTP Request to a *.eu.tf domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.btbtrading .it Domain", "ET WEB_CLIENT Possible %u UTF-16 Encoded Iframe Tag", "ET INFO DYNAMIC_DNS Query to a *.leitud .ee Domain", "ET INFO DYNAMIC_DNS Query to a *.bucu .pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.trickip .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.morganisageek .org Domain", "ET INFO DYNAMIC_DNS Query to a *.maya .se Domain", "ET INFO DYNAMIC_DNS Query to a *.iownyour .biz Domain", "ET INFO m68k File Download Request from IP Address", "ET INFO DYNAMIC_DNS Query to a *.dnsfailover .net Domain", "ET INFO DYNAMIC_DNS Query to a *.rren .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thomastech .net Domain", "ET ATTACK_RESPONSE Bash Script Inbound - Kill Coin Mining Related Processes", "ET INFO DYNAMIC_DNS HTTP Request to a *.poormanscow .com Domain", "ET INFO DYNAMIC_DNS Query to a *.truckstore .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.merseine .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.simple-url .com Domain", "ET INFO DYNAMIC_DNS Query to a *.benjamin .it Domain", "ET WEB_SERVER WebShell Generic - wget http - POST", "ET INFO External IP Lookup (keycdn .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynamai .com Domain", "ET INFO DYNAMIC_DNS Query to a *.iugaming .com Domain", "ET INFO DYNAMIC_DNS Query to *findhere.org Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to *.myredirect.us Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.dyndns-pics .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cybertv .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.donhoo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.etitrans .com Domain", "ET USER_AGENTS Suspicious User-Agent (REBOL)", "ET INFO DYNAMIC_DNS Query to a *.isasecret .com Domain", "ET INFO DYNAMIC_DNS Query to a *.siasolution .com Domain", "ET USER_AGENTS Suspicious User-Agent (Windows 10)", "ET INFO DYNAMIC_DNS HTTP Request to a *.home .kg Domain", "ET INFO DYNAMIC_DNS Query to a *.ve3 .info Domain", "ET HUNTING Possible ELF executable sent when remote host claims to send a Text File", "ET INFO DYNAMIC_DNS Query to a *.networkindia .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ftpserver .biz Domain", "ET HUNTING Generic IOT Downloader Malware in GET (Outbound)", "ET INFO DYNAMIC_DNS Query to a *.dtdns.net Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.bbs)", "ET INFO DYNAMIC_DNS Query to a *.dpo .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bnene .com Domain", "ET JA3 HASH - DeimosC2 Agent Activity", "ET INFO ARM File Download Request from IP Address", "ET INFO DYNAMIC_DNS HTTP Request to a *.barvennon .com Domain", "ET INFO

	DYNAMIC_DNS HTTP Request to a *.zipper-maker .com Domain", "ET INFO Observed DNS Query to .life TLD", "ET HUNTING Observed TinyNuke Admin Panel URL Pattern", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ky .com Domain", "ET INFO DYNAMIC_DNS Query to a *.16-b .it Domain", "ET INFO DYNAMIC_DNS Query to a *.fido .be Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-democrat .com Domain", "ET INFO Suspicious Shellcode Request", "ET INFO DYNAMIC_DNS Query to a *.cloudranger .net Domain", "ET HUNTING Request to .XYZ Domain with Minimal Headers", "ET INFO Observed File Sharing Domain (roamresearch .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.alphasoft .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns .ws Domain", "ET INFO DYNAMIC_DNS Query to a *.hs .vc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homesecuritypc .com Domain", "GPL TELNET Bad Login", "ET INFO DYNAMIC_DNS HTTP Request to a *.salty72 .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.donlafferty .net Domain", "ET POLICY HTTP Request to a *.be.ma domain", "ET INFO DYNAMIC_DNS Query to a *.verymad .net Domain", "GPL ATTACK_RESPONSE id check returned nobody", "ET INFO DYNAMIC_DNS Query to a *.rwbcode .com Domain", "ET POLICY PDF With Embedded File", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns .org Domain", "ET INFO Query for Suspicious .gr.com Domain (gr .com in DNS Lookup)", "ET INFO DYNAMIC_DNS HTTP Request to a *.homingbeacon .net Domain", "ET INFO DYNAMIC_DNS Query to a *.abuser .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.intec .es Domain", "ET INFO DYNAMIC_DNS Query to a *.blizzie .net Domain", "ET INFO DYNAMIC_DNS Query to a *.make .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.radioimpactfm .ro Domain", "ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M2", "ET INFO DYNAMIC_DNS Query to a *.callmark .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mynetav .com Domain", "ET INFO DYNAMIC_DNS Query to a *.herbalhealthyh20 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-az .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homelinux .com Domain", "ET INFO Observed SyncroMSP Remote Management Software Domain in DNS Lookup (repairshopr .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.lain .ch Domain", "ET POLICY DNS Query to .onion proxy Domain (tor2pay.com)", "ET INFO DYNAMIC_DNS Query to a *.ext .io Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing jmx mbeanserver", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-republican .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.on-the-web .tv Domain", "ET WEB_CLIENT Base64 Encoded Java Value", "ET INFO DYNAMIC_DNS HTTP Request to *.myredirect.us Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-la .net Domain", "ET INFO DYNAMIC_DNS Query to a *.tien-shan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.boxathome .net Domain", "ET INFO DYNAMIC_DNS Query to a *.calvaryduncan .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.socalfishkillaz .com Domain", "ET INFO DYNAMIC_DNS Query to a *.game-host .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.possessed .us Domain", "ET WEB_SERVER SQL Errors in HTTP 500 Response (SqlException)", "ET INFO DYNAMIC_DNS Query to a *.dnsking .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.otzo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ubergate .com Domain", "ET INFO DYNAMIC_DNS Query to a *.swphoa .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.3cm .us Domain", "ET HUNTING Observed Suspicious Request nc.exe in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.alanbrothers .com Domain", "ET INFO DYNAMIC_DNS Query to a *.station .moe Domain", "ET INFO DYNAMIC_DNS Query to a *.pushitlive .net Domain", "ET INFO DYNAMIC_DNS Query to a *.keybusinessconnection .com Domain", "ET WEB_SERVER WebShell Generic - net user", "ET INFO DYNAMIC_DNS HTTP Request to a *.horng-bin .com Domain", "ET INFO DYNAMIC_DNS Query to a *.xxxxx .tw Domain", "ET INFO Observed Chocolatey Windows Package Management Domain (chocolatey .org in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-accountant .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ber-engineering .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (V3LU9) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.onmypc .org

	Domain", "ET INFO DYNAMIC_DNS Query to a *.georgiagun .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cbu .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pakasak .com Domain", "ET INFO HTTP Request to a *.surf domain", "ET WEB_CLIENT Hex Obfuscation of substr % Encoding", "ET USER_AGENTS Suspcious LeakIX User-Agent (l9explore)", "ET INFO DYNAMIC_DNS Query to a *.almostmy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xxuz .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.powermotors .com .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hondascooterparts .com Domain", "ET INFO DYNAMIC_DNS Query to a *.senaputra .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sly .io Domain", "ET INFO Observed Lets Encrypt Certificate for Suspicious TLD (.top)", "ET INFO DYNAMIC_DNS Query to a *.whatajack .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-very-bad .org Domain", "ET POLICY DNS Query to .onion proxy Domain (torpaycnf.com)", "ET INFO DYNAMIC_DNS Query to a *.inet2 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.netlord .de Domain", "ET POLICY HTTP Request to a *.dlinkddns.com domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-techie .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ubntddns .com Domain", "ET INFO POWERPC File Download Request from IP Address", "ET INFO DYNAMIC_DNS HTTP Request to a *.xxxy .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.smh .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.skies .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to Abused Domain *.mooo.com", "ET POLICY NSecSoft Remote Monitoring Update/Download Activity M1", "ET HUNTING Suspicious Terse Request for .bmp", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveuser .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tinosmarble .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bine .me Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-photographer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webhop .info Domain", "ET POLICY Possible winexe over SMB - Possible Lateral Movement", "ET INFO Observed IP Tracking Domain (grabify .link in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.vlad .md Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lospenitentes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.donlafferty .net Domain", "ET INFO DYNAMIC_DNS Query to a *.letz .dev Domain", "ET INFO DYNAMIC_DNS Query to a *.francemacau .com Domain", "ET INFO Observed File Sharing Domain (www .cloudme .com in TLS SNI)", "ET HUNTING SUSPICIOUS Excel Add-in Download M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.8bit .ca Domain", "ET INFO Observed Abused Website Archival Domain in DNS Lookup (archive .ph)", "ET INFO DYNAMIC_DNS HTTP Request to a *.masplene .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.htpc .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.sexxxy .biz Domain", "ET USER_AGENTS Observed Suspicious UA (Http-connect)", "ET INFO DYNAMIC_DNS Query to a *.womenclothingtoday .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.appswiss .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.thruhere .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dream .org .il Domain", "ET INFO DYNAMIC_DNS Query to a *.kidsqt .com Domain", "ET INFO Obfuscated Split String (Double Q) 3", "ET INFO DYNAMIC_DNS Query to a *.docuprint .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.hec .to Domain", "ET INFO DYNAMIC_DNS Query to a *.progressivecongressnews .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.trumpetx .net Domain", "ET INFO DYNAMIC_DNS Query to a *.lovethosetrains .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-into-cartoons .com Domain", "ET INFO DYNAMIC_DNS Query to a *.doesntexist .org Domain", "ET INFO DYNAMIC_DNS Query to a *.aksnapshots .com Domain", "ET POLICY Potentially Vulnerable LibSSH Server Observed - Possible Authentication Bypass (CVE-2018-10933)", "ET INFO DYNAMIC_DNS Query to a *.is-a-llama .com Domain", "ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.bloom .us Domain", "ET INFO DYNAMIC_DNS Query to a *.kmodem .org Domain", "ET INFO DYNAMIC_DNS Query to a *.is-an-engineer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.selfip .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.macrofox .org Domain", "ET HUNTING SSL/TLS Certificate Observed (OpenNIC Project API)", "ET INFO DYNAMIC_DNS Query to a

	Suspicious *.dyndns-web.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-mn .com Domain", "ET MALWARE Potential Blackhole Exploit Pack Binary Load Request", "ET INFO HTTP Request to a *.ca.tf domain", "ET USER_AGENTS Suspicious User Agent (KtulhuBrowser)", "ET WEB_SERVER WebShell - MySQL Interface - Auth Prompt", "ET INFO DYNAMIC_DNS HTTP Request to a *.spottt .com Domain", "ET USER_AGENTS Observed Suspicious UA (cctv.mtv)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dleon .cl Domain", "ET INFO Dotted Quad Host VBS Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.scorm .gr Domain", "ET POLICY DNS Query to DynDNS Domain *.onthewifi .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.aksnapshots .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mydissent .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.china .is Domain", "ET INFO DYNAMIC_DNS Query to a *.is-an-artist .com Domain", "ET POLICY File Shared via Zoom", "ET INFO DYNAMIC_DNS HTTP Request to a *.rebol .info Domain", "ET INFO Observed Bablosoft BAS Related SSL Cert (bablosoft .com)", "ET INFO DYNAMIC_DNS Query to a *.shitcunt .info Domain", "ET POLICY DNS Query to .onion proxy Domain (slavetor.com)", "ET INFO DYNAMIC_DNS Query to a *.yasser .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsget .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tomahawkchurch .org Domain", "ET INFO DYNAMIC_DNS Query to a *.baden .ru Domain", "ET INFO HTTP Request to Suspicious *.life Domain", "ET MALWARE Possible Ponmocup Driveby Download", "ET INFO DYNAMIC_DNS Query to a *.mediatriumph .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.antiphone .net Domain", "ET INFO URL Shortening Service Domain in TLS SNI (coki .me)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns .ws Domain", "ET INFO DYNAMIC_DNS Query to a *.fhi .hk Domain", "ET INFO URL Shortening Service Domain in DNS Lookup (s3r .io)", "ET INFO DYNAMIC_DNS HTTP Request to a *.vxe6 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.empires-r .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.truckstore .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.heatmypool .com Domain", "ET INFO DYNAMIC_DNS Query to a *.iceage .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.prs7 .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-co .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ms .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sibmed .org .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.shen .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.mrslove .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ikoona .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mine .nu Domain", "ET INFO DYNAMIC_DNS Query to a *.is-saved .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dsmtp .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dade .si Domain", "ET INFO DYNAMIC_DNS Query to a *.ddns .mobi Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kirelli .net Domain", "ET POLICY Vulnerable Java Version 9.0.x Detected", "ET WEB_CLIENT PDF Name Representation Obfuscation of Action", "ET INFO DYNAMIC_DNS Query to a *.z0d .eu Domain", "ET HUNTING Possible Powershell .ps1 Script Use Over SMB", "ET INFO DYNAMIC_DNS Query to a *.gnutella2 .info Domain", "ET INFO Observed Abused Website Archival Domain (archive .ph in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.isteingeek .de Domain", "ET POLICY HTTP traffic on port 443 (PROPFIND)", "ET INFO DYNAMIC_DNS Query to a *.jake .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.lozan .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.slyip.net Domain", "ET INFO DYNAMIC_DNS Query to a *.bgg .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shadir .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mp3real .ru Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.dnsip.ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ri .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.loginto .me Domain", "ET JA3 HASH - Possible Rclone Client Activity", "ET INFO DYNAMIC_DNS Query to a *.moabphoto .com Domain", "ET INFO DYNAMIC_DNS Query to a *.qthome .org Domain", "ET POLICY BSSID Location Lookup via api .mylnikov .org", "ET HUNTING Suspicious GET Request for .arm file File", "ET INFO DYNAMIC_DNS HTTP Request to a *.merrittcredit .com Domain", "ET INFO DYNAMIC_DNS Query to a *.toythieves .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chaseinator .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.andreymorozov .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.forgot .her .name Domain", "ET INFO DYNAMIC_DNS Query to a *.alanrjr .net Domain", "ET INFO Cloud File Sharing Domain in DNS Lookup (.filebase .io)", "ET INFO DYNAMIC_DNS HTTP Request to a *.klipp .su Domain", "ET INFO DYNAMIC_DNS Query to a *.mynetav .net Domain", "ET INFO External IP Lookup Domain Domain in DNS Lookup (ipbase .com)", "ET INFO DYNAMIC_DNS Query to a *.kanda .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.jpleventos .cl Domain", "ET POLICY DNS Query to .onion proxy Domain (pay2tor.com)", "ET INFO DYNAMIC_DNS Query to a *.sells-for-less .com Domain", "ET EXPLOIT Cisco Smart Install Exploitation Tool - Update Ios and Execute", "ET INFO DYNAMIC_DNS HTTP Request to a *.darktech.org Domain", "ET INFO DYNAMIC_DNS Query to a *.better-than .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sandcherrysystems .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hunnur .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mrbasic.com Domain", "ET HUNTING Powershell Request for paste .ee Page", "ET INFO DYNAMIC_DNS HTTP Request to a *.fearpenguins .com Domain", "ET INFO DYNAMIC_DNS Query to a *.opaline .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.ppalma .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.monkeywerks .net Domain", "ET INFO DYNAMIC_DNS Query to a *.ufodns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.k4w411 .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-hard-worker .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.videounlimit .com Domain", "ET INFO DYNAMIC_DNS Query to a *.forumz .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nv .com Domain", "ET POLICY Observed DNS Query to File Transfer Service Domain (transfer .sh)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-server .com Domain", "ET HUNTING Request to .TOP Domain with Minimal Headers", "ET INFO DYNAMIC_DNS Query to a *.scorm .gr Domain", "ET INFO DYNAMIC_DNS Query to a *.blogdns .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torprivatebrowsing.org)", "ET INFO DYNAMIC_DNS Query to a *.kitayori .cl Domain", "ET POLICY DNS Query to DynDNS Domain *.servesarcasm .com", "ET INFO DYNAMIC_DNS Query to a *.netlord .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thetrist .com Domain", "ET HUNTING Suspicious Domain Request for Possible COVID-19 Domain M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.klockars .com Domain", "ET POLICY HTTP Request to a *.ae.am domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lozan .com Domain", "ET POLICY SMB2 NT Create AndX Request For a .sys File - Possible Lateral Movement", "ET INFO URL Shortener Service Domain in DNS Lookup (yourls .org)", "ET INFO DYNAMIC_DNS Query to a *.zanity .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.navigogroup .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.demoteam .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.monobasin .net Domain", "ET INFO HTTP Request to a *.ml domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-libertarian .com Domain", "ET INFO HTTP Request to a *.pl.tf domain", "ET INFO DYNAMIC_DNS Query to a *.lanas .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.entermypicks .com Domain", "ET WEB_SERVER PHP COOKIE SuperGlobal in POST", "ET USER_AGENTS Observed Suspicious UA (justupdate)", "ET INFO DYNAMIC_DNS Query to a *.is-a-designer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.angellombardi .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.n43 .pw Domain", "ET POLICY SN and CN From MS TS Revoked Cert Chain Seen", "ET INFO Observed DNS Query to DDNS Domain .myfirewall .org", "ET INFO DYNAMIC_DNS HTTP Request to a *.ctx .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.roth .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.audolatry .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jharrigan .net Domain", "ET INFO HTTP Connection To DDNS Domain Adultdns.net", "ET INFO DYNAMIC_DNS Query to a *.stuns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.port0 .org Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.icu)", "ET INFO DYNAMIC_DNS HTTP Request to a *.centralpto .com Domain", "ET INFO DYNAMIC_DNS Query to a *.servegame .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pintravel .ro Domain", "ET INFO DYNAMIC_DNS Query to a *.isa-geek .net Domain", "ET INFO HTTP Request to a .noip.cn domain", "ET

	INFO DYNAMIC_DNS Query to a *.winkel .com .ar Domain", "ET INFO DNS Query to a Suspicious *.orge.pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.green-heroes .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mypop3 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.yao .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.est-a-la-masion .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns .info Domain", "ET INFO DYNAMIC_DNS Query to a *.bloom .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.earlyriserscoffeeshop .com Domain", "GPL FTP tar parameters", "ET INFO DYNAMIC_DNS HTTP Request to a *.sandhofner .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hs .vc Domain", "ET HUNTING Suspicious POST Format", "ET INFO DYNAMIC_DNS Query to a *.geekhardware .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (52b2tlLVdtaU1) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.shakedfamily .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-wiki .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.awiki .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wildsurf .net Domain", "ET INFO DYNAMIC_DNS Query to a *.industrialmill .com Domain", "ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Server Init Vuln Client)", "ET INFO DYNAMIC_DNS HTTP Request to a *.fxnxs .com Domain", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (2b2tlLVJlc3RNZX) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.project .li Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.breakingpar .com Domain", "ET WEB_CLIENT Hex Obfuscation of arguments.callee %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.yhoccotruyen .org Domain", "ET MALWARE Observed DNS Query to Known PUA Host Domain", "ET INFO Dotted Quad Host PPTX Request", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.icu)", "ET INFO DYNAMIC_DNS HTTP Request to a *.66haoyun .com Domain", "ET INFO Obfuscated Split String (Single Q) 1", "ET INFO DYNAMIC_DNS HTTP Request to a *.jungleheart .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.paranormalgroup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.florafamily .com Domain", "ET INFO DYNAMIC_DNS Query to a *.worse-than .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servep2p .com Domain", "ET USER_AGENTS Suspicious User-Agent (Windows XP)", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (YXJ0LVByb2Nlc3) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.hijaxdesigns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dotbot .us Domain", "ET MALWARE DNS query for Morto RDP worm related domain jifr.info", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-geek .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.game-server .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-nurse .com Domain", "ET INFO DYNAMIC_DNS Query to a *.yourspecialtee .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.novgaz-rzn .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sells-for-less .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.indy)", "ET INFO HTTP Connection To DDNS Domain Zapto.org", "ET INFO DYNAMIC_DNS Query to a *.corum .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ddnslive .com Domain", "ET INFO DYNAMIC_DNS Query to a *.my .to Domain", "ET INFO SUSPICIOUS Java Request to DNSDynamic Dynamic DNS Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.operationbim .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shaqnet .nu Domain", "ET HUNTING SUSPICIOUS *.doc.exe in HTTP URL", "ET INFO DYNAMIC_DNS Query to a *.mynetav .org Domain", "ET INFO File Retrieved from File Sharing Site (cloudme .com)", "ET INFO SQLite DLL Retrieval by Name (GET)", "ET HUNTING SUSPICIOUS XXTEA UTF-16 Encoded HTTP Response", "ET INFO DYNAMIC_DNS HTTP Request to a *.ax .lt Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.n-e-t .name Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tallison .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cloudns .net Domain", "ET HUNTING SUSPICIOUS *.rar.exe in HTTP URL", "ET INFO DYNAMIC_DNS Query to a *.gsp .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shareroute .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jcor .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sleeperkidsworld

	.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.milk .is Domain", "ET INFO DYNAMIC_DNS Query to a *.est-mon-blogueur .com Domain", "GPL ATTACK_RESPONSE id check returned root", "ET INFO DYNAMIC_DNS Query to a *.from-ky .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bagus .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.caminobooks .com Domain", "ET POLICY DNS Query to DynDNS Domain *.freedynamicdns .org", "ET INFO DNS Query for a Suspicious *.cu.cc domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-uberleet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ditchyourip .com Domain", "ET POLICY SMB2 NT Create AndX Request For a Powershell .ps1 File", "ET WEB_CLIENT FakeAV scanner page encountered Initializing Virus Protection System", "ET INFO DYNAMIC_DNS HTTP Request to a *.now-dns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wwwhost .us Domain", "ET INFO DYNAMIC_DNS Query to a *.gettrials .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-an-anarchist .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torjam.com)", "ET INFO Non Standard Port DNS Query to google .com (udp)", "ET INFO DYNAMIC_DNS HTTP Request to a *.eolicatalinay .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ar .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.darvin .one .pl Domain", "ET POLICY DNS Query to DynDNS Domain *.hopto .me", "ET INFO DYNAMIC_DNS Query to a *.notici .as Domain", "ET INFO DYNAMIC_DNS Query to a *.ignorelist .com Domain", "ET INFO DYNAMIC_DNS Query to a *.h0stname .net Domain", "ET INFO DYNAMIC_DNS Query to a *.coolfire25 .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.dyn)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-web.com Domain", "ET INFO DYNAMIC_DNS Query to a *.silksky .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mywww .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.parikh .net Domain", "ET INFO DYNAMIC_DNS Query to a *.sexmistrz .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.g33k .com .ve Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lqtai .com Domain", "ET INFO HTTP POST Request to Suspicious *.ml Domain", "ET INFO DYNAMIC_DNS Query to a *.hectorhector .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zanity .net Domain", "ET INFO DYNAMIC_DNS Query to a *.n0p .at Domain", "ET INFO DYNAMIC_DNS Query to a *.gentile .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ftpaccess .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynalias .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mcsoft .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dynip .org Domain", "ET MALWARE [PTsecurity] Possible Trojan.Downloader UserAgent (binary_getter)", "ET INFO PSRC Powershell File Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.okzk .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.malam .or .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.humorvisite .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.liquidsphere .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pwm .hu Domain", "ET INFO DYNAMIC_DNS Query to a *.img .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.caminobooks .com Domain", "ET INFO Suspected Phishing Simulation Related Request (GET)", "ET INFO DYNAMIC_DNS HTTP Request to a *.shekinahphotography .com Domain", "ET HUNTING GET Request to Pastebin .com with PowerShell User-Agent", "ET INFO DYNAMIC_DNS HTTP Request to a *.aen .su Domain", "ET HUNTING Suspicious SSL Certificate detected (Observed in US Government Bid Credential Phish)", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.xyz)", "ET INFO DYNAMIC_DNS HTTP Request to a *.furryplace .eu Domain", "ET SCAN MySQL Malicious Scanning 2", "ET INFO Observed DNS Query to Commonly Abused Preview Domain (preview-domain .com)", "ET INFO DYNAMIC_DNS Query to a *.dyn .mk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.peeinthesnow .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsalias .com Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (SqlException)", "ET INFO DYNAMIC_DNS Query to a *.ldtp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lflinkup .net Domain", "ET INFO Executable Served From /tmp/ Directory - Malware Hosting Behaviour", "ET INFO DYNAMIC_DNS HTTP Request to a *.ayso795 .org Domain", "ET WEB_CLIENT Hex Obfuscation of parseInt %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS Query to a *.ninth .biz Domain", "ET INFO DYNAMIC_DNS HTTP

	Request to a *.ismoke .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zapto .org Domain", "ET INFO HTTP Request to a *.us.tf domain", "ET INFO File Sharing Domain in DNS Lookup (roamresearch .com)", "ET INFO URL Shortening Service Domain in DNS Lookup (n9 .cl)", "ET INFO DYNAMIC_DNS Query to a *.is-an-actress .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ideas-informatica .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.barratella .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sen .org .nz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yourvaluedhomes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.changeip .net Domain", "ET INFO Observed DNS Query to .biz TLD", "ET INFO DYNAMIC_DNS HTTP Request to a *.mascarenhas .inf .br Domain", "ET INFO DYNAMIC_DNS Query to a *.memoryguide .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.18t .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.novgaz-rzn .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xxxy .info Domain", "ET INFO HTTP Request to a *.sg.tf domain", "ET HUNTING Request to .ML Domain with Minimal Headers", "ET INFO DYNAMIC_DNS Query to a *.centralpto .com Domain", "ET ATTACK_RESPONSE UTF16-LE base64 string /This Program/ in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.ladatap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sqlizer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.borkar .in Domain", "ET INFO Dotted Quad Host PPT Request", "ET INFO DYNAMIC_DNS Query to a *.encyclopedia .tw Domain", "ET INFO DYNAMIC_DNS Query to a *.sen .org .nz Domain", "ET INFO DYNAMIC_DNS Query to a *.internetzninja .com Domain", "ET POLICY DNS Query to DynDNS Domain *.serveftp .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.unids .com Domain", "ET POLICY DNS Query to DynDNS Domain *.servemp3 .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.wakingmoon .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.v6 .rocks Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.aeroantenna .com Domain", "ET HUNTING Suspicious GET Request with Possible COVID-19 URI M1", "ET INFO DYNAMIC_DNS Query to a *.networkguru .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hioctanefuel .com Domain", "ET POLICY DNS Query to .onion proxy Domain (payrobotor.com)", "ET INFO Observed SyncroMSP Remote Management Software Domain (repairshopr .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dulcegarii-culinare .ro Domain", "ET INFO Possible Firefox Plugin install", "ET INFO DYNAMIC_DNS Query to a *.k22 .su Domain", "ET INFO DYNAMIC_DNS Query to a *.seasol .net Domain", "ET INFO DYNAMIC_DNS Query to a *.freewww .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.opticalize .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.weixservice .com Domain", "ET INFO DYNAMIC_DNS Query to a *.droidtech .it Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (ERROR syntax error at or near)", "ET INFO DYNAMIC_DNS HTTP Request to a *.merseine .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.multicop .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.nethub .fi Domain", "ET INFO DYNAMIC_DNS Query to a *.lai .ac Domain", "ET INFO DYNAMIC_DNS Query to a *.ruok .org Domain", "ET INFO DYNAMIC_DNS Query to a *.devicars .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.doesntexist .com Domain", "ET WEB_CLIENT PDF Name Representation Obfuscation of /Subtype", "ET WEB_SERVER MorXploit Shell Command", "ET INFO DYNAMIC_DNS Query to a *.suns .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ezwebsites .com Domain", "ET HUNTING Base64 Encoded whoami in HTTP Server Response", "ET INFO DYNAMIC_DNS HTTP Request to a *.yao .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.ericfox .hk Domain", "ET USER_AGENTS Suspicious User-Agent (Windows 7)", "ET INFO DYNAMIC_DNS HTTP Request to a *.movdivx .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.bestdeals.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.itemdb .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.icemail .me .uk Domain", "ET WEB_CLIENT Hex Obfuscation of document.write %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS Query to a *.defensoria-nsjp .gob .mx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.https443 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xcportugal .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-wv .com Domain", "ET INFO DYNAMIC_DNS

	HTTP Request to a *.for-the .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.workisboring .com Domain", "ET INFO DYNAMIC_DNS Query to a *.technicalsupportresources .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dekalo .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.americanunfinished .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.compy .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ducklog .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.extramindcorp .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (nZva2UtV21pTWV0aG) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.688 .org Domain", "ET INFO URL Shortening Service Domain in DNS Lookup (gg-l .xyz)", "ET INFO DYNAMIC_DNS Query to a *.cissp .or .id Domain", "ET INFO DYNAMIC_DNS Query to a *.kompaniet .nu Domain", "ET INFO DYNAMIC_DNS Query to a *.mbiselangor .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.medbury .com Domain", "ET POLICY DNS Query to DynDNS Domain *.servecounterstrike .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.starnerd .com Domain", "ET INFO DYNAMIC_DNS Query to a *.onmypc .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sendsmtp .com Domain", "ET HUNTING Possible Covid19 Themed Email Spam Outbound M6", "ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M3", "ET INFO DYNAMIC_DNS HTTP Request to a *.jbworks .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-an-entertainer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.machinezdesign .com Domain", "ET INFO Observed File Sharing Domain (drive .protonmail .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.tumsun .com Domain", "ET HUNTING Suspicious explorer.exe in URI", "ET INFO HTTP Request to Suspicious *.work Domain", "ET INFO DYNAMIC_DNS Query to a *.seprotec .net .br Domain", "ET INFO DYNAMIC_DNS Query to a *.rock-n-roll .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.serveuser .com Domain", "ET MALWARE DNS Query Gauss Domain *.guest-access.net", "ET INFO Commonly Abused File Sharing Domain (filetransfer .io in TLS SNI)", "ET INFO PS1 Powershell File Request", "ET HUNTING curl User-Agent to Dotted Quad", "ET INFO DYNAMIC_DNS Query to a *.dnsdojo .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.zza .pl Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (pgsql_query)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dontexist .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lettersandscience .net Domain", "ET INFO DYNAMIC_DNS Query to a *.xox .mx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-pa .com Domain", "ET INFO DYNAMIC_DNS Query to a *.isyour .guru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.selfip .net Domain", "ET POLICY Tunneled RDP msts Handshake", "ET INFO DYNAMIC_DNS Query to a *.tftpd .net Domain", "ET INFO DYNAMIC_DNS Query to a *.land-4-sale .us Domain", "ET INFO DYNAMIC_DNS Query to a *.xevna .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.roth .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nh .com Domain", "ET INFO DYNAMIC_DNS Query to a *.navnirwana .com Domain", "ET INFO DYNAMIC_DNS Query to *assexyas.com Domain (Sitelutions)", "ET INFO HTTP Connection To DDNS Domain Myvnc.com", "ET INFO DYNAMIC_DNS Query to a *.irfna .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ra3 .us Domain", "ET INFO Observed Remote Management Software Domain (syncromsp .com in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.oitsc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ozziesworld .com Domain", "ET INFO DYNAMIC_DNS Query to a *.stuff-4-sale .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ownip .net Domain", "ET POLICY DNS Query to DynDNS Domain *.mmafan .biz", "ET WEB_CLIENT SEO Injection/Fraud DNS Lookup (count.trackstatisticsss .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.punked .us Domain", "ET INFO DYNAMIC_DNS Query to a *.bearfacts .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.read-books .org Domain", "ET HUNTING Request to .GQ Domain with Minimal Headers", "ET INFO DYNAMIC_DNS HTTP Request to a *.mbiselangor .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ugo .si Domain", "ET INFO DYNAMIC_DNS Query to a *.medbury .com Domain", "ET MALWARE Incorrectly formatted User-Agent string (dashes instead of semicolons) Likely Hostile", "ET POLICY

	DNS Query to DynDNS Domain *.viewdns .net", "ET INFO DYNAMIC_DNS Query to a *.dotbot .us Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.ez-dns.com Domain", "ET INFO DYNAMIC_DNS Query to a *.joe-joubert .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.4040 .idv .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.organiccrap .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.droidtech .it Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.benjamin .it Domain", "ET INFO DYNAMIC_DNS Query to a *.tzafrir .org .il Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.drm .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.selfip .com Domain", "ET INFO DYNAMIC_DNS Query to a *.minecraftnoob .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.seburn .net Domain", "ET INFO DYNAMIC_DNS Query to a *.for-our .info Domain", "ET INFO DYNAMIC_DNS Query to a *.folklandmanagement .com Domain", "ET INFO DNS Query for Suspicious .gdn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.swds .com .au Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-geek .com Domain", "ET MALWARE Double HTTP/1.1 Header Inbound - Likely Hostile Traffic", "ET INFO DYNAMIC_DNS HTTP Request to a *.sqlizer .com Domain", "ET INFO Obfuscated Split String (Double Q) 8", "ET INFO DYNAMIC_DNS Query to a *.ajalo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.logular .com Domain", "ET INFO DYNAMIC_DNS Query to a *.nathan .to Domain", "ET INFO DYNAMIC_DNS Query to a *.hbmc .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.lowestprices.at Domain (Sitelutions)", "ET WEB_SERVER base64_decode in UA", "ET POLICY DNS Query to .onion proxy Domain (tor2www.com)", "ET INFO Dotted Quad Host M2 (noalert)", "ET INFO DYNAMIC_DNS Query to a *.dnsdojo .org Domain", "ET INFO DYNAMIC_DNS Query to a *.vpndns .net Domain", "ET INFO HTTP POST Request to Suspicious *.cf Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.churchrez .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fartit .com Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Chrome_Default.txt)", "ET INFO DYNAMIC_DNS HTTP Request to a *.b0tnet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-tx .com Domain", "ET HUNTING Suspicious POST Request with Possible COVID-19 Domain M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.gracesiefer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.in-the-band .net Domain", "ET INFO DYNAMIC_DNS Query to a *.redsteedstudios .com Domain", "ET INFO DYNAMIC_DNS Query to a *.star .is Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.at-band-camp .net Domain", "ET HUNTING SUSPICIOUS Possible automated connectivity check (www.google.com)", "ET POLICY DNS Query to DynDNS Domain *.securitytactics .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.myddns .biz Domain", "ET POLICY DNS Query to DynDNS Domain *.stufftoread .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.gettrials .com Domain", "ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .scr filename inside", "ET WEB_SERVER Possible Encrypted Webshell in POST", "ET INFO DYNAMIC_DNS HTTP Request to a *.sovich .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-nj .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servebbs .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dcmusic .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.primavera .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tibet .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrgshrimp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.myogaya .jp Domain", "ET INFO DYNAMIC_DNS Query to a *.axfor .com Domain", "ET INFO Anonymous File Sharing Domain in DNS Lookup (fromsmash .co)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ghostnation .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.neat-url .com Domain", "ET INFO DYNAMIC_DNS Query to a *.rainbowcup .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sexcuatui .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.faqserv .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lai .ac Domain", "ET INFO DYNAMIC_DNS Query to *byinter.net Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.gurdit .com Domain", "ET HUNTING Possible Covid19 Themed Email Spam Outbound M2", "GPL ATTACK_RESPONSE file copied ok", "ET POLICY DNS Query to .onion proxy Domain (tanktor.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.getmyip .com Domain", "ET HUNTING Request To Suspicious Filename via Powershell

	(payload)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ssl443 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.byte4byte .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cw03 .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.lotusblossomconsulting .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.heroinewarrior .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iwantthisjunk .com Domain", "ET HUNTING Suspicious GET Request for .arc File", "ET HUNTING URL Shortening Service Used by Curl (ic9 .in)", "ET INFO DYNAMIC_DNS Query to a *.boblove .org Domain", "ET INFO Obfuscated Split String (Double Q) 4", "ET INFO HTTP Request to a *.tc domain", "ET INFO DYNAMIC_DNS Query to a *.nn-foto .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-caterer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isteingeek .de Domain", "ET INFO DYNAMIC_DNS Query to a *.jesus .si Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sumibi .org Domain", "ET INFO Query for a Suspicious *.upas.su domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.smelly .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.recruitment7 .com Domain", "ET INFO Empty POST with Terse Headers Over Non Standard Port", "ET INFO DYNAMIC_DNS HTTP Request to a *.radioimpactfm .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bkpsports .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-lawyer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hepcats .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ftp .sh Domain", "ET WEB_SERVER HTTP Request to a *.54dfa1cb.com domain - Anuna Checkin - Compromised PHP Site", "ET USER_AGENTS Suspicious User-Agent SimpleClient 1.0", "ET INFO DYNAMIC_DNS Query to *atthissite.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.niigeo .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.simple-url .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.geek)", "ET INFO DYNAMIC_DNS Query to a *.pixelfucker .org Domain", "ET HUNTING SUSPICIOUS IRC - NICK and 3 Letter Country Code", "ET INFO DYNAMIC_DNS Query to a *.mnode .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-personaltrainer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.brokenfuture .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.oceanpolice .com Domain", "ET INFO DYNAMIC_DNS Query to a *.farted .net Domain", "ET INFO Observed DNS Query to DDNS Domain .zzux .com", "ET INFO DYNAMIC_DNS Query to *lowestprices Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ignorelist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ps .ai Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onmypc .us Domain", "ET USER_AGENTS Suspicious UA Observed (YourUserAgent)", "ET INFO DYNAMIC_DNS Query to a *.ps .ai Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.usjepor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.elitter .net Domain", "ET INFO DYNAMIC_DNS Query to a *.paulsfamilyhistory .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.photographs .gs Domain", "ET POLICY DNS Query to DynDNS Domain *.fantasyleague .cc", "ET INFO DYNAMIC_DNS Query to a *.govt .hu Domain", "ET INFO DYNAMIC_DNS Query to a *.voltage .nz Domain", "ET INFO DYNAMIC_DNS Query to *isthebe.st Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.aletoledo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lwts .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.earlyriserscoffeeshop .com Domain", "ET INFO Obfuscated Split String (Single Q) 10", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsdyn .net Domain", "ET POLICY DNS Query to DynDNS Domain *.loginto .me", "ET USER_AGENTS Observed Suspicious UA (My Agent)", "ET INFO DYNAMIC_DNS HTTP Request to a *.devicars .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-mo .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.gopher)", "ET INFO HTTP Connection To DDNS Domain Servehttp.com", "ET DNS DNS Query for vpnoverdns - indicates DNS tunnelling", "ET DOS DNS Amplification Attack Possible Outbound Windows Non-Recursive Root Hint Reserved Port", "ET HUNTING Terse Request for .txt - Likely Hostile", "ET INFO DYNAMIC_DNS HTTP Request to a *.joe .dj Domain", "ET INFO DYNAMIC_DNS Query to a *.merrittcredit .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.coreytech .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homeip .net Domain", "ET WEB_CLIENT [Deepend

	Research] BestaBid FakeFlash Redirect", "ET INFO DYNAMIC_DNS HTTP Request to a *.hiddencorner .org Domain", "ET HUNTING Redirect Link in TikTok URL", "ET INFO DYNAMIC_DNS HTTP Request to a *.dhcp .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.studiovk .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.2mydns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.elitter .net Domain", "ET EXPLOIT Cisco Smart Install Exploitation Tool - ChangeConfig", "ET INFO DYNAMIC_DNS Query to a *.krnc .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.e-cloud .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.3d-game.com Domain", "ET INFO DYNAMIC_DNS Query to a *.lee .mx Domain", "ET WEB_CLIENT Hex Obfuscation of document.write % Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.newpowergroup .com Domain", "ET INFO Anonymous File Sharing Service Domain in DNS Lookup (send .vis .ee)", "ET INFO Dotted Quad Host HTA Request", "ET INFO DYNAMIC_DNS Query to a *.gparente .net .br Domain", "ET POLICY DNS Query to .onion proxy Domain (onion.glass)", "ET INFO DYNAMIC_DNS HTTP Request to a *.writesthisblog .com Domain", "ET INFO DYNAMIC_DNS Query to a *.opior .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hijaxdesigns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gally .jp Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.stuff-4-sale .org Domain", "ET POLICY DNS Query to .onion proxy Domain (poltornik.com)", "ET POLICY Observed DNS Query to DynDNS Domain (dns-report .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ca .com Domain", "ET INFO DYNAMIC_DNS Query to a *.internet-slackers .us Domain", "ET INFO DYNAMIC_DNS Query to a *.expedicionesytrekking .com Domain", "ET INFO DYNAMIC_DNS Query to a *.got-game .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.drupalpixels .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.doesntexist .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.larakaras .com Domain", "ET INFO DYNAMIC_DNS Query to a *.meier .li Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tftpd .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.eimertvink .nl Domain", "ET INFO DYNAMIC_DNS Query to a *.movdivx .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.uk .to Domain", "ET HUNTING Observed DNS Query for EmerDNS TLD (.bazar)", "ET INFO DYNAMIC_DNS Query to a *.mankenskiold .se Domain", "ET INFO DYNAMIC_DNS Query to a *.mandhplum .net Domain", "ET INFO DYNAMIC_DNS Query to a *.alsupnet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.for-more .biz Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.gq)", "ET INFO DYNAMIC_DNS HTTP Request to a *.vcaptains .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.defensoria-nsjp .gob .mx Domain", "ET INFO DYNAMIC_DNS Query to a *.itsaol .com Domain", "ET HUNTING Suspicious lsass.exe in URI", "ET INFO HTTP Request to Suspicious *.ryukyu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.baden .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ajalo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.galipan .org Domain", "ET POLICY HTTP traffic on port 443 (PUT)", "ET INFO DYNAMIC_DNS Query to a *.evils .in Domain", "ET POLICY DNS Query to DynDNS Domain *.geekgalaxy .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.mynetav .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wikaba .com Domain", "GPL FTP CWD ...", "ET INFO Dotted Quad Host M7 (noalert)", "ET INFO DYNAMIC_DNS HTTP Request to a *.wwwhost .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.louis-ip .com Domain", "ET INFO DYNAMIC_DNS Query to a *.teaches-yoga .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynalias .com Domain", "ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M3", "ET USER_AGENTS Suspicious Generic Style UA Observed (My_App)", "ET INFO DYNAMIC_DNS Query to a *.saves-the-whales .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.redsteedstudios .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ri .com Domain", "ET INFO DYNAMIC_DNS Query to a *.machinezdesign .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alexlan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.queerline .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.readmyblog .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.go .dyndns .org Domain", "ET WEB_SERVER PHP SESSION SuperGlobal in POST", "ET INFO DYNAMIC_DNS HTTP Request to a *.ftp1 .biz Domain", "ET INFO

	DYNAMIC_DNS Query to a *.macao .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-tn .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jwork .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.yiamuc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tbt .mx Domain", "ET INFO DYNAMIC_DNS Query to a *.webqi .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sytes.net Domain", "ET INFO DYNAMIC_DNS Query to *.rr.nu Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.fxnxs .com Domain", "ET INFO DYNAMIC_DNS Query to a *.networkoutpost .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bloodforthebloodgod .com Domain", "ET WEB_SERVER SQL Errors in HTTP 500 Response (ERROR syntax error at or near)", "ET INFO DYNAMIC_DNS Query to a *.acmetoy .com Domain", "ET INFO Commonly Abused SSL/TLS Certificate Observed (mylnavyfederal .com)", "ET WEB_SERVER UA WordPress probable DDOS-Attack", "ET INFO DYNAMIC_DNS HTTP Request to a *.maya .se Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (CookiesList.txt)", "ET INFO DYNAMIC_DNS HTTP Request to a *.oljka .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myogaya .jp Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeip .net Domain", "ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M1", "ET INFO DYNAMIC_DNS Query to a *.opticalize .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iz .rs Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gotdns .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.sportseducationinstructors .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bradam .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.abk .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wifizone .org Domain", "ET POLICY DNS Query to .onion proxy Domain (torpacho.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.htclink .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class file Importing Protection Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.leonisbg .com Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.dns-free.ru Domain", "ET INFO DYNAMIC_DNS Query to a *.norushcharge .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-oh .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.net-freaks .com Domain", "ET INFO DYNAMIC_DNS Query to a *.multicop .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.twilightparadox .com Domain", "ET INFO Observed URL Shortening Service Domain (n9 .cl in TLS SNI)", "ET INFO DYNAMIC_DNS HTTP Request to a *.404 .mn Domain", "ET INFO PSM1 Powershell File Request", "ET INFO DYNAMIC_DNS Query to a *.neat-url .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cleansite .info Domain", "ET INFO DYNAMIC_DNS Query to a *.from-nh .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shacknet .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddns .mobi Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mymediapc .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.marieblazek .com Domain", "ET INFO DYNAMIC_DNS Query to a *.albertn .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pgafan .net Domain", "ET INFO DYNAMIC_DNS Query to *uglyas.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.inovasi .co .id Domain", "ET INFO DYNAMIC_DNS Query to a *.www1 .biz Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (RhcnQtUHJvY2) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.viewdns .net Domain", "ET POLICY DNS Query to .onion proxy Domain (torbama.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.run .place Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ny .net Domain", "ET INFO DYNAMIC_DNS Query to a *.onmypc .net Domain", "ET INFO DYNAMIC_DNS Query to a *.ismoke .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.jaytex .org Domain", "ET POLICY DNS Query to DynDNS Domain *.servehumour .com", "ET INFO Obfuscated Split String (Single Q) 13", "ET INFO DYNAMIC_DNS HTTP Request to a *.myhomedns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.logular .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.farted .net Domain", "ET INFO DYNAMIC_DNS Query to a *.propertyshots .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sexxxy .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mysecuritycamera

	.com Domain", "ET INFO HTTP Request to a *.upas.su domain", "GPL ATTACK_RESPONSE index of /cgi-bin/ response", "ET POLICY DNS Query to .onion proxy Domain (onion.direct)", "ET WEB_CLIENT Hex Obfuscation of document.write %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.dixiesewing .com Domain", "ET POLICY HTTP Request to a *.co.cc domain", "ET INFO DYNAMIC_DNS HTTP Request to *.rr.nu Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.gruppuso .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.newsofmaricopa .com Domain", "ET HUNTING Possible Bot CnC Checkin (GET)", "ET INFO Obfuscated Split String (Single Q) 3", "ET INFO DYNAMIC_DNS HTTP Request to a *.firstimage .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.majoitus .ee Domain", "ET INFO DYNAMIC_DNS Query to a *.at-band-camp .net Domain", "ET INFO DYNAMIC_DNS Query to a *.iliensale .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bradam .org Domain", "ET INFO DYNAMIC_DNS Query to a *.longmusic .com Domain", "ET INFO DYNAMIC_DNS Query to a *.xn--ds-bja .org Domain", "ET HUNTING Suspicious Jar name JavaUpdate.jar", "ET INFO DYNAMIC_DNS Query to a *.authorizeddns .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.govt .hu Domain", "ET INFO DYNAMIC_DNS Query to a *.spacegas .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.encyclopedia .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.crafting .xyz Domain", "ET DOS DNS Amplification Attack Inbound", "ET INFO DYNAMIC_DNS HTTP Request to a *.chickenkiller .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jbworks .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ath .cx Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.gq)", "ET INFO DYNAMIC_DNS HTTP Request to a *.eternalimpressions .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.infe .com .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webmdee .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mutsuura .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-actress .com Domain", "ET INFO DYNAMIC_DNS Query to a *.groks-the .info Domain", "ET INFO Office Retrieving .rtf (GET)", "ET INFO DYNAMIC_DNS Query to a *.randyalsup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.moneyhome .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-personaltrainer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bbsindex.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-candidate .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vr .lt Domain", "ET HUNTING SUSPICIOUS IRC - NICK and -PC", "ET INFO Dotted Quad Host TGZ Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.got-game .org Domain", "GPL TFTP Put", "ET INFO DYNAMIC_DNS Query to a *.embeddedonline .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gsp .co .id Domain", "ET WEB_SERVER Possible Encrypted Webshell Download", "ET INFO Generic HeapSpray Construct", "ET INFO InetSim Response from External Source Possible SinkHole", "ET INFO DYNAMIC_DNS HTTP Request to a *.b33r .us Domain", "ET WEB_CLIENT Hex Obfuscation of eval % Encoding", "ET INFO URL Shortening Service Domain in DNS Lookup (vtaurl .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.flink .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pics .mu Domain", "ET HUNTING DNS Lookup to (laurentprotector .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-designer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sequoiapartners .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nedvighimost-sochi .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.jupiterns .org Domain", "ET WEB_CLIENT Hex Obfuscation of unescape %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS Query to a *.mindhackers .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nm7 .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mrslove .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.joe-joubert .com Domain", "ET ADWARE_PUP Win/Malware.FileTour Variant Checkin", "ET INFO DYNAMIC_DNS Query to a *.crossharbour .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-dc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.better-than .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.joiavip .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.pitam .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tumsun .com Domain", "ET POLICY DNS Query to DynDNS Domain

	*.3utilities .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.paumard .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hitremixes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.edrennikov .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sibmed .org .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.porngo .at Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kidsqt .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ix .tc Domain", "ET INFO Query for Suspicious .noip.cn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webhop .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ak .com Domain", "ET POLICY SMB2 NT Create AndX Request For an Executable File", "ET INFO HTTP Connection To DDNS Domain serveblog.net", "ET INFO DYNAMIC_DNS HTTP Request to a *.ufodns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mrface .com Domain", "ET INFO DYNAMIC_DNS Query to a *.paumard .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.noamank .com Domain", "ET INFO DYNAMIC_DNS Query to a *.audolatry .com Domain", "ET INFO Dotted Quad Host M6 (noalert)", "ET INFO DYNAMIC_DNS Query to a *.rogerthedog .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ext .io Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-actor .com Domain", "ET POLICY MAZE Ransomware Victim Publishing Site DNS Lookup (newsmaze .top)", "ET MALWARE Evil Google Drive Download", "ET INFO DYNAMIC_DNS Query to a *.paranormalgroup .com Domain", "ET POLICY DNS Query to DynDNS Domain *.serveexchange .com", "ET INFO HTTP Request to a *.bg.tf domain", "ET SCAN Suspicious inbound to mySQL port 3306", "ET INFO DYNAMIC_DNS Query to a *.wildsurf .net Domain", "ET INFO DYNAMIC_DNS Query to a *.energysemi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.endofinternet .net Domain", "ET INFO DYNAMIC_DNS Query to a *.zyns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.etowns.net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.unibutton .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dynserv .org Domain", "ET INFO DYNAMIC_DNS Query to a *.lflinkup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.minetest .land Domain", "ET INFO DYNAMIC_DNS Query to a *.rtmuller .net Domain", "ET INFO DYNAMIC_DNS Query to a *.nedvighimost-sochi .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.swe .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hobby-site .org Domain", "ET WEB_SERVER WebShell - MySQL Interface - Client Cookie mysql_web_admin*=", "ET INFO DYNAMIC_DNS HTTP Request to a *.opior .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shakedfamily .com Domain", "ET INFO Suspicious Domain (*.gdn) in TLS SNI", "ET INFO DYNAMIC_DNS Query to a *.ycare .org Domain", "ET INFO DYNAMIC_DNS Query to a *.cechire .com Domain", "ET INFO DYNAMIC_DNS Query to a *.erke .biz .tr Domain", "ET HUNTING Hidden embedded HTML Document", "ET INFO DYNAMIC_DNS HTTP Request to a *.likescandy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servesarcasm .com Domain", "ET INFO DYNAMIC_DNS Query to a *.circusslaves .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sendsmtp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.randyalsup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.404 .mn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.k .vu Domain", "ET INFO DYNAMIC_DNS Query to a *.scrapper-site .net Domain", "ET INFO HTTP POST Request to DuckDNS Domain", "ET INFO DYNAMIC_DNS Query to a *.scay .net Domain", "ET INFO DYNAMIC_DNS Query to a *.multiverso .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bugaloop .com Domain", "ET INFO DYNAMIC_DNS Query to a *.nya .pub Domain", "ET INFO PSD1 Powershell File Request", "ET INFO Cloud IPFS Service Domain in DNS Lookup (nftstorage .link)", "ET INFO DYNAMIC_DNS Query to a *.dorthel .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-wa .com Domain", "ET INFO URL Shortening Service Domain in DNS Lookup (www .temporary-url .com)", "ET INFO DYNAMIC_DNS Query to a *.paulkelly .org Domain", "ET WEB_SERVER PHP tag in UA", "ET INFO DYNAMIC_DNS HTTP Request to a *.pixelfucker .com Domain", "ET INFO DYNAMIC_DNS Query to a *.stocktester .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.logntw .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.paulsfamilyhistory .com Domain", "ET EXPLOIT Malformed HeartBeat Response", "ET INFO DYNAMIC_DNS Query to a *.tth .cl

	Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onapon .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.siasolution .com Domain", "ET INFO DYNAMIC_DNS Query to a *.keecha .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sazhenec .ru Domain", "ET USER_AGENTS Suspicious User-Agent (HTTP-Test-Program)", "ET INFO DYNAMIC_DNS HTTP Request to a *.zsh .jp Domain", "ET ATTACK_RESPONSE UTF16 base64 reversed string /This Program/ in DNS TXT Reponse", "ET INFO HTTP Request to Suspicious *.fit Domain", "ET INFO Lockbit Ransomware Related Domain in DNS Lookup (lockbit-decryptor .top)", "ET INFO DYNAMIC_DNS Query to a *.myhousesetup .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onmypc .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-artist .com Domain", "ET INFO DYNAMIC_DNS Query to a *.boxathome .net Domain", "ET HUNTING Generic Powershell Launching Hidden Window", "ET INFO DYNAMIC_DNS Query to a *.esmtp .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bhms .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ketubruk .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.proxydns .co .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-photographer .com Domain", "ET INFO Base64 Encoded powershell.exe in HTTP Response M3", "ET INFO DYNAMIC_DNS HTTP Request to a *.sandmeiers .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kicks-ass .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ppalma .cl Domain", "GPL TELNET Telnet Root not on console", "ET POLICY DNS Query to DynDNS Domain *.pgafan .net", "ET INFO DYNAMIC_DNS Query to a *.ubernerden .com Domain", "ET POLICY HTTP traffic on port 443 (OPTIONS)", "ET INFO DYNAMIC_DNS Query to a *.nux .co .za Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-hunter .com Domain", "ET INFO HTTP Request to a *.c0m.li domain", "ET INFO DYNAMIC_DNS Query to a *.flnet.org Domain", "ET POLICY DNS Query to .onion proxy Domain (torvsusd.com)", "ET POLICY Observed DNS Query to Commonly Abused Cloudflare Domain (trycloudflare .com)", "ET WEB_CLIENT Hex Obfuscation of substr %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.agila .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.champagnewishesandrvdreams .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jedimasters .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.paulkelly .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.geekgalaxy .com Domain", "ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .exe filename inside", "ET INFO DYNAMIC_DNS HTTP Request to a *.001www .com Domain", "ET INFO DYNAMIC_DNS Query to a *.onmypc .org Domain", "ET INFO DYNAMIC_DNS Query to a *.h4ck .me Domain", "ET INFO DYNAMIC_DNS Query to a *.requitas .com Domain", "ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.chrismac .org Domain", "ET INFO Imposter USPS Domain", "ET INFO Observed URL Shortening Service Domain (0sh .org in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.dagz .ru Domain", "ET INFO SUSPICIOUS UA starting with Mozilla/8", "ET POLICY HTTP Request to a *.cz.cc domain", "ET INFO DYNAMIC_DNS Query to a *.noamank .com Domain", "ET POLICY DNS Query to .onion proxy Domain (toralpacho.com)", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (dm9rZS1SZXN0TWV0) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.powermotors .com .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pltimes .net Domain", "ET WEB_SERVER WebShell - Simple - Title", "ET INFO DYNAMIC_DNS Query to a *.dropfiles .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-mail .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nya .pub Domain", "ET INFO DYNAMIC_DNS Query to a *.jolleybeef .com Domain", "ET MALWARE Observed Malicious UA (Skuxray)", "ET INFO DYNAMIC_DNS HTTP Request to a *.r-o-o-t .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.swphoa .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.painefieldcap .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.longmusic .com Domain", "ET WEB_SERVER WebShell - MySQL Interface - Server Set Cookie mysql_web_admin*=", "ET INFO DYNAMIC_DNS HTTP Request to a *.wanip .ch Domain", "ET HUNTING Suspicious GET Request for .ppc File", "ET INFO DYNAMIC_DNS Query to a *.myhomedns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.xn--ds-bja .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yasser .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.staffpro .net Domain", "ET POLICY HTTP Request to a *.co.be domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.celebsplay .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.000000000000000000000 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fr .to Domain", "ET INFO Dotted Quad Host PDF Request", "ET INFO DYNAMIC_DNS Query to a *.dynathome .net Domain", "ET INFO DYNAMIC_DNS Query to a *.from-nd .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-de .com Domain", "ET INFO Compressed Executable SZDD Compress.exe Format Over HTTP", "ET INFO DYNAMIC_DNS HTTP Request to a *.lotusblossomconsulting .com Domain", "ET INFO Obfuscated Split String (Double Q) 11", "ET INFO Chocolatey Windows Package Management Installation File Retrieval", "ET INFO DYNAMIC_DNS Query to a *.greengarden .net .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homenode .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynip .org Domain", "ET INFO DYNAMIC_DNS Query to a *.homeftp .net Domain", "ET INFO DYNAMIC_DNS Query to a *.mathewparkin .com Domain", "ET POLICY DNS Query to .onion proxy Domain (onion.lt)", "ET INFO DYNAMIC_DNS Query to a *.scrapitsoftware .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveirc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yourtrap .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bridge-club-hannover .de Domain", "ET HUNTING Suspicious POST Request with Possible COVID-19 URI M1", "ET INFO DYNAMIC_DNS Query to a *.photographs .gs Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (52b2tlLUNvbW1) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.selfip .info Domain", "ET POLICY Possible WMI .mof Managed Object File Use Over SMB", "ET INFO DYNAMIC_DNS HTTP Request to a *.merseine .com Domain", "ET ATTACK_RESPONSE Cisco TclShell TFTP Download", "ET INFO DYNAMIC_DNS Query to a *.is-a-musician .com Domain", "ET EXPLOIT Metasploit -Java Atomic Exploit Downloaded", "ET INFO DYNAMIC_DNS Query to a *.120v .ac Domain", "ET INFO Query for Suspicious .sg.tf Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.cf)", "ET INFO DYNAMIC_DNS Query to a *.hedbergandson .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zeleznock .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-very-good .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.land-4-sale .us Domain", "ET INFO Commonly Abused File Sharing Domain in DNS Lookup (filetransfer .io)", "ET USER_AGENTS Observed Uclient User-Agent", "ET WEB_CLIENT Hex Obfuscation of Script Tag %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.sococoffee .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsdojo .org Domain", "ET INFO DYNAMIC_DNS Query to a *.mymom .info Domain", "ET INFO DYNAMIC_DNS Query to *passas.us Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.home .dyndns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bloodforthebloodgod .com Domain", "ET HUNTING Suspicious GET Request for .sh4 File", "ET INFO DYNAMIC_DNS HTTP Request to a *.navnirwana .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-at-work .com Domain", "ET USER_AGENTS Observed Malicious User-Agent (FastInvoice)", "ET INFO DYNAMIC_DNS Query to a *.istmein .de Domain", "ET WEB_SERVER PHP ENV SuperGlobal in URI", "ET INFO Observed DNS Query to .work TLD", "ET INFO DYNAMIC_DNS HTTP Request to a *.compucase .com Domain", "ET INFO DYNAMIC_DNS Query to a *.vaizer .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.homeunix .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dns2 .us Domain", "ET INFO Obfuscated Split String (Double Q) 6", "ET INFO DYNAMIC_DNS HTTP Request to a *.mutluay .com Domain", "ET INFO Terse Request For Bitbucket Snippet", "ET INFO DYNAMIC_DNS HTTP Request to a *.surfnet .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.intranetwifi .it Domain", "ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)", "ET INFO Obfuscated Split String (Single Q) 2", "ET INFO DYNAMIC_DNS HTTP Request to a *.health-carereform .com Domain", "ET HUNTING Suspicious GET Request for .x86", "ET INFO DYNAMIC_DNS HTTP Request to *.passas.us Domain (Sitelutions)", "ET POLICY DNS Query to DynDNS Domain *.access .ly", "ET INFO DYNAMIC_DNS HTTP Request to

	*.lookin.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.lwts .ru Domain", "ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)", "ET POLICY HTTP Request to a *.vv.cc domain", "ET POLICY DNS Query to DynDNS Domain *.servehalflife .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.jade-hamburg .de Domain", "ET INFO DYNAMIC_DNS Query to a *.southern .com .my Domain", "ET INFO DYNAMIC_DNS Query to a *.wild1 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.v0x .eu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.giantrobotfactory .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.asadanasemesta .co .id Domain", "ET INFO DYNAMIC_DNS Query to a *.good .one .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.flazzard .com Domain", "ET INFO Possible Microsoft OMI Agent Default TLS Certificate Observed", "ET INFO DYNAMIC_DNS HTTP Request to a *.opaline .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.yihtah .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeplex .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dogdammit .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.veta .su Domain", "ET HUNTING Possible Covid19 Themed Email Spam Outbound M4", "ET INFO DYNAMIC_DNS HTTP Request to a *.toythieves .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ptchat .net Domain", "ET INFO DYNAMIC_DNS Query to a *.lostgumball .com Domain", "ET INFO DYNAMIC_DNS Query to a *.scieron.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rav-kraski .ru Domain", "ET POLICY DNS Query to DynDNS Domain *.health-carereform .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.tobuy .us Domain", "ET WEB_SERVER PHP POST SuperGlobal in URI", "ET INFO DYNAMIC_DNS Query to a *.kfco .net Domain", "ET INFO DYNAMIC_DNS Query to a *.china .is Domain", "ET INFO Java .jar request to dotted-quad domain", "ET INFO DYNAMIC_DNS Query to a *.breakingpar .com Domain", "ET INFO DYNAMIC_DNS Query to a *.easefun .hk Domain", "ET POLICY DNS Query to DynDNS Domain *.dvrcam .info", "ET SCAN Suspicious inbound to mSQL port 4333", "ET INFO DYNAMIC_DNS HTTP Request to a *.n0p .at Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.wolf-tec .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dontexist .net Domain", "ET INFO DYNAMIC_DNS Query to a *.generi .cc Domain", "ET HUNTING Terse Request for EXE from DigitalOcean Spaces", "ET INFO DYNAMIC_DNS Query to a *.bot .nu Domain", "ET POLICY DNS Query to DynDNS Domain *.brasilia .me", "ET INFO DYNAMIC_DNS HTTP Request to a *.eiresol .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sulsel .go .id Domain", "ET POLICY DNS Query to DynDNS Domain *.serveblog .net", "ET INFO DYNAMIC_DNS Query to a *.is-a-geek .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-at-work .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.meier .li Domain", "ET INFO DYNAMIC_DNS Query to a *.artitech .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tantrym .com Domain", "ET USER_AGENTS MSF Meterpreter Default User Agent", "ET INFO Observed TA453 Related URL Shortening Service TLS SNI (litby .us)", "ET INFO DYNAMIC_DNS Query to a *.myddns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.brokenfuture .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.2dons .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tenspot .net Domain", "ET PHISHING Possible Phishing Redirect 2018-01-30", "ET INFO Observed Collaboration/File Sharing Platform Domain (www .notion .so in TLS SNI)", "ET INFO Obfuscated Split String (Double Q) 10", "ET INFO DYNAMIC_DNS Query to a *.alam-maritim .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.idigo .org Domain", "ET INFO DYNAMIC_DNS Query to a *.pusilkom .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.keine-panik .net Domain", "ET INFO DYNAMIC_DNS Query to a *.windmillstravel .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dubya .net Domain", "ET INFO DYNAMIC_DNS Query to a *.hot-hed .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (GFydC1Qcm9jZX) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.kanda .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.v6 .navy Domain", "ET INFO DYNAMIC_DNS Query to a *.dynssl .com Domain", "ET POLICY HTTP HEAD invalid method case outbound", "ET INFO DYNAMIC_DNS Query to a *.dyndns-blog .com Domain", "ET INFO

	DYNAMIC_DNS HTTP Request to a *.dns .army Domain", "ET INFO DYNAMIC_DNS Query to a *.for-more .biz Domain", "ET HUNTING Suspicious GET Request with Possible COVID-19 Domain M2", "ET HUNTING Request to 000webhostapp Domain with Minimal Headers", "ET INFO DYNAMIC_DNS Query to a *.klodia .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-wi .com Domain", "ET INFO Query for Suspicious .nl.ai Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.anal-slavery .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.forgot .her .name Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.neoneptune .com Domain", "ET INFO DYNAMIC_DNS Query to a *.v6 .army Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.robot-armies .com Domain", "ET HUNTING Inbound Powershell Creating .lnk File", "ET INFO DYNAMIC_DNS HTTP Request to a *.falcongreen .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.scieron.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-guru .com Domain", "ET POLICY HTTP traffic on port 443 (POST)", "ET INFO DYNAMIC_DNS HTTP Request to a *.qc .to Domain", "ET INFO DYNAMIC_DNS Query to a *.compuinter .com Domain", "ET POLICY RDP Wrapper Download (ini)", "ET INFO DYNAMIC_DNS Query to a *.linuxstart .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.palvelin .net Domain", "ET HUNTING Suspicious GET Request with Possible COVID-19 URI M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.forgot .his .name Domain", "ET USER_AGENTS Suspicious User-Agent (HTTP_CONNECT_)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ubernerden .com Domain", "ET INFO DYNAMIC_DNS Query to a *.vcaptains .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-certified .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myvnc .com Domain", "ET INFO DYNAMIC_DNS Query to *.myfw.us Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.radio-zvez .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.firesidegrillandbar .com Domain", "ET HUNTING Possible cs2nginx Proxy Redirect", "ET INFO Obfuscated Split String (Double Q) 12", "ET INFO DYNAMIC_DNS Query to a *.hpc .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.geofuzz .net Domain", "ET INFO DYNAMIC_DNS Query to a *.what2no .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gotdns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.huepfler .com Domain", "ET INFO DYNAMIC_DNS Query to a *.whyboner .com Domain", "ET INFO DYNAMIC_DNS Query to a *.e-m-a-i-l .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hedbergandson .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pbohara .com Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (Zva2UtV21pTWV) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.agila .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.dns-report .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dprdsulsel .go .id Domain", "ET WEB_CLIENT PDF With Embedded U3D", "ET INFO DYNAMIC_DNS HTTP Request to a *.zzux .com Domain", "ET INFO HTTP Request to a *.date domain", "ET INFO DYNAMIC_DNS Query to a *.erotikload .at Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-hard-worker .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myftp .org Domain", "ET INFO DYNAMIC_DNS Query to a *.mylogisoft .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ddj .co .za Domain", "ET POLICY DNS Query to DynDNS Domain *.golffan .us", "ET INFO DYNAMIC_DNS Query to a *.is-a-rockstar .com Domain", "ET WEB_CLIENT Hex Obfuscation of String.fromCharCode %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-mi .com Domain", "ET SCAN OpenVASVT RCE Test String in HTTP Request Outbound", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (RhcnQtUHJ) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.cnstefancelmare .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.clickip .de Domain", "ET WEB_SERVER PHP SERVER SuperGlobal in URI", "ET INFO DYNAMIC_DNS Query to a *.run .place Domain", "ET INFO DYNAMIC_DNS Query to a *.localghost .org Domain", "ET INFO DYNAMIC_DNS Query to a *.wakingmoon .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servequake .com Domain", "ET INFO DYNAMIC_DNS Query to a *.rpz .su Domain", "ET MALWARE Generic -POST To file.php w/Extended ASCII Characters", "ET INFO DYNAMIC_DNS Query to a *.kreider .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fedea .com .ar Domain",

	"ET INFO DYNAMIC_DNS HTTP Request to a *.falcongreenenergy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.seasol .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-wi .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dx .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.v6 .navy Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.spelar .se Domain", "ET INFO DYNAMIC_DNS Query to a *.truewan .co .za Domain", "ET INFO DYNAMIC_DNS Query to a *.mysecondarydns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tountas .org Domain", "ET POLICY DNS Query to DynDNS Domain *.serveminecraft .net", "ET INFO DYNAMIC_DNS Query to a *.loscantarostemuco .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.point2this .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ne .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hatenboer .org Domain", "ET INFO DYNAMIC_DNS Query to a *.sdp-mos .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-student .com Domain", "ET POLICY DNS Query to .onion proxy Domain (pay4tor.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.demoteam .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.teleconomiser .com Domain", "ET INFO DYNAMIC_DNS Query to a *.thinksnow .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.star .is Domain", "ET INFO DYNAMIC_DNS Query to a *.stuff-4-sale .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.radio-zvez .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.aussievitamin .com Domain", "ET INFO DYNAMIC_DNS Query to a *.newpowergroup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.kik .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ca .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.l5 .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-democrat .com Domain", "ET INFO DYNAMIC_DNS Query to a *.devwonders .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alam-maritim .com .my Domain", "ET INFO DYNAMIC_DNS Query to a *.blogsite .org Domain", "ET INFO DNS Query to google .com Non Standard Port (tcp)", "ET MALWARE Generic -POST To gate.php w/Extended ASCII Characters (Likely Zeus Derivative)", "ET INFO DYNAMIC_DNS Query to a *.ljhb .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.staffpro .net Domain", "ET INFO DYNAMIC_DNS Query to a *.infe .com .br Domain", "ET INFO DYNAMIC_DNS Query to a *.changeip .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.chebicon .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.moochurch .org Domain", "ET INFO DYNAMIC_DNS Query to a *.wileymetal .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ryanbauman .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.salford-hall .co .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.3n .cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.happyforever .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-sc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.as19557 .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ideas-informatica .com .ar Domain", "GPL ATTACK_RESPONSE command error", "ET INFO DYNAMIC_DNS HTTP Request to a *.zyns .com Domain", "ET INFO DYNAMIC_DNS Query to a *.idigo .org Domain", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.ml)", "ET INFO DYNAMIC_DNS Query to a *.videounlimit .com Domain", "ET INFO DYNAMIC_DNS Query to a *.shacknet .us Domain", "ET INFO DYNAMIC_DNS Query to a *.myphotos .cc Domain", "ET INFO DYNAMIC_DNS Query to a *.alltransportme .com Domain", "ET MALWARE Observed HTTP Request to Known PUA Host Domain", "ET INFO DYNAMIC_DNS Query to a *.from-pa .com Domain", "ET INFO HTTP Request to Suspicious *.desi Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.isgre.at Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.authorizeddns .net Domain", "ET MALWARE SUSPICIOUS UA (iexplore)", "ET INFO DYNAMIC_DNS HTTP Request to a *.loscantarostemuco .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveftp .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyn-dns.ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nunc .se Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddnsking .com Domain", "ET INFO DYNAMIC_DNS Query to a *.work .gd Domain", "ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL", "ET INFO http string in hex Possible Obfuscated Exploit Redirect", "ET INFO DYNAMIC_DNS Query to a *.dark-byte .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.xox .mx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.dailyholycrap .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sjschroeder .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.derekcturner .net Domain", "ET INFO DYNAMIC_DNS Query to a *.fridg .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hackershack .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cleansite .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-ip .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lebtimnetz .de Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myiphost .com Domain", "ET INFO JNLP embedded file", "ET INFO DYNAMIC_DNS HTTP Request to a *.mooo .info Domain", "ET INFO DYNAMIC_DNS Query to a *.tibet .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blue-jade .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.irfna .com Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.gdn)", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynssl .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.neo)", "ET INFO DYNAMIC_DNS Query to a *.kawa-kun .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.findhere.org Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ham-radio-op .net Domain", "ET INFO Observed certreq User-Agent (NDES client)", "ET SQL MySQL mysql.user Dump (Used in Metasploit Auth-Bypass Module)", "ET USER_AGENTS Observed Suspicious UA (easyhttp client)", "ET INFO DYNAMIC_DNS Query to a *.robbieb .me .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.dsmtp .com Domain", "ET INFO DYNAMIC_DNS Query to a *.oceanpolice .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ok .com Domain", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class file Accessing Security Manager", "ET INFO DYNAMIC_DNS HTTP Request to a *.iownyour .org Domain", "ET INFO DYNAMIC_DNS Query to a *.giantrobotfactory .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.triviem .cl Domain", "ET WEB_CLIENT Hex Obfuscation of parseInt %u UTF-8 Encoding", "ET HUNTING SUSPICIOUS Possible Office Doc with Embedded VBA Project (Wide)", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oastify .com)", "ET INFO JAR Size Under 30K Size - Potentially Hostile", "ET POLICY DNS Query to DynDNS Domain *.privatizehealthinsurance .net", "ET INFO DYNAMIC_DNS HTTP Request to a *.scottexteriors .com Domain", "ET SCAN Suspicious inbound to Oracle SQL port 1521", "ET WEB_CLIENT PDF With Embedded Adobe Shockwave Flash Possibly Related to Remote Code Execution Attempt", "ET HUNTING NOP Sled in HTTP Header Inbound - Possible Exploit Activity", "ET INFO DYNAMIC_DNS HTTP Request to a *.servegame .com Domain", "ET INFO Query for Suspicious .int.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.hmsolucoes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-bookkeeper .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-al .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-knight .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dansted .org Domain", "ET USER_AGENTS Suspicious User-Agent (test-upload)", "ET INFO DYNAMIC_DNS HTTP Request to a *.good .one .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.jharrigan .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ftpserver .biz Domain", "ET WEB_CLIENT Possible # Encoded Iframe Tag", "ET WEB_CLIENT eval String.fromCharCode String Which May Be Malicious", "ET INFO DYNAMIC_DNS Query to a *.rav-kraski .ru Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.o)", "ET INFO DYNAMIC_DNS Query to a *.sammah .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hansa-tmp .cn Domain", "ET INFO HTTP POST Request to Suspicious *.icu domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cityofgreen .com .my Domain", "ET INFO DYNAMIC_DNS Query to a *.aintno .info Domain", "ET ATTACK_RESPONSE UTF8 base64 reversed string /This Program/ in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.2to1agri .com Domain", "ET INFO RealThinClient Session Init", "ET INFO DYNAMIC_DNS HTTP Request to a *.chesta .com Domain", "ET INFO DYNAMIC_DNS Query to a *.e-cloud .ch Domain", "ET INFO x86 File Download Request from IP Address", "ET INFO DYNAMIC_DNS HTTP Request to a *.yurigoron .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.antrak .org .tr Domain", "ET INFO DYNAMIC_DNS Query to a *.reves .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.docuprint .com .ar Domain", "ET INFO DYNAMIC_DNS Query to a *.mine .bz Domain", "ET INFO

	DYNAMIC_DNS HTTP Request to a *.shacknet .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mynumber .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.acmetoy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.n43 .pw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.internetzninja .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dtdns.net Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ocry .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shit .vc Domain", "ET MALWARE DNS Query Known Reveton Domain whatwillber.com", "ET INFO DYNAMIC_DNS HTTP Request to a *.bad .mn Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-chef .org Domain", "ET INFO DYNAMIC_DNS Query to a *.academic .org .il Domain", "ET INFO DYNAMIC_DNS Query to a *.seahorsenet .com Domain", "ET INFO DYNAMIC_DNS Query to a *.punked .us Domain", "ET INFO DYNAMIC_DNS Query to a *.furryplace .eu Domain", "ET INFO DYNAMIC_DNS Query to a *.afela .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dontexist .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypicture .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nhlfan .net Domain", "ET WEB_SERVER WebShell Generic - netsh firewall", "ET INFO DYNAMIC_DNS HTTP Request to a *.dekalo .net Domain", "ET INFO Observed URL Shortening Service Domain (kutti .co in TLS SNI)", "ET POLICY Tunneled RDP Handshake", "ET INFO Observed Peer-to-Peer File Sharing Service Domain (ipfs .io in TLS SNI)", "ET INFO DYNAMIC_DNS Query to *.passinggas.net Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.afela .org Domain", "ET INFO Base64 Encoded powershell.exe in HTTP Response M2", "ET INFO DYNAMIC_DNS Query to a *.punkassgamers .com Domain", "ET HUNTING Suspicious GET Request for .x64", "ET INFO DYNAMIC_DNS HTTP Request to a *.parquecidades-eim .pt Domain", "ET HUNTING Observed DNS Query for EmerDNS TLD (.coin)", "ET INFO DYNAMIC_DNS HTTP Request to a *.boblove .org Domain", "ET HUNTING Generic Powershell Starting Wscript Process", "ET INFO DYNAMIC_DNS HTTP Request to a *.freewww .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jaytex .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.texashotoilers .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mchini .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sbinfo .com Domain", "ET INFO DYNAMIC_DNS Query to a *.aletoledo .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nathan .to Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ct .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kir22 .ru Domain", "ET POLICY DNS Query to DynDNS Domain *.myeffect .net", "ET INFO DYNAMIC_DNS Query to a *.darvin .one .pl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.0bit .org Domain", "ET INFO DYNAMIC_DNS Query to a *.myz .info Domain", "ET INFO DYNAMIC_DNS Query to a *.bhms .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hin .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thruhere .net Domain", "ET INFO DYNAMIC_DNS Query to a *.falcongreen .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.onthenetas.com Domain (Sitelutions)", "ET USER_AGENTS Observed Suspicious UA (IExplorer 34)", "ET INFO DYNAMIC_DNS HTTP Request to a *.voltage .nz Domain", "ET INFO HTTP Request to a *.osa.pl domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.entermypicks .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sdp-mos .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.istmein .de Domain", "ET INFO DYNAMIC_DNS Query to a *.for-the .biz Domain", "ET HUNTING Observed DNS Query for FurNIC TLD (.fur)", "ET INFO DYNAMIC_DNS HTTP Request to a *.abuser .eu Domain", "ET USER_AGENTS Observed Suspicious UA (grab)", "ET INFO DYNAMIC_DNS HTTP Request to a *.mypop3 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lilyspadd .com Domain", "ET INFO DYNAMIC_DNS Query to a *.66haoyun .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torchek.com)", "ET INFO DYNAMIC_DNS Query to a *.happyforever .com Domain", "ET INFO DYNAMIC_DNS Query to a *.efrati .org Domain", "ET JA3 HASH - Possible RustyBuer Server Response", "ET HUNTING Suspicious GET Request for .i468 File", "ET INFO Obfuscated Split String (Double Q) 7", "ET INFO DYNAMIC_DNS Query to a *.priamaakcia .sk Domain", "ET INFO DYNAMIC_DNS Query to a *.susangilmore .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-anarchist .com Domain", "ET INFO DYNAMIC_DNS Query to a

	*.ndra .biz Domain", "ET INFO Cloud IPFS Service Domain in DNS Lookup (fleek .co)", "ET INFO DYNAMIC_DNS Query to a *.linux70 .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.monopolepower .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-fl .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.barrel-of-knowledge .info Domain", "ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)", "ET INFO DYNAMIC_DNS Query to a *.plugs .it Domain", "ET INFO DYNAMIC_DNS Query to a *.shaqnet .nu Domain", "ET HUNTING jpg download from fileupload .site", "ET INFO DYNAMIC_DNS Query to a *.pittentrepreneur .com Domain", "ET HUNTING Possible COVID-19 Domain in SSL Certificate M1", "ET INFO DYNAMIC_DNS Query to a *.thegiblins .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.webhop .net Domain", "ET POLICY HTTP traffic on port 443 (CONNECT)", "ET INFO Peer-to-Peer File Sharing Service Domain in DNS Lookup (ipfs .io)", "ET USER_AGENTS Suspicious UA Observed (Ave, Caesar!)", "ET EXPLOIT Possible TLS HeartBleed Unencrypted Request Method 4 (Inbound to Common SSL Port)", "ET INFO DYNAMIC_DNS HTTP Request to a *.xcv .cx Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dagz .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.free-pic .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.technicalsupportresources .com Domain", "ET WEB_CLIENT PDF With Embedded Flash Possible Remote Code Execution Attempt", "ET INFO DYNAMIC_DNS Query to a *.mine .tk Domain", "ET INFO DYNAMIC_DNS Query to a *.alexlan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.2dons .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yihtah .net Domain", "ET INFO DYNAMIC_DNS Query to a *.crabdance .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iantaylor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-office .com Domain", "ET HUNTING Suspicious Embedded Shockwave Flash In PDF", "ET INFO DYNAMIC_DNS Query to a *.fiid .net Domain", "ET INFO DYNAMIC_DNS Query to a *.starscene .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-*.com domain", "ET INFO MIPS File Download Request from IP Address", "ET INFO DYNAMIC_DNS HTTP Request to a *.clarkstock .com Domain", "ET INFO DYNAMIC_DNS Query to a *.uk .to Domain", "ET INFO DYNAMIC_DNS Query to a *.garmanage .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.montyconsulting .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-cubicle-slave .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-bruinsfan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myactivedirectory .com Domain", "ET POLICY DNS Query to DynDNS Domain *.servebeer .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.pusilkom .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-remote .com Domain", "ET INFO DYNAMIC_DNS Query to a *.chocolatespicacho .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sells-for-u .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.caribbeanpremierhotels .com Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.oss)", "ET HUNTING Suspicious Possible Zip DL containing single VBS script", "ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.creery .org Domain", "ET INFO DYNAMIC_DNS Query to a *.ax .lt Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-nurse .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servehttp .com Domain", "ET INFO SUSPICIOUS Java Request to NOIP Dynamic DNS Domain", "ET POLICY DNS Query to DynDNS Domain *.webhop .me", "ET INFO DYNAMIC_DNS Query to a *.24-7 .ro Domain", "ET INFO GET to Puu.sh for TXT File with Minimal Headers", "ET INFO DYNAMIC_DNS HTTP Request to a *.chatnook.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.silksky .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.a4t .in Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oast .live)", "ET INFO DYNAMIC_DNS Query to a *.texashotoilers .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jake .eu Domain", "ET INFO HTTP Request to a *.asia domain", "ET INFO DYNAMIC_DNS Query to a *.doesntexist .com Domain", "ET HUNTING .exec in HTTP Header Inbound - Possible Exploit Activity", "ET INFO DYNAMIC_DNS HTTP Request to a *.thompent .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thegiblins .com Domain", "ET INFO DYNAMIC_DNS Query to a *.broke-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a

	*.endofinternet .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tantrym .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tcp4 .me Domain", "ET INFO DYNAMIC_DNS Query to a *.from-sc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-an-accountant .com Domain", "ET WEB_CLIENT Hex Obfuscation of eval %u UTF-16 Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.enemyterritory .org Domain", "ET HUNTING Request to .GA Domain with Minimal Headers", "ET WEB_SERVER PHP ENV SuperGlobal in POST", "ET INFO DYNAMIC_DNS Query to a *.soundcast .me Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.greengarden .net .br Domain", "ET INFO DYNAMIC_DNS Query to a *.veta .su Domain", "ET INFO URL Shortening/Redirect Service Domain in DNS Lookup (cutit .org)", "ET INFO DYNAMIC_DNS HTTP Request to a *.minecraftr .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kaznets .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-mt .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homeftp .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-lawyer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dnsalias .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blogdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mza .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.uglyas.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.dateeasily .com Domain", "ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (V4dC5FbmNvZ) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.n4t .co Domain", "ET INFO DYNAMIC_DNS Query to a *.kaznets .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.teachmetofish .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.myftp .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rude .li Domain", "ET INFO DNS Query for a Suspicious *.ae.am domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-candidate .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsup .net Domain", "ET INFO HTTP Request to a *.int.tf domain", "ET INFO DYNAMIC_DNS Query to a *.oitsc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.edrennikov .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.kbgz .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shogun .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.shitgoddamnhellfuck .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ufcfan .org Domain", "ET POLICY DNS Query to DynDNS Domain *.ciscofreak .com", "ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response from Common SSL Port (Outbound from Server)", "ET INFO DNS Query to a *.slyip.net Dynamic DNS Domain", "ET HUNTING Request To Suspicious Filename via Powershell (key)", "ET INFO DYNAMIC_DNS Query to a *.veriler .com Domain", "ET POLICY Observed URL Shortening Service Domain (longurl .in in TLS SNI)", "ET INFO DYNAMIC_DNS Query to a *.arrowtechnical .co .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.eiresol .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torwinner.com)", "ET POLICY Vulnerable Java Version 1.7.x Detected", "ET WEB_SERVER WebShell Generic - reg HKEY_LOCAL_MACHINE", "ET INFO DYNAMIC_DNS HTTP Request to a *.lotusshipping .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cnr .com .pk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fragmentary .info Domain", "ET INFO DYNAMIC_DNS Query to a *.dynv6 .net Domain", "ET INFO HTTP Request to a *.uni.cc domain", "ET WEB_SERVER IIS INDEX_ALLOCATION Auth Bypass Attempt", "ET HUNTING [@Silv0123] Possible Fake Microsoft Office User-Agent Observed", "ET INFO DYNAMIC_DNS HTTP Request to a *.youpc .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.svmblocker .com Domain", "ET INFO Possible RTF File With Obfuscated Version Header", "ET INFO DYNAMIC_DNS Query to a *.ftp .sh Domain", "ET INFO DYNAMIC_DNS Query to a *.serverpit .com Domain", "ET INFO HTTP Request to a *.at.tf domain", "ET INFO Abused Hosting Domain in DNS Lookup (digital-ministry .ru)", "ET INFO DYNAMIC_DNS Query to a *.robinhud .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tantrum .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servehalflife .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.kwik.to Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.ikwb .com Domain", "ET INFO MIPSEL File Download Request from IP Address", "ET INFO DYNAMIC_DNS Query to a *.jedimasters .net Domain", "ET INFO DYNAMIC_DNS Query to a *.glengall .com

	Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.golffan .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.slyip.com Domain", "ET INFO JJEncode Encoded Script", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveftp .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kitayori .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.fmg .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.swhydro .com Domain", "ET WEB_CLIENT PDF With Adobe Audition Session File Handling Buffer Overflow Flowbit Set", "ET USER_AGENTS Suspicious User-Agent (example/1.0)", "ET INFO DYNAMIC_DNS Query to a *.pics .mu Domain", "ET INFO Possible Overflow Attempt - Abnormally Large SMTP EHLO Inbound", "ET INFO DYNAMIC_DNS Query to a *.aispilot .com Domain", "ET POLICY Powershell Command With Execution Bypass Argument Over SMB - Likely Lateral Movement", "ET INFO DYNAMIC_DNS Query to a *.zaibar .ro Domain", "ET HUNTING SUSPICIOUS Reassigned Eval Function 2", "ET INFO DYNAMIC_DNS HTTP Request to a *.podzone .org Domain", "ET USER_AGENTS Observed Suspicious UA (\xa4)", "ET INFO DYNAMIC_DNS HTTP Request to a *.osclabs .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.contactme .cl Domain", "ET WEB_SERVER WebShell - MySQL Interface - Database List", "ET INFO Possible Sharepoint Resource Infection", "ET WEB_SERVER PHP GET SuperGlobal in URI", "ET INFO DYNAMIC_DNS Query to a *.gruppuso .com Domain", "ET INFO DYNAMIC_DNS Query to a *.deaftone.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nufszone .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jupiterns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.churchrez .org Domain", "ET INFO DYNAMIC_DNS Query to a *.serveusers .com Domain", "ET MALWARE SMTP Subject Line Contains C Path and EXE Possible Trojan Reporting Execution Path/Binary Name", "ET INFO Dotted Quad Host RAR Request", "ET INFO HTTP Request to a 3322.org.cn Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iceage .com .my Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pii .at Domain", "ET INFO DYNAMIC_DNS Query to a *.traeumtgerade .de Domain", "ET USER_AGENTS Suspicious User-Agent (Embarcadero URI Client/1.0)", "ET INFO DYNAMIC_DNS HTTP Request to a *.stuns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.cylone .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jwork .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.stocktester .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.ham-radio-op .net Domain", "ET WEB_SERVER Webserver Resolving Known Webshell CnC Domain (anonymousfox)", "ET INFO DYNAMIC_DNS Query to a *.2waky .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dubya .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.primeent .in Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.freedynamicdns .org Domain", "ET HUNTING SUSPICIOUS IRC - NICK and Win", "ET INFO DYNAMIC_DNS HTTP Request to a *.hopto .org Domain", "ET HUNTING Observed AutoDesk Domain in TLS SNI (api .autodesk .com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.hbmc .net Domain", "ET INFO DYNAMIC_DNS Query to a *.001www .com Domain", "ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1", "ET INFO DYNAMIC_DNS Query to a *.pce-cihazlari .com .tr Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.saucedchicago .com Domain", "ET INFO DYNAMIC_DNS Query to a *.usrsrc .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsalias .net Domain", "ET POLICY DNS Query to .onion proxy Domain (torwild.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ericfox .hk Domain", "ET INFO DYNAMIC_DNS Query to a *.dns .navy Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-an-engineer .com Domain", "ET INFO DYNAMIC_DNS Query to a *.isa-hockeynut .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.madhacker .biz Domain", "ET INFO HTTP Connection To DDNS Domain Redirectme.net", "ET INFO DYNAMIC_DNS HTTP Request to a *.keriss .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sammah .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.shitgoddamnhellfuck .com Domain", "ET INFO DYNAMIC_DNS Query to a *.etitrans .com Domain", "ET INFO DYNAMIC_DNS Query to a *.uzhi .ru Domain", "ET INFO DYNAMIC_DNS Query to a Suspicious *.dyn-dns.ru Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-home .com Domain", "ET POLICY Vulnerable Java Version 18.0.x Detected", "ET INFO DYNAMIC_DNS Query to a *.aussievitamin .com Domain", "ET

	INFO DYNAMIC_DNS Query to a *.is-into-anime .com Domain", "ET POLICY RDP Wrapper Download (bat)", "ET INFO DYNAMIC_DNS HTTP Request to a *.compuinter .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sandcherrysystems .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.v0x .eu Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homedns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.isthebe.st Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.3dxtras .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.ontheweb.nu Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ionexusa .com Domain", "ET INFO DYNAMIC_DNS Query to a *.usakoi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sne .jp Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.macao .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.puffballofevil .com Domain", "ET INFO DYNAMIC_DNS Query to *ontheweb.nu Domain (Sitelutions)", "ET INFO DYNAMIC_DNS HTTP Request to a *.host2go .net Domain", "ET HUNTING Office UA Retrieving Content on Unusually High Port", "ET INFO DYNAMIC_DNS HTTP Request to a *.southquay .com Domain", "ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response from Common SSL Port (Outbound from Client)", "ET INFO DYNAMIC_DNS Query to a *.mystakidis .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-mn .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ghostnation .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.nowddns .com Domain", "ET POLICY DNS Query to .onion proxy Domain (tor4pay.com)", "ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response", "ET INFO DYNAMIC_DNS Query to a *.minecraft .pe Domain", "ET INFO DYNAMIC_DNS Query to a *.toshibanetcam .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.industrialmill .com Domain", "ET MALWARE DNS Query Gauss Domain *.bestcomputeradvisor.com", "ET INFO DYNAMIC_DNS Query to a *.dyndns .tv Domain", "ET INFO DYNAMIC_DNS Query to a *.r-o-o-t .net Domain", "ET WEB_SERVER PHP REQUEST SuperGlobal in POST", "ET INFO DYNAMIC_DNS Query to a *.from-nm .com Domain", "ET INFO RealThinClient Outbound Communication", "ET INFO DYNAMIC_DNS HTTP Request to a *.liquidsphere .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-va .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.whatajack .com Domain", "ET INFO Obfuscated Split String (Double Q) 9", "ET INFO DYNAMIC_DNS Query to a *.alte .ca Domain", "ET SCAN Suspicious inbound to PostgreSQL port 5432", "ET INFO DYNAMIC_DNS Query to a *.offbitch .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sumibi .org Domain", "ET WEB_CLIENT Hex Obfuscation of arguments.callee % Encoding", "ET INFO DYNAMIC_DNS Query to a *.is-a-conservative .com Domain", "ET HUNTING Invalid User-Agent - MSIE 9 on Windows NT 5", "ET INFO URL Shortening Service Domain in DNS Lookup (kutti .co)", "ET INFO DYNAMIC_DNS Query to a *.gotdns .ch Domain", "ET EXPLOIT Possible TLS HeartBleed Unencrypted Request Method 3 (Inbound to Common SSL Port)", "ET HUNTING Generic Powershell DownloadFile Command", "ET INFO HTTP Request to a *.de.tf domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.access .ly Domain", "ET INFO DYNAMIC_DNS Query to a *.go .dyndns .org Domain", "ET INFO DYNAMIC_DNS Query to a *.sells-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.onmypc .biz Domain", "ET INFO Obfuscated Split String (Single Q) 11", "ET INFO DYNAMIC_DNS HTTP Request to a *.hot-hed .com Domain", "ET WEB_CLIENT Hex Obfuscation of substr %u UTF-8 Encoding", "ET INFO DYNAMIC_DNS Query to a *.tbt .mx Domain", "ET INFO DYNAMIC_DNS Query to a *.sococoffee .com Domain", "ET INFO Interactsh Domain in DNS Lookup (.interact .sh)", "ET INFO DYNAMIC_DNS Query to a *.cobra200 .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.traeumtgerade .de Domain", "ET INFO Dotted Quad Host DOC Request", "ET INFO DYNAMIC_DNS Query to a *.lotusshipping .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dumb1 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homeftp .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.intec .es Domain", "ET INFO DYNAMIC_DNS Query to a *.from-or .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.entergod .com Domain", "ET INFO DYNAMIC_DNS Query to a *.myiphost .com Domain", "ET INFO DYNAMIC_DNS Query to a *.justdied .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mysecuritycamera .net

	Domain", "ET INFO DYNAMIC_DNS Query to a *.sexcuatui .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-bookkeeper .com Domain", "ET INFO DYNAMIC_DNS Query to a *.lospenitentes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.freetruthordare .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jcor .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.from-wv .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jlengineering .se Domain", "ET USER_AGENTS Suspicious User Agent (explorersvc)", "ET POLICY Inbound RDP Connection with TLS Security Protocol Requested", "ET INFO Observed DNS Query to .world TLD", "ET INFO DYNAMIC_DNS HTTP Request to a *.herbalhealthyh20 .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lanas .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-pr .com Domain", "ET INFO DYNAMIC_DNS Query to a *.joiavip .com .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-chef .net Domain", "ET INFO DYNAMIC_DNS Query to a *.here-for-more .info Domain", "ET USER_AGENTS Suspicious User-Agent (urlRequest)", "ET INFO DYNAMIC_DNS Query to a *.thainewasia .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thinksnow .net Domain", "ET USER_AGENTS Observed Suspicious UA (system_file/2.0)", "ET INFO DYNAMIC_DNS Query to a *.chaseinator .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ma .com Domain", "ET INFO DYNAMIC_DNS Query to a *.from-md .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.riaspengantinluwes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.toh .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cashit .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tx2600 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.wikaba .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servebeer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-linux-user .org Domain", "ET INFO DYNAMIC_DNS Query to a *.sourcekeeper .com Domain", "ET INFO DYNAMIC_DNS Query to a *.caribbeanpremierhotels .com Domain", "ET POLICY DNS Query to DynDNS Domain *.servequake .com", "ET INFO DYNAMIC_DNS HTTP Request to a *.ucvradio .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ssmailer .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bouncers4rent .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.apostolof .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.www1 .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ddns.info Domain", "ET INFO DYNAMIC_DNS Query to a *.changeip .biz Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oast .online)", "ET INFO DYNAMIC_DNS Query to a *.cybertv .tv Domain", "ET INFO DYNAMIC_DNS Query to a *.falcongreenenergy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lee .mx Domain", "ET INFO DYNAMIC_DNS Query to a *.carcano .me Domain", "ET INFO DYNAMIC_DNS Query to a *.angellombardi .com Domain", "ET INFO DYNAMIC_DNS Query to a *.shareroute .org Domain", "ET EXPLOIT Cisco Smart Install Exploitation Tool - GetConfig", "ET INFO DYNAMIC_DNS Query to a *.pixelfucker .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jodymaroni .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ptchat .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-ar .com Domain", "ET INFO DYNAMIC_DNS Query to a *.jnrcs .org Domain", "ET HUNTING Google Adwords Conversion not from Google", "ET HUNTING Possible Covid19 Themed Email Spam Outbound M5", "ET INFO DYNAMIC_DNS HTTP Request to a *.as19557 .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ralphs .com .au Domain", "ET INFO DYNAMIC_DNS Query to a *.argusdenshi .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.alanrjr .net Domain", "ET INFO DYNAMIC_DNS Query to a *.evs .net .br Domain", "ET INFO DYNAMIC_DNS Query to a *.primeent .in Domain", "GPL TELNET TELNET login failed", "ET WEB_SERVER WebShell Generic - ELF File Uploaded", "ET INFO DYNAMIC_DNS HTTP Request to a *.dtdns .org Domain", "ET HUNTING SUSPICIOUS SMTP EXE - EXE SMTP Attachment", "ET INFO DYNAMIC_DNS HTTP Request to a *.h0stname .net Domain", "ET INFO DYNAMIC_DNS Query to a *.mza .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-gone .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-very-evil .org Domain", "ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.epic)", "ET INFO DYNAMIC_DNS Query to a *.solfa .org Domain", "ET INFO DYNAMIC_DNS Query to a

	*.dynamicdns .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.duckdns .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.4nmn .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ourhobby .com Domain", "ET INFO DYNAMIC_DNS Query to a *.onmypc .info Domain", "ET INFO DYNAMIC_DNS Query to a *.linkin .tw Domain", "ET INFO Out-of-Band Interaction Domain in DNS Lookup (oast .me)", "ET HUNTING Suspicious POST Request with Possible COVID-19 URI M2", "ET INFO DYNAMIC_DNS HTTP Request to a *.javahound .com Domain", "ET INFO DYNAMIC_DNS Query to a *.australia .ai Domain", "ET INFO HTTP Request to a *.buzz domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-at-home .com Domain", "ET INFO Suspicious Self Signed SSL Certificate to 'My Company Ltd'", "ET INFO DYNAMIC_DNS Query to a *.surfnet .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.pltimes .net Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns-free .com Domain", "ET POLICY Proxy TRACE Request - inbound", "ET INFO DYNAMIC_DNS Query to a *.from-ut .com Domain", "ET USER_AGENTS Observed Suspicious UA (Hello-World)", "ET GAMES Growtopia Hack - WrongGrow CnC Activity", "ET INFO DYNAMIC_DNS Query to a *.tru .io Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-vt .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rainbowcup .com Domain", "ET INFO DYNAMIC_DNS Query to a *.riaspengantinluwes .com Domain", "ET INFO Suspicious Domain (*.icu) in TLS SNI", "ET INFO DYNAMIC_DNS Query to a *.tecnova .com .br Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.actsministries .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bellasclown .com Domain", "ET INFO Doc Template Downloaded from DDNS Site", "ET INFO External IP Lookup Domain in DNS Lookup (ip .bablosoft .com)", "ET INFO DYNAMIC_DNS Query to a *.iownyour .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.partybag .com Domain", "ET HUNTING SUSPICIOUS Possible automated connectivity check (www.yahoo.com)", "ET INFO DYNAMIC_DNS Query to a *.0bit .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.carcano .me Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.visalawyer .co .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.albertn .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.thenest .org Domain", "ET INFO DYNAMIC_DNS Query to a *.likescandy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.groks-this .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hec .to Domain", "ET INFO DYNAMIC_DNS Query to a *.annaffiare .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.v6 .army Domain", "ET INFO DYNAMIC_DNS Query to a *.cleansite .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.damnserver .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.corum .com Domain", "ET INFO DNS Query for a Suspicious *.qc.cx domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.callmark .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bagus .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dynamai .com Domain", "ET INFO URL Shortener Service Domain in DNS Lookup (s .id)", "ET INFO DYNAMIC_DNS Query to a *.organiccrap .com Domain", "ET HUNTING SUSPICIOUS Possible Office Doc with Embedded VBA Project", "ET INFO DYNAMIC_DNS HTTP Request to a *.fintech-llc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sitaci .com Domain", "ET INFO DYNAMIC_DNS Query to a *.sarah-lai .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sulsel .go .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.serveexchange .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ospachat .com Domain", "ET INFO HTTP Request to a *.ch.tf domain", "ET INFO DYNAMIC_DNS Query to a *.galecsy .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homeunix .net Domain", "ET INFO DYNAMIC_DNS Query to a *.wifizone .org Domain", "ET INFO DNS Query to Free Hosting Domain (freevnn . com)", "ET POLICY Serialized Java Payload via RMI Response", "ET HUNTING SUSPICIOUS IRC - PRIVMSG *.(exe|tar|tgz|zip) download command", "ET INFO DYNAMIC_DNS Query to a *.3cm .us Domain", "ET INFO DYNAMIC_DNS Query to a *.shekinahphotography .com Domain", "ET INFO DYNAMIC_DNS Query to a *.birdsofnorthamerica .ca Domain", "ET ADWARE_PUP Observed DNS Query to Known PUA Host Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ketubruk .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ezua .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.coolfire25 .com Domain", "ET INFO DYNAMIC_DNS

	Query to a *.prs7 .org Domain", "ET WEB_CLIENT Hex Obfuscation of charCodeAt % Encoding", "ET INFO DYNAMIC_DNS HTTP Request to a *.spacetechnology .net Domain", "ET HUNTING Observed DNS Query for EmerDNS TLD (.lib)", "ET INFO Minimal HTTP GET Request to Bit.ly", "ET HUNTING Possible Covid19 Themed Email Spam Outbound M3", "ET INFO DYNAMIC_DNS Query to a *.teachmetofish .net Domain", "GPL ATTACK_RESPONSE id check returned web", "ET INFO File Sharing Service Domain in DNS Lookup (link .storjshare .io)", "ET POLICY DNS Query to DynDNS Domain *.ilovecollege .info", "ET INFO DYNAMIC_DNS HTTP Request to a *.axfor .com Domain", "ET INFO DYNAMIC_DNS Query to a *.ssott .com Domain", "ET INFO DYNAMIC_DNS Query to a *.hiddencorner .org Domain", "ET INFO DYNAMIC_DNS Query to a *.aptrc .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.kmodem .org Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-doctor .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rock-n-roll .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sportseducationinstructors .org Domain", "ET INFO DYNAMIC_DNS Query to a *.blacknapkins .org Domain", "ET INFO DYNAMIC_DNS Query to a *.kirelli .net Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (dm9rZS1XbWlNZXRob2) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.klockars .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.lflinkup .org Domain", "ET INFO DYNAMIC_DNS Query to a *.myjamesonline .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dynu .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mine .nu Domain", "ET INFO Obfuscated Split String (Single Q) 5", "ET INFO DYNAMIC_DNS HTTP Request to a *.fatdiary .org Domain", "ET INFO DYNAMIC_DNS Query to a *.from-ga .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-with-theband .com Domain", "ET MALWARE Suspicious flash_player.exe Download", "ET HUNTING SUSPICIOUS *.pdf.exe in HTTP HEADER", "ET INFO DYNAMIC_DNS HTTP Request to a *.softwarefinesse .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torgateway.org)", "ET WEB_SERVER WebShell - Romanian Webshell", "ET INFO DYNAMIC_DNS HTTP Request to a *.forss .to Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.groks-this .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.fhi .hk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.homesecuritymac .com Domain", "ET HUNTING Windows Commands and Variables in DNS Reply", "ET INFO DYNAMIC_DNS Query to a *.mynumber .org Domain", "ET INFO DYNAMIC_DNS Query to a *.reasonman .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mynetav .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.x3mfly .com Domain", "ET INFO DYNAMIC_DNS Query to a *.is-into-cars .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mudchute .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.blogsite .org Domain", "ET INFO DYNAMIC_DNS Query to a *.us .to Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-me .org Domain", "ET INFO DYNAMIC_DNS Query to a *.smirt .ch Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bmvl .ru Domain", "ET INFO DYNAMIC_DNS Query to a *.apostolof .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.athissite.com Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.shacknet .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cohens .org .il Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ubntddns .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.smirt .ch Domain", "ET INFO DYNAMIC_DNS Query to a *.compy .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-hunter .com Domain", "ET INFO DYNAMIC_DNS Query to a *.pintravel .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-lost .org Domain", "ET INFO DYNAMIC_DNS Query to a *.jumpingcrab .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.be .sexy Domain", "ET INFO DYNAMIC_DNS Query to a *.good-newz .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.triki .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.is-with-theband .com Domain", "ET INFO DYNAMIC_DNS Query to a *.zelslonik .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-celticsfan .org Domain", "ET INFO DYNAMIC_DNS Query to a *.likes-pie .com Domain", "ET INFO DYNAMIC_DNS Query to a *.chickenkiller .com Domain", "ET INFO DYNAMIC_DNS Query to a *.wayner .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.knowsitall .info Domain", "ET INFO DYNAMIC_DNS

	Query to a *.reg .my .id Domain", "ET INFO DYNAMIC_DNS Query to a *.jodymaroni .com Domain", "ET HUNTING Suspicious Request for Doc to IP Address with Terse Headers", "ET INFO DYNAMIC_DNS Query to a *.datacommunicationsinc .com Domain", "ET INFO DYNAMIC_DNS Query to a *.biometrika .cl Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-liberal .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.here-for-more .info Domain", "ET INFO DYNAMIC_DNS Query to a *.dns1 .us Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.plugs .it Domain", "ET INFO DYNAMIC_DNS Query to a *.b0tnet .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsfailover .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.livewave .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.asadanasemesta .co .id Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.rren .ch Domain", "ET INFO Observed Remote Management Software Domain in DNS Lookup (syncromsp .com)", "ET INFO DYNAMIC_DNS Query to a *.ra3 .us Domain", "ET INFO DYNAMIC_DNS Query to a *.edns .biz Domain", "ET INFO DYNAMIC_DNS Query to a *.visalawyer .co .uk Domain", "ET INFO DYNAMIC_DNS Query to a *.nm7 .cc Domain", "ET POLICY HTTP Request to a *.noc.su domain", "ET POLICY DNS Query to .onion proxy Domain (bladetor.com)", "ET INFO DYNAMIC_DNS HTTP Request to a *.gatesweb .info Domain", "ET INFO DYNAMIC_DNS Query to a *.is-a-soxfan .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.leitungsen .de Domain", "ET INFO DYNAMIC_DNS Query to a *.pogramkran .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.servebbs .net Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (FydC1Qcm9) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.gilead .org .il Domain", "ET INFO DYNAMIC_DNS Query to a *.from-wy .com Domain", "ET INFO HTTP Request to a *.orge.pl Domain", "ET INFO DYNAMIC_DNS Query to a *.dulcegarii-culinare .ro Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.sino .tw Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (dy1PYmp) in DNS TXT Reponse", "ET INFO DYNAMIC_DNS HTTP Request to a *.redirectme .net Domain", "ET POLICY DNS Query to DynDNS Domain *.redirectme .net", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-conservative .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.3utilities .com Domain", "ET INFO Doc Requesting Remote Template (.dot)", "ET INFO Query for Suspicious .cz.tf Domain", "ET INFO DYNAMIC_DNS Query to a *.jungleheart .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dubya .info Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.barbaforte .org Domain", "ET INFO DYNAMIC_DNS Query to a *.tedfullwood .com Domain", "ET INFO DYNAMIC_DNS Query to a *.selfip .org Domain", "ET INFO DYNAMIC_DNS Query to a *.cloudns .net Domain", "ET POLICY DNS Query to DynDNS Domain *.servehttp .com", "ET POLICY Vulnerable Java Version 14.0.x Detected", "ET POLICY HTTP POST invalid method case outbound", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (History/Firefox_)", "ET INFO Query for Suspicious .net.tf Domain", "ET USER_AGENTS Observed Suspicious UA (Hello, World)", "ET INFO DYNAMIC_DNS Query to a *.monitoryourinternet .com Domain", "ET POLICY Vulnerable Java Version 15.0.x Detected", "ET INFO DYNAMIC_DNS Query to a *.answersbot .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnset .com Domain", "ET INFO PS1XML Powershell File Request", "ET INFO DYNAMIC_DNS HTTP Request to a *.buyshouses .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hioctanefuel .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-a-therapist .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.getamonkey .com Domain", "ET INFO DYNAMIC_DNS Query to a *.bugaloop .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.tdkare .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dsmtp .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.airlinemeals .net Domain", "ET INFO DYNAMIC_DNS Query to a *.lczipper .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.winkel .com .ar Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.freeddns .us Domain", "ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.ml)", "ET INFO DYNAMIC_DNS HTTP Request to a *.showmyhomes .com Domain", "ET INFO DYNAMIC_DNS Query to a *.tafca .co .uk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.24-7 .ro Domain", "ET POLICY

	DNS Query to DynDNS Domain *.unusualperson .com", "ET INFO DYNAMIC_DNS Query to a *.ttkacz .com Domain", "ET INFO DYNAMIC_DNS Query to a *.est-le-patron .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.linux70 .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-nd .com Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Hardware.txt)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ryanandjen .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.vpndns .net Domain", "ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (ctT2J) in DNS TXT Response", "ET INFO DYNAMIC_DNS HTTP Request to a *.hackershack .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.seahorsenet .com Domain", "ET INFO DYNAMIC_DNS Query to a *.homingbeacon .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.iamallama .com Domain", "ET WEB_CLIENT SEO Injection/Fraud Domain in DNS Lookup (stat.trackstatisticsss .com)", "ET INFO DYNAMIC_DNS Query to a *.slyip.com Domain", "ET POLICY Vulnerable Java Version 1.4.x Detected", "ET INFO DYNAMIC_DNS Query to a *.bedwell .org Domain", "ET INFO HTTP POST to WP Theme Directory Without Referer", "ET INFO DYNAMIC_DNS Query to a *.xxuz .com Domain", "ET INFO DYNAMIC_DNS Query to a *.isageek .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.circusslaves .com Domain", "ET POLICY DNS Query to .onion proxy Domain (torpovider.org)", "ET INFO DYNAMIC_DNS HTTP Request to a *.h4ck .me Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jundy .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.hobby-site .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.americajhon .com .pe Domain", "ET INFO DYNAMIC_DNS Query to a *.synoserver .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.civvic .ro Domain", "ET INFO DYNAMIC_DNS Query to a *.kaohsiung .tv Domain", "ET POLICY DNS Query to .onion proxy Domain (browsetor.com)", "ET INFO DYNAMIC_DNS Query to a *.homelinux .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.pittentrepreneur .com Domain", "ET HUNTING SUSPICIOUS IRC - NICK and Possible Windows XP/7", "ET INFO DYNAMIC_DNS HTTP Request to a *.pedie .info Domain", "ET WEB_SERVER PHP SESSION SuperGlobal in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.recruitment7 .com Domain", "ET INFO DYNAMIC_DNS Query to a *.melakaboy .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dougtreadwell .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.midjava .com Domain", "ET INFO Lockbit Ransomware Related Domain in DNS Lookup (bigblog .at)", "ET INFO DYNAMIC_DNS Query to a *.360technologies .ca Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cbu .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.womenclothingtoday .com Domain", "ET INFO DYNAMIC_DNS Query to a *.poormanscow .com Domain", "ET INFO DYNAMIC_DNS Query to a *.smlsoft .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.likes-pie .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.isa-hockeynut .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.inet2 .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to *.byinter.net Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.hondascooterparts .com Domain", "ET INFO DYNAMIC_DNS Query to a *.mylftv .com Domain", "ET INFO DYNAMIC_DNS Query to a *.shogun .ca Domain", "ET INFO DYNAMIC_DNS Query to a *.lqtai .com Domain", "ET INFO DYNAMIC_DNS Query to a *.btarena .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.cnr .com .pk Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-il .com Domain", "ET INFO DYNAMIC_DNS Query to a *.djbomba .one .pl Domain", "ET ATTACK_RESPONSE UTF8 base64 string /This Program/ in DNS TXT Reponse", "ET INFO DYNAMIC_DNS Query to a *.from-va .com Domain", "ET INFO DYNAMIC_DNS Query to a *.cloudbusinessportal .com Domain", "ET INFO DYNAMIC_DNS Query to a *.wwwhost .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.uzhi .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.themcleans .us Domain", "ET INFO HTTP Connection To DDNS Domain myftp.com", "ET INFO DYNAMIC_DNS HTTP Request to a *.sexidude .com Domain", "ET INFO DYNAMIC_DNS Query to a *.dailyview .tw Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsalias.ru Domain", "ET INFO DYNAMIC_DNS Query to a *.isa-geek .com Domain", "ET INFO DYNAMIC_DNS Query to *.kwik.to Domain (Sitelutions)", "ET INFO DYNAMIC_DNS Query to a *.ugo .si Domain", "ET INFO DYNAMIC_DNS HTTP

	Request to a *.mnode .net Domain", "ET POLICY DNS Query to DynDNS Domain *.mydissent .net", "ET POLICY HTTP connection to net78.net Free Web Hosting (Used by Various Trojans)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ham .gd Domain", "ET HUNTING Double User-Agent (User-Agent User-Agent)", "ET POLICY Inbound RDP Connection with Minimal Security Protocol Requested", "ET INFO DNS Query for Suspicious .co.cc Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.mkahowes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.reves .cl Domain", "ET INFO DYNAMIC_DNS Query to a *.battlecore .ru Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.couchpotatofries .org Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns-blog .com Domain", "ET EXPLOIT Possible Zephyr RTOS ICMPv4 Stack Buffer Overflow", "ET INFO DYNAMIC_DNS HTTP Request to a *.dnsip.ru Domain", "ET HUNTING Observed Suspicious Reversed String Inbound (StrReverse)", "ET INFO DYNAMIC_DNS HTTP Request to a *.ygto .com Domain", "ET INFO DYNAMIC_DNS Query to a *.d-n-s .name Domain", "ET INFO DYNAMIC_DNS Query to a *.gigaportal .pl Domain", "ET INFO DYNAMIC_DNS Query to a *.jonward .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ubergate .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.from-id .com Domain", "ET INFO DYNAMIC_DNS Query to a *.on-the-web .tv Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.2waky .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ber-engineering .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.does-it .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.for-better .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.space-to-rent .com Domain", "ET INFO DYNAMIC_DNS Query to a *.2mydns .net Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.yiff .fi Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.gotgeeks.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bbsindex.com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.bmrresources .com Domain", "ET WEB_CLIENT Google Chrome Pdfium JPEG2000 Heap Overflow", "ET INFO DYNAMIC_DNS HTTP Request to a *.rogerthedog .com Domain", "ET ATTACK_RESPONSE Output of id command from HTTP server", "ET INFO DYNAMIC_DNS HTTP Request to a *.homelinux .org Domain", "ET INFO HTTP POST Request to Suspicious *.ma Domain", "ET INFO HTTP Connection To DDNS Domain Hopto.org", "ET INFO DYNAMIC_DNS Query to a *.green-heroes .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.jumpingcrab .com Domain", "ET WEB_SERVER PHP GET SuperGlobal in POST", "ET INFO DYNAMIC_DNS Query to a *.home .kg Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.is-very-sweet .org Domain", "ET INFO DYNAMIC_DNS Query to a *.nx .tc Domain", "ET INFO DYNAMIC_DNS Query to a *.geofuzz .net Domain", "ET WEB_SERVER WebShell - Symlink_Sa", "ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server)", "ET HUNTING Suspicious rundll32.exe in URI", "ET INFO DYNAMIC_DNS HTTP Request to a *.psybnc .org Domain", "ET INFO DYNAMIC_DNS Query to a *.https443 .net Domain", "ET INFO DYNAMIC_DNS Query to a *.joe .dj Domain", "ET INFO DYNAMIC_DNS Query to a *.cleansite .us Domain", "ET INFO DYNAMIC_DNS Query to a *.motorwisemechanical .com .au Domain", "ET INFO DYNAMIC_DNS Query to a *.tscng .org Domain", "ET INFO DYNAMIC_DNS Query to a *.now-dns .top Domain", "ET INFO HTTP Request to a *.co.com.au domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.ycare .org Domain", "ET INFO DYNAMIC_DNS Query to a *.dyndns .biz Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.aptrc .tw Domain", "ET POLICY HTTP traffic on port 443 (DELETE)", "ET INFO DYNAMIC_DNS Query to a *.eternalimpressions .com Domain", "ET PHISHING Observed DNS Query to Known Scam/Phishing Domain", "ET INFO Obfuscated Split String (Single Q) 8", "ET INFO DYNAMIC_DNS HTTP Request to a *.khabbaby .com Domain", "ET INFO DYNAMIC_DNS HTTP Request to a *.empires-r .us Domain", "ET POLICY Vulnerable Java Version 1.8.x Detected"
Неизвестный тип трафика	"ET JA3 Hash - Possible Malware - USPS Malspam", "ET JA3 Hash - Possible Malware - Neutrino", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M3", "ET JA3 Hash - Possible Malware - NuclearEK", "ET JA3 Hash - [Abuse.ch] Possible Adware", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M8", "ET HUNTING Double Extension VBS File Downloaded from Discord (Request)", "ET JA3

	Hash - [Abuse.ch] Possible Troldesh Ransomware", "ET JA3 Hash - Possible Malware - Various Malfams", "ET USER_AGENTS User-Agent (_TEST_)", "ET JA3 Hash - Possible Malware - Various EK", "ET JA3 Hash - Possible Malware - Boleto Malspam", "ET JA3 Hash - Possible Malware - Various Malspam/RigEK/Dreambot", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M5", "ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from Internal Host - NOTIFY", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M3", "ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from External Host - NOTIFY", "ET HUNTING Double Extension ZIP File Downloaded from Discord (Request)", "ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from Internal Host - SUBSCRIBE/UNSUBSCRIBE", "ET JA3 Hash - Possible Malware - Fake Firefox Font Update", "ET JA3 Hash - Possible Malware - TBot / Skynet Tor Botnet", "ET JA3 Hash - Possible Malware - Dridex", "ET INFO Generic - Mozilla 4.0 EXE Request", "ET JA3 Hash - sqlmap (tested: v1.0-dev kali)", "ET HUNTING Double Extension EXE File Downloaded from Discord (Request)", "ET HUNTING SUSPICIOUS .LNK File Inside of Zip", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M9", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M1", "ET JA3 Hash - [Abuse.ch] Possible Tofsee", "ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M2", "ET JA3 HASH - Possible InnocenceBot CnC", "ET JA3 Hash - [Abuse.ch] Possible Dridex", "ET USER_AGENTS Node XMLHTTP User-Agent", "ET JA3 Hash - Rapid7 Nexpose", "ET JA3 Hash - Possible Malware - Various Malspam/RigEK", "ET JA3 Hash - Possible Malware - RigEK", "ET JA3 Hash - [Abuse.ch] Possible Gozi", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M7", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M4", "ET JA3 Hash - Possible Malware - Various RigEK/Cryptowall/Dridex", "ET JA3 Hash - Nikto (tested v2.1.6)", "ET JA3 Hash - Metasploit HeartBleed Scanner", "ET JA3 Hash - WPScan (tested: 2.9 Kali)", "ET INFO Suspicious Empty Accept-Encoding Header", "ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M3", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M6", "ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from External Host - SUBSCRIBE/UNSUBSCRIBE", "ET JA3 Hash - Metasploit CCS Scanner", "ET HUNTING Double Extension PIF File Downloaded from Discord (Request)", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M6", "ET JA3 Hash - [Abuse.ch] Possible Torrentlocker", "ET HUNTING Base64 Encoded ipconfig In Server Response M2", "ET JA3 Hash - Possible Malware - Eitest Chrome Popup", "ET JA3 Hash - [Abuse.ch] Possible Adwind", "ET JA3 Hash - Metaploit http scanner (tested: 4.11.5 Kali)", "ET JA3 Hash - Possible Malware - AnglerEK", "ET JA3 HASH - Possible BAZAR Backdoor CnC", "ET HUNTING Base64 Encoded ipconfig In Server Response M1", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M5", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M9", "ET JA3 Hash - Possible Malware - Trickbot", "ET JA3 Hash - Possible Malware - Gootkit", "ET JA3 Hash - [Abuse.ch] Possible Ransomware", "ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)", "ET JA3 Hash - [Abuse.ch] Possible Quakbot", "ET JA3 Hash - Possible Malware - Malspam", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M2", "ET JA3 Hash - mitmproxy", "ET JA3 Hash - Nikto (tested 2.1.6 - Kali)", "ET JA3 Hash - [Abuse.ch] Possible Trickbot", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M2", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M7", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M1", "ET JA3 Hash - sqlmap (tested: v1.0.7.0 OS X)", "ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M1", "ET JA3 Hash - Possible Superfish", "ET JA3 Hash - [Abuse.ch] Possible Gootkit", "ET JA3 Hash - Possible Malware - Eitest/AnglerEK", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M4", "ET JA3 Hash - Metasploit SSL Scanner", "ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M8", "ET GAMES Multiple Game Cheat Application Related Activity", "ET HUNTING Base64 Encoded ipconfig In Server Response M3"
Блокирование атак	"ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 69", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 684", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 148", "ET COMPROMISED Known Compromised or Hostile Host

	Traffic group 76", "ET CINS Active Threat Intelligence Poor Reputation IP group 53", "GPL NETBIOS SMB DCERPC Workstation Service bind attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 64", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 699", "ET TOR Known Tor Exit Node Traffic group 119", "ET CINS Active Threat Intelligence Poor Reputation IP group 80", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 174", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 92", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 17", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 9", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 155", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 72", "GPL RPC tooltalk UDP overflow attempt", "ET TOR Known Tor Exit Node Traffic group 64", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 87", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 179", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 16", "ET CINS Active Threat Intelligence Poor Reputation IP group 21", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 686", "ET CINS Active Threat Intelligence Poor Reputation IP group 58", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 26", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 42", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 81", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 293", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 85", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 204", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 608", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 614", "ET TOR Known Tor Exit Node Traffic group 7", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 207", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 115", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 2", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 58", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 52", "ET TOR Known Tor Exit Node Traffic group 35", "ET TOR Known Tor Exit Node Traffic group 62", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 116", "ET WEB_SPECIFIC_APPS Webmin Directory Traversal", "ET DROP Spamhaus DROP Listed Traffic Inbound group 33", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 50", "GPL NETBIOS SMB-DS DCERPC Workstation Service unicode bind attempt", "ET TOR Known Tor Exit Node Traffic group 116", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 7", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 250", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 120", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 137", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 749", "ET TOR Known Tor Exit Node Traffic group 76", "ET CINS Active Threat Intelligence Poor Reputation IP group 31", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 57", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 66", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 161", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 95", "ET CINS Active Threat Intelligence Poor Reputation IP group 77", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 199", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 11", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 654", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 13", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 783", "GPL SNMP null community string attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 609", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 140", "ET TOR Known Tor Exit Node Traffic group 117", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 726", "ET TOR Known Tor Exit Node Traffic group 48", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 128", "ET CINS Active Threat Intelligence Poor Reputation IP group 54", "ET CINS Active Threat Intelligence Poor Reputation IP group 82", "ET DROP Spamhaus DROP Listed Traffic Inbound group 15", "ET ATTACK_RESPONSE Obfuscated Batch Script Inbound M1", "ET SNMP missing community string attempt 2", "ET 3CORESec Poor Reputation IP group 6", "ET TOR Known Tor Relay/Router (Not Exit)

	Node Traffic group 76", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 709", "ET DROP Spamhaus DROP Listed Traffic Inbound group 8", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 48", "ET DROP Spamhaus DROP Listed Traffic Inbound group 3", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 79", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 253", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 753", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 768", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 1", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 65", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 72", "GPL MISC CVS invalid module response", "ET TOR Known Tor Exit Node Traffic group 86", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 103", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 5", "ET TOR Known Tor Exit Node Traffic group 90", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 20", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 201", "ET TOR Known Tor Exit Node Traffic group 108", "ET TOR Known Tor Exit Node Traffic group 106", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 214", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 156", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 730", "ET CINS Active Threat Intelligence Poor Reputation IP group 71", "ET DROP Spamhaus DROP Listed Traffic Inbound group 28", "ET 3CORESec Poor Reputation IP group 9", "GPL FTP PORT bounce attempt", "ET CINS Active Threat Intelligence Poor Reputation IP group 91", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 650", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 106", "ET TOR Known Tor Exit Node Traffic group 80", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 277", "ET TOR Known Tor Exit Node Traffic group 57", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 701", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 315", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 161", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 23", "ET 3CORESec Poor Reputation IP group 1", "ET CINS Active Threat Intelligence Poor Reputation IP group 96", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 15", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 56", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 295", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 78", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 169", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 398", "ET 3CORESec Poor Reputation IP group 15", "ET CINS Active Threat Intelligence Poor Reputation IP group 98", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 3", "GPL MISC UPnP Location overflow", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 37", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 52", "ET 3CORESec Poor Reputation IP group 7", "ET CINS Active Threat Intelligence Poor Reputation IP group 44", "ET CINS Active Threat Intelligence Poor Reputation IP group 46", "GPL NETBIOS DCERPC Workstation Service direct service access attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 202", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 232", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 260", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 152", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 690", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 188", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 68", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 223", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 385", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 55", "GPL MISC CVS non-relative path error response", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 10", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 63", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 50", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 34", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 685", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 141", "ET DROP Spamhaus DROP Listed Traffic Inbound group 29", "GPL RPC sadmind query with root credentials attempt UDP", "ET TOR

	Known Tor Exit Node Traffic group 52", "ET 3CORESec Poor Reputation IP group 28", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 111", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 595", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 651", "ET TOR Known Tor Exit Node Traffic group 32", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 301", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 781", "ET CINS Active Threat Intelligence Poor Reputation IP group 85", "ET CINS Active Threat Intelligence Poor Reputation IP group 57", "ET CINS Active Threat Intelligence Poor Reputation IP group 34", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 1", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 245", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 226", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 679", "ET DROP Spamhaus DROP Listed Traffic Inbound group 35", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 154", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 405", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 612", "GPL IMAP delete overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 639", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 101", "ET TOR Known Tor Exit Node Traffic group 70", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 40", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 630", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 194", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 629", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 75", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 107", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 712", "ET CINS Active Threat Intelligence Poor Reputation IP group 3", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 36", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 310", "GPL NETBIOS DCERPC Workstation Service direct service bind attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 782", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 164", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 284", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 176", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 460", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 112", "ET TOR Known Tor Exit Node Traffic group 83", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 647", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 391", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 775", "GPL IMAP unsubscribe literal overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 143", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 624", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 164", "ET TOR Known Tor Exit Node Traffic group 28", "ET TOR Known Tor Exit Node Traffic group 68", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 796", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 53", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 54", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 10", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 137", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 158", "ET DROP Spamhaus DROP Listed Traffic Inbound group 13", "ET DROP Spamhaus DROP Listed Traffic Inbound group 26", "ET TOR Known Tor Exit Node Traffic group 94", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 632", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 642", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 167", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 71", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 748", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 198", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 119", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 312", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 384", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 646", "GPL IMAP rename overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 733", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 105", "ET

	TOR Known Tor Relay/Router (Not Exit) Node Traffic group 3", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 397", "ET CINS Active Threat Intelligence Poor Reputation IP group 63", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 151", "ET TOR Known Tor Exit Node Traffic group 38", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 183", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 113", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 403", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 741", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 40", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 802", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 204", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 171", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 660", "ET CINS Active Threat Intelligence Poor Reputation IP group 4", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 82", "ET CINS Active Threat Intelligence Poor Reputation IP group 18", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 144", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 126", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 734", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 762", "ET EXPLOIT CISCO FIREWALL SNMP Buffer Overflow Extrabacon (CVE-2016-6366)", "ET TOR Known Tor Exit Node Traffic group 23", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 22", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 90", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 401", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 392", "ET TOR Known Tor Exit Node Traffic group 39", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 409", "ET TOR Known Tor Exit Node Traffic group 82", "ET 3CORESec Poor Reputation IP group 5", "ET CINS Active Threat Intelligence Poor Reputation IP group 6", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 100", "ET 3CORESec Poor Reputation IP group 26", "ET CINS Active Threat Intelligence Poor Reputation IP group 90", "ET CINS Active Threat Intelligence Poor Reputation IP group 70", "ET SNMP missing community string attempt 1", "ET TOR Known Tor Exit Node Traffic group 61", "ET TOR Known Tor Exit Node Traffic group 10", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 46", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 131", "ET TOR Known Tor Exit Node Traffic group 50", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 270", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 95", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 143", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 652", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 682", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 8", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 269", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 99", "ET TOR Known Tor Exit Node Traffic group 96", "GPL SNMP PROTOS test-suite-trap-app attempt", "ET 3CORESec Poor Reputation IP group 25", "ET CINS Active Threat Intelligence Poor Reputation IP group 43", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 145", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 175", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 262", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 620", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 170", "ET CINS Active Threat Intelligence Poor Reputation IP group 45", "GPL IMAP subscribe overflow attempt", "ET CINS Active Threat Intelligence Poor Reputation IP group 50", "ET CINS Active Threat Intelligence Poor Reputation IP group 27", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 628", "ET DROP Spamhaus DROP Listed Traffic Inbound group 24", "ET DROP Spamhaus DROP Listed Traffic Inbound group 31", "GPL MISC UPnP malformed advertisement", "ET VOIP Possible Misuse Call from Cisco ooh323", "ET TOR Known Tor Exit Node Traffic group 79", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 2", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 66", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 156", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 234", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 643", "GPL IMAP EXPLOIT

	partial body overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 700", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 787", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 12", "ET CINS Active Threat Intelligence Poor Reputation IP group 37", "ET DROP Spamhaus DROP Listed Traffic Inbound group 22", "ET TOR Known Tor Exit Node Traffic group 16", "ET CINS Active Threat Intelligence Poor Reputation IP group 5", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 167", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 383", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 606", "ET CINS Active Threat Intelligence Poor Reputation IP group 28", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 208", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 691", "ET DROP Spamhaus DROP Listed Traffic Inbound group 6", "ET TOR Known Tor Exit Node Traffic group 99", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 313", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 792", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 680", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 41", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 135", "ET CINS Active Threat Intelligence Poor Reputation IP group 47", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 23", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 138", "ET CINS Active Threat Intelligence Poor Reputation IP group 88", "ET TOR Known Tor Exit Node Traffic group 46", "ET TOR Known Tor Exit Node Traffic group 95", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 186", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 708", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 212", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 237", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 296", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 136", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 735", "ET WEB_SERVER Double Encoded Characters in URI (../)", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 104", "ET CINS Active Threat Intelligence Poor Reputation IP group 2", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 133", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 127", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 283", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 150", "ET TOR Known Tor Exit Node Traffic group 47", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 244", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 236", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 38", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 209", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 282", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 134", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 698", "ET CINS Active Threat Intelligence Poor Reputation IP group 1", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 77", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 151", "ET TOR Known Tor Exit Node Traffic group 98", "GPL RPC mountd UDP mount path overflow attempt", "ET TOR Known Tor Exit Node Traffic group 104", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 86", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 67", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 297", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 596", "ET WEB_CLIENT Winzip 15.0 WZFLDVW.OCX IconIndex Property Denial of Service", "ET TOR Known Tor Exit Node Traffic group 27", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 175", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 625", "ET CINS Active Threat Intelligence Poor Reputation IP group 100", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 314", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 731", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 196", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 93", "ET TOR Known Tor Exit Node Traffic group 53", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 694", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 142", "GPL FTP RNFR ././ attempt", "ET TOR Known Tor Exit Node Traffic

	group 40", "ET TOR Known Tor Exit Node Traffic group 103", "GPL RPC mountd TCP mount path overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 4", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 172", "GPL IMAP auth overflow attempt", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 51", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 60", "ET CINS Active Threat Intelligence Poor Reputation IP group 32", "ET 3CORESec Poor Reputation IP group 11", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 661", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 678", "ET CINS Active Threat Intelligence Poor Reputation IP group 8", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 780", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 65", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 109", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 9", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 46", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 92", "ET CINS Active Threat Intelligence Poor Reputation IP group 14", "ET CINS Active Threat Intelligence Poor Reputation IP group 79", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 761", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 68", "ET CINS Active Threat Intelligence Poor Reputation IP group 11", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 21", "ET CINS Active Threat Intelligence Poor Reputation IP group 41", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 213", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 114", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 144", "ET TOR Known Tor Exit Node Traffic group 84", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 172", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 697", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 738", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 108", "ET TOR Known Tor Exit Node Traffic group 14", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 757", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 309", "ET DROP Spamhaus DROP Listed Traffic Inbound group 5", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 795", "ET CINS Active Threat Intelligence Poor Reputation IP group 48", "ET CINS Active Threat Intelligence Poor Reputation IP group 74", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 8", "GPL MISC CVS invalid directory response", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 16", "ET TOR Known Tor Exit Node Traffic group 111", "ET TOR Known Tor Exit Node Traffic group 115", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 97", "ET TOR Known Tor Exit Node Traffic group 33", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 617", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 619", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 683", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 132", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 162", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 663", "ET TOR Known Tor Exit Node Traffic group 4", "ET CINS Active Threat Intelligence Poor Reputation IP group 99", "ET TOR Known Tor Exit Node Traffic group 31", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 119", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 601", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 44", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 134", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 793", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 759", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 739", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 355", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 115", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 77", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 676", "ET TOR Known Tor Exit Node Traffic group 92", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 723", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 124", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 316", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 275", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 657", "ET

	TOR Known Tor Relay/Router (Not Exit) Node Traffic group 669", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 724", "ET CINS Active Threat Intelligence Poor Reputation IP group 78", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 791", "ET TOR Known Tor Exit Node Traffic group 122", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 274", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 665", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 113", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 1", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 192", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 727", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 771", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 5", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 82", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 371", "ET CINS Active Threat Intelligence Poor Reputation IP group 16", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 157", "ET TOR Known Tor Exit Node Traffic group 69", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 122", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 713", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 714", "ET 3CORESec Poor Reputation IP group 16", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 667", "ET CINS Active Threat Intelligence Poor Reputation IP group 30", "ET TOR Known Tor Exit Node Traffic group 114", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 374", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 75", "GPL RPC sadmind query with root credentials attempt TCP", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 235", "ET CINS Active Threat Intelligence Poor Reputation IP group 94", "ET TOR Known Tor Exit Node Traffic group 121", "GPL VOIP EXPLOIT SIP UDP Softphone overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 389", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 752", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 664", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 91", "GPL NETBIOS SMB-DS DCEPRC ORPCThis request flood attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 666", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 210", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 272", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 30", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 273", "ET TOR Known Tor Exit Node Traffic group 123", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 196", "ET TOR Known Tor Exit Node Traffic group 63", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 18", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 41", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 259", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 758", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 132", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 790", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 670", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 149", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 206", "ET CINS Active Threat Intelligence Poor Reputation IP group 17", "ET TOR Known Tor Exit Node Traffic group 44", "ET TOR Known Tor Exit Node Traffic group 30", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 600", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 129", "ET TOR Known Tor Exit Node Traffic group 2", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 98", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 243", "ET TOR Known Tor Exit Node Traffic group 72", "ET CINS Active Threat Intelligence Poor Reputation IP group 13", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 672", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 64", "ET TOR Known Tor Exit Node Traffic group 43", "ET CINS Active Threat Intelligence Poor Reputation IP group 60", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 185", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 146", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 769", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 774", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 287", "ET TOR Known Tor

	Relay/Router (Not Exit) Node Traffic group 803", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 96", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 67", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 202", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 121", "ET TOR Known Tor Exit Node Traffic group 22", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 231", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 25", "ET TOR Known Tor Exit Node Traffic group 59", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 31", "ET CINS Active Threat Intelligence Poor Reputation IP group 61", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 24", "ET CINS Active Threat Intelligence Poor Reputation IP group 19", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 267", "ET CINS Active Threat Intelligence Poor Reputation IP group 95", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 640", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 85", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 201", "ET DROP Spamhaus DROP Listed Traffic Inbound group 7", "ET TOR Known Tor Exit Node Traffic group 42", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 307", "ET TOR Known Tor Exit Node Traffic group 125", "ET TOR Known Tor Exit Node Traffic group 49", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 97", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 180", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 93", "ET TOR Known Tor Exit Node Traffic group 58", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 105", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 188", "ET VOIP Possible Misuse Call from MERA RTU", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 386", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 195", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 88", "ET TOR Known Tor Exit Node Traffic group 34", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 79", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 615", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 688", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 81", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 58", "ET DROP Spamhaus DROP Listed Traffic Inbound group 19", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 291", "ET 3CORESec Poor Reputation IP group 14", "ET CINS Active Threat Intelligence Poor Reputation IP group 87", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 194", "ET CINS Active Threat Intelligence Poor Reputation IP group 73", "ET TOR Known Tor Exit Node Traffic group 93", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 39", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 785", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 8", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 139", "ET DROP Spamhaus DROP Listed Traffic Inbound group 34", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 59", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 91", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 168", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 276", "ET CINS Active Threat Intelligence Poor Reputation IP group 51", "ET TOR Known Tor Exit Node Traffic group 1", "GPL RPC tooltalk TCP overflow attempt", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 3", "ET TOR Known Tor Exit Node Traffic group 37", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 159", "ET TOR Known Tor Exit Node Traffic group 97", "ET TOR Known Tor Exit Node Traffic group 77", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 197", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 675", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 765", "ET DROP Spamhaus DROP Listed Traffic Inbound group 17", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 45", "ET DROP Spamhaus DROP Listed Traffic Inbound group 2", "ET TOR Known Tor Exit Node Traffic group 85", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 29", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 807", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 141", "ET TOR Known Tor Relay/Router (Not

	Exit) Node Traffic group 109", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 308", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 103", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 715", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 147", "ET SCAN Redis SSH Key Overwrite Probing", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 183", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 766", "ET CINS Active Threat Intelligence Poor Reputation IP group 22", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 100", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 212", "ET CINS Active Threat Intelligence Poor Reputation IP group 12", "ET CINS Active Threat Intelligence Poor Reputation IP group 69", "ET CINS Active Threat Intelligence Poor Reputation IP group 40", "ET DROP Spamhaus DROP Listed Traffic Inbound group 4", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 71", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 148", "ET CINS Active Threat Intelligence Poor Reputation IP group 20", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 108", "ET CINS Active Threat Intelligence Poor Reputation IP group 35", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 98", "ET TOR Known Tor Exit Node Traffic group 89", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 218", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 233", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 290", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 393", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 722", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 152", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 256", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 725", "ET 3CORESec Poor Reputation IP group 18", "ET DROP Dshield Block Listed Source group 1", "ET TOR Known Tor Exit Node Traffic group 17", "ET CINS Active Threat Intelligence Poor Reputation IP group 26", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 674", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 30", "ET TOR Known Tor Exit Node Traffic group 109", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 737", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 190", "ET TOR Known Tor Exit Node Traffic group 29", "GPL IMAP unsubscribe overflow attempt", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 83", "ET TOR Known Tor Exit Node Traffic group 12", "ET CINS Active Threat Intelligence Poor Reputation IP group 64", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 80", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 658", "ET TOR Known Tor Exit Node Traffic group 101", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 90", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 44", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 59", "ET CINS Active Threat Intelligence Poor Reputation IP group 33", "ET TOR Known Tor Exit Node Traffic group 15", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 29", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 214", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 176", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 804", "ET TOR Known Tor Exit Node Traffic group 112", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 125", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 375", "ET CINS Active Threat Intelligence Poor Reputation IP group 36", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 224", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 380", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 271", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 292", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 157", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 746", "ET DROP Spamhaus DROP Listed Traffic Inbound group 30", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 298", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 294", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 743", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 19", "ET 3CORESec Poor Reputation IP group 22", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 191", "GPL FTP SITE CPWD overflow attempt", "ET TOR Known Tor

	Relay/Router (Not Exit) Node Traffic group 286", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 388", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 265", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 800", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 131", "ET DROP Spamhaus DROP Listed Traffic Inbound group 9", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 27", "ET DROP Spamhaus DROP Listed Traffic Inbound group 23", "ET TOR Known Tor Exit Node Traffic group 25", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 14", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 117", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 716", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 747", "ET TOR Known Tor Exit Node Traffic group 60", "ET TOR Known Tor Exit Node Traffic group 87", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 73", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 124", "ET SCAN ProxyReconBot CONNECT method to Mail", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 207", "ET TOR Known Tor Exit Node Traffic group 45", "ET CINS Active Threat Intelligence Poor Reputation IP group 39", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 671", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 289", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 755", "ET DROP Spamhaus DROP Listed Traffic Inbound group 25", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 56", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 728", "GPL IMAP fetch overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 11", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 379", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 655", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 128", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 145", "GPL SQL Slammer Worm propagation attempt", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 11", "ET TOR Known Tor Exit Node Traffic group 9", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 78", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 215", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 773", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 216", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 209", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 39", "GPL IMAP status overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 165", "ET CINS Active Threat Intelligence Poor Reputation IP group 42", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 159", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 142", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 89", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 801", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 32", "ET 3CORESec Poor Reputation IP group 3", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 49", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 258", "ET SNMP missing community string attempt 4", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 610", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 217", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 736", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 798", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 213", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 305", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 627", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 160", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 116", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 94", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 693", "ET EXPLOIT Exploit MS05-002 Malformed .ANI stack overflow attack", "ET TOR Known Tor Exit Node Traffic group 36", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 84", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 43", "ET CINS Active Threat Intelligence Poor Reputation IP group 65", "ET CINS Active Threat Intelligence Poor Reputation IP group 75", "ET 3CORESec Poor Reputation IP group 17", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 139", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 300", "ET TOR Known Tor

	Relay/Router (Not Exit) Node Traffic group 255", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 146", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 87", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 51", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 649", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 54", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 99", "ET 3CORESec Poor Reputation IP group 20", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 123", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 63", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 602", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 742", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 779", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 147", "ET CINS Active Threat Intelligence Poor Reputation IP group 25", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 6", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 49", "ET CINS Active Threat Intelligence Poor Reputation IP group 86", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 219", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 120", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 96", "ET CINS Active Threat Intelligence Poor Reputation IP group 29", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 763", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 182", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 306", "ET 3CORESec Poor Reputation IP group 30", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 402", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 129", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 805", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 611", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 740", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 613", "ET CINS Active Threat Intelligence Poor Reputation IP group 83", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 57", "ET EXPLOIT Pwdump3e pwservice.exe Access port 445", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 177", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 5", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 382", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 102", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 14", "ET EXPLOIT Observed Mirai/Gafgyt Post Brute Force Activity (GET)", "GPL IMAP append overflow attempt", "ET TOR Known Tor Exit Node Traffic group 91", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 7", "GPL RPC CMSD TCP CMSD_INSERT buffer overflow attempt", "ET TOR Known Tor Exit Node Traffic group 78", "ET TOR Known Tor Exit Node Traffic group 110", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 42", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 720", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 178", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 126", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 149", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 395", "ET TOR Known Tor Exit Node Traffic group 118", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 38", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 703", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 228", "ET ATTACK_RESPONSE Possible PowerShell AMSI Bypass Inbound", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 160", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 777", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 181", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 689", "ET ATTACK_RESPONSE Obfuscated Batch Script Inbound M2", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 47", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 60", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 304", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 706", "ET TOR Known Tor Exit Node Traffic group 13", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 638", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 168", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 127", "ET TOR Known Tor Relay/Router (Not

	Exit) Node Traffic group 15", "ET TOR Known Tor Exit Node Traffic group 107", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 778", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 373", "ET DROP Spamhaus DROP Listed Traffic Inbound group 16", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 197", "ET CINS Active Threat Intelligence Poor Reputation IP group 67", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 171", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 623", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 184", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 192", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 48", "ET EXPLOIT Pwdump3e pwservice.exe Access port 139", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 2", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 110", "ET CINS Active Threat Intelligence Poor Reputation IP group 68", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 118", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 169", "ET CINS Active Threat Intelligence Poor Reputation IP group 66", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 594", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 754", "ET INFO Request to Hidden Environment File", "ET CINS Active Threat Intelligence Poor Reputation IP group 15", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 695", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 208", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 6", "ET TOR Known Tor Exit Node Traffic group 8", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 187", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 387", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 719", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 225", "ET CINS Active Threat Intelligence Poor Reputation IP group 52", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 114", "ET EXPLOIT Pwdump3e Password Hash Retrieval port 445", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 12", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 285", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 751", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 163", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 637", "ET TOR Known Tor Exit Node Traffic group 113", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 74", "ET TOR Known Tor Exit Node Traffic group 41", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 266", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 687", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 696", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 408", "GPL MISC rwhoisd format string attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 182", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 299", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 211", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 399", "ET TOR Known Tor Exit Node Traffic group 66", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 107", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 710", "ET 3CORESec Poor Reputation IP group 29", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 764", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 4", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 264", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 200", "ET 3CORESec Poor Reputation IP group 10", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 104", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 246", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 711", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 396", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 177", "ET 3CORESec Poor Reputation IP group 19", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 69", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 191", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 28", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 210", "ET CINS Active Threat Intelligence Poor Reputation IP group 81", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 189", "GPL MISC CVS double free exploit attempt response", "ET TOR

	Known Tor Relay/Router (Not Exit) Node Traffic group 622", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 772", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 705", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 187", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 4", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 6", "ET 3CORESec Poor Reputation IP group 23", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 130", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 797", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 377", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 173", "GPL IMAP find overflow attempt", "GPL MISC CVS missing cvsroot response", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 13", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 47", "ET CINS Active Threat Intelligence Poor Reputation IP group 84", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 199", "ET DROP Spamhaus DROP Listed Traffic Inbound group 12", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 205", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 229", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 247", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 390", "ET CINS Active Threat Intelligence Poor Reputation IP group 38", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 400", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 599", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 634", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 55", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 74", "ET 3CORESec Poor Reputation IP group 4", "ET TOR Known Tor Exit Node Traffic group 71", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 45", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 597", "ET CINS Active Threat Intelligence Poor Reputation IP group 92", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 241", "ET CINS Active Threat Intelligence Poor Reputation IP group 24", "GPL RPC kcms_server directory traversal attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 604", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 31", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 278", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 186", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 221", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 635", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 19", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 394", "ET CINS Active Threat Intelligence Poor Reputation IP group 62", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 659", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 677", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 249", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 26", "GPL MISC CVS invalid repository response", "ET CINS Active Threat Intelligence Poor Reputation IP group 7", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 140", "ET TOR Known Tor Exit Node Traffic group 81", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 33", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 7", "ET TOR Known Tor Exit Node Traffic group 56", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 702", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 170", "ET TOR Known Tor Exit Node Traffic group 102", "ET EXPLOIT [Rapid7] Zyxel ZTP setWanPortSt mtu Parameter Exploit Attempt (CVE-2022-30525)", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 195", "ET WEB_CLIENT Winzip 15.0 WZFLDVW.OCX Text Property Denial of Service", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 27", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 370", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 603", "ET 3CORESec Poor Reputation IP group 31", "GPL MISC CVS invalid user authentication response", "ET Threatview.io High Confidence Cobalt Strike C2 IP group 10", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 211", "ET CINS Active Threat Intelligence Poor Reputation IP group 97", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 34", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 279", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 788", "ET 3CORESec Poor Reputation IP group 27", "ET

	COMPROMISED Known Compromised or Hostile Host Traffic group 35", "GPL IMAP copy literal overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 53", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 263", "ET TOR Known Tor Exit Node Traffic group 11", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 626", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 135", "GPL RPC RQUOTA getquota overflow attempt UDP", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 24", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 799", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 158", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 86", "ET TOR Known Tor Exit Node Traffic group 3", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 70", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 122", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 36", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 644", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 648", "ET CINS Active Threat Intelligence Poor Reputation IP group 9", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 121", "ET CINS Active Threat Intelligence Poor Reputation IP group 49", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 123", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 181", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 61", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 37", "ET TOR Known Tor Exit Node Traffic group 55", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 138", "ET TOR Known Tor Exit Node Traffic group 120", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 174", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 633", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 189", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 70", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 178", "GPL IMAP examine overflow attempt", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 73", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 248", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 110", "ET DROP Spamhaus DROP Listed Traffic Inbound group 20", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 786", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 179", "ET EXPLOIT FireEye Detection Evasion %temp% attempt - Inbound", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 153", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 251", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 645", "ET DROP Spamhaus DROP Listed Traffic Inbound group 11", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 62", "GPL WORM Slammer Worm propagation attempt OUTBOUND", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 125", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 203", "ET CINS Active Threat Intelligence Poor Reputation IP group 76", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 62", "ET DROP Spamhaus DROP Listed Traffic Inbound group 27", "ET 3CORESec Poor Reputation IP group 2", "ET TOR Known Tor Exit Node Traffic group 26", "ET TOR Known Tor Exit Node Traffic group 67", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 163", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 230", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 239", "ET DROP Spamhaus DROP Listed Traffic Inbound group 36", "ET TOR Known Tor Exit Node Traffic group 24", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 252", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 368", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 605", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 618", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 718", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 721", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 118", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 18", "ET DROP Spamhaus DROP Listed Traffic Inbound group 10", "ET CINS Active Threat Intelligence Poor Reputation IP group 93", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 21", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 376", "ET DROP Spamhaus DROP

	Listed Traffic Inbound group 1", "GPL NETBIOS SMB DCERPC Workstation Service unicode bind attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 136", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 165", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 20", "ET TOR Known Tor Exit Node Traffic group 73", "ET INFO PDF embedded in XDP file (Possibly Malicious)", "ET TOR Known Tor Exit Node Traffic group 100", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 704", "ET TOR Known Tor Exit Node Traffic group 18", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 717", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 729", "ET CINS Active Threat Intelligence Poor Reputation IP group 56", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 101", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 193", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 166", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 227", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 166", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 776", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 407", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 378", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 668", "ET CINS Active Threat Intelligence Poor Reputation IP group 55", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 770", "ET POLICY Possible Windows Binary Observed in SSL/TLS Certificate", "ET 3CORESec Poor Reputation IP group 13", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 598", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 369", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 80", "ET DROP Spamhaus DROP Listed Traffic Inbound group 18", "ET DROP Spamhaus DROP Listed Traffic Inbound group 32", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 656", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 112", "GPL IMAP subscribe literal overflow attempt", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 17", "ET EXPLOIT Pwdump3e Password Hash Retrieval port 139", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 89", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 12", "ET TOR Known Tor Exit Node Traffic group 75", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 185", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 9", "ET DROP Spamhaus DROP Listed Traffic Inbound group 14", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 117", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 707", "ET TOR Known Tor Exit Node Traffic group 124", "ET 3CORESec Poor Reputation IP group 12", "ET TOR Known Tor Exit Node Traffic group 88", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 673", "ET TOR Known Tor Exit Node Traffic group 6", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 193", "ET DROP Spamhaus DROP Listed Traffic Inbound group 21", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 222", "ET INFO Query for Suspicious shell .now .sh Domain", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 621", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 288", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 653", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 767", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 784", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 28", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 205", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 257", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 745", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 200", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 806", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 616", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 102", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 756", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 281", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 61", "GPL NETBIOS SMB-DS DCERPC Workstation Service bind attempt", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 84", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 662", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 25", "ET

	TOR Known Tor Relay/Router (Not Exit) Node Traffic group 162", "ET TOR Known Tor Exit Node Traffic group 105", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 302", "ET TOR Known Tor Exit Node Traffic group 65", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 203", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 130", "ET TOR Known Tor Exit Node Traffic group 21", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 22", "ET CINS Active Threat Intelligence Poor Reputation IP group 72", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 94", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 372", "ET 3CORESec Poor Reputation IP group 8", "ET 3CORESec Poor Reputation IP group 24", "ET CINS Active Threat Intelligence Poor Reputation IP group 10", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 111", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 238", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 636", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 153", "ET CINS Active Threat Intelligence Poor Reputation IP group 89", "ET TOR Known Tor Exit Node Traffic group 54", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 381", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 43", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 681", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 198", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 83", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 88", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 35", "ET TOR Known Tor Exit Node Traffic group 20", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 154", "ET TOR Known Tor Exit Node Traffic group 74", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 33", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 106", "ET INFO Possible Rogue LoJack Asset Tracking Agent", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 206", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 303", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 760", "ET CINS Active Threat Intelligence Poor Reputation IP group 23", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 692", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 180", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 150", "ET TOR Known Tor Exit Node Traffic group 19", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 750", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 744", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 242", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 133", "ET TOR Known Tor Exit Node Traffic group 5", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 173", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 254", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 155", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 261", "ET 3CORESec Poor Reputation IP group 21", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 190", "ET TOR Known Tor Exit Node Traffic group 51", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 607", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 631", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 732", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 789", "ET CINS Active Threat Intelligence Poor Reputation IP group 59", "GPL IMAP authenticate overflow attempt", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 794", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 240", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 280", "ET COMPROMISED Known Compromised or Hostile Host Traffic group 32", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 641", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 268", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 220", "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 311"
Авторизация с подозрительным логином	"GPL SMTP AUTH LOGON brute force attempt", "ET EXPLOIT Pwdump4 Session Established GetHash port 445", "GPL FTP pass wh00t", "ET EXPLOIT Pwdump4 Session Established GetHash port 139", "GPL FTP iss scan", "ET EXPLOIT Pwdump3e Session Established Reg-Entry port 445", "ET EXPLOIT Pwdump3e Session Established Reg-Entry port 139", "GPL FTP piss scan", "GPL FTP satan scan", "ET PHISHING Suspicious Fake

	Login - Possible Phishing - 2018-12-31", "GPL FTP saint scan", "GPL SCAN adm scan", "GPL TELNET root login"
Обнаружение подозрительных команд	"ET ATTACK_RESPONSE FTP inaccessible directory access LPT4", "ET ATTACK_RESPONSE FTP inaccessible directory access LPT2", "ET ATTACK_RESPONSE FTP inaccessible directory access NULL", "ET ATTACK_RESPONSE FTP inaccessible directory access COM4", "ET ATTACK_RESPONSE FTP inaccessible directory access LPT3", "ET ATTACK_RESPONSE FTP inaccessible directory access COM3", "ET ATTACK_RESPONSE FTP inaccessible directory access COM2", "ET ATTACK_RESPONSE FTP inaccessible directory access AUX", "ET ATTACK_RESPONSE FTP inaccessible directory access LPT1", "ET ATTACK_RESPONSE FTP inaccessible directory access COM1"
Атаки на получение прав пользователя	"ET ATTACK_RESPONSE Metasploit Meterpreter Registry Interation Detected", "ET ATTACK_RESPONSE net user Command Output via HTTP POST", "ET MALWARE Metasploit Meterpreter stdapi_* Command Request", "ET MALWARE Metasploit Meterpreter core_channel_* Command Request", "ET MALWARE Metasploit Meterpreter stdapi_* Command Response", "ET ATTACK_RESPONSE Net User Command Response", "ET WEB_SERVER RFI Scanner Success (Fx29ID)", "ET MALWARE Metasploit Meterpreter core_channel_* Command Response"
Обновления Windows	"Windows Updates"
Попытки авторизации с логином и паролем по-умолчанию	"ET EXPLOIT HiSilicon DVR - Default Application Backdoor Password", "GPL POLICY Linksys router default password login attempt", "GPL POLICY Sun JavaServer default password login attempt", "GPL POLICY Linksys router default username and password login attempt", "ET EXPLOIT HiSilicon DVR - Default Telnet Root Password Inbound"
Обнаружение нарушений стандартов сетевых протоколов	"ET HUNTING Suspicious FTP 220 Banner on Local Port (-)", "ET POLICY IRC DCC file transfer request on non-std port"
Блокирование подозрительных RPC-запросов	"GPL RPC portmap rusers request UDP", "GPL RPC portmap ttdbserv request TCP", "GPL RPC portmap SET attempt TCP 111", "GPL RPC portmap snmpXdmi request TCP", "GPL RPC portmap selection_svc request UDP", "GPL RPC portmap proxy attempt UDP", "GPL RPC portmap cachefsd request UDP", "GPL RPC portmap admind request UDP", "GPL RPC portmap bootparam request UDP", "GPL RPC portmap rexd request UDP", "GPL RPC portmap ttdbserv request UDP", "GPL RPC portmap espd request TCP", "GPL RPC portmap pcnfsd request TCP", "GPL RPC portmap proxy integer overflow attempt TCP", "GPL RPC yppasswd username overflow attempt UDP", "GPL RPC portmap yppasswd request TCP", "GPL RPC portmap snmpXdmi request UDP", "GPL RPC portmap amountd request TCP", "GPL RPC portmap proxy attempt TCP", "GPL RPC portmap rwalld request UDP", "GPL RPC portmap UNSET attempt UDP 111", "GPL RPC portmap listing UDP 111", "GPL RPC portmap kcms_server request TCP", "GPL RPC portmap ypupdated request UDP", "GPL RPC portmap ypserv request UDP", "GPL RPC portmap NFS request UDP", "GPL RPC portmap yppasswd request UDP", "GPL RPC portmap mountd request UDP", "GPL RPC portmap rstatd request UDP", "GPL RPC portmap rstatd request TCP", "GPL RPC portmap pcnfsd request UDP", "GPL RPC portmap status request UDP", "GPL RPC portmap sadmind request UDP", "GPL RPC portmap selection_svc request TCP", "GPL RPC portmap ypupdated request TCP", "GPL RPC portmap sadmind request TCP", "GPL RPC portmap network-status-monitor request UDP", "GPL RPC portmap cmsd request TCP", "GPL RPC portmap SET attempt UDP 111", "GPL RPC portmap status request TCP", "GPL RPC portmap RQUOTA request TCP", "GPL RPC portmap nisd request TCP", "GPL RPC portmap ypserv request TCP", "GPL RPC portmap cmsd request UDP", "GPL RPC portmap rusers request TCP", "GPL RPC portmap amountd request UDP", "GPL RPC portmap nisd request UDP", "GPL RPC portmap bootparam request TCP", "GPL RPC portmap NFS request TCP", "GPL RPC portmap UNSET attempt TCP 111", "GPL RPC portmap rwalld request TCP", "GPL RPC portmap network-status-monitor request TCP", "GPL RPC portmap rexd request TCP", "GPL RPC portmap RQUOTA request UDP", "GPL RPC portmap cachefsd request TCP", "GPL RPC portmap listing TCP 111", "GPL RPC portmap espd request UDP", "GPL RPC portmap kcms_server request UDP", "GPL RPC portmap rpc.xfsmd request TCP", "GPL RPC portmap admind request TCP"

Блокирование попыток запуска исполняемого кода	"GPL EXPLOIT kadmind buffer overflow attempt", "ET SHELLCODE Possible 0x0a0a0a0a Heap Spray Attempt", "ET SHELLCODE Possible UTF-16 u9090 NOP SLED", "ET SHELLCODE Unescape Variable Unicode Shellcode", "ET SHELLCODE Rothenburg Shellcode", "ET SHELLCODE Execve(/bin/sh) Shellcode", "ET SHELLCODE Possible UTF-16 %u9090 NOP SLED", "ET SHELLCODE Common 0a0a0a0a Heap Spray String", "ET SHELLCODE Linux/x86-64 - Polymorphic Setuid(0) & Execve(/bin/sh) Shellcode", "GPL SQL MSSQL shellcode attempt 2", "ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0d0d0d0d", "ET SHELLCODE Linux/x86-64 - Reverse Shell Shellcode", "GPL SHELLCODE HP-UX NOOP", "GPL SHELLCODE Digital UNIX NOOP", "ET SHELLCODE Possible Unescape Encoded Content With Split String Obfuscation 2", "ET SHELLCODE Possible UTF-8 %u90 NOP SLED", "ET SHELLCODE Common %u0c%u0c%u0c%u0c UTF-8 Heap Spray String", "ET SHELLCODE Possible 0x0c0c0c0c Heap Spray Attempt", "ET SHELLCODE Possible Call with No Offset UDP Shellcode", "GPL SHELLCODE x86 0xEB0C NOOP", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0a0a0a0a", "ET SHELLCODE Possible %u4141%u4141 UTF-16 Heap Spray Attempt", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 41414141", "ET SHELLCODE Possible Call with No Offset TCP Shellcode", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript NOP SLED", "GPL SHELLCODE x86 0x71FB7BAB NOOP unicode", "ET INFO Possible Hex Obfuscated JavaScript Heap Spray 0a0a0a0a", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0b0b0b0b", "ET SHELLCODE Possible Backslash Unicode Heap Spray Attempt", "GPL SHELLCODE x86 0x71FB7BAB NOOP", "ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0b0b0b0b", "ET SHELLCODE Common %0c%0c%0c%0c Heap Spray String", "ET SHELLCODE Linux/x86-64 - Polymorphic Flush IPTables Shellcode", "ET SHELLCODE Bindshell2 Decoder Shellcode (UDP)", "ET SHELLCODE Possible %u0d0d%u0d0d UTF-16 Heap Spray Attempt", "ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0c0c0c0c", "ET SHELLCODE Javascript Split String Unicode Heap Spray Attempt", "ET SHELLCODE Possible 0x0b0b0b0b Heap Spray Attempt", "ET SHELLCODE Possible %u0d%u0d%u0d%u0d UTF-8 Heap Spray Attempt", "GPL SHELLCODE MSSQL shellcode attempt", "ET SHELLCODE Common %u0a0a%u0a0a UTF-16 Heap Spray String", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0d0d0d0d", "ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt", "ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0c0c0c0c", "GPL SHELLCODE SGI NOOP", "ET SHELLCODE Common %u0a%u0a%u0a%u0a UTF-8 Heap Spray String", "ET SHELLCODE Possible 0x0d0d0d0d Heap Spray Attempt", "ET SHELLCODE Possible Vertical Slash Unicode Heap Spray Attempt", "GPL SHELLCODE Linux shellcode", "GPL SHELLCODE AIX NOOP", "GPL SQL shellcode attempt", "ET SHELLCODE Unescape Hex Obfuscated Content", "ET SHELLCODE Hex Obfuscated JavaScript NOP SLED", "ET SHELLCODE Possible %0d%0d%0d%0d Heap Spray Attempt", "GPL SHELLCODE sparc NOOP", "ET SHELLCODE Possible Unescape Encoded Content With Split String Obfuscation", "ET SHELLCODE Possible Encoded %90 NOP SLED", "ET SHELLCODE Common %u0c0c%u0c0c UTF-16 Heap Spray String", "ET SHELLCODE Possible %u41%u41%u41%u41 UTF-8 Heap Spray Attempt"
Попытки проведения DoS-атак	"ET DOS Possible Memcached DDoS Amplification Response Outbound", "ET WEB_CLIENT Great Cannon DDoS JS M2", "ET DOS Possible SSDP Amplification Scan in Progress", "ET DOS Likely NTP DDoS In Progress PEER_LIST Response to Non-Ephemeral Port IMPL 0x02", "ET EXPLOIT Netgear Seventh Inferno CVE-2021-41314 (new line injection)", "ET SCAN Kingcope KillApache.pl Apache mod_deflate DoS attempt", "ET DOS Likely NTP DDoS In Progress Multiple UNSETTRAP Mode 6 Responses", "ET DOS Possible Sentinal LM Amplification attack (Request) Inbound", "GPL EXPLOIT NTLM ASN.1 vulnerability scan attempt", "ET VOIP Multiple Unauthorized SIP Responses TCP", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x02", "ET DOS Potential CLDAP Amplification Reflection", "ET DOS Trojan.BlackRev V1.Botnet HTTP Login POST Flood Traffic Inbound", "ET DOS Possible Memcached DDoS Amplification Query (set)", "ET DOS Likely NTP DDoS In Progress PEER_LIST Response to Non-Ephemeral Port IMPL 0x03", "ET DOS Terse HTTP GET Likely AnonMafiaIC DDoS tool", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST_SUM

	Requests IMPL 0x02", "ET DOS Linux/Tsunami DOS User-Agent (x00_-gawa.sa.pilipinas.2015) INBOUND", "ET WEB_SERVER Possible Apache DDos UA Observed (DDos Apache) Outbound", "ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M1", "ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x02", "GPL VOIP SIP 407 Proxy Authentication Required Flood", "ET DOS CLDAP Amplification Reflection (PoC based)", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed GET_RESTRICT Requests IMPL 0x02", "ET SCADA RealWin SCADA System Buffer Overflow", "GPL NETBIOS SMB NTLMSSP invalid mechlistMIC attempt", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST Requests IMPL 0x02", "GPL VOIP SIP INVITE message flooding", "ET DOS Possible NTP DDoS Multiple MON_LIST Seq 0 Response Spanning Multiple Packets IMPL 0x03", "ET EXPLOIT Possible MicroLogix 1100 PCCC DoS Condition (CVE-2017-7924)", "ET DOS Likely NTP DDoS In Progress GET_RESTRICT Response to Non-Ephemeral Port IMPL 0x03", "ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M2", "GPL VOIP SIP 401 Unauthorized Flood", "ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M4", "ET DOS HTTP GET AAAAAAAA Likely FireFlood", "ET DOS Terse HTTP GET Likely LOIC", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Service Stop", "ET DOS CallStranger - Attempted UPnP Reflected Amplified TCP with Multiple Callbacks (CVE-2020-12695)", "ET DOS Possible Memcached DDoS Amplification Inbound", "ET DOS Possible NTP DDoS Multiple MON_LIST Seq 0 Response Spanning Multiple Packets IMPL 0x02", "ET VOIP INVITE Message Flood UDP", "ET DOS Possible Sentinal LM Application attack in progress Outbound (Response)", "ET DOS MC-SQLR Response Outbound Possible DDoS Participation", "GPL FTP SITE NEWER attempt", "ET DOS Bittorrent User-Agent inbound - possible DDOS", "ET WEB_CLIENT Possible Apache DDos UA Observed (DDos Apache) Inbound", "ET WEB_SPECIFIC_APPS Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway - Process Kill", "ET WEB_CLIENT Great Cannon DDoS JS M3", "GPL NETBIOS SMB-DS DCERPC NTLMSSP invalid mechlistMIC attempt", "ET DOS SMB Tree_Connect Stack Overflow Attempt (CVE-2017-0016)", "ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M3", "ET SCAN Apache mod_deflate DoS via many multiple byte Range values", "ET WEB_SERVER Apache APR apr_fnmatch Stack Overflow Denial of Service", "ET DOS Likely NTP DDoS In Progress PEER_LIST_SUM Response to Non-Ephemeral Port IMPL 0x03", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03", "GPL NETBIOS DCERPC invalid bind attempt", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST_SUM Requests IMPL 0x03", "ET DOS LOIC Javascript DDoS Outbound", "ET DOS Possible Sentinal LM Amplification attack (Response) Inbound", "ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x03", "ET DOS Likely NTP DDoS In Progress PEER_LIST_SUM Response to Non-Ephemeral Port IMPL 0x02", "ET DOS Terse HTTP GET Likely GoodBye 5.2 DDoS tool", "ET WEB_CLIENT Great Cannon DDoS JS M1", "ET EXPLOIT Win32/Industroyer DDOS Siemens SIPROTEC (CVE-2015-5374)", "ET WEB_CLIENT Great Cannon DDoS JS M4", "ET DOS MC-SQLR Response Inbound Possible DDoS Target", "ET VOIP REGISTER Message Flood TCP", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed GET_RESTRICT Requests IMPL 0x03", "ET WEB_SERVER Possible Cherokee Web Server GET AUX Request Denial Of Service Attempt", "ET DOS Excessive Large Tree Connect Response", "ET DOS Possible WordPress Pingback DDoS in Progress (Inbound)", "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST Requests IMPL 0x03", "GPL NETBIOS SMB DCERPC invalid bind attempt", "ET WEB_SERVER PHP Large Subnormal Double Precision Floating Point Number PHP DoS in URI", "ET WEB_SERVER LOIC Javascript DDoS Inbound", "ET VOIP Multiple Unauthorized SIP Responses UDP", "ET DOS Microsoft Windows LSASS Remote Memory Corruption (CVE-2017-0004)", "ET VOIP INVITE Message Flood TCP", "ET DOS Terse HTTP GET Likely AnonGhost DDoS tool", "ET WEB_SERVER PHP Large Subnormal Double Precision Floating Point Number PHP DoS Inbound", "GPL NETBIOS DOS RFPoison", "ET DOS Likely NTP DDoS In Progress GET_RESTRICT Response to Non-Ephemeral Port IMPL 0x02", "ET DOS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA", "ET VOIP REGISTER Message Flood UDP"

Запросы на скомпрометированные ресурсы	"ET P2P Ares traffic", "ET CHAT Skype VOIP Checking Version (Startup)", "ET P2P Bittorrent P2P Client User-Agent (rTorrent)", "ET POLICY Cryptocurrency Miner Checkin", "ET POLICY Possible SSLv2 Negotiation in Progress ClientMaster Key SSL2_IDEA_128_CBC_WITH_MD5", "ET POLICY File Downloaded from Discord", "ET POLICY DNS Query to .onion proxy Domain (tor4free.org)", "ET CHAT ICQ Status Change (2)", "ET POLICY Possible HTTP-TUNNEL detected", "ET HUNTING Observed Suspicious SSL Cert (Metasploit in TLS Subject)", "ET POLICY bridges.torproject.org over TLS with SNI", "ET POLICY DNS Query to .onion proxy Domain (allepohelpto.com)", "ET POLICY DNS Query to a Reverse Proxy Service Observed", "ET POLICY Wifi Geolocation Lookup Attempt", "ET P2P Edonkey Publicize File ACK", "ET PHISHING Request for Possible Outlook Phishing Hosted on Github.io", "ET POLICY Netviewer.com Remote Control Proxy Test", "ET POLICY DNS Query to .onion proxy domain (onion .pet)", "ET CHAT Yahoo IM Client Install", "ET POLICY .onion.ly Proxy domain in SNI", "ET POLICY TeamViewer Dyngate User-Agent", "ET POLICY CBS Streaming Video", "ET POLICY Observed Filesharing Domain (privatlab .com in TLS SNI)", "ET POLICY BingBar ToolBar User-Agent (BingBar)", "ET POLICY ToDesk Remote Access Control Tool", "ET POLICY DNS Query to .onion proxy Domain (partnersinvestpayto.com)", "ET CHAT Skype User-Agent detected", "ET GAMES GameHouse License Check", "ET INFO [eSentire] Possible Kali Linux Updates", "ET POLICY PTsecurity Remote Desktop AeroAdmin Server Hello", "ET POLICY SSL/TLS Certificate Observed (Free File Hosting Service (api .anonfiles .com))", "ET POLICY iTunes User Agent", "ET POLICY Outbound HTTP Request with BITS_POST Method", "ET POLICY Maxmind geoip check to /app/geoip.js", "ET PHISHING DNS Lookup for Possible Common Brand Phishing Hosted on Legitimate Windows Service", "ET P2P TOR 1.0 Status Update", "ET GAMES Moonlight Hack Actvity (GET)", "ET P2P TOR 1.0 Inbound Circuit Traffic", "ET POLICY Logmein.com Host List Download", "ET POLICY Bitmessage Activity", "ET POLICY Socks5 Proxy to Onion (set)", "ET GAMES Blizzard Web Downloader Install Detected", "ET POLICY Possible SSLv2 Negotiation in Progress Client Master Key SSL2_RC2_128_CBC_EXPORT40_WITH_MD5", "ET POLICY Windows 3.1 User-Agent Detected - Possible Malware or Non-Updated System", "ET POLICY Netflix Streaming Player Access", "ET POLICY HTTP POST to MEGA Userstorage", "ET INFO Observed Initial NKN POST Request", "ET P2P GnucDNA UDP Ultrapeer Traffic", "ET POLICY Orkut.com Social Site Access", "ET POLICY Observed SSL Cert (Pastebin-style Service paste .c-net)", "ET GAMES Guild Wars connection", "ET P2P Bittorrent P2P Client User-Agent (Enhanced CTorrent 3.x)", "ET POLICY SSL/TLS Certificate Observed (Free File Hosting Service (uplovd .com))", "ET POLICY DNS Query to .onion proxy Domain (effectwaytopay.com)", "ET POLICY Executable and linking format (ELF) file download", "ET POLICY Possible Kali Linux hostname in DHCP Request Packet", "ET P2P Octoshape P2P streaming media", "ET POLICY tor4u tor2web .onion Proxy domain in SNI", "ET POLICY Onion2Web Tor Proxy Cookie", "ET POLICY Remote Access - RView - Host - *.rview.com", "ET POLICY Possible Autodiscover Credentials Leak via Basic Auth", "ET P2P Gnutella Connect", "ET POLICY Mobile Device Posting Phone Number", "ET POLICY External IP Lookup (avast .com)", "ET POLICY Pandora Usage", "ET POLICY DNS Query to .onion proxy Domain (bolistatapay.com)", "ET POLICY Android Adups Firmware DNS Query 4", "ET POLICY Protocol 41 IPv6 encapsulation potential 6in4 IPv6 tunnel active", "ET POLICY External Geo IP Lookup (api .db-ip .com)", "ET POLICY External IP Lookup via 3322 .org", "ET P2P BitTorrent DHT announce_peers request", "ET POLICY External IP Lookup via ad4989 .co .kr", "ET POLICY Observed iesnare/iovation Tracking Activity", "ET INFO Adilbo HTML Encoder Observed", "ET INFO Observed DNS Query to .myq-see .com DDNS Domain", "ET CHAT Gadu-Gadu IM Login Server Request", "ET POLICY NetSupport GeoLocation Lookup Request", "ET POLICY JavaClass Returned Via Non-Anonymous Outbound LDAPv3 Bind Request", "ET TFTP Outbound TFTP Error Message", "ET POLICY External IP Lookup (ipchicken .com)", "ET POLICY DNS Query to .onion proxy Domain (tordomain.org)", "ET ADWARE_PUP PUP/PUA OSSProxy HTTP Header", "ET CHAT Google Talk (Jabber) Client Login", "ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted", "ET POLICY Google Talk TLS Client Traffic", "ET PHISHING Request for Possible Account Phishing Hosted on Github.io", "ET POLICY Xpopup Instant Messenger Downloading

	Configuration", "ET POLICY Http Client Body contains pin= in cleartext", "ET POLICY IP Check Response (rl. ammyy. com)", "ET HUNTING Observed Suspicious SSL Cert (Metasploit Self Signed CA)", "ET POLICY Windows Quicktime User-Agent EOL With Known Bugs", "ET POLICY Observed DNS Query to IP Lookup Domain (me .shodan .io)", "ET POLICY Http Client Body contains passwd= in cleartext", "ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System", "ET PHISHING Request for Possible Facebook Phishing Hosted on Github.io", "ET INFO DNS Query to a *.ngrok domain (ngrok.io)", "ET POLICY Windows-Based OpenSSL Tunnel Connection Outbound 2", "ET P2P eMule KAD Network Connection Request(2)", "ET POLICY Office Document Containing AutoExec Macro Via smtp", "ET POLICY Unsupported/Fake FireFox Version 1.", "ET POLICY Unsupported/Fake Internet Explorer Version MSIE 1.", "ET INFO Possible System Enumeration via WMI Queries (AntiVirusProduct)", "ET POLICY Observed Potential Spyware Domain (app .hubstaff .com) in TLS SNI", "ET POLICY TraceMyIP IP lookup", "ET POLICY DNS Query to .onion proxy Domain (solutionsaccountor.com)", "ET POLICY DNS Query to .onion proxy Domain (torwillsmith.com)", "ET POLICY Possible SSLv2 Negotiation in Progress Client Master Key SSL2_DES_64_CBC_WITH_MD5", "ET POLICY DNS Query for Invisible Internet Project Domain (I2P)", "ET P2P Vuze BT UDP Connection (5)", "ET POLICY InstallIQ Updater Software request", "ET POLICY Android Adups Firmware DNS Query 3", "ET POLICY IP Check Domain (myexternalip .com in TLS SNI)", "ET POLICY DNS Query to .onion proxy Domain (bananator.com)", "ET POLICY Hotmail Compose Message Access", "ET POLICY DNS Query to .onion proxy Domain (torinvestment2.com)", "ET POLICY Pastebin-style Service (paste .ee) in TLS SNI", "ET GAMES Wolfteam HileYapak Server Response", "ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set", "ET POLICY TOR .exit Pseudo TLD DNS Query", "ET POLICY Privdog Update check", "ET POLICY Oracle T3 Response with CVE-2020-2551 Vulnerable Version (12.1.3)", "ET POLICY DNS Query to a *.ngrok domain (ngrok.com)", "ET POLICY Outdated Flash Version M1", "ET POLICY VMware User-Agent Outbound", "ET POLICY Dropbox.com Offsite File Backup in Use", "ET POLICY IP Check wtfismyip.com", "ET PHISHING Request for Possible DHL Phishing Hosted on Github.io", "ET POLICY DNS Query to .onion proxy Domain (batmantor.com)", "GPL P2P BitTorrent announce request", "ET MALWARE IRC DCC chat request on non-standard port", "ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 6 or 7 set", "ET POLICY TOR Consensus Data Requested", "ET POLICY Observed DNS Query to Free Hosting Domain (.free .bg)", "ET POLICY IPFS Domain (storage .snark .art in TLS SNI)", "ET CHAT GaduGadu Chat Server Welcome Packet", "ET INFO DYNAMIC_DNS HTTP Request to a *.autoddns.com Domain", "ET P2P eMule KAD Network Firewalled Request", "ET HUNTING Suspicious Use of rzd URL Shortener Service", "ET POLICY Possible IP Check api.ipify.org", "ET POLICY Softango.com Installer POSTing Data", "ET P2P Bittorrent P2P Client User-Agent (Transmission/1.x)", "ET INFO HTTP URI contains pasa=", "ET P2P Morpheus Update Request", "ET POLICY My2022/Beijing2022 App (TLS SNI) 2", "GPL P2P GNUTella client request", "ET GAMES Gold VIP Club Casino Client in Use", "ET POLICY Burp Collaborator Certificate Inbound", "ET POLICY DNS Query to .onion proxy Domain (torpayoptions.com)", "ET POLICY Kindle Fire Browser User-Agent Outbound", "ET P2P Vagaa peer-to-peer (Transfer)", "GPL P2P BitTorrent transfer", "ET POLICY Pirate Browser Download", "ET POLICY Office Document Containing AutoOpen Macro Via smtp", "ET POLICY DNS Query to .onion proxy domain (onion .ws)", "ET POLICY Hotmail Inbox Access", "ET POLICY Coral Web Proxy/Content Distribution Net Use", "ET POLICY DNS Query to .onion proxy Domain (torstorm.org)", "ET POLICY NBC Streaming Video", "ET TFTP Outbound TFTP Read Request", "ET POLICY DNS Query to a *.neokred domain - Likely Hostile", "ET POLICY IP Check Domain (iplogger .org in TLS SNI)", "ET POLICY ICP Email Send via HTTP - Often Trojan Install Reports", "ET POLICY Burp Collaborator Domain in DNS Query", "ET P2P Bittorrent P2P Client User-Agent (Opera/10.x)", "ET CHAT ICQ Status Change (1)", "ET POLICY Microsoft Online Storage Client Hello TLSv1 Possible OneDrive (storage.live .com)", "ET POLICY Possible SSLv2 Negotiation in Progress Client Master Key SSL2_RC4_128_WITH_MD5", "ET PHISHING Request for Possible Office Phishing Hosted on Github.io", "ET GAMES Blizzard

	Downloader Client User-Agent (Blizzard Downloader 2.x)", "ET POLICY Outbound SMTP NTLM Authentication Observed", "ET POLICY IP Check Domain (address .works)", "ET POLICY CNET Custom Installer Possible Bundled Bloatware", "ET POLICY NEPHILIM Ransomware Victim Publishing Site DNS Lookup (hxt254aygrsziejn .onion) DNS Lookup", "ET POLICY PTsecurity Remote Desktop AeroAdmin handshake", "ET POLICY My2022/Beijing2022 App (DNS Lookup) 3", "ET POLICY DivX Client SSL Connection via Self-Signed SSL Cert", "ET PHISHING Request for Possible Ebay Phishing Hosted on Github.io", "ET POLICY AOL Webmail Message Send", "ET P2P Bittorrent P2P Client User-Agent (FDM 3.x)", "ET MALWARE IRC DNS request on non-standard port", "ET POLICY Hamas Terrorist Propaganda TV Channel (aqsatv.ps)", "ET POLICY Smilebox Spyware Download", "ET P2P KuGoo P2P Connection", "ET POLICY W32/Installiq.Adware Install Information Beacon", "ET POLICY I2P Reseed Domain Lookup (i2p-netdb.innovatio.no)", "ET POLICY I2P Reseed Domain Lookup (us.reseed.i2p2.no)", "ET POLICY I2P Seeds File Request", "ET P2P BitTorrent Announce", "ET POLICY SSL/TLS Certificate Observed (Commercial Proxy Provider geosurf .io)", "ET GAMES Moonlight Hack Domain in DNS Lookup", "ET POLICY Myspace Login Attempt", "ET POLICY Geo Location IP info online service (geoiptool.com)", "ET POLICY Remote Desktop AeroAdmin handshake", "ET POLICY Possible ProxyShell Anonymous Access Connection", "ET POLICY Outdated Flash Version M2", "ET POLICY Request for Coinhive Browser Monero Miner M2", "ET POLICY Possible Psiphon Proxy Tool traffic", "ET P2P BitTorrent - Torrent File Downloaded", "ET POLICY Dropbox Client Broadcasting", "ET P2P Ocelot BitTorrent Server in Use", "ET MALWARE Possible Chimera Ransomware - Bitmessage Activity", "ET POLICY ipchicken .com DNS Lookup", "ET POLICY External IP Address Request via wttr .in", "ET POLICY DNS Query to .onion Proxy Domain (connect2tor.org)", "ET POLICY Oracle T3 Response with CVE-2020-2551 Vulnerable Version (10.3.6)", "ET POLICY OpenVPN Update Check", "ET P2P Vuze BT UDP Connection (3)", "ET ADWARE_PUP Suspected PUP/PUA User-Agent (OSSProxy)", "ET POLICY IP Check (rl. ammyy. com)", "ET POLICY DNS Query to .onion proxy Domain (torgateway.li)", "ET HUNTING Suspicious Windows Installer UA for non-MSI", "ET MALWARE Observed CDC Ransomware User-Agent", "ET GAMES STEAM Connection (v2)", "ET P2P Libtorrent User-Agent", "ET POLICY Radmin Remote Control Session Setup Initiate OUTBOUND", "ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System (Win98)", "ET PHISHING Request for Possible Paypal Phishing Hosted on Github.io", "ET P2P BitTorrent DHT get_peers request", "ET POLICY Metacafe.com Social Site Access", "ET POLICY DNS Query to .onion proxy Domain (trusteetor.com)", "ET P2P TOR 1.0 Outbound Circuit Traffic", "ET INFO Control Panel Applet File Download", "ET POLICY Http Client Body contains pword= in cleartext", "ET INFO URL Shortening Service Domain in TLS SNI (hyp .ae)", "ET POLICY Bomgar Remote Assistance Tool Download", "ET CHAT ICQ Login", "ET POLICY My2022/Beijing2022 App (DNS Lookup) 2", "ET INFO DYNAMIC_DNS Query to *.myddns.me Domain", "ET HUNTING Observed Interesting Content-Type Inbound (application/x-sh)", "ET P2P Bittorrent P2P Client User-Agent (BitTornado)", "ET POLICY [401TRG] DropBox Access via API (SNI)", "ET POLICY Smilebox Software/Adware Checkin", "ET POLICY AskSearch Toolbar Spyware User-Agent (AskTBar) 2", "ET INFO DYNAMIC_DNS HTTP Request to a *.myddns.me Domain", "ET POLICY GeoIP Lookup (nydus.battle.net)", "ET POLICY Request for Jsecoin Browser Miner M2", "ET POLICY myip.ru IP lookup", "ET TFTP Outbound TFTP ACK", "ET POLICY I2P Reseed Domain Lookup (netdb.i2p2.no)", "ET USER_AGENTS Steam HTTP Client User-Agent", "ET POLICY External Timezone Check (earthtools.org)", "ET POLICY DNS Query to .onion proxy Domain (optionstopaytos.com)", "ET POLICY DNS Query to .onion proxy Domain (tostotor.com)", "ET POLICY Akamai NetSession Interface PUTing data", "ET POLICY Observed DeepFreezeWeb User-Agent", "ET HUNTING Suspicious EXE Download Content-Type image/jpeg", "ET P2P ed2k request part", "ET POLICY DropBox User Content Access over SSL", "ET INFO ARM File Requested via WGET (set)", "ET P2P Manolito Ping", "ET SNMP Attempt to retrieve Cisco Config via TFTP (CISCO-CONFIG-COPY)", "ET USER_AGENTS Non-standard User-Agent (PATCHER)", "ET POLICY Observed DNS Query to Coin Mining Domain (nanopool .org)", "ET POLICY Nimiq Miner Initiating

	Mining Session with Skypool", "ET POLICY Netop Remote Control Usage", "ET P2P Direct Connect Traffic (client-server)", "ET PHISHING Request for Possible Webmail Phishing Hosted on Github.io", "ET POLICY possible Xiaomi phone data leakage DNS", "ET POLICY IOS Download from Vshare Marketplace (Possible DarkSideLoading)", "ET POLICY Pastebin-style Service nrecom in DNS Query", "ET P2P Vuze BT UDP Connection", "ET POLICY Quad9 DNS Over TLS Certificate Inbound", "ET POLICY HTTP Request to Illegal Drug Sales Site (SilkRoad)", "ET POLICY Observed Connection Manager Administration Kit (cmdl32.exe) User-Agent", "ET PHISHING Request for Possible Binance Phishing Hosted on Github.io", "ET POLICY Observed ApoioViewer Remote Access Tool Domain (apoioviewer .com in TLS SNI)", "ET POLICY DNS Query to .onion proxy Domain (sshowmethemoney.com)", "ET POLICY eBook Generator User-Agent (EBook)", "ET POLICY Unsupported/Fake Windows NT Version 4.", "ET POLICY HTTP Request to WebDAV CloudMe Service", "ET POLICY localtunnel Reverse Proxy Domain (localtunnel .me in DNS Lookup)", "ET POLICY Possible Grams DarkMarket Search DNS Domain Lookup", "ET POLICY Website Hosting Service Observed in DNS Query", "ET POLICY Observed SSL Cert (Pastebin-style Service nrecom)", "ET POLICY Exe32Pack Packed Executable Download", "ET POLICY Remote Access - RView - SSL Certificate Seen", "ET POLICY Unsupported/Fake Internet Explorer Version MSIE 2.", "ET POLICY Pastebin-style Service paste .c-net in DNS Query", "ET P2P ed2k file request answer", "ET POLICY IP Check Domain (showmyipaddress .com in HTTP Host)", "ET GAMES Playit Activity (playit .gg)", "ET P2P Azureus P2P Client User-Agent", "ET POLICY DNS Query to .onion proxy Domain (onion . ly)", "ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent", "ET P2P Soulseek Filesearch Results", "ET POLICY F5 BIG-IP Publicly Accessible Exposed REST API Detected", "ET P2P Edonkey Connect Request", "ET P2P Bittorrent P2P Client User-Agent (BTSP)", "ET POLICY OperaUnite URL Registration", "ET POLICY Observed SSL Cert (DoH Service)", "ET POLICY IncrediMail Install Callback", "ET POLICY Possible ProxyShell Hide IP Installation file download", "ET POLICY F5 BIG-IP Exposed REST API GET (flowbit set)", "ET P2P BitTorrent Traffic", "ET P2P Gnutella TCP Traffic", "ET PHISHING Request for Possible Microsoft Phishing Hosted on Github.io", "ET POLICY Unsupported/Fake Windows NT Version 5.0", "ET POLICY StumbleUpon Submission Detected", "ET POLICY Http Client Body contains passphrase= in cleartext", "ET POLICY TuneIn Internet Radio Usage Detected", "ET POLICY Successful LDAPSv3 LDAPS_START_TLS Request Outbound", "ET POLICY Observed nc (netcat) EXE Inbound", "ET POLICY Club World Casino Client in Use", "ET POLICY OS X Software Update Request Outbound", "ET POLICY Observed IP Check Domain Domain (address .works in TLS SNI)", "ET POLICY Carbonite.com Backup Software User-Agent (Carbonite Installer)", "ET POLICY Disposable Email Provider Domain in DNS Lookup (www .yopmail .com)", "ET TFTP Outbound TFTP Write Request", "ET P2P ThunderNetwork UDP Traffic", "ET POLICY DNS Query to .onion proxy Domain (onion.cab)", "ET P2P BitTorrent DHT nodes reply", "ET WEB_SERVER HTTPing Usage Inbound", "ET P2P eMule KAD Network Server Status Request", "ET P2P Manolito Connection (1)", "ET P2P MS WUDO Peer Sync", "ET P2P Pando Client User-Agent Detected", "ET POLICY External Oracle T3 Requests Inbound", "ET PHISHING Request for Possible Common Brand Phishing Hosted on Legitimate Windows Service", "ET POLICY File Sharing Site in DNS Lookup (satoshidisk .com)", "ET POLICY Windows-Based OpenSSL Tunnel Connection Outbound 3", "ET POLICY Successful GIOP/IIOP Request Outbound", "ET P2P Bittorrent P2P Client User-Agent (BitComet)", "ET POLICY Application Crash Report Sent to Microsoft", "ET PHISHING Request for Possible Docusign Phishing Hosted on Github.io", "ET POLICY QQ Browser WUP Request - qbpcstatf.stat", "ET POLICY possible Xiaomi phone data leakage HTTP", "ET POLICY Privdog Activation", "ET GAMES MINECRAFT Server response inbound", "ET GAMES Nintendo Wii User-Agent", "ET INFO Possible System Enumeration via WMI Queries (FirewallProduct)", "ET POLICY FOX-SRT - Juniper ScreenOS SSH World Reachable", "ET POLICY IP Check (myip .com)", "ET CHAT Yahoo IM voicechat", "ET POLICY Observed Wifi Geolocation Domain (api .mylnikov .org in TLS SNI)", "ET POLICY Google Desktop User-Agent Detected", "ET POLICY Hola VPN Activity - X-Hola-* Headers", "ET POLICY DNS Query to .onion proxy Domain (torgate.es)", "ET POLICY Office Document Download Containing AutoExec Macro", "ET INFO Possible

	System Enumeration via WMI Queries (AntiSpywareProduct)", "ET POLICY gogo6/Freenet6 Authentication Attempt", "ET POLICY NSISDL Iplookup.php IPCheck", "ET POLICY Oracle T3 Response with CVE-2020-2551 Vulnerable Version (12.2.1)", "ET POLICY DNS Query to .onion proxy Domain (solutionstopaytor33.com)", "ET POLICY DNS Query to .onion proxy Domain (dogotor.com)", "ET P2P Kazaa over UDP", "ET POLICY 3proxy Domain Domain in DNS Lookup (3proxy .ru)", "ET POLICY DNS Query to .onion proxy Domain (statepaytor.com)", "ET POLICY Hotmail Message Access", "ET CHAT ICQ Status Invisible", "ET POLICY DNS Query to .onion proxy Domain (cheetosnotburitos.com)", "ET POLICY Unsupported/Fake FireFox Version 0.", "ET POLICY DNS Query for Observed CVE-2021-44228 Security Scanner Domain (dns .cyberwar .nl)", "ET POLICY IP Check Domain (freegeoip .live in TLS SNI)", "ET POLICY HotSpotShield Activity", "ET POLICY NEPHILIM Ransomware Victim Publishing Site DNS Lookup (corpleaks .net)", "ET POLICY Android Dalvik Executable File Download", "ET P2P Bittorrent P2P Client User-Agent (uTorrent)", "ET P2P Client User-Agent (Shareaza 2.x)", "ET P2P Morpheus Install", "ET CHAT Yahoo IM Unavailable Status", "ET USER_AGENTS ESET Installer", "ET P2P eMule KAD Network Connection Request", "ET POLICY Unsupported/Fake Internet Explorer Version MSIE 5.", "ET P2P Tor Get Server Request", "ET P2P Vuze BT UDP Connection (4)", "ET POLICY Android Adups Firmware DNS Query 5", "ET POLICY GG Url Shortener Observed in DNS Query", "ET POLICY Logmein.com Update Activity", "ET POLICY AmeriTechnology Group - CHARM Client", "ET POLICY DNS Query to .onion proxy Domain (clusterpaytor.com)", "ET POLICY OnePlus phone data leakage", "ET INFO HTTP POST contains pasa form", "ET P2P FFTorrent P2P Client User-Agent (FFTorrent/x.x.x)", "ET P2P BitTorrent peer sync", "ET P2P Bittorrent P2P Client User-Agent (Deluge 1.x.x)", "ET P2P QVOD P2P Sharing Traffic detected (tcp)", "ET POLICY Observed DNS Query to Pastebin-style Service (wtools .io)", "ET POLICY Observed File Transfer Service SSL/TLS Certificate (transfer .sh)", "ET POLICY Possible SSLv2 Negotiation in Progress Client Master Key SSL2_RC2_128_CBC_WITH_MD5", "ET POLICY Dropbox DNS Lookup - Possible Offsite File Backup in Use", "ET POLICY request for hide-my-ip.com autoupdate", "ET POLICY I2P Reseed Domain Lookup (reseed.i2p-projekt.de)", "ET POLICY Successful Anonymous LDAPv3 Bind Request Outbound", "ET INFO Possible TURKTRUST Spoofed Google Cert", "ET POLICY Chisel SOCKS Proxy Startup Observed", "ET POLICY DNS Query to DynDNS *.dyn-ip24 .de Domain", "GPL P2P eDonkey server response", "ET POLICY 3proxy Domain Domain in DNS Lookup (3proxy .org)", "ET POLICY localtunnel Connection Setup Attempt", "ET POLICY JavaClass Returned Via Anonymous Outbound LDAPv3 Bind Request", "ET CHAT Yahoo IM file transfer request", "ET POLICY tor4u tor2web .onion Proxy DNS lookup", "ET P2P Edonkey Search Request (search by name)", "ET POLICY Microsoft Online Storage Client Hello TLSv1 Possible OneDrive (storage.msn .com)", "ET POLICY CNET TechTracker Software Manager request", "ET P2P BitTorrent DHT find_node request", "ET POLICY Office Document Download Containing AutoOpen Macro", "ET POLICY XenArmor Password Recovery License Check", "ET P2P BTWebClient UA uTorrent in use", "ET INFO DYNAMIC_DNS Query to *.autoddns .com Domain", "ET POLICY DNS Query to .onion proxy Domain (optionsketchupay.com)", "ET P2P Limewire P2P UDP Traffic", "ET POLICY Observed SSL Cert (Tor Proxy Domain (.onion. pet))", "ET POLICY Observed DNS Query for Suspicious TLD (.management)", "ET POLICY Unsupported/Fake Internet Explorer Version MSIE 3.", "ET POLICY Middle Earth Illegal Marketplace Tor Hidden Service DNS Query", "ET POLICY Windows-Based OpenSSL Tunnel Outbound", "ET POLICY IP Check Domain (iplogger .org in DNS Lookup)", "ET POLICY Autoit Windows Automation tool User-Agent in HTTP Request - Possibly Hostile", "ET POLICY DNS Query to .onion proxy Domain (forkinvestpay.com)", "ET POLICY DNS Query to .onion proxy Domain (anonym.to)", "ET POLICY Android Adups Firmware DNS Query", "ET POLICY Http Client Body contains upin= in cleartext", "ET POLICY localtunnel Sucessful Connection Setup", "ET POLICY Cleartext WordPress Login", "ET POLICY Observed SSL Cert (DNS Service)", "ET INFO Suspicious Darkwave Popads Pop Under Redirect", "ET POLICY Android Adups Firmware DNS Query 2", "ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)", "ET P2P Vuze BT Connection", "ET POLICY DNS Query to .onion proxy Domain

	(marketcryptopartners.com)", "ET P2P Morpheus Install ini Download", "ET P2P Gnutella TCP Ultrapeer Traffic", "ET CHAT ICQ Message", "ET P2P Possible Torrent Download via HTTP Request", "ET POLICY I2P Seeds File Download", "ET POLICY possible OnePlus phone data leakage DNS", "ET POLICY DNS Query to .onion proxy Domain (onion.top)", "ET POLICY Skypool Coin Mining Pool DNS Lookup", "ET POLICY onion.cab tor2web .onion Proxy domain in SNI", "ET INFO HTTP POST contains pasa= in cleartext", "ET P2P Tor Get Status Request", "ET POLICY localtunnel Reverse Proxy Domain (localtunnel .me in TLS SNI)", "ET POLICY Privdog Checkin", "ET POLICY DNS Query to .onion proxy Domain (paypartnerstodo.com)", "ET POLICY External IP Lookup (ipify .org)", "ET POLICY QQ Browser WUP Request - qbkpireportbakf.stat", "ET POLICY Self Signed SSL Certificate (Snake Oil CA)", "ET POLICY I2P Reseed Domain Lookup (uk.reseed.i2p2.no)", "ET ATTACK_RESPONSE Weak Netbios Lanman Auth Challenge Detected", "ET POLICY DNS Update From External net", "ET POLICY Unsupported/Fake FireFox Version 2.", "ET POLICY I2P Retrieving reseed info", "ET POLICY User-Agent (Launcher)", "ET POLICY Logmein.com/Join.me SSL Remote Control Access", "ET TFTP Outbound TFTP Data Transfer with Cisco config", "ET PHISHING Request for Possible Adobe Phishing Hosted on Github.io", "ET USER_AGENTS WildTangent User-Agent (WT Games App)", "ET POLICY Burp Collaborator Domain in TLS SNI", "ET POLICY Nessus Vulnerability Scanner Plugins Update", "ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR", "ET POLICY LumOffice Uploading Screenshot", "ET POLICY DNS Query to .onion proxy Domain (optionstorpay22.com)", "ET POLICY Monitoring Software Domain (sneek .io) in TLS SNI", "ET POLICY CNET TechTracker User-Agent (CNET TechTracker)", "ET POLICY I2P Reseed Domain Lookup (i2p.mooo.com)", "ET POLICY moanmyip .com DNS Lookup", "ET GAMES Second Life setup download", "ET POLICY My2022/Beijing2022 App (TLS SNI) 3", "ET POLICY Proxy Judge Discovery/Evasion (prxjdg.cgi)", "ET POLICY Possible ethereum traffic", "ET TFTP Outbound TFTP Data Transfer With Cisco Config 2", "ET POLICY 2Downloadz.com File Sharing User-Agent", "ET POLICY request to .xxx TLD", "ET P2P eDonkey Server Status Request", "ET POLICY DNS Query to .onion proxy Domain (tormaster.fr)", "ET POLICY Observed URL Shortening Service SSL/TLS Cert (rb.gy)", "ET DNS DNS Query for Illegal Drug Sales Site (SilkRoad)", "ET USER_AGENTS Suspicious User Agent (AskInstallChecker)", "ET P2P TOR 1.0 Server Key Retrieval", "ET POLICY CommandCam Download", "ET INFO .exe File requested over FTP", "ET INFO NoxPlayer Simulator Update Activity", "ET POLICY AOL Toolbar User-Agent (AOLToolbar)", "ET POLICY DNS Query For XXX Adult Site Top Level Domain", "ET POLICY Google Music Streaming", "ET POLICY Softango.com Installer Checking For Update", "ET POLICY Http Client Body contains otp= in cleartext", "ET POLICY Request to Suspicious Games at pcgame.gamedia.cn", "ET POLICY [401TRG] DropBox Access via API (Certificate)", "ET POLICY Owncloud Observed Self Signed TLS Certificate", "ET POLICY Observed DNS Query to .burpcollector .net Domain", "ET POLICY DNS Query to .onion proxy Domain (onion.am)", "ET POLICY My2022/Beijing2022 App (TLS SNI) 1", "ET POLICY Possible SSLv2 Negotiation in Progress Server Hello", "ET P2P Soulseek", "ET TFTP Outbound TFTP Data Transfer", "ET POLICY Cryptocurrency Miner Checkin M2", "ET POLICY IP Logger Redirect Domain in SNI", "ET POLICY Hotmail Access Full Mode", "ET P2P BitTorrent DHT ping request", "ET POLICY Babylon User-Agent (Translation App Observed in PPI MALWARE)", "ET P2P LimeWire P2P Traffic", "ET CHAT Google IM traffic Jabber client sign-on", "ET P2P Bittorrent P2P Client User-Agent (KTorrent/3.x.x)", "ET P2P SoulSeek P2P Login Response", "ET POLICY Possible EXE Download Request to ngrok", "ET POLICY External IP Lookup (moanmyip .com)", "ET POLICY DNS Query to .onion proxy Domain (welcome2tor.org)", "ET POLICY Centralops.net Domain Dossier Utility Probe", "ET INFO Observed HTTP Request to *.pythonanywhere .com Domain", "ET POLICY Android Download from Vshare Marketplace (Possible DarkSideLoading)", "ET P2P Vuze BT UDP Connection (2)", "ET POLICY Download Request to Hotfile.com", "ET POLICY Unsupported/Fake Internet Explorer Version MSIE 4.", "ET POLICY Observed SSL Cert (Tor Proxy Domain (.onion. ws))", "ET MALWARE IRC Channel join on non-standard port", "ET POLICY HTTP Request to IP Logging Service (2no .co)", "ET POLICY DNS Query to .onion proxy Domain

	(torpaysolutions.com)", "ET POLICY DNS Query to .onion proxy Domain (monsterbbc.com)", "ET P2P Ares Server Connection", "ET POLICY Successful Non-Anonymous LDAPv3 Bind Request Outbound"
Обновления Cisco	"Cisco Updates"
Трафик устаревшего уязвимого ПО	"ET INFO turbo.net SSL/TLS Certificate Observed (VDI and App Virtualization Service)", "ET POLICY Splashtop Remote Control Session Keepalive Response", "ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)", "ET POLICY Incoming Chromoting Session Response", "ET USER_AGENTS Suspicious User-Agent (XXX) Often Sony Update Related", "ET MALWARE Suspicious Accept-Language HTTP Header zh-cn likely Kernelbot/Conficker Trojan Related", "ET SMTP Spamcop.net Block Message", "ET SCAN Naver Webcrawler User-Agent (Naver.me)", "ET POLICY SSL MiTM Vulnerable iOS 4.x CDMA iPhone device", "ET INFO MP4 in HTTP Flowbit Set", "ET INFO Adobe Flash Uncompressed in HTTP Flowbit Set", "ET WEB_CLIENT HTA File Download Flowbit Set", "ET INFO MP4 in HTTP Flowbit Set M2", "ET POLICY Cisco Device New Config Built", "ET POLICY Splashtop Remote Control Session Start Request", "ET POLICY Maxthon Browser Background Agent UA (MxAgent)", "ET INFO McAfee AV Download - Set", "ET INFO Adobe PDF in HTTP Flowbit Set", "ET SMTP Sorbs.net Block Message", "ET WEB_CLIENT Oracle Java 6 Object Tag launchjnlp docbase Parameters Flowbits Set", "ET INFO Observed Free Hosting Domain (*.000webhostapp .com in DNS Lookup)", "ET SCAN Exabot Webcrawler User Agent", "ET SMTP Robtex.com Block Message", "ET INFO MP4 in HTTP Flowbit Set M3", "ET POLICY external cPanel login", "ET POLICY Windows Mobile 7.0 User-Agent detected", "ET POLICY COCCOC Browser (VN) Installed", "ET WEB_CLIENT AVI RIFF Chunk Access Flowbit Set", "ET INFO Adobe FDF in HTTP Flowbit Set", "ET POLICY Dyndns Client User-Agent", "ET POLICY Ask Webcrawler User-Agent", "ET SCAN AOL Webcrawler User-Agent", "ET INFO Apache Spark RPC - CheckExistence Request (set)", "ET POLICY external cPanel password change", "ET INFO McAfee AV Download (set)", "ET INFO Apache Spark RPC - Auth Request (set)", "ET POLICY Cisco Device in Config Mode", "ET POLICY Radmin Remote Control Session Authentication Response", "ET INFO Windows Powershell User-Agent Usage", "ET INFO ATF file in HTTP Flowbit Set", "ET SMTP Abuseat.org Block Message", "ET POLICY Dyndns Client IP Check", "ET POLICY Executable Download From DropBox", "ET INFO MP3 with ID3 in HTTP Flowbit Set", "ET SCAN Bing Webcrawler User-Agent (BingBot)", "ET WEB_CLIENT DXF Extension File Detection Access Flowbit Set", "ET INFO form-data flowbit set (noalert)", "ET POLICY Spotify P2P Client", "ET INFO Observed SSL Cert for Free Hosting Domain (*.000webhostapp .com)", "ET SCAN Google Webcrawler User-Agent (Mediapartners-Google)", "ET POLICY Splashtop Remote Control Session Keepalive", "ET POLICY Splashtop Remote Control Checkin", "ET SCAN PRO Search Crawler Probe", "ET SCAN Yandex Webcrawler User-Agent (YandexBot)", "ET WEB_CLIENT VLC Media Player Aegisub Advanced SubStation (.ass) File Request flowbit set", "ET POLICY Dell MyWay Remote control agent", "ET POLICY Radmin Remote Control Session Authentication Initiate", "ET HUNTING Set flow on bmp file get", "ET INFO Opera Adblocker Update Flowbit Set", "ET POLICY Outgoing Chromoting Session Response", "ET SCAN DuckDuckGo Webcrawler User-Agent (DuckDuckBot)"
Обновления Adobe	"Adobe Updates"
Защита SMTP протокола	"SMTP protocol attacked"
Телеметрия Windows	"Windows Telemetry"
Подозрительное обращение к файлам	"GPL FTP .forward", "GPL FTP shadow retrieval attempt", "ET HUNTING Generic CollectGarbage in Hex", "ET POLICY PsExec service created", "ET POLICY RemoteControlX rctrlx service created", "GPL FTP passwd retrieval attempt", "ET EXPLOIT PWDump4 Password dumping exe copied to victim", "GPL FTP authorized_keys file transferred", "ET HUNTING SUSPICIOUS Path to BusyBox", "ET EXPLOIT Pwdump6 Session Established test file created on victim"
Пулы криптомайнеров	"ET COINMINER W32/BitCoinMiner.MultiThreat Stratum Protocol Mining.Notify Initial Connection Server Response", "ET COINMINER Random Hash Pascalcoin Miner Checkin", "ET MALWARE WatchDog Coinminer Payload Delivery Domain in DNS Lookup (oracle .zzhreceive .top)", "ET COINMINER CoinHive In-Browser Miner Detected", "ET

	COINMINER PrimeCoinMiner.Protominer", "ET MALWARE Win32/Nitrokod CnC Domain (Intelserviceupdate .com) in DNS Lookup", "ET COINMINER W32/BitCoinMiner.MultiThreat Getblocktemplate Protocol Server Coinbasetxn Begin Mining Response", "ET COINMINER W32/BitCoinMiner.MultiThreat Getblocktemplate Protocol Server Connection", "ET COINMINER Observed Malicious SSL Cert (Coinhive URL Shortener)", "ET COINMINER Win32/Ymacco.AA2F Checking (Multiple OS)", "ET MALWARE Win32/Nitrokod Domain (nitrokod .com) in TLS SNI", "ET MALWARE MegalodonHTTP CoinMiner Activity", "ET MALWARE ELF.Initdz.Coinminer C2 Systeminfo (D2)", "ET COINMINER Possible BitCoin Miner User-Agent (miner)", "ET ADWARE_PUP BitCoinPlus Embedded site forcing visitors to mine BitCoins", "Mining pool", "ET MALWARE Win32/Nitrokod CnC Domain (nitrokod .com) in DNS Lookup", "ET COINMINER Observed Suspicious SSL Cert (Minerpool - CoinMining)", "ET POLICY Bitcoin Mining Server Stratum Protocol HTTP Header", "ET MALWARE MSIL/CoinMiner Performing System Checkin", "ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Retrieving New Malware From Server", "ET POLICY BitCoin User-Agent Likely Bitcoin Miner", "ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Server Checkin", "ET COINMINER Observed Malicious SSL Cert (Coin-Hive In Browser Mining)", "ET COINMINER Observed DNS Query to Browser Coinminer (crypto-loot[.]com)", "ET COINMINER CoinMiner Domain in DNS Lookup (pool .hashvault .pro)", "ET WEB_CLIENT Fake FlashPlayer Update Leading to CoinMiner M1 2018-10-12", "ET WEB_CLIENT Fake FlashPlayer Update Leading to CoinMiner M2 2018-10-12", "ET MALWARE Observed DNS Query to Cryptojacking Domain (a-dog .top)", "ET MALWARE Observed CoinMiner CnC Domain (endpsbn1u6m8f .x .pipedream .net in TLS SNI)", "ET COINMINER W32/BitCoinMiner.MultiThreat Subscribe/Authorize Stratum Protocol Message", "ET MALWARE Injected WP Keylogger/Coinminer Domain Detected (cloudflare .solutions in DNS Lookup)", "ET COINMINER CoinMiner Known Malicious Stratum Authline (2022-03-11 1)", "ET COINMINER CoinMiner Known Malicious Stratum Authline (2022-03-11 2)", "ET COINMINER Observed DNS Query to herominers Domain (herominers .com)", "ET MALWARE Win32/Nitrokod Domain (intelserviceupdate .com) in TLS SNI", "ET MALWARE C3Pool CoinMiner Setup Script Download", "ET INFO Bitcoin QR Code Generated via Btcfrog.com", "ET MALWARE Clipsa Stealer - Coinminer Download", "ET MALWARE Observed CoinMiner CnC Domain (enoyq5xy70oq .x .pipedream .net in TLS SNI)", "ET COINMINER Panchan Mining Rig CnC Activity (Outbound)", "ET MALWARE W32/Coinminer.Backdoor CnC Beacon", "ET MALWARE Win32/Unk.Coinminer Checkin", "ET POLICY poclbm BitCoin miner", "ET MALWARE W32/Zeus.BitcoinMiner Variant CnC Beacon", "ET COINMINER Crypto Coin Miner Login", "ET MALWARE Bitcoin variant Checkin", "ET COINMINER W32/BitCoinMiner.MultiThreat Stratum Protocol Mining.Notify Work Server Response", "ET COINMINER Bitcoin Mining Extensions Header", "ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Retrieving Server IP Addresses", "ET MALWARE Win32/Nitrokod Domain (nvidiacenter .com) in TLS SNI", "ET INFO Observed DNS Query to Cryptocurrency Mining Pool Domain (xmr .2miners .com)", "ET COINMINER CoinMiner Malicious Authline Seen After CVE-2017-10271 Exploit", "ET COINMINER CoinMiner Known Malicious Stratum Authline (2017-07-17 7)", "ET MALWARE Observed CoinMiner CnC Domain (en24zuggh3ywlj .x .pipedream .net in TLS SNI)", "ET MALWARE Win32/Nitrokod CnC Domain (nvidiacenter .com) in DNS Lookup", "ET COINMINER Cryptexplorer API Check - Potential CoinMiner Traffic"
Атаки на получение привилегий администратора	"ET EXPLOIT Xiongmai/HiSilicon DVR - Successful Auth - Possilbe CVE-2020-22253 Attempt", "ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system", "ET ATTACK_RESPONSE Non-Local Burp Proxy Error", "GPL TFTP GET Admin.dll", "GPL TFTP GET shadow", "ET ATTACK_RESPONSE Microsoft WMIC Prompt Outbound", "ET ATTACK_RESPONSE Apache Spark RPC - Unauthenticated RegisterApplication - Successfully Registered (CVE-2020-9480)", "ET WEB_SERVER PHP WebShell Embedded In JPG (OUTBOUND)", "ET ATTACK_RESPONSE Windows 7 CMD Shell from Local System", "ET WEB_SERVER Successful FortiOS Auth Bypass Attempt - Config Leaked (CVE-2022-40684)", "ET ATTACK_RESPONSE Microsoft CScript Banner Outbound", "ET ATTACK_RESPONSE SysInternals sc.exe Output Outbound", "ET WEB_SERVER WEBSHELL JSP/Backdoor Shell Access", "ET WEB_SERVER PHP WebShell Embedded In

	PNG (OUTBOUND)", "ET WEB_SERVER Successful FortiOS Auth Bypass Attempt - Administrative Details Leaked (CVE-2022-40684)", "ET EXPLOIT Cisco REST API Container for Cisco IOS XE Software Authentication Bypass - Successful Exploit (CVE-2019-12643)", "ET WEB_SERVER Successful FortiOS Auth Bypass Attempt - SSH Key Upload (CVE-2022-40684)", "ET POLICY Dameware Remote Control Service Install", "ET EXPLOIT Bonitasoft Successful Default User Login Attempt (Possible Staging for CVE-2022-25237)", "ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system 2", "ET WEB_SERVER PHP WebShell Embedded In GIF (INBOUND)", "GPL TFTP GET passwd", "ET ATTACK_RESPONSE Microsoft Netsh Firewall Disable Output Outbound", "ET WEB_SERVER PHP WebShell Embedded In GIF (OUTBOUND)", "ET WEB_SERVER WEBSHELL CFM Shell Access", "ET EXPLOIT Cisco REST API Container for Cisco IOS XE Software Authentication Bypass - Token Usage (CVE-2019-12643)", "ET EXPLOIT Open MGate Device", "ET EXPLOIT Xiongmai/HiSilicon DVR - Successful Telnet Opening - Successful CVE-2020-22253 Attempt", "GPL TFTP GET nc.exe", "ET WEB_SERVER PHP WebShell Embedded In JPG (INBOUND)", "ET WEB_SERVER PHP WebShell Embedded In PNG (INBOUND)", "GPL EXPLOIT Microsoft cmd.exe banner", "ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound", "ET SCAN Tomcat upload from external source"
Определение внешнего IP-адреса	"ET POLICY External IP Address Lookup (bei .kr)", "ET POLICY External IP Lookup (www. netikus .net)", "ET MALWARE Possible Emissary External IP Lookup", "ET HUNTING Observed Suspicious SSL Cert (External IP Lookup - ident .me)", "ET POLICY External IP Lookup", "ET MALWARE TA402/Molerats External IP Lookup Activity", "ET POLICY External IP Lookup - Bravica", "ET MALWARE Upatre External IP Check", "ET POLICY External IP Lookup - www.ip.cn", "ET POLICY Observed External IP Lookup Domain (ipconfig .cf in TLS SNI)", "ET POLICY External IP Address Lookup via iplocation.com", "ET INFO External IP Lookup Domain (freegeiop .net in DNS lookup)", "ET POLICY External IP Lookup (whois .pconline .com .cn)", "ET POLICY check.torproject.org IP lookup/Tor Usage check over HTTP", "ET POLICY External IP Lookup - checkip.dyndns.org", "ET POLICY External IP Lookup ip-api.com", "ET POLICY External IP Lookup ipinfo.io", "ET POLICY Internal Host Getting External IP Address - ip2city.asp", "ET POLICY Possible External IP Lookup myip.kz", "ET POLICY External IP Lookup / Tor Checker Domain (check.torproject .org in DNS lookup)", "ET POLICY External IP Lookup - free .ipwhois .io", "ET POLICY External IP Lookup (api .ipstack .com)", "ET POLICY External IP Lookup Domain (ipapi .co in DNS lookup)", "ET POLICY External IP Address Lookup - b4secure .com", "ET INFO External IP Lookup Domain DNS Lookup (ip .dnsexit .com)", "ET POLICY External IP Check myexternalip.com", "ET INFO External IP Address Lookup Domain (get .geojs .io) in TLS SNI", "ET POLICY External IP Lookup (ip .anysrc .net)", "ET POLICY Observed IP Lookup Domain (formyip .com in DNS Lookup)", "ET POLICY Observed DNS Query to External IP Lookup Domain (iplocation .truevue .org)", "ET POLICY Observed External IP Lookup SSL Cert", "ET INFO Observed External IP Lookup Domain in TLS SNI (api .myip .com)", "ET POLICY Observed IP Lookup Domain (l2 .io in DNS Lookup)", "ET POLICY External IP Lookup Domain (ifconfig .me)", "ET POLICY External IP Lookup - ip2location.com", "ET POLICY External IP Lookup (api .ipaddress .com)", "ET POLICY External IP Lookup (tinytools.nu)", "ET POLICY External IP Lookup ip-score.com", "ET POLICY External IP Lookup - iplocation .truevue .org", "ET POLICY Known External IP Lookup Service Domain in SNI", "ET POLICY Possible External IP Lookup www.whatsmyip.us", "ET POLICY IP Check (ip. jsontest .com)", "ET INFO External IP Address Lookup Domain (eth0 .me) in DNS Lookup", "ET INFO Observed External IP Lookup Domain (icanhazip .com in TLS SNI)", "ET POLICY Observed IP Lookup Domain (l2 .io in TLS SNI)", "ET POLICY External IP Lookup getip.pw", "ET INFO External IP Lookup Domain (peoplesearch .real .com) in DNS Lookup", "ET POLICY External IP Lookup maxmind.com", "ET MALWARE Win32/Backdoor.Dripion External IP Check", "ET POLICY External IP Lookup - ipecho.net", "ET POLICY External IP Lookup - meuip.net.br", "ET POLICY External IP Lookup Domain (myip .opendns .com in DNS lookup)", "ET POLICY External IP Lookup api.ipify.org", "ET POLICY External IP Address Lookup DNS Query (2ip .ua)", "ET POLICY External IP Lookup Domain (curlmyip .net in DNS lookup)", "ET INFO External IP Address Lookup Domain (ifconfig .pro) in DNS Lookup", "ET POLICY

	External IP Lookup (www .net .cn)", "ET POLICY IP Lookup Geoip.co.uk", "ET POLICY External IP Lookup Domain (up .jkc8 .com)", "ET POLICY Internal Host Retrieving External IP Via myip.ozymo.com", "ET POLICY External IP Lookup SSL/TLS Certificate (ifconfig .me)", "ET INFO External IP Lookup Domain (ip-api .io) in DNS Lookup", "ET POLICY External IP Address Lookup via dawhois.com", "ET POLICY Possible External IP Lookup ip.webmasterhome.cn", "ET POLICY go-external-ip library User-Agent", "ET MALWARE Kriptovor External IP Lookup checkip.dyndns.org", "ET POLICY External IP Lookup / Tor Checker Domain (bridges.torproject .org in DNS lookup)", "ET POLICY check.torproject.org IP lookup/Tor Usage check over TLS with SNI", "ET POLICY External IP Lookup (extreme-ip-lookup .com)", "ET INFO External IP Lookup Domain in DNS Query (checkip .dyndns .org)", "ET POLICY External IP Address Lookup via vtransmit .com", "ET POLICY External IP Lookup - ip.tyk.nu", "ET POLICY Internal Host Retrieving External IP Address (monip.outils-rezo. info)", "ET POLICY External IP Lookup Request", "ET POLICY External IP Lookup Attempt To Wipmania", "ET INFO External IP Address Lookup Domain (get .geojs .io) in DNS Lookup", "ET POLICY External IP Lookup trackip.net", "ET POLICY External IP Lookup sina.com.cn", "ET POLICY Internal Host Retrieving External IP via myip.dnsomatic.com", "ET POLICY External IP Lookup ip2nation.com", "ET POLICY Possible External IP Lookup SSL Cert Observed (ipinfo.io)", "ET POLICY Observed IP Lookup Domain (formyip .com in TLS SNI)", "ET POLICY DynDNS CheckIp External IP Address Server Response", "ET POLICY External IP Lookup - ip-whois", "ET POLICY Possible External IP Lookup whoer.net"
Обнаружение DoS-атак	"GPL FTP CWD ~<CR><NEWLINE> attempt", "ET DOS Possible Microsoft Windows HTTP2 Reset Flood Denial of Service Inbound (CVE-2019-9514)", "ET DOS User-Agent used in known DDoS Attacks Detected inbound 2", "ET DOS User-Agent used in known DDoS Attacks Detected outbound 2", "ET DOS Inbound GoldenEye DoS attack", "ET DOS User-Agent used in known DDoS Attacks Detected inbound", "ET EXPLOIT Possible OpenSSL Infinite Loop Inducing Cert Inbound via TCP (CVE-2022-0778)", "GPL FTP CWD .... attempt", "ET SCADA Golden FTP Server PASS Command Remote Buffer Overflow Attempt", "ET DOS User-Agent used in known DDoS Attacks Detected outbound", "GPL FTP CWD ~ attempt", "ET SCADA Siemens FactoryLink 8 CSService Logging Buffer Overflow Vulnerability", "ET SCADA DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow Vulnerability", "ET EXPLOIT Possible OpenSSL Infinite Loop Inducing Cert Inbound via UDP (CVE-2022-0778)", "ET EXPLOIT CHIYU IoT Devices - Denial of Service"
Управление вредоносным ПО	"ET MALWARE Win32.Kazy Checkin", "ET MALWARE Win32/HydraCrypt CnC Beacon 3", "ET MALWARE Win32/LODEINFO v0.3.5 CnC Checkin", "ET MALWARE STRRAT Initial HTTP Activity", "ET MALWARE DonotGroup CnC Domain in DNS Lookup (drinkeatgood .space)", "ET MALWARE Win32/Unknown Stealer Command (domaindetect) (Outbound)", "ET MALWARE Kronos Checkin M2", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (esnoptdkkiirzewlpgmccbwuynvxjumf .name)", "ET MALWARE Social-bos.biz related trojan checkin (trackid=hex)", "ET MALWARE SPEAR CnC Beacon", "ET MALWARE W32/DownloaderAgent.fajk Successful Infection CnC Beacon", "ET MALWARE Observed DNS Query to DarkCrystal Rat Domain (datagroup .ddns .net) (2022-06-27)", "ET MALWARE W32/Skintrim CnC Checkin", "ET MALWARE S400 RAT Client Checkin via Discord", "ET MALWARE FIN8 ShellTea CnC in DNS Lookup", "ET MALWARE WooSIP Downloader CnC CreateFolderOnServer", "ET MALWARE MSIL/CoalaBot CnC Activity", "ET MALWARE StormKitty Exfil via AnonFiles", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 28", "ET MALWARE Win32/Sisron/BackDoor.Cybergate.1 Checkin", "ET MALWARE JavaRAT CnC Checkin", "ET MALWARE Ursnif Checkin", "ET MALWARE [TGI] Cobalt Strike Malleable C2 Request (O365 Profile)", "ET MALWARE MSIL/Modi RAT CnC Command Inbound (plugin)", "ET MALWARE General Win32 Backdoor Checkin POST Packet 1", "ET MALWARE lolzilla JS/PHP WebSkimmer - Data Exfil", "ET MALWARE Observed DNS Query to RisePro Domain (vi-files .com)", "ET MALWARE MSIL/Modi RAT CnC Checkin (DesktopPreview)", "ET MALWARE Gatak CnC", "ET MALWARE W32/Tobfy.Ransomware Invalid URI CnC Request", "ET MALWARE TAIDOOR CnC Domain in DNS Lookup (www.cnaweb.mrslove .com)", "ET MALWARE MSIL.L4L Stealer Systeminfo Exfiltration", "ET MALWARE

	W32/StartPage.eba Dropper Checkin", "ET MALWARE AZORult v3.3 Server Response M1", "ET MOBILE_MALWARE Android/SndApps.SM Sending Information to CnC", "ET MALWARE W32/GamesForum.InfoStealer Reporting to CnC", "ET MALWARE Win32/DarkRAT CnC Activity", "ET MALWARE Cobalt Strike Malleable C2 (OneDrive)", "ET MALWARE Turkojan C&C nxt Command (nxt)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 85", "ET MALWARE PS/Unk.EB.Spreader CnC Checkin", "ET MALWARE Fakealert.Rena CnC Checkin 2", "ET MALWARE W32/SpeedingUpMyPC.Rootkit Install CnC Beacon", "ET MALWARE Diavol Communicating with CnC - Services Request", "ET MALWARE Win32/7ev3n Ransomware Initial Checkin", "ET MALWARE ELF/STDbot CnC Activity (UNK attack)", "ET MALWARE Geocon CnC Request", "ET MALWARE VBA/Agent.AAV CnC Checkin", "ET MALWARE Sarwent CnC Command (update)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M19", "ET MALWARE Internet Protection FakeAV checkin", "ET MALWARE Win32/BlackCarat Response from CnC", "ET MALWARE Backdoor.Win32.VB.Alsci/Dragon Eye RAT Checkin (sending user info)", "ET MALWARE Dridex POST CnC Beacon 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 98", "ET MALWARE Win32/AZORult V3.3 Client Checkin M7", "ET MALWARE TABMSGSQL/Sluegot.C Checkin", "ET MOBILE_MALWARE Android.Bgserv POST of Data to CnC Server", "ET MALWARE Trojan.Generic.5325921 Checkin", "ET MALWARE Win32/Neutrino Bot Fake 404 Checkin Response", "ET MALWARE Win32/Mingloa CnC Checkin", "ET MALWARE Win32/Sefnit Initial Checkin", "ET MALWARE MirrorBlast CnC Activity M3", "ET MALWARE Win32/Backdoor.YesMaster CnC Checkin", "ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile Response", "ET MALWARE CrownAdPro CnC Activity M3", "ET MALWARE Win32/Fareit Checkin 2", "ET MALWARE Diavol Communicating with CnC - Ext Request", "ET MALWARE PSEmpire Checkin via POST", "ET MALWARE Rogue.Win32/FakePAV Checkin", "ET MALWARE Win32/AZORult V3.2 Client Checkin M17", "ET MALWARE ABUSE.CH Locky C2 Domain (jjjooyeohgghgtwn in DNS Lookup)", "ET MALWARE Bifrose/Cycbot Checkin 2", "ET MALWARE Win32/TrojanProxy.JpiProx.B CnC Beacon 1", "ET MALWARE Sakula/Mivast RAT CnC Beacon 6", "ET MALWARE W32/Citadel Download From CnC Server /files/ attachment", "ET MALWARE Ransomware/Cerber Checkin M3 (4)", "ET MALWARE Cobalt Strike Malleable C2 (Safebrowse Profile) GET", "ET MALWARE Betabot Checkin 5", "ET MALWARE CROSSWALK CnC Checkin", "ET MALWARE Cobalt Strike Malleable C2 (Meterpreter)", "ET MALWARE nspps Backdoor - Sending SOCKS Details", "ET MALWARE Sekhmet Ransomware CnC Activity", "ET MALWARE Konni Stage 2 Payload Exfiltrating Data", "ET MALWARE Win32 Cloaker Related Post Infection Checkin", "ET MALWARE Win32/VB.QTV CnC Checkin", "ET MALWARE OilRig OopsIE CnC Checkin M2", "ET MALWARE W32/Asprox.Bot Knock Variant CnC Beacon", "ET MALWARE lu0bot Loader HTTP Response", "ET MALWARE Tendrit CnC Beacon 2", "ET MALWARE Win32/Backdoor.Agent.qweydh CnC Activity", "ET MALWARE FormBook CnC Checkin (GET)", "ET MALWARE LuminosityLink - CnC Password Exfil", "ET MALWARE WEBC2-CLOVER Download UA", "ET MALWARE Qudox CnC Actiivty", "ET MALWARE Nymaim.BA CnC M1", "ET MALWARE APT/Bitter Related Checkin Activity (GET)", "ET MALWARE Downloader.Banload2.KZU Checkin 2", "ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (chromup)", "ET MALWARE Win32/ErbiumStealer CnC Activity (GetBuild)", "ET MALWARE Win32/Kryptik.BSYO Checkin 2", "ET MALWARE Trojan-Dropper.Win32.StartPage.dvm or Mebromi Bios Rootkit CnC Count Checkin", "ET MALWARE CobianRAT Receiving Additional Commands From CnC", "ET MALWARE Win32/Agent.ACBD CnC Activity", "ET MALWARE PoshC2 - Observed Default URI Structure M30", "ET MALWARE Gamut Spambot Checkin 2", "ET MALWARE Win32/Spy.Agent.POX Variant CnC", "ET MALWARE NOBELIUM - Cobalt Strike Malleable Profile M2", "ET MALWARE Tick Group Payload - Reporting Error to CnC", "ET MALWARE ZeroAccess Checkin", "ET MALWARE Diavol Communicating with CnC - Landing Request", "ET MALWARE OLDBAIT Checkin sptr", "ET MALWARE MSIL/Modi RAT CnC Command Inbound (in)", "ET MALWARE Win32.Raccoon Stealer Checkin M6", "ET MALWARE Cnzz.cn Related Dropper Checkin", "ET MALWARE Observed BatLoader Domain (installationsoftware1 .com) in TLS SNI", "ET MALWARE

	Win32/Nitol.B Checkin", "ET MALWARE HabitsRAT Checkin", "ET MALWARE RouteX CnC Domain (c13a856f4a879a89e9a638207efd6c94 .biz) in DNS Lookup", "ET MALWARE Amadey Stealer CnC - BotKiller Module Checkin", "ET MALWARE Fareit/Pony Downloader Checkin 2", "ET MALWARE DoS.Linux/Elknot.E Checkin", "ET MALWARE MSIL/SkidRat CnC Checkin M2", "ET MALWARE TR/Spy.Gen checkin via dns ANY query", "ET MALWARE EarthWorm/Termite IoT Agent CnC Response", "ET MALWARE Fullspace.cc or Related Checkin (2)", "ET MALWARE Observed BOUNCEBEAM Backdoor CnC Domain (cloudflare .5156game .com in TLS SNI)", "ET MALWARE ELF/Roboto - Possible Encrypted Roboto P2P Payload Requested M1", "ET MALWARE Operation Cobra Venom WSF Stage 2 - CnC Checkin", "ET MALWARE W32/Emotet CnC Checkin", "ET MALWARE Lemon_Duck Powershell CnC Activity M14", "ET MALWARE Win32/Uwamson.A!ml CnC Checkin", "ET MALWARE MSIL/Azula Logger CnC Activity", "ET MALWARE Gh0st RAT Backdoor Checkin", "ET MALWARE MSIL/Agent.ATS CnC Activity", "ET MALWARE Win32/FakeXPA Checkin URL", "ET MOBILE_MALWARE Android.KorBanker Successful Fake Banking App Install CnC Server Acknowledgement", "ET MALWARE Win32.Renos/Artro Trojan Checkin M1", "ET MALWARE DonotGroup/Patchwork CnC DNS Lookup", "ET MALWARE Downloader.Win32.Tesch.A Server CnC Sending Executable", "ET MALWARE ELF/RapperBot CnC Checkin M2", "ET MALWARE DADJOKE/Rail Tycoon Payload Extraction", "ET MALWARE Win32/Trickbot Data Exfiltration M2", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 9", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.t (TLS SNI)", "ET MALWARE MirrorThief CnC Domain in DNS Lookup", "ET MALWARE Request for utu.dat Likely Ponmocup checkin", "ET MALWARE BigLock Ransomware CnC Activity (name)", "ET MALWARE Win32/Bulta CnC Beacon", "ET MALWARE W32.Nemim Checkin", "ET MALWARE W32/24x7Help.ScareWare CnC Beacon", "ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M1", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Remote Desktop)", "ET MALWARE LokiBot Request for C2 Commands Detected M2", "ET MALWARE Plead TSCookie CnC Checkin M3", "ET MALWARE Win32/Agent.XST/UP007 Checkin 2", "ET MALWARE Nemty Ransomware CnC Checkin", "ET MALWARE Win32/AZORult V3.3 Client Checkin M20", "ET MALWARE KeyloggerOnline Keylogger Checkin (sleep)", "ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (RIFF)", "ET MALWARE Win32/Neutrino Checkin 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 10", "ET MALWARE DOUBLEBACK CnC Activity", "ET MALWARE MSIL/GravityRAT CnC Checkin M2", "ET MALWARE WooSIP Downloader CnC WriteMetadataOnServer", "ET MALWARE H1N1 Loader CnC Beacon M1", "ET MALWARE Sarwent CnC Response (download_exec)", "ET MALWARE Win32.Raccoon Stealer Checkin Response M5", "ET MALWARE S400 RAT Client Checkin", "ET MALWARE Win64/Agent.BP Checkin", "ET MALWARE NAZAR EYService OSInfo response", "ET MALWARE Bladabindi/njrat CnC Keep-Alive (OUTBOUND)", "ET MALWARE Ttint XORed CnC Checkin", "ET MALWARE Formbook 0.3 Checkin", "ET MALWARE ProxyBox - HTTP CnC - .com.tw/check_version.php", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 3", "ET MALWARE Win32/CONFUCIUS_B CnC Checkin", "ET MALWARE Linux/ShellshockCampaign.DDOSBot Execute Shell Command CnC Server Message", "ET MALWARE Win32/Packed.BlackMoon.A CnC Checkin", "ET MALWARE X-Files Stealer CnC Exfil Activity M2", "ET MALWARE Win32/Emotet CnC Activity (POST) M8", "ET MALWARE W32/InstallMonster.Downloader Checkin", "ET MALWARE CASHY200 Style DNS Query - Request Command Beacon", "ET MALWARE Cobalt Strike Beacon (WooCommerce Profile)", "ET MALWARE Parallax CnC Response Activity M8", "ET MALWARE Koobface Trojan HTTP Post Checkin", "ET MALWARE Win32/TrojanDownloader.Small.AWO CnC Activity", "ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Started", "ET MALWARE Win32/CopperStealer CnC Activity M3", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher.a CnC Beacon", "ET MALWARE Reimageplus Ransomware Checkin", "ET MALWARE OSX/Mami CnC Checkin", "ET MALWARE [PTsecurity] Remcos RAT Checkin 69", "ET MALWARE ZhCAT.HackTool Operation Cleaver HTTP CnC Beacon", "ET MALWARE Win32/APT28 Host Fingerprint Exfiltration via IMAP", "ET MALWARE W32/Bingoml!tr CnC Activity",

	"ET MALWARE Inter Skimmer CnC Domain in DNS Lookup", "ET MALWARE Win32/VB.NBI CnC Checkin", "ET MALWARE Win32/Pift DNS TXT CnC Lookup ppift.net", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/nt/th", "ET MALWARE Sharik/Smoke CnC Beacon 12", "ET MOBILE_MALWARE Suspected SandCat Related CnC", "ET MALWARE CozyCar V2 CnC Beacon", "ET MALWARE Win32/TaskPerformer Downloader CnC Activity", "ET MALWARE Downloader.Win32.Tesch.A Bot Command Checkin 2", "ET MALWARE MintStealer CnC Activity (POST)", "ET MALWARE Backdoor.TurlaCarbon.A C2 HTTP Request", "ET MALWARE DarkGate CnC Requesting Data Exfiltration from Bot", "ET MALWARE Plead TSCookie CnC Checkin M1", "ET MALWARE Win32/Travnet.A Checkin", "ET MALWARE Pteranodon Backdoor Checkin", "ET MALWARE VikroStealer CnC Exfil", "ET MALWARE Jaff Ransomware Checkin M1", "ET MALWARE DNSBin Demo - Data Inbound", "ET MALWARE Ransomware/Cerber Checkin M3 (12)", "ET MALWARE MSIL/G2 Stealer/GravityRAT CnC Checkin", "ET MALWARE Bitter RAT HTTP CnC Beacon", "ET MALWARE Remcos RAT Checkin 23", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 12", "ET MALWARE LeChiffre Ransomware CnC", "ET MALWARE Soraya C2 User-Agent (VHIbot/1.0)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M8", "ET MOBILE_MALWARE Android/Drinik Activity (POST)", "ET MALWARE Trustezeb Checkin to CnC", "ET MALWARE Win32.Hupigon.dkwt Related Checkin", "ET MALWARE MirrorBlast CnC Activity M2", "ET MALWARE Win32/Poweliks.A Checkin 2", "ET MALWARE eleethub botnet CnC Domain in DNS Lookup (irc.eleethub .com)", "ET MALWARE Linux/Ssemgrvd sshd Backdoor HTTP CNC 1", "ET MALWARE Win32/WarHawk Activity (fileupload)", "ET MALWARE MSIL/Small.FU Variant CnC Activity M1", "ET MALWARE Win32/Agent.WVW CnC Beacon 3", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI)", "ET MALWARE W32/Zbot.Variant CnC Response", "ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (tommyforgreendream .icu) in TLS SNI", "ET MALWARE Win32/Mole Ransomware CnC Beacon", "ET MALWARE Andariel Backdoor Actvity (Response)", "ET MALWARE Poweliks Clickfraud CnC M4", "ET MALWARE Platinum APT Activity", "ET MALWARE PoshC2 - Observed Default URI Structure M9", "ET MALWARE Zebrocy Backdoor CnC Activity", "ET MALWARE FrameworkPOS CnC Server Reporting IP Address To Agent", "ET MALWARE Win32/Valak - Stage 2 - Response - Task", "ET MALWARE Win32/HydraCrypt CnC Beacon 1", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (yhgrffndvzbtoilmundkmvbaxrjtqsew .com)", "ET MALWARE Win32/Remcos RAT Checkin 810", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/dllhost/ac", "ET MALWARE TinyLoader.B1 Checkin x64", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 103", "ET MALWARE Win32.Rovnix.I Checkin", "ET MALWARE ModPipe CnC Activity (POST)", "ET MALWARE Farfli HTTP Checkin Activity", "ET MALWARE Bookworm CnC Beacon", "ET MALWARE Zeus POST Request to CnC sk1 and bn1 post parameters", "ET MALWARE DPRK HIDDEN COBRA Botnet C2 Host Beacon", "ET MOBILE_MALWARE Android/HeHe.Spy ReportMessageRequest CnC Beacon", "ET MALWARE MSIL.BackNet Checkin", "ET MALWARE Win32/Toby.N Multilocker Checkin", "ET MALWARE Win32/Bisonal RC4 Encrypted 8 Byte Static CnC Checkin", "ET MALWARE Trojan.Win32.Antavmu.guw Checkin", "ET MALWARE Win32/RisePro CnC Command Outbound (pingmap)", "ET MALWARE Fullz House Credit Card Skimmer Data Exfil", "ET MALWARE Gift Cardshark CnC Domain in DNS Lookup", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 95", "ET MALWARE BigLock Ransomware CnC Activity (gen)", "ET MALWARE Xbash CnC DNS Lookup (censys .xyz)", "ET MALWARE MICROPSIA CnC Domain Observed in SNI (samwinchester .club)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M5", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 8", "ET MALWARE xpsecuritycenter.com Fake AntiVirus GET-Install Checkin", "ET MALWARE Win32/Xtrat.A Checkin", "ET MALWARE BatLoader CnC Domain (cloudsteamview .com) in DNS Lookup", "ET MALWARE [PTsecurity] DorkBot.Downloader CnC Beacon", "ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (clon .collectfasttracks .com) in TLS SNI", "ET MOBILE_MALWARE Android/CoolPaperLeak Sending Information To CnC", "ET MALWARE Win32/Unk.BrowserStealer Data Exfil M2", "ET MALWARE Generic Checkin -

	MSCommonInfoEx", "ET MALWARE Ixeshe/Mecklow Checkin 2", "ET MALWARE Ousaban Banker KeepAlive Response", "ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (ifn1h8ag1g .com in TLS SNI)", "ET MALWARE Alina Checkin", "ET MALWARE Trojan.Win32.VBKrypt.cugq/Umbra Checkin", "ET MALWARE r0 CnC Architecture POST 3", "ET MALWARE Win32/Neutrino Checkin 6", "ET MALWARE Worm.VBS.ayr CnC command (is-enum-driver)", "ET MALWARE Perl/Calfbot C&C DNS request", "ET MALWARE Possible Red October proxy CnC 3", "ET MALWARE Suspected APT LuckyMouse BlueTraveller CnC", "ET MALWARE BOUNCEBEAM Backdoor CnC Activity", "ET MALWARE OilRig OopsIE CnC Checkin M4", "ET MALWARE Mirai/OMG Proxy Variant CnC in DNS Lookup (rpnew.mm .my)", "ET MALWARE KimJongRAT cnc exe pull", "ET MALWARE Win32/Trapwot FakeAV Post Infection CnC Beacon", "ET MALWARE Win32/SVCReady Loader - Screenshot", "ET MALWARE Win32/IceXLoader Sending System Information (POST)", "ET MALWARE DADJOKE/Rail Tycoon Payload Execution", "ET MALWARE Storm/Waledac 3.0 Checkin 2", "ET MALWARE Octopus Backdoor Related Domain in DNS Lookup", "ET MALWARE Win32/Upgilf CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 89", "ET MALWARE Ransomware/Cerber Checkin 2", "ET MALWARE Manjusaka C2 Heartbeat Response", "ET MALWARE Win32/Injector.ULH CnC Activity", "ET MALWARE Koobface C&C availability check", "ET MALWARE ViperSoftX HTTP CnC Activity", "ET MALWARE Win32/Onliner Mailer Module Communicating with CnC", "ET MALWARE Chafer Win32/TREKX Uploading to CnC (Modified CAB)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12", "ET MALWARE Blackenergy Bot Checkin to C&C", "ET MALWARE Oilrig Stealer CnC Checkin", "ET MALWARE Foudre Checkin M3", "ET MALWARE Infostealer.Mysayad Checkin 2", "ET MALWARE Win32.Spy/TVRat Checkin", "ET MALWARE Fileless infection dropped by EK CnC Beacon", "ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Checkin", "ET MALWARE NSIS/TrojanDownloader.Agent.NZK CnC Activity M1", "ET MALWARE Observed DNS Query to RisePro Domain (fixgroupfactor .com)", "ET MALWARE W32.Daws/Sanny CnC Initial Beacon", "ET MALWARE Win32/Unknown Stealer Command Response (filegrab) (Inbound)", "ET MALWARE Unknown AutoIt Bot - Initial Server Response", "ET MALWARE Shiz or Rohimafo Reporting Listening Socket to CnC Server", "ET MALWARE Matanbuchus Loader CnC M1", "ET MALWARE Win32/Remcos RAT Checkin 809", "ET MALWARE Suspected CHAOS CnC Inbound (getos)", "ET MALWARE Lop_com or variant Checkin (9kgen_up)", "ET MALWARE Bravix Checkin", "ET MALWARE Win32/PSW.Agent.OIN CnC Activity", "ET MALWARE Bozok.RAT checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 60", "ET MALWARE Ursnif Variant CnC Beacon 3", "ET MALWARE Win32/Ropest.H CnC - INBOUND", "ET MALWARE KLog Nick Keylogger Checkin", "ET MALWARE BazaLoader CnC Activity", "ET MALWARE Win32/Goofy Guineapig CnC Activity (GET) M2", "ET MALWARE W32/Emotet.v4 Checkin", "ET MALWARE NEWPASS CnC Client Checkin", "ET MALWARE Parallax CnC Activity M7 (set)", "ET MALWARE MAGICHOUND.LEASH IRC CnC Beacon", "ET MALWARE BalkanDoor CnC Checkin - Server Response", "ET MALWARE OSX/GMERA.B CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 34", "ET MALWARE Ursnif Variant CnC Beacon", "ET MALWARE Vicious Panda CnC Activity", "ET MALWARE DNSBin Demo - Data Exfil", "ET MALWARE Win32.Agent.Y!c CnC Checkin", "ET MALWARE OilRig QUADAGENT CnC Domain in SNI", "ET MALWARE APT 41 LOWKEY Backdoor - Ping Error Code sent to CnC", "ET MALWARE Observed MAZE Ransomware CnC Domain (plaintsotherest .net in TLS SNI)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 38", "ET MALWARE Trojan.JS.Agent.dwz Checkin", "ET MALWARE AZORult v3.2 Server Response M1", "ET WEB_SERVER FOX-SRT - Backdoor - CryptoPHP Shell C2 POST", "ET MALWARE AlphaCrypt CnC Beacon 5", "ET MALWARE FakeAV Variant CnC Beacon", "ET MALWARE r0 CnC GET", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic", "ET MALWARE Linux.Mumblehard Command Status CnC", "ET MALWARE [PTsecurity] Donut Ransomware CnC Checkin", "ET MALWARE AZORult v3.2 Server Response M3", "ET MALWARE Chthonic CnC Beacon 6", "ET MALWARE Magician/M461c14n Ransomware CnC Checkin", "ET MALWARE FastPOS Version Checkin", "ET MALWARE

	Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 29", "ET MALWARE APT-Q-37/Manling Flower Payload - CnC Checkin", "ET MALWARE Win32/AZORult V3.3 Client Checkin M14", "ET MOBILE_MALWARE Android/FakeTimer.A Reporting to CnC", "ET MALWARE Emotet Post Drop C2 Comms", "ET MALWARE Ixeshe/Mecklow Checkin", "ET MALWARE Observed Cryptor Ransomware CnC Domain (e3kok4ekzalzapsf .onion .ws in TLS SNI)", "ET MALWARE SSV Agent CnC Activity", "ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (gabriellalovecats .com) in DNS Lookup", "ET MALWARE Terse Upload to Free Image Hosting Provider (uploads .im) - Likely Malware", "ET MALWARE Cobalt Strike Malleable C2 (Havex APT)", "ET MALWARE MSIL/Bobik CnC Traffic", "ET MALWARE Linux/B1txor20 Backdoor Related Domain in DNS Lookup", "ET MALWARE Win32/RisePro CnC Activity (GET)", "ET MALWARE Win32/Injector.DSQR CnC Activity (POST)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M11", "ET MALWARE Win32/VB.QPK CnC Checkin", "ET MALWARE Diavol Communicating with CnC - Register M1", "ET MALWARE Lost Door Checkin", "ET MALWARE Linux/Ssemgrvd sshd Backdoor HTTP CNC 2", "ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Command Tunneling M2", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Process Listing)", "ET MALWARE W32/PointOfSales.Misc CnC Activity", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M1", "ET MALWARE Observed DNS Query to RisePro Domain (gg-loader .com)", "ET MALWARE Win32/Kryptik.BSYO Checkin", "ET MALWARE SUNSHUTTLE CnC Activity", "ET MALWARE Andariel Backdoor Activity (Checkin)", "ET MALWARE Chthonic CnC Beacon 5", "ET MALWARE Arechclient2 Backdoor CnC Init", "ET MALWARE Win32/Aura Ransomware CnC Activity", "ET MALWARE Win32/Plurox Backdoor CnC Checkin", "ET MALWARE Miuref/Boaxxe Checkin", "ET MALWARE MICROPSIA Screenshot Upload M3", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23", "ET MALWARE Observed DNS Query to RisePro Domain (uni-files .com)", "ET MALWARE Banload POST Checkin (dados)", "ET MALWARE Win32/Remcos RAT Checkin 54", "ET MALWARE [PT MALWARE] Hacked Mikrotik C2 Request", "ET MALWARE Emotet Wifi Bruter Module Checkin", "ET MALWARE Link Implant CnC Activity (POST)", "ET MALWARE HackTool.Linux.SSHBRUTE.A Haiduc Initial Compromise C2 POST", "ET MALWARE TrochilusRAT CnC Beacon 1", "ET MALWARE Win32/Onliner Receiving Commands from CnC", "ET MALWARE Pteranodon Backdoor CnC POST", "ET MALWARE FakeM RAT CnC Beacon", "ET MALWARE NanoCore RAT CnC 27", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.1)", "ET MALWARE HAWKBALL CnC Sending System Information", "ET MALWARE DDG Botnet CnC Job Request", "ET MALWARE StormKitty Data Exfil via Telegram", "ET MALWARE ELF/RedXOR CnC Checkin", "ET MALWARE Linux/ChinaZ 2.0 DDoS Bot Checkin 3", "ET MALWARE PoshC2 - Observed Default URI Structure M26", "ET MALWARE Dyreza RAT Checkin 3", "ET MALWARE Win32/Snatch Ransomware - Encryption Finished", "ET MALWARE Trojan.Karagany C&C Response", "ET MALWARE DeathStalker/Janicab CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 82", "ET MALWARE Win32.PEx.Delphi.1151005043 Post-infection Checkin", "ET MALWARE Dropper Checkin (often scripts.dlv4.com related)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 70", "ET MALWARE nspps Backdoor - Task Response", "ET MALWARE Win32/MillionLoader CnC Init Activity", "ET MALWARE Matanbuchus Loader Server Response", "ET MALWARE Tortoiseshell/HMH Download Request", "ET MALWARE WEBC2-ADSPACE Server Response", "ET MALWARE Win32/Trapwot FakeAV Checkin", "ET MALWARE BePush/Kilim CnC Beacon", "ET MALWARE SEASALT Client Checkin", "ET MALWARE Win32/Rodecap CnC Checkin", "ET MALWARE Ragnarok Ransomware CnC Activity M1", "ET MALWARE Trojan-Ransom.Win32.Blocker.dham Checkin", "ET MALWARE Win32/LODEINFO v0.3.6 CnC Checkin", "ET MALWARE Parallax CnC Activity M17 (set)", "ET MALWARE r0 CnC Report POST", "ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 3", "ET MALWARE W32/Depyot.Downloader CnC Beacon", "ET MALWARE Trojan-Banker.Win32.Agent Checkin", "ET MALWARE MSIL/Autorun.AD Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (16)", "ET MALWARE Illusion Bot (Lussilon) Checkin", "ET MALWARE Win32/Spectre Ransomware CnC Checkin", "ET MALWARE

	MICROPSIA CnC Checkin M2", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (deliverygoodstrategies .com) in DNS Lookup", "ET MALWARE Shiz/Rohimafo Checkin", "ET MOBILE_MALWARE Android/Smspacem CnC Communication Attempt", "ET MALWARE Win32/Adware.Agent.NSU CnC Activity", "ET MALWARE Win32/Valak <v9 - Stage 2 - Request", "ET MALWARE W32/Kazy.325252 Variant CnC Beacon 2", "ET MALWARE Diavol Communicating with CnC - Register M2", "ET MALWARE Soraya C2 User-Agent (x09)", "ET MALWARE Tortoiseshell/SysKit CnC Activity", "ET MALWARE Base64 Encoded Windows Command Prompt (Outbound)", "ET MALWARE Ave Maria/Warzone RAT Credential Exfil", "ET MALWARE Operation Cobra Venom WSF Stage 1 - CnC Checkin", "ET MALWARE Syrutrk/Gibon/Bredolab Checkin", "ET MALWARE SoulSearcher Checkin M1", "ET MALWARE Xbash CnC DNS Lookup (scanaan .tk)", "ET MALWARE W32/FloatingCloud.Banker CnC Beacon", "ET MALWARE BKDR_SLOTH.A Checkin", "ET MALWARE MuddyWater Payload - CnC Checkin", "ET MALWARE Inbound MonetizeUs/LNKR Struct", "ET MALWARE Hupigon URL Infection Checkin Detected", "ET MALWARE General Banker.PWS POST Checkin", "ET MALWARE Loxes/Mongall Related CnC Beacon M3 (GET)", "ET MALWARE Mocelpa Client Hello CnC Beacon", "ET MALWARE Win32/Backdoor.Small.ao CnC Checkin", "ET MALWARE W32/Beebus HTTP POST CnC Beacon", "ET MALWARE W32/Zemra.DDoS.Bot Variant CnC Beacon", "ET MALWARE KilerRAT CnC - Remote Shell", "ET MALWARE YAHOOYLO Stealer CnC Exfil", "ET MALWARE DCRat Initial CnC Activity", "ET MALWARE W32/DirCrypt.Ransomware CnC Checkin", "ET MALWARE Cobalt Strike Malleable C2 Profile (Teams) M2", "ET MALWARE Alureon Checkin", "ET MALWARE Linux/SSHDoor.A Reporting Backdoor CnC Beacon", "ET MALWARE Octopus Malware CnC Server Connectivity Check", "ET MALWARE MargulasRAT Keep-Alive Inbound M1", "ET MALWARE Stealbit Variant Data Exfil M2", "ET MALWARE W32/Emotet CnC Beacon 3", "ET MALWARE NOBELIUM - Cobalt Strike Malleable Profile M1", "ET MALWARE Bladabindi/njrat CnC Command Response (Process listing)", "ET MALWARE Observed DNS Query to RisePro Domain (pickofiles .com)", "ET MALWARE Shurl0ckr Ransomware CnC (kdvm5fd6tn6jsbwh .onion .to in DNS Lookup)", "ET MALWARE Corebot Checkin", "ET MALWARE Worm.VBS.ayr CnC command (is-cmd-shell)", "ET MALWARE OSX/AlienSpy RAT Checkin", "ET MALWARE Ursa Loader CnC Checkin", "ET MALWARE Dyre CnC Checkin", "ET MALWARE DNS Query for known ShadowPad CnC 1", "ET MALWARE SAD Ransomware CnC Activity", "ET MALWARE Alphacrypt/TeslaCrypt Ransomware CnC Beacon", "ET MALWARE Win32/Ursnif LDR4 Beacon (POST)", "ET MALWARE ThiefQuest CnC Domain in DNS Lookup", "ET MALWARE Win32/Emotet CnC Activity (POST) M3", "ET MALWARE Win32.Sality-GR Checkin 2", "ET MALWARE Py/Beapy CnC Checkin", "ET MALWARE RShell Backdoor Keepalive", "ET MALWARE Trojan-Spy.Win32.KeyLogger.acuj Checkin", "ET MALWARE Pushdo.S CnC response", "ET MALWARE Volatile Cedar Win32.Explosive HTTP CnC Beacon 1", "ET MALWARE Ransomware Locky CnC Beacon 21 May", "ET MALWARE Zbot CnC GET /lost.dat", "ET MALWARE Cobalt Strike Beacon Activity (Wordpress Profile)", "ET MALWARE APT Mustang Panda CnC Activity", "ET MALWARE xCaon Embedded Encrypted Command in Webpage", "ET MALWARE Aveo C2 Request", "ET MALWARE Downeks Checkin", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI)", "ET MALWARE Operation Tripoli Related CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 64", "ET MALWARE Backdoor.Win32.Agent.bjjv Checkin", "ET MALWARE W32/Rshot.Backdoor File Upload CnC Beacon", "ET MALWARE Win32.Crypren/Zcrypt Ransomware Checkin", "ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2 (set) M1", "ET MALWARE Android Infostealer CnC Check-In", "ET MALWARE MassLogger Client Data Exfil SMTP", "ET MALWARE Backdoor.Win32.ZZSlash/Redosdru.E checkin", "ET MALWARE Win32/VB.SDB CnC Beacon", "ET MALWARE ABUSE.CH Zloader CnC Domain Detected", "ET MALWARE Win32/Backdoor.Graphon Checkin Activity (GET)", "ET MALWARE PowerTrick Task Request", "ET MALWARE r0 CnC Architecture POST 2", "ET MALWARE Win32/Teslacrypt Ransomware HTTP CnC Beacon M1", "ET MALWARE APT/Bitter CnC Exfiltration via TCP", "ET WEB_SERVER FOX-SRT - Backdoor - CryptoPHP Shell C2 POST (fsockopen)", "ET MALWARE Suspected CHAOS CnC Inbound (keylogger start)", "ET

	MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a CnC Beacon", "ET MALWARE Linux/Moose NAT Traversal CnC Beacon set", "ET MALWARE MINEBRIDGE/MINEDOOR CnC Checkin", "ET MALWARE Capfire4 Checkin (register machine)", "ET MALWARE Python.Ragua Checkin", "ET MALWARE ISRStealer Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (3)", "ET MALWARE Variant.Kazy.174106 Checkin", "ET MALWARE Downloader.Win32.Tesch.A Server CnC Checkin Reply", "ET MALWARE Win32/Remcos RAT Checkin 55", "ET MALWARE DNS Query for known ShadowPad CnC 4", "ET MALWARE Bladabindi/njrat CnC Command (Kill Process)", "ET MALWARE Danabot CnC Checkin", "ET MALWARE HiveRAT CnC Activity M1", "ET MALWARE r0 CnC Architecture GET 2", "ET MALWARE Gasket CnC Checkin", "ET MALWARE SSL/TLS Certificate Observed (Buer Loader)", "ET MALWARE Gozi/BlackNet Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (m-rise .pro)", "ET MALWARE Win32/Pift DNS TXT CnC Lookup ppidn.net", "ET MALWARE W32/Briba CnC POST Beacon", "ET MALWARE W32/Asprox.ClickFraudBot POST CnC Beacon", "ET MALWARE Sakula/Mivast RAT CnC Beacon 7", "ET MALWARE W32/HelloBridge.Backdoor Register CnC Beacon", "ET MALWARE Sharik/Smoke CnC Beacon 10", "ET MALWARE [PTsecurity] Win32/SocStealer.Socelars C2 Response", "ET MALWARE Win32/Valak - Plugin Data Exfil", "ET MALWARE Possible Ursnif/Gamaredon Related VNC Module CnC Beacon", "ET MALWARE W32/FakeAlert Fake Security Tool Checkin", "ET MALWARE BlackTech/PLEAD TSCookie CnC Checkin M2", "ET MALWARE Webshell Access with Known Password Inbound - Possibly Iran-based", "ET MALWARE Lop.gfr/Swizzor HTTP Update/Checkin", "ET MALWARE Win32/PSW.WOW.NLZ CnC Activity", "ET MALWARE Backdoor Win32/Hupigon.CK Server Checkin", "ET MALWARE Win32/CryPy Ransomware CnC Checkin", "ET MALWARE MSIL/NewHT Ransomware CnC Checkin", "ET MALWARE Possible Darkhotel Higasia Downloader Requesting Module", "ET MALWARE Win32/Qbot CnC Activity M3 (POST)", "ET MALWARE W32/ServStart.Variant CnC Beacon", "ET MALWARE ArtraDownloader/TeleRAT Checkin", "ET MALWARE Platinum APT - Titanium Payload CnC Checkin (x64)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 45", "ET MALWARE Win32/AZORult V3.3 Client Checkin M1", "ET MALWARE Win32/SVCReady Loader - Logs", "ET MALWARE Linux/Venom CnC Beacon", "ET MALWARE Win32/Backdoor.Daxin CnC Activity", "ET MALWARE MSIL/GravityRAT CnC Domain (msoftupdates .com in DNS Lookup)", "ET MALWARE Tinba Checkin 2", "ET MALWARE CryptoShield Ransomware Checkin", "ET MALWARE MSIL/Modi RAT CnC Screenshot Outbound", "ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)", "ET MALWARE Jasper URI Path Observed M1", "ET MALWARE Jupyter Stealer CnC Checkin", "ET MALWARE Win32/Datper CnC Activity", "ET MALWARE PureCrypter Requesting Injector M1", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 40", "ET MALWARE MSIL/Karmen Ransomware CnC Activity", "ET MALWARE Win32.Raccoon Stealer Checkin Response M4", "ET MALWARE BrushaLoader CnC Domain in SNI", "ET MALWARE DownloaderExchanger/Cbeplay Variant Checkin", "ET MALWARE RampantKitten APT TelB Python Variant - CnC Checkin M1", "ET MALWARE BITTERBUG Checkin", "ET MALWARE Mirage Campaign checkin", "ET MALWARE Locky CnC Checkin Dec 5 M1", "ET MALWARE Tinba Checkin 3", "ET MALWARE UBoatRAT CnC Check-in", "ET MALWARE Kratos Silent Miner Checkin via Discord", "ET MALWARE ServHelper CnC Inital Checkin", "ET MALWARE Lunar Builder Exfil Response", "ET MOBILE_MALWARE Android.Zitmo Forwarding SMS Message to CnC Server", "ET MALWARE DNS Query for known ShadowPad CnC 8", "ET MALWARE Piptea.a Related Trojan Checkin (2)", "ET MALWARE Observed DNS Query to RisePro Domain (factor1right .com)", "ET MALWARE Win32/DanijBot CnC Checkin", "ET MALWARE Dridex/Bugat/Feodo POST Checkin", "ET MALWARE PoisonIvy HTTP CnC Beacon", "ET MALWARE Taurus Stealer CnC Host Checkin", "ET MALWARE Sidewalk CnC Checkin", "ET MALWARE [PTsecurity] Remcos RAT Checkin 86", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 83", "ET MALWARE Bifrose/Cycbot Checkin", "ET MALWARE Win32/AZORult V3.3 Client Checkin M19", "ET MALWARE Unattributed CnC Domain in DNS Lookup (secured-mail .online)", "ET MALWARE Panda Banker C2 Domain (uiaoduiiej .chimkent .su in DNS Lookup)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 6", "ET

	MALWARE Sarwent CnC Command (download)", "ET MALWARE Win32/TrojanDownloader.Delf.BXC CnC Beacon", "ET MALWARE Bamital Headers - Likely CnC Beacon", "ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 2", "ET MALWARE ServHelper CnC Command (Whoami)", "ET MALWARE Lyposit Ransomware Checkin 2", "ET MALWARE Win32/Backdoor Checkin (POST)", "ET MALWARE Vawtrak/NeverQuest Checkin", "ET MALWARE Linux/Lady CnC Beacon 2", "ET MALWARE Sarwent CnC Response (rdp_exec)", "ET MALWARE Win32/ProtonBot CnC Response", "ET MALWARE Win32/IceXLoader Sending Initial Checkin (POST)", "ET MALWARE ELF/RapperBot CnC Checkin M1", "ET MALWARE Shamoon V3 CnC Checkin", "ET MALWARE W32/Wadolin.Downloader CnC Beacon", "ET MALWARE Trojan.Win32.Yakes.pwo Checkin", "ET MALWARE Banload CnC Activity", "ET MALWARE Proyecto RAT Variant - Yopmail Stage 2 CnC Retrieval", "ET MALWARE Win32/Autophyte.F C2 Domain (www .apshenyihl .com in TLS SNI)", "ET MALWARE Urlzone/Bebloh/Bublik Checkin /was/uid.php", "ET MALWARE Zentom FakeAV Checkin", "ET MALWARE W32/Bakcorox.A ProxyBot CnC Server Connection", "ET MALWARE Win32/AZORult V3.2 Client Checkin M14", "ET MALWARE Houdini/Hworm CnC Checkin M1", "ET MALWARE Win32/Retadup CnC Checkin M2", "ET MALWARE FighterPOS CnC Beacon 1", "ET MALWARE Conficker/KernelBot/MS08-067 related Trojan Checkin", "ET MALWARE DCRat CnC Activity M13", "ET MALWARE Win32/Agent.WMN CnC Beacon", "ET MALWARE Win32/AgentTesla Variant Exfil via Telegram", "ET MALWARE CryptoPatronum Ransomware CnC Checkin", "ET MALWARE Common Downloader Install Report URL (farfly checkin)", "ET MALWARE Unattributed CnC Domain in DNS Lookup (wipro365 .com)", "ET MALWARE PunkeyPOS HTTP CnC Beacon 4", "ET MALWARE PCRat/Gh0st CnC Beacon Request (Xfire variant)", "ET MALWARE Cryptojoker Checkin", "ET MALWARE Possible Darkhotel Higasia Downloader Checkin", "ET MALWARE Lazarus Maldoc CnC", "ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (transadforward .icu) in TLS SNI", "ET MALWARE Bladabindi/njrat CnC Command Response (Remote Desktop)", "ET MALWARE Win32/Remcos RAT Checkin 68", "ET MALWARE Win32/Farfli.CUY CnC Server Response", "ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Beacon)", "ET MALWARE Anchor_DNS stickseed Variant CnC Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (8)", "ET MALWARE CBReplay Checkin", "ET MALWARE DustySky CnC Beacon", "ET MALWARE Win32/Remcos RAT Checkin 61", "ET MALWARE Enigma Locker Checkin", "ET MALWARE PHPs Labyrinth Backdoor Stage2 CnC Activity M1", "ET MALWARE Win32/Agent.TWI CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 62", "ET MALWARE Covenant .NET Framework P2P C&C Protocol Gruntsvc Named Pipe Interaction", "ET MALWARE W32.Downloader Tibs.jy Reporting to C&C (2)", "ET MALWARE Vawtrak HTTP CnC Beacon", "ET MOBILE_MALWARE CoolReaper CnC Beacon 2", "ET MALWARE Win32.Application.ThunderN.A Checkin", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Download Command Error", "ET MALWARE Win32/Tofsee Malformed Spam Template String", "ET MALWARE Possible Win32/Qbot/Quakbot Checkin via HTTP GET", "ET MALWARE Evrial Stealer CnC Activity M2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 81", "ET MALWARE Smart Fortress FakeAV/Kryptik.ABNC Checkin", "ET MALWARE [PTsecurity] Remcos RAT Checkin 26", "ET MALWARE r0 CnC Architecture POST 4", "ET MALWARE BatLoader CnC Domain (tableau-cloud .com) in DNS Lookup", "ET MALWARE FlashBack Mac OSX malware Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 72", "ET MOBILE_MALWARE Android/HippoSms Method Request to CnC", "ET MALWARE EvilNum CnC Client Data Exfil", "ET MALWARE RCtrl Backdoor CnC Checkin M2", "ET ADWARE_PUP RelevantKnowledge Adware CnC Beacon", "ET MALWARE Lyposit Ransomware Checkin 1", "ET MALWARE NewPosThings Checkin", "ET MALWARE FTCode Stealer Init Activity", "ET MALWARE r0 CnC POST", "ET MALWARE DTLoader Binary Request", "ET MALWARE Aurora/OneKeyLocker Ransomware CnC Checkin", "ET MALWARE APT39/Chafer Payload - CnC Checkin M1", "ET MALWARE Hoax.Win32.BadJoke/DownLoader1.57593 Checkin", "ET MALWARE Andromeda Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic

	(OUTBOUND) 96", "ET MALWARE Dridex CnC Request - Spam/Worm Component", "ET MALWARE MSIL/HadesLocker Ransomware Checkin", "ET MALWARE FrauDrop Checkin", "ET JA3 Hash - Suspected Meterpreter Reverse Shell M2 (set)", "ET MALWARE Backdoor.Win32.Aldibot.A Checkin", "ET MALWARE W32/Nymaim Checkin M2", "ET MALWARE W32/Hesperus.Banker Nlog.php Variant Sending Data To CnC", "ET MALWARE Gimemo Ransomware Checkin", "ET MALWARE Win32/Remcos RAT Checkin 59", "ET MALWARE Observed BatLoader Domain (internalchecksso .com) in TLS SNI", "ET MALWARE Observed DNS Query to RisePro Domain (xx1-files .com)", "ET MALWARE Mac Trojan HTTP Checkin (accept-language violation)", "ET MALWARE FRat WebSockets Request M2", "ET MALWARE Win32/LockScreen CnC Beacon 2", "ET MALWARE Win32/RisePro CnC Server Response M4", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 58", "ET MALWARE Unattributed CnC Domain in DNS Lookup (xsecuremail .com)", "ET MALWARE Win32/HunterStealer/AlfonsoStealer/PhoenixStealer CnC Exfil", "ET MALWARE DEEP PANDA Checkin 1", "ET MALWARE lu0bot Loader HTTP Request", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Message)", "ET MALWARE ASNAROK CnC Domain in DNS Lookup", "ET MALWARE Monsoon Tinytyphon CnC Beacon Exfiltrating Docs", "ET MALWARE Win32/Agent.WVW CnC Beacon 2", "ET MALWARE TeleBots VBS Backdoor CnC Beacon 1", "ET MALWARE njRAT/Bladabindi Variant (Lime) CnC Checkin", "ET MALWARE Win32/FlawedAmmyy RAT CnC Checkin", "ET MALWARE Win32.Small.AB or related Post-infection checkin", "ET MALWARE Cobalt Strike Malleable C2 Profile (__session__id Cookie)", "ET MALWARE Go/Anubis CnC Activity (POST)", "ET MALWARE ELF/Mayhem Checkin", "ET MALWARE OSX/NukeSped Variant CnC Activity", "ET MALWARE Worm.VBS.ayr CnC command (is-enum-process)", "ET MALWARE Amadey CnC Check-In", "ET MALWARE Possible OceanLotus C2 Checkin", "ET MALWARE Sharik/Smoke CnC Beacon 7", "ET MALWARE Win32/RisePro CnC Server Response M5", "ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Download)", "ET MALWARE W32/Dridex POST CnC Beacon", "ET MALWARE Bedep HTTP POST CnC Beacon", "ET MALWARE Win32.TreasureHunter Checkin", "ET MALWARE ELF/Muhstik Botnet CnC Activity", "ET MALWARE Win32/Htbot.B Checkin", "ET MALWARE Lookup of Algorithm Generated Zeus CnC Domain (DGA)", "ET MALWARE Babax Stealer Exfil via Telegram", "ET MALWARE Cohhoc RAT CnC Request", "ET MALWARE Bladabindi/njrat CnC Command (Get Passwords)", "ET MALWARE Win32/AZORult V3.3 Client Checkin M8", "ET MALWARE VBS/TrojanDownloader.Agent.SEB Checkin", "ET MALWARE W32/Backdoor.BlackMonay Checkin", "ET MALWARE Bolek HTTP Checkin", "ET MALWARE QRat.Java.RAT Post-Checkin Request", "ET MALWARE SYNful Knock Cisco IOS Router Implant CnC Beacon (INBOUND)", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (etzndtcvqvyxajpcgwkzsoweaubilflh .com)", "ET MALWARE QRat.Java.RAT Checkin Response", "ET MALWARE Win32/AZORult V3.3 Client Checkin M4", "ET MALWARE [PTsecurity] Remcos RAT Checkin 85", "ET MALWARE Dooptroop CnC Beacon", "ET MALWARE Nyanw0rm CnC Keep-Alive (Outbound) M1", "ET MALWARE ProxyBox - HTTP CnC - POST 1-letter.php", "ET MALWARE Cobalt Strike Malleable C2 (Unknown Profile)", "ET MALWARE Win32/AZORult V3.3 Client Checkin M16", "ET MALWARE Emotet Checkin", "ET MALWARE contacy.info Trojan Checkin (User agent clk_jdfhid)", "ET MALWARE Plead TSCookie CnC Checkin M4", "ET MALWARE W32/Kbot.Backdoor Variant CnC Beacon", "ET MALWARE W32/Numnet.Downloader CnC Checkin 2", "ET MALWARE AllaKore CnC Activity", "ET MALWARE Win32/Trojan.Agent.AXMO CnC Beacon", "ET MALWARE Win32/Goofy Guineapig CnC Activity (GET) M1", "ET MALWARE Win32/Autophyte.F C2 Domain (www .ap8898 .com in DNS Lookup)", "ET MALWARE Win32/Remcos RAT Checkin 64", "ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)", "ET MALWARE Java/QRat Checkin", "ET MALWARE Win32/IcedID WebSocket Request M2", "ET MALWARE JsOutProx CnC Activity - Inbound", "ET MALWARE Sharik/Smoke CnC Beacon 9", "ET MALWARE Cobalt Strike Malleable C2 (Adobe RTMP)", "ET MALWARE Loxes/Mongall Related CnC Beacon M4 (GET)", "ET MALWARE Troj/ReRol.A Checkin 1", "ET MALWARE Observed DNS Query to RisePro Domain (neo-files .com)", "ET MALWARE Soraya C2 User-Agent (default)", "ET MALWARE Ransomware/Cerber

	Checkin M3 (5)", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (nfcomizsdseqiomzqrxwvtprxbljkpgd .name)", "ET MALWARE MintStealer CnC Activity (GET)", "ET MALWARE Win32/Onliner CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 104", "ET MOBILE_MALWARE Android.KorBanker Fake Banking App Install CnC Beacon", "ET MALWARE Cobalt Strike Malleable C2 (QiHoo Profile)", "ET MALWARE SuperKillerX CnC Activity", "ET MALWARE W32/Mevade.Variant CnC POST", "ET MALWARE Py/MechaFlounder CnC Checkin", "ET MALWARE Urlzone/Bebloh/Bublik Checkin /was/vas.php", "ET MALWARE Win32/CopperStealer CnC Activity", "ET MALWARE Tick Group Payload - Submitting Encrypted Data to CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5", "ET MALWARE Win32/Reconyc.equo Checkin", "ET MALWARE Linux/BillGates Checkin Response", "ET MALWARE PoshC2 - Observed Default URI Structure M28", "ET MALWARE Sarwent CnC Response (update_exec)", "ET MALWARE FakeAV.dfze/FakeAV!IK Checkin", "ET MALWARE FAKE/ROGUE AV/Security Application Checkin", "ET MALWARE Observed MAZE Ransomware CnC Domain (thesawmeinrew .net in TLS SNI)", "ET MALWARE Locky CnC Checkin HTTP Pattern", "ET MALWARE Xwo CnC Activity", "ET MALWARE Win32/Agent.AAIB Variant CnC", "ET MALWARE LokiBot Request for C2 Commands Detected M1", "ET MALWARE Win32/AZORult V3.2 Client Checkin M2", "ET MALWARE BatLoader CnC Domain (internalchecksssso .com) in DNS Lookup", "ET MALWARE njrat ver 0.7d Malware CnC Callback (File Manager Actions)", "ET MALWARE Win32/Neutrino Checkin", "ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (syn.broadcaster)", "ET MALWARE MSIL/Revenge-RAT Keep-Alive Activity (Outbound) M2", "ET MALWARE GoldenSpy CnC Activity", "ET MALWARE Observed DNS Query to RisePro Domain (greatsofteasy .com)", "ET MALWARE Zbot CnC POST /common/timestamps.php", "ET MALWARE Win32/AZORult V3.3 Client Checkin M11", "ET MALWARE Parallax CnC Response Activity M15", "ET MALWARE Win32.Rioselx.A Checkin", "ET MALWARE W32/Lici Initial Checkin", "ET MALWARE Perl/Shellbot.SM IRC CnC Checkin", "ET MALWARE Win64/Havex Checkin", "ET MALWARE Infostealer.Bancos ProxyChanger Checkin", "ET MALWARE MSIL/Modi RAT CnC Command Inbound (info)", "ET MALWARE MargulasRAT Keep-Alive Inbound M2", "ET MALWARE Domen SocEng CnC Observed in DNS Query", "ET MALWARE Parallax CnC Response Activity M10", "ET MALWARE [TGI] Cobalt Strike Malleable C2 Response (O365 Profile) M2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 46", "ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (afghannewsnetwork .com)", "ET MALWARE Ransomware.Hidden-Tear Variant CnC Checkin", "ET MALWARE W32/Madness Checkin", "ET MALWARE KeyBoy CnC Beacon", "ET MALWARE Mirai pTea Variant - Initial CnC Checkin Inbound", "ET MALWARE Win32/Zeprox.B Checkin", "ET MALWARE Carberp checkin task", "ET MALWARE PoshC2 - Observed Default URI Structure M6", "ET MALWARE Win32/Urausy.C Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (fvp-files .com)", "ET MALWARE Win32/Braincrypt Ransomware CnC Checkin", "ET MALWARE Parallax CnC Activity M6 (set)", "ET MALWARE Alfa/Alpha Ransomware Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M18", "ET JA3 Hash - Suspected Cobalt Strike Malleable C2 (ja3s) M1", "ET MALWARE Trojan.Agent.AIXD Checkin", "ET MALWARE Tordal/Hancitor/Chanitor Checkin", "ET MALWARE W32/Patchwork.Backdoor CnC Check-in M2", "ET MALWARE Backdoor.Win32.VB.brg C&C Checkin", "ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2 (set) M2", "ET MALWARE ABUSE.CH Locky C2 Domain (dypmoywmjrevboat in DNS Lookup)", "ET MALWARE Fake ProtonVPN/AZORult CnC Domain Query", "ET MALWARE Chafer Win32/TREKX Uploading to CnC", "ET MOBILE_MALWARE DNS Query Targeted Tibetan Android Malware C2 Domain", "ET MALWARE Iron/Maktub Locker Ransomware CnC Checkin", "ET MOBILE_MALWARE PJobRat CnC Checkin", "ET MALWARE Dyreza RAT Checkin 2", "ET MALWARE Observed DNS Query to RisePro Domain (webproduct25 .com)", "ET MALWARE ELF/AbcBot Requesting Commands from CnC", "ET MALWARE Win32/AZORult V3.2 Client Checkin M3", "ET MALWARE W32/Liftoh.Downloader Images CnC Beacon", "ET MALWARE AppleJeus - Union Crypto CnC Activity", "ET MALWARE Soraya C2 User-Agent (SBTCM)", "ET MALWARE Ousaban Banker Server

	Response M1", "ET MALWARE Cobalt Strike Malleable C2 Profile (Teams) M1", "ET MALWARE NORTHSTAR Command Response", "ET MALWARE r0 CnC Check", "ET MALWARE AlphaCrypt CnC Beacon 3", "ET MALWARE APT LuckyMouse Polpo Malware CnC", "ET MALWARE Georgian Targeted Attack - Trojan Checkin", "ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 5", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 65", "ET MALWARE Downloader Win32.Small.agoy Checkin", "ET MALWARE TrochilusRAT CnC Beacon 2", "ET USER_AGENTS WaterDropX PRISM UA Observed", "ET MALWARE CrownAdPro CnC Activity M4", "ET MALWARE APT28/SkinnyBoy Checkin", "ET MALWARE WaterDropX PRISM CnC Checkin", "ET MALWARE Win32/SVCReady Loader - SysInfo M2", "ET MALWARE FakeAvCn-A Checkin 1", "ET MALWARE W32/Dinwod.Dropper Win32/Xtrat.B CnC Beacon", "ET MALWARE Darkshell.A Checkin XOR C0 Win XP", "ET MALWARE W32/Kegotip CnC Beacon", "ET MALWARE WaterDropX PRISM CnC Response", "ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M5", "ET MALWARE PHPs Labyrinth Backdoor Stage2 CnC Activity M2", "ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (googlmail)", "ET MALWARE Parallax CnC Activity M10 (set)", "ET MALWARE FormBook CnC Checkin (POST) M2", "ET MALWARE DistTrack/Shamoon CnC Beacon M2", "ET MALWARE Win32/Remcos RAT Checkin 756", "ET MALWARE Win32/Chinad Checkin", "ET MALWARE Win32/RCAP CnC Checkin", "ET MALWARE Monsoon Tinytyphon CnC Beacon GET", "ET MALWARE Ave Maria/Warzone RAT Encrypted CnC Checkin", "ET MALWARE [PTsecurity] W32/Rodecap.StealRat C2 Payload (GIF)", "ET MALWARE VirRansom/VirLock Checkin", "ET MALWARE Win32.Banker.bqba Checkin", "ET MALWARE Papras Banking Trojan Checkin", "ET MALWARE W32/SpeedingUpMyPC.Rootkit Successful Install GET Type CnC Beacon", "ET MALWARE JasperLoader CnC Checkin", "ET MALWARE ISMAgent Receiving Commands from CnC Server", "ET MALWARE Win32/Cutwail.BE Checkin 1", "ET MALWARE Win32/Krypton Stealer CnC Checkin", "ET MALWARE Locky CnC Checkin", "ET MALWARE Lunar Builder Exfil via Discord M2", "ET MALWARE Soraya C2 User-Agent (Vulture)", "ET MALWARE [PTsecurity] Bitter RAT C2 Response", "ET MALWARE Win32/RisePro CnC Command Outbound (set_file)", "ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (securityupdated)", "ET MALWARE W32/Hesperus.Banker Tr-mail Variant Sending Data To CnC", "ET MALWARE Backdoor Win32/Zegost.Q CnC traffic (OUTBOUND)", "ET MALWARE RouteX CnC Domain (3ec9b600789b3bacf2c72ebae142a9c3 .net) in DNS Lookup", "ET MALWARE MSIL/Filecoder.EK CnC Checkin", "ET MOBILE_MALWARE Android Lightspy Implant CnC", "ET MALWARE TickGroup Datper CnC Checkin M1", "ET MALWARE VBS.ARS Checkin", "ET MALWARE Evrial Stealer CnC Activity", "ET MALWARE W32/Citadel File.php CnC POST", "ET MALWARE Win32/Unk.VBScript Requesting Instruction from CnC", "ET MALWARE Evrial Stealer Retrieving CnC Information", "ET MALWARE Win32/Colibri Loader Activity", "ET MALWARE W32/Caphaw CnC Configuration File Request", "ET MALWARE Win32.Meredrop Checkin", "ET MALWARE MSIL/Agent.TRM Data Exfil (sysinfo)", "ET MALWARE DNS Query for known ShadowPad CnC 5", "ET MALWARE Sarwent CnC Response (cmd_exec)", "ET MALWARE DNS Request for Zaletelly CnC Domain", "ET MALWARE Gasket Submitting Logs to CnC", "ET MALWARE Arbitrium-RAT CnC Activity", "ET MALWARE Observed DNS Query to RisePro Domain (torggissoft .com)", "ET MALWARE Win32.YordanyanActiveAgent CnC Reporting", "ET MALWARE ServHelper CnC Command (Net User)", "ET MALWARE Win32/ASPC Bot CnC Checkin M2", "ET MALWARE DistTrack/Shamoon CnC Beacon M1", "ET JA3 HASH - Possible AnchorMail CnC Traffic", "ET MALWARE Win32/StreamFlaw.A Checkin", "ET MALWARE MedusaHTTP CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 100", "ET MALWARE Win32/Ramsay CnC Checkin", "ET MALWARE CoreDDRAT CnC Activity", "ET MALWARE NetBackdoor Checkin", "ET MALWARE Cobalt Strike CnC Activity", "ET MALWARE Win32/Autophyte.F C2 Domain (www .apshenyihl .com in DNS Lookup)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 47", "ET MALWARE Win32/Sabsik.TE.B!ml CnC Checkin", "ET MALWARE Win32/SVCReady Loader - SysInfo M1", "ET MALWARE ELF/Emptiness v2 XOR (b2bb01039307baa2) CnC Checkin", "ET MALWARE Night Dragon CnC Traffic

	Outbound 2", "ET MALWARE Cobalt Strike Malleable C2 (Custom)", "ET MALWARE Ousaban Banker Checkin M2", "ET MALWARE BackSwap Trojan C2 Domain Observed (debasuin .nl in TLS SNI)", "ET MALWARE W32/Banload.VZS Banker POST CnC Beacon 1", "ET MALWARE Diavol HTTP Cookie Observed", "ET MALWARE MilkyBoy CnC Data Exfil", "ET MALWARE Win32/Spy.Pavica.FH Variant CnC Activity", "ET MALWARE Win32/ASPC Bot CnC Checkin M1", "ET MALWARE Nexus Stealer CnC Data Exfil", "ET MALWARE KPOT Stealer Initial CnC Activity M4", "ET MALWARE APT/TransparentTribe Style Request", "ET MALWARE Medfos/Midhos Checkin", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Directory Change Command Success", "ET MALWARE Cobalt Strike Malleable C2 Webbug Profile", "ET MALWARE Win32/AZORult V3.2 Client Checkin M12", "ET MALWARE Observed DNS Query to RisePro Domain (my-rise .pro)", "ET MALWARE TinyTurla CnC Activity", "ET MALWARE Win32/Redyms.A Checkin", "ET MALWARE DDoS.XOR Checkin 2", "ET MALWARE Win32/Emotet CnC Activity (POST) M7", "ET MALWARE SNIcat - Detected C2 Commands (SIZE)", "ET MALWARE Nbar.co.kr Related Trojan Checkin", "ET MALWARE Parallax CnC Activity (set) M16", "ET MALWARE Mevade Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 51", "ET MALWARE BYOB - Python Backdoor Stager Download", "ET MALWARE Nymaim.BA CnC M2", "ET MALWARE SoulSearcher Checkin M2", "ET MALWARE EVILNUM CnC Connectivity Check", "ET MALWARE TeleBots BCS-server CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 92", "ET MALWARE Observed DNS Query to RisePro Domain (pu-file .com)", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Download Command Success", "ET MALWARE Observed Malicious DNS Query (Reyptson Ransomware CnC)", "ET MALWARE Xbash CnC DNS Lookup (realnewstime .xyz)", "ET MALWARE Win32/CryptFile2 Ransomware Checkin M2", "ET MALWARE Razy Variant Checkin", "ET MALWARE Yayih.A Checkin 3", "ET MALWARE Agent.BAAB Checkin", "ET MALWARE [eSentire] Remcos RAT Checkin 24", "ET MALWARE BazaBackdoor Variant CnC Activity M4", "ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M3", "ET MALWARE Backdoor.Win32/Likseput.A Checkin", "ET MALWARE Win32/Small.NMZ CnC Checkin", "ET MALWARE StealRat Checkin", "ET MALWARE W32/GCman.Backdoor CnC Beacon", "ET MALWARE Cobalt Strike Beacon Activity (GET)", "ET MALWARE Instagram Like Bot (like4u) CnC Activity M1", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M7", "ET MALWARE Knock.php Shiz or Rohimafo CnC Server Contact URL", "ET MALWARE Backdoor.Meciv Checkin", "ET MALWARE Java/QRat Variant Checkin", "ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (malwarehunterteam .bit in DNS Lookup)", "ET MALWARE Dridex/Bugat/Feodo GET Checkin", "ET MALWARE Moose CnC Request M1", "ET MALWARE Kishop.A checkin", "ET MALWARE XPSecurityCenter FakeAV Checkin", "ET MALWARE FIN6 StealerOne CnC DNS Query", "ET MOBILE_MALWARE Android/Plankton.P Commands Request to CnC Server", "ET MALWARE LuckyCat/TROJ_WIMMIE Checkin", "ET MALWARE HTTPCore CnC Task Response", "ET MALWARE Win32/Orchard Botnet Activity", "ET MALWARE Win32/AZORult V3.2 Client Checkin M10", "ET MALWARE Win32/SandCat CnC Checkin", "ET MALWARE DDG Botnet Miner Download", "ET MALWARE Win32/Sinresby.B Downloader CnC Activity M2", "ET MALWARE Win32.FakeAV.Rean Checkin", "ET MALWARE Linux/Agent.HX CnC Activity M2", "ET MALWARE CASHY200 Style DNS Query - Sending Hostname", "ET MALWARE Unknown Maldoc CnC Activity (2022-07-25)", "ET MALWARE MSIL/Agent.DNL Server Response Task (whoami)", "ET MALWARE Win32/Retadup CnC Checkin M1", "ET MALWARE Dropper Checkin 2 (often scripts.dlv4.com related)", "ET MALWARE MSIL/BlackGuard Stealer Exfil Activity", "ET MALWARE Win32.FakeAV.chhq Checkin", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 2", "ET MALWARE Bandook v1.35 Initial Connection and Report", "ET MALWARE LuminosityLink - Inbound Data Channel CnC Delimiter", "ET MALWARE CopperStealer - Remote Desktop - CnC Server Response via Pastebin", "ET MALWARE Murlo Trojan Checkin", "ET MALWARE Win32/Zegost!ml CnC Checkin", "ET MALWARE njRAT Variant Outbound CnC Beacon", "ET MALWARE Win32/Unk.BrowserStealer Data Exfil M1", "ET MALWARE Backdoor.Elise CnC Beacon 2 M2", "ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M4", "ET

	MALWARE SpyAgent C&C Activity (Response)", "ET MALWARE Bifrose Client Checkin", "ET MALWARE NightfallGT Mercurial Grabber", "ET MALWARE RouteX CnC Domain (dcb5684707f6c66492aaa9f7d9bfb5a6 .biz) in DNS Lookup", "ET MALWARE Win32/Parite.B Checkin 3", "ET MALWARE RouteX CnC Domain (2fa3c2fa16c47d9b9bff8986a42b048f .com) in DNS Lookup", "ET MALWARE Gh0st Trojan CnC 3", "ET MALWARE BigLock Ransomware CnC Activity (info)", "ET MALWARE MageCart CnC Domain in SNI", "ET MALWARE W32/TrojanSpy.MSIL Set Done Day CnC Beacon", "ET MALWARE Observed DNS Query to RisePro Domain (qd-file .com)", "ET MALWARE ELF/MooBot Mirai DDoS Variant Server Response M2", "ET MALWARE W32/Virus-Encoder Ransomware Checkin", "ET MALWARE OSX/WireLurker CnC Beacon", "ET MALWARE MargulasRAT Checkin M2", "ET MALWARE Suspected CHAOS CnC Inbound (download command)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 27", "ET MALWARE Win32/SystemBC CnC Checkin (null key) M2", "ET MALWARE Win32/SystemBC CnC Checkin (null key) M1", "ET MALWARE Win32/AutoIt.NU Miner Dropper CnC Checkin", "ET MALWARE HYDSEVEN VBS CnC Host Information Checkin", "ET MALWARE Linux/Moose HTTP CnC Beacon Response", "ET MALWARE IIStealer CnC Domain in DNS Lookup (xinxx .allsoulu .com)", "ET MALWARE Win32/AZORult V3.3 Client Checkin M15", "ET MALWARE MRCR1 Ransomware Checkin M1", "ET MALWARE W32/Snojan.BNQKZQH User-Agent", "ET MALWARE DonotGroup CnC Observed in DNS Query", "ET MALWARE Jasper URI Path Observed M4", "ET MALWARE Win32/Remcos RAT Checkin 62", "ET ADWARE_PUP Haken Clicker CnC Activity", "ET MALWARE Win32/MALWARECAT Exfil via SMTP", "ET MALWARE Win32/IceXLoader Sending Command Acknowledgement (POST)", "ET MALWARE Win32/Nivdort Checkin", "ET MALWARE Rootkit TDSS/Alureon Checkin 2", "ET MALWARE L0rdix Stealer CnC Data Exfil", "ET MALWARE MSIL/SamMiner CnC Checkin M2", "ET MALWARE Win32.Banload.BTQP Checkin 2", "ET MALWARE Win32/Syndicasec Encoded Response Embedded in HTML Title Tags Inbound", "ET MALWARE W32/Trickbot C2 (networkDll module)", "ET MALWARE PXJ Ransomware CnC Activity", "ET MALWARE Possible TickGroup Snack CnC Activity", "ET MALWARE Andromeda Checkin Dec 29 2014", "ET MOBILE_MALWARE Android.Walkinwat Sending Data to CnC Server", "ET MALWARE Syrian Malware Checkin", "ET MALWARE MSIL/SkidRat CnC Checkin M3", "ET MALWARE RDP Brute Force Bot Checkin", "ET MALWARE Win32/LODEINFO CnC Checkin", "ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (CONNECT)", "ET MALWARE WooSIP Downloader CnC DeleteFileOnServer", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 13", "ET MALWARE DirectsX Checkin Response", "ET MALWARE DNS Query for known ShadowPad CnC 10", "ET MALWARE W32/Citadel.Arx Varient CnC Beacon 2", "ET MOBILE_MALWARE Android/HeHe.Spy RegisterRequest CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 32", "ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND)", "ET MALWARE Suspected Snugy DNS Backdoor CnC Activity (Hostname Send)", "ET MALWARE Win64/Spy.Agent.EU CnC Checkin", "ET MALWARE Possible Siloscape IRC CnC JOIN Command Observed", "ET MALWARE W32/Fin4.InfoStealer Uploading User Credentials CnC Beacon", "ET MALWARE Win32/SDBbot CnC Checkin", "ET MALWARE Win32/Kryptik.FVVZ Variant CnC Checkin 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 80", "ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (widget .shoreoa .com)", "ET MALWARE BBSRAT GET request CnC", "ET MALWARE Lunar Builder CnC Activity", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/win/cab", "ET MALWARE LokiBot Checkin", "ET MALWARE Soraya C2 User-Agent (rhyno321)", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.3)", "ET MALWARE Loxes/Mongall Related CnC Beacon (GET)", "ET MALWARE MirrorThief CnC in DNS Lookup", "ET MALWARE LinuxNet.perlbot Checkin Via IRC", "ET MALWARE MSIL/CoderVir Stealer Zip Upload", "ET MALWARE Win32/Bancos.AMM CnC Beacon", "ET MALWARE Banker PWS/Infostealer HTTP GET Checkin", "ET MALWARE Win32/Dorv InfoStealer CnC DNS Query", "ET MALWARE TinyLoader.B2 Checkin no architecture", "ET MALWARE DADJOKE/Rail Tycoon Initial Macro Execution", "ET EXPLOIT TP-Link Archer C2 and Archer C20i Remote Code

	Execution", "ET MALWARE Lemon_Duck Powershell CnC Checkin M2", "ET MALWARE Observed Malicious SSL Cert (Klingon RAT)", "ET MALWARE Win32/Enemyfear Stealer Exfil", "ET MALWARE W32/Farfli.BHQ!tr Dropper CnC Beacon", "ET MALWARE Win32/Remcos RAT Checkin 60", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 44", "ET MALWARE AZORult v3.2 Server Response M2", "ET MALWARE Win32/Comrerop Checkin to FTP server", "ET MALWARE W32/TrojanSpy.MSIL Get New MAC CnC Beacon", "ET MALWARE Win32/ASPC Bot CnC Checkin M3", "ET MALWARE Observed DNS Query to RisePro Domain (testitsoft .com)", "ET MALWARE W32/Bilakip.A Downloader API Ping CnC Beacon", "ET MALWARE OSX/WireLurker checkin", "ET MALWARE ELF/Mirai.shiina CnC Domain in DNS Query", "ET MALWARE StartPage jsp checkin", "ET MALWARE Jaff Ransomware Checkin", "ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 2", "ET MALWARE Win32/Teslacrypt Ransomware HTTP CnC Beacon M2", "ET MALWARE Python Monero Miner CnC DNS Query", "ET MALWARE Gamut Spambot Checkin Response", "ET MALWARE Grandoreiro CnC Activity (vbs)", "ET MALWARE Observed DNS Query to RisePro Domain (gg-download .com)", "ET MALWARE VNCStartServer USR Variant CnC Beacon", "ET MALWARE DDoS.XOR Checkin via HTTP", "ET MALWARE Infostealer.Jackpos Checkin", "ET MALWARE MSIL/Modi RAT CnC Command Inbound (aw)", "ET MALWARE slock Ransomware CnC Activity", "ET MALWARE DNS Query for known ShadowPad CnC 9", "ET MALWARE Win32/Sisproc Variant POST to CnC Server", "ET MALWARE Plurox CnC Domain in DNS Lookup", "ET WEB_SERVER Possible Darkleech C2", "ET MALWARE Cobalt Strike Beacon Observed (MASB UA)", "ET MALWARE EVILNUM CnC Response", "ET MALWARE Suspected CHAOS CnC Inbound (persistence enable)", "ET MALWARE MSIL/NxRansomware C2 Domain Detected (0cf5ff34 .ngrok .io in DNS Lookup)", "ET MALWARE Win32/Emotet HTML Template Response", "ET MALWARE Zeus Bot GET to Bing checking Internet connectivity", "ET MALWARE Suspected Monero Miner CnC Channel Secondary Domain Lookup", "ET MALWARE ChaseBot CnC Checkin", "ET MALWARE EvilNum CnC Error Report", "ET MALWARE DNSBin Demo (requestbin .net) - Data Exfil", "ET MOBILE_MALWARE Android.YzhcSms CnC Keepalive Message", "ET MALWARE Win32/Khaosz.A!MTB Checkin", "ET MALWARE TinyLoader.A Checkin x64", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 109", "ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)", "ET MALWARE Win32.Glupteba/ClIEcker CnC Checkin", "ET MALWARE Win32/44Caliber Stealer Variant Activity (POST)", "ET MALWARE Webshell Upload Command Inbound - Possibly Iran-based", "ET MALWARE Win32/WarHawk Activity (task_done)", "ET MALWARE Win32/AZORult V3.3 Client Checkin M21", "ET MALWARE Observed Malicious SSL Cert (Go/Chaos Botnet)", "ET MALWARE WSHRAT CnC Checkin", "ET MALWARE Trickbot Checkin Response", "ET MALWARE Win32/Sharik C2 Incoming Traffic", "ET MALWARE MSIL/SamMiner CnC Checkin M1", "ET MALWARE Legion Loader Activity Observed (carlos_castaneda)", "ET MALWARE NSIS/TrojanDownloader.Agent.NZK Server Response", "ET MALWARE Win32/OnLineGames GetMyIP Style Checkin", "ET MALWARE WEBC2-RAVE UA", "ET MALWARE DarkIRC Bot CnC Domain Lookup", "ET MALWARE Ousaban Banker Checkin M1", "ET MALWARE Win32/AZORult V3.3 Client Checkin M12", "ET MALWARE Trojan.JS.QLP Checkin", "ET MALWARE MSIL/GravityRAT CnC Domain (msoftupdates .eu in DNS Lookup)", "ET MALWARE W32/Symmi.46846 CnC Beacon", "ET MALWARE ConPtyShell Server Command (whoami)", "ET MALWARE Observed BatLoader Domain (tableau-cloud .com) in TLS SNI", "ET MALWARE Win32/Remcos RAT Checkin 65", "ET MALWARE Win32/AZORult V3.3 Client Checkin M24", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 3", "ET MALWARE Query to Known CnC Domain msnsolution.nicaze.net", "ET MALWARE Worm.VBS Dunihi/Houdini/H-Worm Checkin UA", "ET MALWARE LumOffice Checkin", "ET MALWARE OSX/Shlayer CnC Landing M2", "ET MALWARE Cobalt Strike Malleable C2 (Safebrowse Profile) POST", "ET MALWARE Win32/Kelihos.F Checkin", "ET MALWARE MagikPOS Downloader Checkin", "ET MALWARE W32/Witch.3FA0!tr CnC Actiivty M2", "ET MALWARE Possible Mask C2 Traffic", "ET MALWARE Win32/Vibem.C CnC Activity", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 75", "ET MALWARE W32/NSISDL.Downloader

	CnC Server Response", "ET MALWARE Win32/TrojanDownloader.Agent.FC CnC Activity", "ET MOBILE_MALWARE Android/Geost CnC Checkin", "ET MALWARE Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)", "ET MALWARE Win32/Trickbot Data Exfiltration M3", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET", "ET MALWARE Dragonfly Backdoor.Goodor Go Implant CnC Beacon 1", "ET MALWARE Suspected HARDPULSE Request", "ET MALWARE Instagram Like Bot (like4u) CnC Activity M2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 35", "ET MALWARE LuminosityLink - CnC", "ET MOBILE_MALWARE Android.Trojan.AndroRAT.CE Checkin", "ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Done", "ET MALWARE Moose CnC Response", "ET MALWARE Win32/GenCBL.XS CnC Activity", "ET MALWARE Moist Stealer CnC Exfil", "ET MALWARE Win32/Small.NO Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M8", "ET ACTIVEX Cisco Linksys WVC200 Wireless-G PTZ Internet Video Camera PlayerPT ActiveX Control PlayerPT.ocx Access 2", "ET MALWARE MSIL/Crimson Rat CnC Exfil", "ET MALWARE Buer Loader Download Request", "ET MALWARE PlugX/Korplug CnC Activity", "ET MALWARE Gazer HTTP POST Checkin", "ET MALWARE Lemon_Duck Linux Shell Script CnC Activity", "ET MALWARE Baraka Ransomware CnC activity email SMTP", "ET MALWARE Chafer CnC DNS Query", "ET MALWARE TickGroup BROLER.F CnC Check-in", "ET MALWARE PlugX UDP CnC Beacon", "ET MALWARE MSIL/Alcatrez Locker Ransomware CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 59", "ET MALWARE W32/Citadel Pro File.php CnC POST", "ET MALWARE Diavol Communicating with CnC - Ignore Request", "ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M2", "ET MALWARE EvilGrab/Vidgrab Checkin", "ET MALWARE APT 41 LOWKEY Backdoor - Ping Success Code sent to CnC", "ET MALWARE Dridex POST Checkin", "ET MALWARE Amarula IRC Botnet Connection Request", "ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (afrepublic .xyz)", "ET MALWARE Win32/RisePro CnC Command Outbound (freezeStats)", "ET MALWARE W32/Echmark/MarkiRAT CnC Activity M3", "ET MALWARE Lemon_Duck CnC Activity", "ET MALWARE PoshC2 - Observed Default URI Structure M32", "ET MALWARE Win32/Nitol.A Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 52", "ET MALWARE Win32/TrojanDownloader.Agent.FLZ CnC Activity", "ET MALWARE Win32/AZORult V3.3 Client Checkin M18", "ET MALWARE Suspected APT15/NICKEL KETRUM CnC Activity (GET)", "ET MALWARE Possible SQUIRRELWAFFLE Server Response", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M3", "ET MALWARE W32/Alina.POS-Trojan Checkin", "ET MALWARE W32/UltimateDefender.FakeAV Checkin", "ET MALWARE Backdoor.Elise CnC Beacon 3 M1", "ET MALWARE Win32/Remcos RAT Checkin 67", "ET MALWARE Yayih.A Checkin 2", "ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (PNG)", "ET MALWARE Asterope Checkin", "ET MALWARE FastPOS Initial Checkin", "ET MALWARE JunkMiner Downloader Communicating with CnC", "ET MALWARE W32/Kimsuky Sending Encrypted System Information to CnC", "ET MALWARE Win32/Virut.BN Checkin", "ET MALWARE W32/SPARS/ARS Stealer Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 99", "ET MALWARE Suspected Zebrocy Implant CnC Checkin", "ET MALWARE FakeAV.EGZ Checkin 2", "ET MALWARE Win32/ViSystem CnC Checkin", "ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M4", "ET MALWARE Yahoo550.com Related Downloader/Trojan Checkin", "ET MALWARE RCtrl Backdoor CnC Checkin M1", "ET MALWARE Win32/PSW.QQPass.OZV Variant Checkin", "ET MALWARE Daemonize.ft HTTP Checkin", "ET MALWARE DDG Botnet CnC Slave POST", "ET MALWARE NORTHSTAR Interactive Client CnC", "ET MALWARE PunkeyPOS HTTP CnC Beacon 9", "ET MALWARE BadPatch CnC Activity", "ET MALWARE CopperStealer - Remote Desktop - CnC Server Request via Pastebin", "ET MALWARE Turkojan C&C Browse Drive Command (BROWSC)", "ET MALWARE Nazar Implant - Sending Basic System Info to CnC", "ET MALWARE W32/Iyus.H Initial CnC Beacon", "ET MALWARE Poweliks Clickfraud CnC M3", "ET MALWARE Backdoor.Esion CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 15", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 66", "ET MALWARE TeleBots VBS Backdoor CnC Beacon 2", "ET

	MALWARE OSX/OceanLotus.D Sending Data to CnC", "ET MALWARE Teslarvng Ransomware CnC Activity M2", "ET MALWARE Tatanga/Win32.Kexject.A Checkin", "ET MALWARE MSIL/Matrix Ransomware CnC Activity", "ET MALWARE Win32/Agent.WVW CnC Beacon 1", "ET MALWARE Loxes/Mongall Related CnC Beacon M2 (GET)", "ET MALWARE Win32.Chroject.B Requesting ClickFraud Commands from CnC", "ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M1", "ET MALWARE Possible W32/Citadel Download From CnC Server Self Referenced /files/ attachment", "ET MALWARE Infostealer.Jackpos Checkin 2", "ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 4", "ET MALWARE Ransomware/Cerber Checkin M3 (15)", "ET MALWARE [PTsecurity] Remcos RAT Checkin 73", "ET MALWARE Unattributed CnC Domain in DNS Lookup (secure-message .online)", "ET MALWARE Win32/Unk.BrowserStealer Data Exfil M3", "ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (count .trackstatisticsss .com) in TLS SNI", "ET MALWARE Win32/Kryptik.HNBU CryptoMiner - GetTasks Request", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Ermak.a Checkin", "ET MALWARE Glupteba CnC Domain in DNS Lookup", "ET MALWARE Likely FakeAV/Fakeinit/FraudLoad Checkin", "ET MALWARE Win32/Remcos RAT Checkin 27", "ET MALWARE ABUSE.CH Locky C2 Domain (yaynawvtuqcarjwc in DNS Lookup)", "ET MALWARE PoshC2 - Observed Default URI Structure M5", "ET MALWARE Possible Generic RAT over Telegram API", "ET MALWARE Observed Awad Bot CnC Domain (hawad .000webhostapp .com in TLS SNI)", "ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (s22231232fdnsjds .top in TLS SNI)", "ET MALWARE [PTsecurity] Trojan.JS.Agent.dwz Checkin 2", "ET MALWARE Win32/SystemHijack.gen CnC Checkin", "ET MALWARE Win32/Remcos RAT Checkin 56", "ET MALWARE lu0bot Loader HTTP Request M3", "ET MALWARE Win32/Pterodo CnC VNC Connect Request", "ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M3", "ET MALWARE Win32/Downloader.Small.BIL CnC Checkin", "ET MALWARE Banker Trojan (General) HTTP Checkin (vit)", "ET MALWARE Reborn Stealer 2021 Exfil attempt via Telegram", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.0)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 31", "ET MALWARE Win32.Zegost CnC Checkin", "ET MALWARE Linux.DDoS Checkin", "ET MALWARE Magniber Ransomware Retrieving Instructions", "ET MALWARE Night Dragon CnC Beacon Outbound", "ET MALWARE Trojan.Nurjax Checkin", "ET MALWARE FF-RAT Stage 1 CnC Checkin", "ET MALWARE STRRAT CnC Checkin", "ET MALWARE Satan/5ss5c Ransomware CnC Activity", "ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Client Request (set)", "ET MALWARE Zeus.Downloader Campaign Unknown Initial CnC Beacon", "ET MALWARE SmokeLoader Checkin", "ET MALWARE SuperFish CnC Beacon 1", "ET MALWARE Win32/Bot.Sezin CnC Checkin", "ET MALWARE Buer Loader Successful Payload Download", "ET MALWARE Win32/Small.NQT!tr CnC Activity", "ET MALWARE ApolloLocker Ransomware CnC Checkin 2", "ET MALWARE Ousaban Banker KeepAlive", "ET MALWARE TA402/Molerats CnC Activity", "ET MALWARE Backdoor.Elise CnC Beacon 3 M2", "ET MALWARE APT/TransparentTribe CnC Checkin", "ET MALWARE TeamBot CnC Activity", "ET MALWARE W32/Ferret DDOS Bot CnC Beacon 2", "ET MALWARE Linux/ChinaZ DDoS Bot Checkin 2", "ET MALWARE Densmail.com Related Trojan Checkin", "ET MALWARE GanDownloader CnC Checkin", "ET MALWARE SMSHoax Riskware checkin", "ET MALWARE Win32/Tflower Ransomware CnC Checkin", "ET MALWARE RouteX CnC Domain (0a0074066c49886a39b5a3072582f5d6 .net) in DNS Lookup", "ET MALWARE Win32/DanijBot CnC Task Status", "ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup", "ET MALWARE [eSentire] Win32/GandCrab v4/5 Ransomware CnC Activity", "ET MALWARE Observed DNS Query to RisePro Domain (softs-portal .com)", "ET MALWARE Cobalt Strike Malleable C2 (Wordpress Profile)", "ET MALWARE PowerShell/Agent.A DNS File Transfer CnC Beacon", "ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M3", "ET MALWARE Felismus CnC Beacon 2", "ET MALWARE STRRAT Requesting License Check", "ET MALWARE RHttpCtrl Backdoor CnC", "ET MALWARE Backdoor.Win32.Poison.AU checkin", "ET MALWARE Win32/Unknown Stealer Command (loader) (Outbound)", "ET MALWARE Win32/AZORult V3.3 Client

	Checkin M13", "ET MALWARE PunkeyPOS HTTP CnC Beacon 3", "ET MALWARE Matryoshka CnC Beacon 1", "ET MALWARE Dooptroop Dropper Checkin", "ET MALWARE Backdoor.Win32.PEx.942728546 Checkin", "ET MALWARE OilRig OopsIE CnC Checkin M3", "ET MALWARE Megalodon/Gomorrah/CosaNostra HTTP Bot CnC Exfil", "ET MALWARE KPOT Stealer Initial CnC Activity M5", "ET MALWARE SSL/TLS Certificate Observed (Maldoc CnC)", "ET MOBILE_MALWARE Android Vultr Checkin", "ET MALWARE Win32/AZORult V3.2 Client Checkin M7", "ET MALWARE TinyLoader.B2 Checkin x64", "ET MALWARE W32/Asprox.ClickFraudBot CnC Beacon", "ET MALWARE Possible Darkhotel Higasia Downloader Connectivity Check", "ET MALWARE ELF/Emptiness v1 CnC Checkin", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/ms/check", "ET MALWARE Ponmocup C2 Sending Data to Controller 2", "ET MALWARE DNS Query for known ShadowPad CnC 2", "ET MALWARE Win32/Urausy.C Checkin 2", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (clon .collectfasttracks .com) in DNS Lookup", "ET MALWARE Zeus GameOver Checkin", "ET MOBILE_MALWARE Android Brunhilda Dropper (protectionguardapp .club in TLS SNI)", "ET MALWARE Fodcha Bot CnC Checkin", "ET MALWARE W32.FakeEzQ.kr Checkin", "ET MALWARE Sarwent CnC Command (rdp)", "ET MALWARE Win32.Fareit.A/Pony Downloader Checkin (2)", "ET MALWARE Ransomware/Cerber Checkin M3 (11)", "ET MALWARE Observed DNS Query to RisePro Domain (hero-files .com)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 94", "ET MALWARE Win32.Genome Initial Checkin", "ET MALWARE ASNAROK Domain in TLS SNI", "ET MALWARE Win32/Unk Downloader CnC Activity", "ET MALWARE Dalexis CnC Beacon", "ET MALWARE PHP Skimmer Exfil Attempt", "ET MALWARE Win32/AZORult V3.3 Client Checkin M17", "ET MALWARE Win32/Backdoor.Randrew.A CnC Checkin", "ET MALWARE Linux/Yangji.A Checkin", "ET MALWARE AveMaria Initial CnC Checkin", "ET MALWARE JsOutProx CnC Activity - Outbound", "ET MALWARE Upatre User-Agent", "ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 2", "ET MALWARE Hong Kong SWC Attack PcClient CnC Beacon", "ET MALWARE Pteranodon Variant 2 Backdoor Checkin", "ET MALWARE Win32/AZORult V3.2 Client Checkin M18", "ET MALWARE jFect HTTP CnC Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M11", "ET MALWARE Possible NanoCore C2 60B", "ET MALWARE Win32/Phorpiex Template 6 Active - Outbound Malicious Email Spam", "ET MALWARE TickGroup Datper CnC Checkin M3", "ET MALWARE W32/Karagany.Downloader CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 37", "ET MALWARE Lazarus FALLCHILL Fake SSL Checkin 1", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 16", "ET MALWARE Win32/Keatep.B Checkin", "ET MALWARE Trojan.Win32.Qadars Checkin", "ET MALWARE Win32/Zemot Checkin", "ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M3", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 5", "ET MALWARE Win32/Fluxer CnC Checkin", "ET MALWARE Backdoor.Graybird Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 48", "ET MALWARE Win32/Beapy/Lemon_Duck CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 9", "ET MALWARE Gootkit Checkin User-Agent 2", "ET MALWARE Sarwent CnC Response (powershell_exec)", "ET MALWARE Sharik/Smoke CnC Beacon 2", "ET ACTIVEX Cisco Linksys WVC200 Wireless-G PTZ Internet Video Camera PlayerPT ActiveX Control PlayerPT.ocx Access 1", "ET MALWARE QuasarRAT/zgRAT C2 Activity (set)", "ET MALWARE WEBMONITOR RAT CnC Domain in DNS Lookup (dabmaster.wm01 .to)", "ET MALWARE MargulasRAT Keep-Alive Outbound M1", "ET MALWARE OS X Backdoor Checkin", "ET MALWARE Possible iKittens OSX MacDownloader CNC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 39", "ET MALWARE Kazy Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 68", "ET MALWARE OilRig CnC DNS Lookup (defender-update .com)", "ET MALWARE Suspected CHAOS CnC Inbound (upload command)", "ET MALWARE PunkeyPOS HTTP CnC Beacon Fake UA", "ET MALWARE Possible APT 41 Fake Server Response", "ET MALWARE Turkojan C&C Keepalive (BAGLANTI)", "ET MALWARE Potao CnC POST Response", "ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (equisdeperson .space in TLS SNI)", "ET MALWARE Moose CnC Request M2", "ET

	MALWARE RouteX CnC Domain (cba4a6e5d3c956548a337c52388473f1 .com) in DNS Lookup", "ET MALWARE Remcos 3.x Unencrypted Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (elite-hacks .ru)", "ET MALWARE Xbash CnC DNS Lookup (3g2upl4pq6kufc4m .tk)", "ET MOBILE_MALWARE Observed Trojan-Spy.AndroidOS.Agent.abe Domain in TLS SNI", "ET MALWARE MRCR1 Ransomware Checkin M2", "ET MALWARE Trojan/MSIL.bfsx Checkin", "ET MALWARE MSIL/SkidRat CnC Checkin M1", "ET MALWARE KeyloggerOnline Keylogger Checkin (kill)", "ET MALWARE Generic njRAT/Bladabindi CnC Activity (ll)", "ET MALWARE [PTsecurity] DorkBot.Downloader CnC Response", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (wcmbqxzeuopnvyfmhkstaretfciywdrl .name)", "ET MALWARE Mermaid Ransomware Variant CnC Activity M2", "ET MALWARE Parallax CnC Response Activity M14", "ET MALWARE CoinVault CnC Beacon M2", "ET MALWARE Glupteba CnC Checkin", "ET MALWARE Win32/Fake Anti-Pegasus AV CnC Exfil", "ET MALWARE PowerShell/Agent.A DNS Checkin", "ET MALWARE Carberp CnC request POST /set/task.html", "ET MALWARE BandarChor Ransomware Checkin", "ET MALWARE Win32/Unk HeavensGate Loader CnC in DNS Lookup", "ET MALWARE ICEFOG-P Variant CnC Checkin M1", "ET MOBILE_MALWARE Observed Android/SpyLoan.9ef8bf95 Domain (api .dreamloan .cc in TLS SNI)", "ET MALWARE Generic Downloader checkin (3)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M13", "ET MALWARE Win32/RisePro CnC Command Outbound (get_loaders)", "ET MALWARE Win32.Fareit.A/Pony Downloader Checkin", "ET MALWARE MSIL/Eredel Stealer CnC Checkin", "ET MALWARE MSIL/Agent.TRM Checkin Response", "ET MALWARE Revcode RAT CnC", "ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M2 (Group String Len 2+)", "ET MALWARE PoisonIvy.E Keepalive to CnC", "ET MALWARE Gamut Spambot Checkin", "ET MALWARE PlugX CnC Beacon", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 10.0)", "ET MALWARE VirTool.Win32/VBInject.gen!DM Checkin", "ET MALWARE Linux/Moose NAT Traversal CnC Beacon - Sleep", "ET MALWARE EvilNum CnC Checkin Response", "ET MALWARE Fbot/Satori CnC DNS Lookup (ukrainianhorseriding .com)", "ET MALWARE Rerdom/Asprox CnC Beacon", "ET MALWARE Trojan.BlackRev Botnet Monitor Request CnC Beacon", "ET MALWARE Win32/RA-based.NCX CnC Checkin", "ET MALWARE W32/TrojanSpy.MSIL Fetch Time CnC Beacon", "ET MALWARE Win32/Fosniw MacTryCnt CnC Style Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 69", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 7", "ET MALWARE SA Banker Checkin", "ET MALWARE Win32/WarHawk Activity (task)", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (pdjwebrfgdyzljmwtxcoyomapxtzchvn .com)", "ET MALWARE Mac Flashback Checkin 1", "ET MALWARE Win32.Raccoon Stealer CnC Activity (dependency download)", "ET MALWARE Win32/Scarsi Variant CnC Activity", "ET MALWARE Win32/RisePro CnC Command Outbound (get_settings)", "ET MALWARE Win32/TinyNuke CnC Checkin", "ET MALWARE W32/Pterodo.CL CnC Checkin", "ET MALWARE r0 CnC Architecture GET 4", "ET MALWARE Tsyrval Panda CnC Beacon", "ET MALWARE Remcos 3.x Unencrypted Server Response", "ET MALWARE AZORult Variant.4 Checkin M2", "ET MALWARE Arechclient2 Backdoor CnC Checkin", "ET MALWARE Linux/DDoS.Sotdas/IptabLex Checkin", "ET MALWARE KeyLogger related to FindPOS CnC Beacon", "ET MALWARE GCleaner Downloader Activity M4", "ET MALWARE [eSentire] Win32/Spy.Banker CnC Command (DOWNLOAD)", "ET MALWARE W32/Caphaw Requesting Additional Modules From CnC", "ET MALWARE 44 Caliber Stealer Data Exfil via Discord", "ET MALWARE Win32/Bisonal CnC Checkin", "ET MALWARE SystemBC Powershell bot registration", "ET MALWARE ConPtyShell Server Close Shell", "ET MALWARE CASHY200 Style DNS Query - Initial Hello Beacon", "ET MALWARE W32.Geodo/Emotet Checkin Fake 404 Response", "ET MALWARE Possible Linux/Moose Telnet CnC Beacon", "ET MALWARE MSIL/Kryptik.XSY Data Exfil via SMTP", "ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (transadforward .icu) in DNS Lookup", "ET MALWARE Worm.VBS.ayr CnC command (is-enum-folder)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17", "ET MALWARE Winsoft.E Checkin 2", "ET MALWARE Cobalt Strike Beacon (Custom Wordpress Profile)", "ET

	MALWARE TinyLoader.A Checkin x86", "ET MALWARE Win32/Emotet CnC Activity (POST)", "ET MALWARE Unknown Possibly Ransomware (Dropped by RIG) CnC Beacon", "ET MALWARE Chthonic Checkin", "ET MOBILE_MALWARE Suspected PROJECTSPY CnC (video)", "ET MALWARE Zeus Panda CnC Domain (in DNS Lookup)", "ET MALWARE Foudre Checkin M1", "ET MALWARE Zacom/NFlog Checkin", "ET MALWARE W32/Asprox php.dll.crp POST CnC Beacon", "ET MALWARE BlackTech/PLEAD TSCookie CnC Checkin M1", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 71", "ET MALWARE Win32.Hack.PcClient.g CnC (OUTBOUND) XOR b5", "ET MALWARE FrameworkPOS Covert DNS CnC Beacon 2", "ET MALWARE Possible XServer Backdoor Certificate Observed", "ET MALWARE Linux/LuaBot CnC Beacon Response", "ET MALWARE WEBC2-DIV UA", "ET MALWARE Win32/PSW.Agent.OMP Variant CnC Activity", "ET MALWARE OilRig CnC DNS Lookup (windowspatch .com)", "ET MALWARE Book of Eli CnC Checkin", "ET MALWARE Win32.Shiz.fxm/Agent-TBT Checkin", "ET MALWARE W32/KeyLogger.ACQH!tr Checkin", "ET MALWARE MSIL/Small.FU Variant CnC Activity M2", "ET MALWARE OSX/Keydnap DNS Query to CnC", "ET MALWARE RouteX CnC Domain (18bca7c5fd709ac468ba148c590ef6bf .net) in DNS Lookup", "ET MOBILE_MALWARE Android.C2P.Qd!c Ransomware CnC Beacon", "ET MALWARE Linux.Trojan.IptabLex Variant Checkin", "ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (letsmakeparty3 .ga) in TLS SNI", "ET MALWARE Alphacrypt/TeslaCrypt Ransomware CnC Beacon Response", "ET MALWARE Observed OSX/NukeSped Variant CnC Domain (fudcitydelivers .com) in TLS SNI", "ET MALWARE PPI User-Agent (InstallCapital)", "ET MALWARE Cobalt Strike Malleable C2 (MSDN Query Profile)", "ET MALWARE CoreDn CnC Checkin M2", "ET MALWARE ShadowPad CnC Domain in DNS Lookup (ns .rtechs .org)", "ET MALWARE Observed OSX/NukeSped Variant CnC Domain (sctemarkets .com) in TLS SNI", "ET MALWARE STARSYPOUND Client Checkin", "ET MALWARE RouteX CnC Domain (73780fbd309561e201a4aee9914d882d .org) in DNS Lookup", "ET MALWARE Win32/Satana Ransomware Checkin", "ET MOBILE_MALWARE Android/Netisend.A Posting Information to CnC", "ET MALWARE Cobalt Strike Malleable C2 (Magnitude EK)", "ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Upload)", "ET MALWARE Win32.Lager Trojan Initial Checkin", "ET MALWARE Cookies/Cookiebag Checkin", "ET MALWARE Win32.Genome.boescz Checkin", "ET MALWARE X2000M.Agent Checkin Jan 24 2017", "ET MALWARE Bamital checkin", "ET MALWARE Trojan.Win32.Buzus Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M20", "ET MALWARE OLDBAIT Checkin 2 brvc", "ET MALWARE Win32/DMA Locker CnC Checkin", "ET MALWARE Secure-Soft.Stealer Checkin", "ET MALWARE Sorano Stealer CnC Checkin", "ET MALWARE MargulasRAT Keep-Alive Outbound M2", "ET MALWARE DonotGroup Stage 2 CnC Domain in DNS Lookup", "ET MALWARE Exorcist 2.0 Ransomware CnC Activity", "ET MALWARE Win32/Spy.Banker.ABCG Checkin", "ET MALWARE MSIL/Diezen CnC Checkin M1", "ET MALWARE Backdoor.Win32/Momibot Checkin", "ET MALWARE TA457 Backdoor CnC Activity", "ET MALWARE Jasper URI Path Observed M3", "ET MALWARE Suspected CHAOS CnC Inbound (screenshot command)", "ET MALWARE Soraya C2 User-Agent", "ET MALWARE Win32/Delf.TJJ Variant CnC Activity", "ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 2", "ET MALWARE W32/HelloBridge.Backdoor Login CnC Beacon", "ET MALWARE IP Grabber CnC Activity", "ET MALWARE W32/Fullstuff Initial Checkin", "ET MALWARE Win32/Spy.Odlanor CnC Checkin", "ET MALWARE Win32/AZORult V3.3 Client Checkin M9", "ET MALWARE Bookworm CnC Beacon 2", "ET MALWARE W32/118GotYourNo Reporting to CnC", "ET MALWARE Possible Kimsuky Related Exfil", "ET MALWARE APT Mustang Panda Payload - CnC Checkin", "ET MALWARE PWS Win32/Lmir.BMQ checkin", "ET MALWARE VikroStealer Retrieving Config", "ET MALWARE Sharik/Smoke CnC Beacon 8", "ET MALWARE Plead TSCookie CnC Checkin M2", "ET MALWARE TrueBot/Silence.Downloader CnC Checkin 3", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102", "ET MALWARE Plasmabot CnC Host Checkin", "ET MALWARE Win32/Cryptrun.B/MSUpdater C&C traffic 1", "ET MALWARE lu0bot Loader HTTP Response M2", "ET MALWARE Win32/Sharik Checkin", "ET MALWARE CFR DRIVEBY CVE-2012-4792 DNS Query for C2 domain", "ET MALWARE Bot

	Backdoor Checkin/registration Request", "ET MALWARE Koobface Checkin via POST", "ET MALWARE XcodeGhost CnC Checkin", "ET MALWARE Win32/Sarwent Initial Checkin CnC Response", "ET MALWARE Backdoor Lanfiltrator Checkin", "ET MALWARE Bamital Checkin Response 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 6", "ET MALWARE Win32/Unknown Stealer Command (geoblock) (Outbound)", "ET MALWARE Fodcha Bot CnC Heartbeat Response", "ET MOBILE_MALWARE Android JadeRAT CnC Beacon", "ET MALWARE Win32/Remcos RAT Checkin 84", "ET MALWARE CASHY200 Style DNS Query - Getting CnC Data", "ET MALWARE Parallax CnC Response Activity M6", "ET MALWARE W32/Downloader_x.EJK!tr CnC Activity", "ET MALWARE Win32/Recslurp.D C2 Response", "ET MALWARE BigLock Ransomware CnC Activity (id)", "ET MALWARE MSIL/Unk.HT-Based Ransomware CnC Checkin", "ET MALWARE Win32/Hyteod CnC Beacon", "ET MALWARE Jasmin Ransomware C2 Checkin", "ET MALWARE LuminosityLink - Outbound Data Channel CnC Delimiter", "ET MALWARE Xbash CnC DNS Lookup (blockbitcoin .com)", "ET MALWARE AgentTesla PWS HTTP CnC Checkin", "ET MALWARE Trojan/MSIL.DOTHETUK CnC Activity", "ET MALWARE nspps Backdoor CnC Activity", "ET MALWARE Qadars CnC DNS Lookup (liveskansys.com)", "ET MALWARE Observed DNS Query to RisePro Domain (upxlead .com)", "ET MALWARE Yahoyah CnC Beacon", "ET MALWARE Clipsa Stealer - CnC Checkin", "ET MALWARE Volatile Cedar Win32.Explosive CnC Beacon 3", "ET MALWARE Danabot Key Exchange Request", "ET MALWARE PoshC2 - Observed Default URI Structure M27", "ET MALWARE Suspected Brute Ratel CnC Activity (POST)", "ET MALWARE MilkyBoy CnC Activity", "ET MALWARE Xbash CnC DNS Lookup (leakingprivacy .tk)", "ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 4", "ET MALWARE ArtraDownloader CnC Checkin", "ET MALWARE Citadel Checkin", "ET MALWARE JS/Unk Downloader 0 Byte POST CnC Checkin", "ET MALWARE FlawedGrace CnC Activity", "ET MALWARE DecryptmyFiles Ransomware CnC (POST)", "ET MALWARE W32/Nolja Trojan Downloader Initial Checkin", "ET MALWARE Trojan-Downloader.Win32.AutoIt.mj Checkin", "ET MALWARE W32/TrojanSpy.MSIL Fetch Header CnC Beacon", "ET MALWARE CASHY200 Style DNS Query - Finished Sending Results", "ET MALWARE FakeAV Win32/Antivirus2008 CnC Beacon", "ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (CERT)", "ET MALWARE General Win32 Backdoor Checkin POST", "ET MALWARE Linux/LuaBot CnC Beacon", "ET MALWARE MICROPSIA Sending JPG Screenshot to CnC with .his Extension", "ET MALWARE Diavol CnC Checkin", "ET MALWARE Win32/7ev3n Ransomware Process Checkin", "ET MALWARE [PTsecurity] Possible Backdoor.Win32.TeamBot / RTM C2 Response", "ET MALWARE SNIcat - Detected C2 Commands (CD)", "ET MALWARE Bamital Checkin", "ET MALWARE OSX/Mokes.A CnC Heartbeat", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 97", "ET MALWARE njrat ver 0.7d Malware CnC Callback Response (Get Passwords)", "ET MALWARE Possible DACLS RAT CnC (Log Check)", "ET MALWARE Win32/Sabsik.FL.B!ml Checkin", "ET MALWARE ELF/Emptiness CnC Domain in DNS Query", "ET MALWARE Cobalt Strike Beacon CnC", "ET MALWARE MSIL/Crimson CnC Server Command (info) M1", "ET MALWARE Linux/ShellshockCampaign.DDOSBot UDP Flood CnC Server Message", "ET MALWARE GCleaner Downloader Activity M5", "ET MALWARE Win32/Remcos RAT Checkin 781", "ET MOBILE_MALWARE Android/FakeAhnAV.A CnC Beacon", "ET MALWARE Aurora Ransomware CnC Checkin", "ET MALWARE Overtoolbar.net Backdoor ICMP Checkin Request", "ET MALWARE W32/Kazy.325252 Variant CnC Beacon 1", "ET MALWARE Matiex Keylogger Exfil Via Telegram", "ET MALWARE W32/BlackEnergy Dirconf CnC Beacon", "ET MALWARE DustySky/Gaza Cybergang Group1 CnC Domain in DNS Lookup (time-loss .dns05 .com)", "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M2 (_2F)", "ET MALWARE Darkness DDoS Bot Checkin", "ET MALWARE Win32/Remcos RAT Checkin 57", "ET MALWARE Observed DNS Query to RisePro Domain (my-rise .cc)", "ET MALWARE SpyEye Checkin version 1.3.25 or later", "ET MALWARE Poweliks Clickfraud CnC M2", "ET MALWARE Win32/AZORult V3.2 Client Checkin M23", "ET MALWARE SLOTHFULMEDIA RAT CnC (POST)", "ET MALWARE PowerTrick Task Checkin M1", "ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M3", "ET

	MALWARE W32/SpeedingUpMyPC.Rootkit CnC Beacon", "ET MALWARE Win32/Emotet CnC Checkin (POST)", "ET MALWARE W32/Emotet Empty CnC Beacon", "ET MALWARE Mirai pTea Variant - Bot Upload Command Inbound", "ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (gdcb .bit in DNS Lookup)", "ET MALWARE Linux/Moose HTTP CnC Beacon", "ET MALWARE DirectsX CnC Checkin", "ET MALWARE Win32/Vools Variant CnC Checkin", "ET MALWARE Sefnit Checkin", "ET MALWARE Win32/CryptFile2 Ransomware Checkin", "ET MALWARE Observed DNS Query to Reborn/Ovidiy Stealer CnC Domain", "ET MALWARE W32/Mepaow.Backdoor Initial Checkin to Intermediary Pre-CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 18", "ET MALWARE Backdoor.Win32.RShot Checkin", "ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Checkin 3", "ET MALWARE ServHelper RAT CnC Domain Observed in SNI", "ET MALWARE Observed Buer Loader CnC Domain (kkjjhhdff .site in TLS SNI)", "ET MALWARE SNIcat - Detected C2 Commands (LS)", "ET MALWARE Win32/Ursnif Checkin", "ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup", "ET MALWARE Zalupko/Koceg/Mandaph HTTP Checkin (2)", "ET MALWARE Sage Ransomware Checkin Primer", "ET MALWARE Suspected SPECULOOS Backdoor CnC Init Packet Masquerading as SNI Request to live .com", "ET MALWARE BrushaLoader CnC DNS Lookup", "ET MALWARE SNIcat - Detected C2 Commands (EXIT)", "ET MALWARE BAZAR CnC Domain in DNS Lookup", "ET MALWARE W32/Tobfy.Ransomware CnC Request - status.php", "ET MALWARE ELF/Samba CnC Checkin", "ET MALWARE CozyCar CnC Beacon", "ET MOBILE_MALWARE PJobRat System Exfil to CnC", "ET MALWARE NightfallGT Discord Nitro Ransomware", "ET MALWARE Observed DNS Query to RisePro Domain (get-24files .com)", "ET MALWARE Swizzor Checkin (kgen_up)", "ET MALWARE Win64/Agent.NL Variant CnC Activity", "ET MALWARE BatLoader CnC Domain (installationupgrade6 .com) in DNS Lookup", "ET MALWARE Win32/Neurevt.A/Betabot checkin", "ET MALWARE TA402/Molerats Pierogi CnC Response (Download)", "ET MALWARE S400 RAT Server Response", "ET MALWARE Win32/AZORult V3.2 Client Checkin M22", "ET MALWARE Cobalt Strike Malleable C2 (Microsoft Update GET)", "ET MALWARE ELF.STD.ddos Checkin", "ET MALWARE Dropper.Win32.Agent.ahju Checkin", "ET MALWARE PLATINUM Dipsind CnC Beacon", "ET MALWARE Zeus Bot GET to Google checking Internet connectivity", "ET MALWARE Cobalt Strike Malleable C2 OCSP Profile", "ET MALWARE Dialer.MC(vf) HTTP Request - Checkin", "ET MALWARE Kimsuky Operation Blue Estimate CnC Activity", "ET MALWARE Konni RAT Exfiltrating Data", "ET MALWARE Shifr Ransomware CnC DNS Query (ojdue4474qghybjb)", "ET MALWARE vSkimmer.PoS Checkin", "ET MALWARE Alman Dropper Checkin", "ET MALWARE r0 CnC Architecture POST 1", "ET MALWARE W32/Fsysna.Downloader CnC Beacon", "ET MALWARE CoreDDRAT Screenshot Exfil", "ET MALWARE MINEBRIDGE CnC Activity", "ET MALWARE SpamTool.Win32.Agent.gy/Grum/Tedroo Or Similar HTTP Checkin", "ET MALWARE [TGI] BlackRAT Checkin Response", "ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Prepare to Receive Data", "ET MALWARE Downeks Variant CnC Beacon", "ET MALWARE DiamondFox HTTP Post CnC Checkin M3", "ET MALWARE Win32/Comisproc Checkin", "ET MALWARE Win32/Backdoor.Dripion HTTP CnC Checkin", "ET MALWARE Win32/Varenyky Spambot CnC in DNS Query", "ET MALWARE Win32/AZORult V3.3 Client Checkin M3", "ET MALWARE Kazy/Kryptor/Cycbot Trojan Checkin", "ET MALWARE Trojan-Dropper.Delf Checkin", "ET MALWARE Cridex Post to CnC", "ET MALWARE ELF/TooEasy Miner CnC Checkin", "ET MALWARE Sage Ransomware Checkin", "ET MALWARE SNIcat - Detected C2 Commands (finito)", "ET MALWARE Win32/Phorpiex CnC Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M25", "ET MALWARE Win32/Striked Ransomware CnC Checkin", "ET MALWARE MageCart JS Retrieval", "ET MALWARE W32/Trustezeb.C CnC Beacon", "ET MALWARE Observed DNS Query to RisePro Domain (uc-files .com)", "ET MALWARE W32/GMUnpacker.Downloader Download Instructions Response From CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 107", "ET MALWARE Win32/Valak - Stage 2 - Response - Plugin", "ET MALWARE Remote Desktop Spy Install Checkin", "ET MALWARE CoreDn CnC Checkin M1", "ET MALWARE BatLoader CnC Domain (logmeincloudss .com) in DNS Lookup", "ET MALWARE HCRootkit CnC Domain

	in DNS Lookup (hkxpqdtgsucylodaejmzmtnkpfvojabe .com)", "ET MALWARE ELF/Mirai.shiina v3 CnC Checkin", "ET MALWARE CASHY200 Style DNS Query - Sending Number of Queries", "ET MALWARE Locky CnC checkin Nov 21", "ET MALWARE Win32/FFDroider CnC Activity M2", "ET MALWARE Punto Loader Checkin", "ET MALWARE Win32/Emotet CnC Activity (POST) M6", "ET MALWARE Bladabindi/njrat CnC Command (Remote Shell)", "ET MALWARE Win32/Radonskra.B C2 Check-in", "ET MALWARE RampantKitten APT TelB Python Variant - CnC Checkin M2", "ET MALWARE PoshC2 - Observed Default URI Structure M24", "ET MALWARE W32/Koobface Variant Checkin Attempt", "ET MALWARE BackSwap Trojan C2 Domain Observed (debasuin .nl in DNS Lookup)", "ET MALWARE Linux/Agent.HX CnC Activity (set)", "ET MALWARE Trojan.Win32.Cosmu.xet CnC Beacon", "ET MALWARE Trojan.Win32.VB.cefz Checkin", "ET MALWARE Parallax CnC Response Activity M16", "ET MALWARE Win32/Matsnu.L Checkin", "ET MALWARE Win32/Enchanim C2 Injection Download", "ET MALWARE Win32/Agent.UOI CnC Checkin", "ET MALWARE Linux/MayhemBruter Checkin", "ET MALWARE Hiloti/Mufanom Downloader Checkin", "ET MALWARE OSX/Shlayer CnC Activity M1", "ET MALWARE BandarChor/CryptON Ransomware Checkin", "ET MALWARE [PTsecurity] Win32/SpyAgent.Raptor (realtime-spy) CnC activity 2", "ET MALWARE Cloud Atlas CnC Beacon", "ET MALWARE NOBELIUM (TA421) EnvyScout Fingerprint Checkin", "ET MALWARE r0 CnC Architecture GET 3", "ET MOBILE_MALWARE Android/Drinik Checkin Activity (POST)", "ET MALWARE Win32/Xtrat C2 Response", "ET MALWARE W32/Jiwerks.A Checkin", "ET MALWARE Soraya C2 User-Agent (xehanort321)", "ET MALWARE GoBrut/StealthWorker Service Bruter CnC Checkin", "ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (republicofaf .xyz)", "ET MALWARE VPNFilter htpx Module C2 Request", "ET MALWARE Parallax CnC Activity (set) M14", "ET MALWARE CyberGate RAT Checkin", "ET MALWARE Win32/Farfli.CUY KeepAlive M1", "ET MALWARE ZeuS Post to C&C footer.php", "ET MALWARE PoshC2 - Observed Default URI Structure M17", "ET MALWARE Trojan.Win32.Genome.aetqe Checkin", "ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (tommyforgreendream .icu) in DNS Lookup", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (lobbydesires .com) in DNS Lookup", "ET MALWARE Backdoor.Win32/PcClient.AA Checkin", "ET MALWARE KeyloggerOnline Keylogger Checkin (go https)", "ET MALWARE Win32/Backdoor.Agent.qweydh CnC Checkin M2", "ET MALWARE [TGI] BlackRAT Checkin", "ET MALWARE Lyceum Backdoor CnC Activity M1", "ET MALWARE Win32/Emotet CnC Checkin Response", "ET MALWARE Kronos Checkin", "ET MALWARE SuperSocialat Plugin Backdoor Code Execution Attempt", "ET MALWARE MAGICHOUND.RETRIEVER CnC Beacon", "ET MALWARE Win32/TrojanDownloader.Agent.APBB Checkin", "ET MALWARE Gamaredon CnC Domain in DNS Lookup", "ET MALWARE Observed Cobalt Strike CnC Domain (yawero .com in TLS SNI)", "ET MALWARE Ponmocup C2 Sending Data to Controller 1", "ET MALWARE NgrBot IRC CnC Channel Join", "ET MALWARE Win32/AZORult V3.2 Client Checkin M20", "ET MALWARE Cryptolocker Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 93", "ET MALWARE Troj/ReRol.A Checkin 2", "ET MALWARE PS/PowerRatankba CnC DNS Lookup", "ET MALWARE Win32/Remcos RAT Checkin 30", "ET MALWARE Win32/Neutrino Checkin 3", "ET MALWARE Pay2Key Ransomware - Sending RSA Key", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 53", "ET MALWARE MSIL/GravityRAT CnC Domain (mylogisoft .com in DNS Lookup)", "ET MOBILE_MALWARE Android Brunhilda Dropper (readyqrscanner .club in TLS SNI)", "ET MALWARE W32/Pterodo CnC Checkin", "ET MALWARE SQUIRRELWAFFLE Server Response", "ET MALWARE CryptoLuck / YafunnLocker Ransomware CnC Checkin", "ET MALWARE AppleJeus - JMT Trading CnC Activity (Windows Variant)", "ET MALWARE Win32/Dostre CnC Activity", "ET MALWARE PoshC2 - Observed Default URI Structure M31", "ET MALWARE Turkojan C&C Logs Parse Command (LOGS1)", "ET MALWARE W32/Dadobra.Downloader/DNSChanger Dnsmake CnC Beacon", "ET MALWARE Diavol Communicating with CnC - Wipe Request", "ET MALWARE Downloader.Banload2.KZU Checkin 1", "ET MALWARE Win32/Spy.KeyLogger.ODN Checkin", "ET JA3 Hash - Suspected Meterpreter Reverse

	Shell M1 (set)", "ET MALWARE DNS Query For TURNEDUP.Backdoor / NanoCore CnC (microsoftupdated)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 50", "ET MALWARE OILRIG CnC POST", "ET MALWARE TripleNine RAT Checkin", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.RedAlert CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 4", "ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M2", "ET MALWARE OSX/Shlayer CnC Activity M3", "ET MALWARE Sinowal/sinonet/mebroot/Torpig infected host checkin", "ET MALWARE CenterPOS CnC 2", "ET MALWARE 9002 RAT C&C DNS request", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 43", "ET MALWARE Nazar Implant - Sending Ping Response to CnC", "ET MALWARE Ave Maria RAT CnC Domain in DNS Lookup (uknwn.linkpc .net)", "ET MALWARE Win32/Swrort.A Checkin 3", "ET MALWARE Win32/CopperStealer Installer Started", "ET MALWARE Lyceum Backdoor CnC Activity M3", "ET MALWARE Win32/Remcos RAT Checkin 28", "ET MALWARE Lazarus Downloader (JEUSD) CnC Beacon", "ET MALWARE Backdoor.Win32/Likseput.A Checkin Windows Vista/7/8", "ET MALWARE Stabuniq Checkin", "ET MALWARE Win32/Geodo Checkin", "ET MALWARE ArrobarLoader CnC Checkin M1", "ET MALWARE MSIL/BlackGuard Stealer Variant Exfil via Telegram", "ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M3", "ET MALWARE Win32/PirateMatryoshka CnC DNS Query", "ET MALWARE SNIcat - Detected C2 Commands (EX)", "ET MALWARE PoshC2 - Observed Default URI Structure M21", "ET MALWARE Likely Linux/IptabLesX C2 Domain Lookup (GroUndHog.MapSnode.CoM)", "ET MOBILE_MALWARE Android.AdSms Retrieving XML File from CnC Server", "ET MALWARE ViperSoftX CnC Activity M1", "ET MALWARE AppleJeus - Kupay Wallet CnC Activity", "ET MOBILE_MALWARE Android Gymdrop Dropper (onlinefitnessanalysis .com in TLS SNI)", "ET MALWARE JS Sniffer Framework Sending to CnC", "ET MALWARE Higaisa CnC Activity", "ET MALWARE Linux/HiddenWasp CnC Request (set)", "ET MALWARE W32/Syndicasec.Backdoor CnC Beacon", "ET MALWARE W32/Lalus Trojan Downloader Checkin", "ET MALWARE OSX/SHLAYER CnC Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 105", "ET MALWARE Phorpiex CnC Domain in DNS Lookup", "ET MALWARE W32/Downloader.FakeFlashPlayer Status.Php CnC Beacon", "ET MALWARE RegSubsDat Checkin", "ET MALWARE Trojan.Dropper.Win32.Dapato.braa.AMN CnC traffic", "ET MALWARE Diavol Communicating with CnC - Key Request", "ET MALWARE Putter Panda HTTPClient CnC HTTP Request", "ET MALWARE Win32/Spy.Banker.ACUT CnC Checkin", "ET MALWARE Xbash CnC DNS Lookup (vfk2k5s5tfjr27tz .tk)", "ET MALWARE [eSentire] Remcos RAT Checkin 25", "ET MALWARE Win32.Drun Checkin", "ET MALWARE W32/Patchwork.Backdoor Communicating with CnC", "ET MALWARE Panda Banker CnC", "ET MALWARE SPEAR CnC Beacon 2", "ET MALWARE PoshC2 - Observed Default URI Structure M1", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 74", "ET MALWARE RShell Backdoor Initial CnC Checkin", "ET MALWARE AlienSpy RAT Checkin Set", "ET MALWARE Linux/HiddenWasp CnC Response", "ET MALWARE Ransom.Win32.Birele.gsg Checkin", "ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M4", "ET MALWARE Win32/Unk.BrowserStealer CnC Checkin", "ET MALWARE ServHelper CnC Command (Reg Add)", "ET MALWARE Win32/Tofsee Pharma Spam Template Active - Outbound Email Spam", "ET MALWARE DCRat CnC Activity", "ET MALWARE W32/Zzinfor.A Retrieving Instructions From CnC Server", "ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 1", "ET MALWARE MSIL/Diezen CnC Checkin M2", "ET MALWARE SolarSys CnC Activity M1", "ET MALWARE Win32/Kryptik.HCZR Variant Initial Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (vip-space .com)", "ET MALWARE CobianRAT Receiving Commands From CnC", "ET MALWARE Win32/ArtraDownloader Checkin", "ET MALWARE Ironhalo CnC Beacon", "ET MALWARE DonotGroup CnC Domain in DNS Lookup", "ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M1", "ET MALWARE OSX/Shlayer CnC Activity M4", "ET MALWARE Win32.Agent.cyt (Or variant) HTTP POST Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic

	(OUTBOUND) 84", "ET MALWARE OSX/Flashback.K first execution checkin", "ET MALWARE Higaisa CnC (ipconfig)", "ET MALWARE Possible T-RAT Encrypted Zip Request M1", "ET MALWARE Linux/ChinaZ DDoS Bot Checkin", "ET MALWARE TA457 Backdoor CnC Response", "ET MALWARE Lunar Builder Exfil via Discord M1", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M5", "ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 1", "ET MALWARE Win32/Kryptik.GSKY CnC Checkin", "ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup", "ET MALWARE W32.DarkVNC Variant Checkin", "ET MALWARE Octopus Malware CnC Activity", "ET MALWARE ICEFOG JAVAFOG JAR checkin", "ET MALWARE Netwire RAT Client Check-in (socket created)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 33", "ET MALWARE Possible T-RAT Encrypted Zip Request M2", "ET MALWARE ShivaGood Ransomware CnC Checkin", "ET MALWARE LankerBoy HTTP CnC Beacon", "ET MALWARE Tinba Checkin", "ET MALWARE Cobalt Strike Malleable C2 Request (Stackoverflow Profile)", "ET MALWARE Linux/Lady CnC Beacon 1", "ET MALWARE Zacom/NFlog HTTP POST Fake UA CnC Beacon", "ET ADWARE_PUP ZoomInfo Contact Contributor Install", "ET MALWARE Backdoor.Elise CnC Beacon 1 M2", "ET MALWARE [PTsecurity] Tinba Checkin 4", "ET MALWARE FAKE AV HTTP CnC Post", "ET MALWARE ELF/AbcBot CnC Checkin", "ET MALWARE HTTPCore CnC Tasking File", "ET MALWARE Ransomware/Cerber Checkin M3 (7)", "ET MALWARE Win32/Rarog Stealer CnC Keep-Alive", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 76", "ET MALWARE Cobalt Strike C2 Profile (news_indexedimages)", "ET MALWARE Win32/Delf.OKR Variant CnC M1", "ET MALWARE HighTide trojan Checkin", "ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Sending Data", "ET MALWARE Dmechant Exfil Passwords via SMTP", "ET MALWARE MS_D0wnl0ad3r Checkin", "ET MALWARE Win32.Vilsel Checkin", "ET MALWARE Backdoor.Win32.Sykipot Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M10", "ET MALWARE AstroBot CnC Activity", "ET MALWARE Observed Glupteba CnC Domain (venoxcontrol .com in TLS SNI)", "ET MALWARE Go/Hack Browser Data Exfil Attempt", "ET MALWARE W32/Banload.VZS Banker POST CnC Beacon 2", "ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Command Tunneling M1", "ET MALWARE MSIL/Juliens Botnet CnC Activity M1", "ET MALWARE CoinVault CnC Beacon M1", "ET MALWARE Lyceum Backdoor CnC Activity M2", "ET MALWARE Win32/RisePro CnC Command Outbound (get_grabbers)", "ET MALWARE [PTsecurity] Trojan.JS.Agent.dwz Checkin 1", "ET MALWARE Win32/Gasti.tm Checkin Activity", "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)", "ET MALWARE Likely Geodo/Emotet CnC Beacon", "ET MALWARE Dirt Jumper/Russkill3 Checkin", "ET MALWARE DMSpammer HTTP Post Checkin", "ET MALWARE FIN8 ShellTea CnC in DNS Query", "ET MALWARE Win32/AZORult V3.3 Client Checkin M6", "ET MALWARE Win32/Wacapew.C!ml CnC Checkin", "ET MALWARE W32/Asprox CnC Beacon", "ET MALWARE Win32/WarHawk Activity (cmd)", "ET MALWARE Win32/Usteal.B Checkin", "ET MALWARE Win32/Blacknix CnC Heartbeat", "ET MALWARE [PTsecurity] Remcos RAT Checkin 72", "ET MALWARE Win32/IcedID Requesting Encoded Binary M5", "ET MALWARE Win32/WarHawk Activity (filemgr)", "ET MALWARE Parallax CnC Response Activity M7", "ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (ssl .arkouthrie .com)", "ET MALWARE Win32/Eris Ransomware CnC Checkin", "ET MALWARE Win32.Nitol.K Variant CnC", "ET MALWARE Lemon_Duck Powershell - RDP Credential Exfil", "ET MALWARE LYCEUM MSIL/DanBot CnC Checkin", "ET MALWARE Tendrit CnC Beacon 1", "ET MALWARE NORTHSTAR Command Sent to Client", "ET MALWARE Win32/CryptFile2 / Revenge Ransomware Checkin M3", "ET MALWARE PHPs Labyrinth Backdoor Stage1 CnC Activity", "ET MALWARE Win32/Emotet.C Checkin", "ET MALWARE Cobalt Strike Malleable C2 Beacon (Custom)", "ET MALWARE BYOB - Python Backdoor Loader Download", "ET MALWARE UNC2628 BEACON Activity (GET)", "ET MALWARE MSIL.L4L Stealer IP Check", "ET MALWARE SNIcat - Detected C2 Commands (LD)", "ET MALWARE Win32/Agent.XST Checkin", "ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark Uploading to CnC", "ET MALWARE DNS Query for DNSpionage CnC Domain", "ET MALWARE Win32.Crypt.nc Checkin", "ET MALWARE Unknown Mailer CnC Beacon 2", "ET

	MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M4", "ET MALWARE Observed FIN12 Related Cobalt Strike Domain (netrie .com in TLS SNI)", "ET MALWARE PurpleFox Backdoor/Rootkit Checkin", "ET MALWARE ABUSE.CH Locky C2 Domain (lvanwwbyabcfevyi in DNS Lookup)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 19", "ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M2", "ET MALWARE Win32/ErbiumStealer Panel CnC Checkin", "ET MALWARE Observed DNS Query to Gryphon CnC Domain / GlobeImposter Payment Domain", "ET MALWARE MSIL/Almashreq CnC Checkin", "ET MOBILE_MALWARE Android/Smsilence.A Sending SMS Messages CnC Beacon", "ET MALWARE Bredolab CnC URL Detected", "ET MALWARE ShadowPad CnC Domain in DNS Lookup (soft .mssysinfo .xyz)", "ET MALWARE Ragnarok Ransomware CnC Activity M2", "ET MALWARE Sharik/Smoke CnC Beacon 11", "ET MALWARE DCRat CnC Activity M11", "ET MALWARE Possible Red October proxy CnC 1", "ET MALWARE Win32/Tofsee Unique Email Body Byte Sequence Observed", "ET MALWARE ISMAgent CnC Checkin 1", "ET MALWARE Arbitrium-RAT Observed User-Agent (JustKidding)", "ET MALWARE HTA.BabyShark Checkin", "ET MALWARE CrownAdPro CnC Activity M2", "ET MALWARE Win32/Unk.Joia CnC Activity", "ET MALWARE Win32/RiskWare.YouXun.AD CnC Activity", "ET MALWARE DDoS.XOR Checkin 3", "ET MALWARE Win32/Emotet CnC Activity (POST) M2", "ET MOBILE_MALWARE Android/HeHe.Spy GetTaskRequest CnC Beacon", "ET MALWARE Havex RAT CnC Server Response HTML Tag", "ET MALWARE RouteX CnC Domain (aaafc94b3a37b75ae9cb60afc42e86fe .org) in DNS Lookup", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/ms/flush", "ET MALWARE Backoff POS Checkin", "ET MALWARE Linux.Mumblehard Initial Checkin", "ET MALWARE Win32/Enchanim C2 Client Check-in", "ET MALWARE DustySky/Gaza Cybergang Group1 CnC Domain in DNS Lookup (dji-msi .2waky .com)", "ET MALWARE Win32/Delf.OKR Variant CnC M2", "ET MALWARE DNS Query for known ShadowPad CnC 7", "ET MALWARE Shafttt MySQL Bruteforce Bot CnC Beacon", "ET MALWARE Meredrop/Nusump Checkin", "ET MALWARE Suspected Monero Miner CnC Channel TXT Lookup", "ET MALWARE Win32/AZORult V3.2 Client Checkin M9", "ET MALWARE Possible Kelihos .eu CnC Domain Generation Algorithm (DGA) Lookup NXDOMAIN Response", "ET MALWARE Comfoo Checkin", "ET MALWARE Octopus Malware CnC Server Request", "ET MALWARE DarkWay Client Checkin", "ET MALWARE Win32/RisePro CnC Command Outbound (get_marks)", "ET MALWARE TDSS/TDL/Alureon MBR rootkit Checkin", "ET MALWARE HiveRAT CnC Activity M2", "ET MALWARE Nebuler/Dialer.qn HTTP Request - Checkin", "ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M2", "ET MALWARE Lyceum Golang HTTP Backdoor Connectivity Check", "ET MALWARE Linux/Agent.HX CnC Activity M1", "ET MALWARE Win32/Chekafe.A or Related Infection Checkin", "ET MALWARE PunkeyPOS HTTP CnC Beacon 2", "ET MALWARE Kriptovor Checkin", "ET MALWARE PowerSploit/PowerView SMTP Data Exfil", "ET MALWARE Webshell Landing Outbound - Possibly Iran-based", "ET MALWARE Lunar Builder Exfil Attempt", "ET MALWARE Win32/BlackNET CnC Requesting Command", "ET MALWARE Win32/Sinresby.B Downloader CnC Activity M1", "ET MALWARE Trojan.Dirtjump Checkin", "ET MALWARE Hangover Campaign Keylogger 2 checkin", "ET MALWARE Cobalt Strike Malleable C2 (TrevorForget Profile)", "ET MOBILE_MALWARE DNS Query for gongfu-android.com DroidKungFu CnC Server", "ET MALWARE Win32.Pamesg/ArchSMS.HL CnC Checkin", "ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M1", "ET MALWARE Matanbuchus Loader CnC M2", "ET MALWARE CobianRAT Receiving Config Commands from CnC", "ET MALWARE Win32/BlackCarat XORed (0x77) CnC Checkin", "ET MALWARE NORTHSTAR Client CnC Checkin", "ET MALWARE MSIL/Crimson Client Command Response (info)", "ET MALWARE Observed MageCart CnC Domain (mcdnn .net in TLS SNI)", "ET MALWARE Win32/Boaxxe.BR CnC Beacon", "ET MALWARE FatalRAT CnC Activity", "ET MALWARE Win32.Cerberus RAT Checkin Outbound", "ET MALWARE Silent Miner Changelog Checkin", "ET MALWARE Qarallax RAT Keepalive C2", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Remote Shell)", "ET MALWARE Fbot Blockchain Based CnC DNS Lookup (musl .lib)", "ET MALWARE

	Suspected Snugy DNS Backdoor Initial Beacon", "ET MALWARE Rhadamanthys Stealer - Payload Download Request", "ET MALWARE Win32/Ramnit Checkin", "ET MALWARE APT28/SkinnyBoy Payload Request", "ET MALWARE Onkods.A Downloader Checkin", "ET MALWARE IndigoZebra APT BoxCaon DropBox Activity (POST)", "ET MALWARE Backdoor.Elise CnC Beacon 1 M1", "ET MALWARE Matsnu Checkin", "ET MALWARE Win32/Blacknix CnC Checkin", "ET MALWARE TDSServ or Tidserv variant Checkin", "ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Hqwar.hf Checkin", "ET MALWARE ArcDoor Intial Checkin", "ET MALWARE Win32/Recslurp.D C2 Request (no alert)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M16", "ET MALWARE W32/Emotet CnC Beacon 1", "ET MALWARE W32/Asprox Passgrub POST CnC Beacon", "ET MALWARE Win32/MOOZ.THCCABO CoinMiner CnC Checkin", "ET MALWARE Georbot checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 55", "ET MALWARE Infostealer.Bancos Checkin via SMTP", "ET MALWARE LockPOS CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 87", "ET MALWARE Win32/Emold.C Checkin", "ET MALWARE MSIL/n2019cov (COVID-19) Ransomware CnC Checkin", "ET MALWARE Stealbit Variant Data Exfil M1", "ET MOBILE_MALWARE ActionSpy CnC (POST)", "ET HUNTING Suspicious GET Request (Likely Pentester CnC)", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.EQO Variant CnC Activity", "ET MALWARE Bzub2 Related RPC/Http Checkin", "ET MALWARE Win32/Pift Checkin 1", "ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M4", "ET MALWARE GlitchPOS CnC Checkin", "ET MALWARE Win32.YordanyanActiveAgent Generic CnC Pattern", "ET MALWARE Observed DNS Query to RisePro Domain (myrise .pro)", "ET MALWARE Oficla Checkin (1)", "ET MALWARE AppleJeus - JMT Trading CnC Activity (OSX Variant)", "ET MALWARE Cobalt Strike Malleable C2 Amazon Profile", "ET MALWARE Potao CnC", "ET MALWARE Bitter RAT HTTP CnC Beacon M2", "ET MALWARE Zbot/Zeus or Related Infection Checkin", "ET MALWARE Mozi Botnet DHT Config Sent", "ET MALWARE W32/Citadel.Arx Variant CnC Beacon 1", "ET MALWARE PoshC2 - Observed Default URI Structure M29", "ET MALWARE Simda.C Checkin", "ET MALWARE W32.Blackshades/Shadesrat Backdoor CnC Beacon", "ET MALWARE Win32/SystemBC CnC Checkin", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b CnC Beacon", "ET MALWARE Backdoor.Win32.Svlk Client Checkin", "ET MALWARE M3RAT CnC Checkin Outbound", "ET MALWARE PlugX Checkin", "ET MALWARE Observed DNS Query to Known Fenrir Ransomware CnC Domain", "ET MALWARE Suspected CHAOS CnC Inbound (openurl)", "ET MALWARE Win32.Chroject.B Receiving ClickFraud Commands from CnC 2", "ET MALWARE Kazy/Kryptor/Cycbot Trojan Checkin 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 106", "ET MALWARE Win32/InnaputRAT CnC DNS Lookup (ajdhsfhiudsfhsi .top)", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.0)", "ET MALWARE Variant.Zusy.45802 Checkin", "ET MALWARE Mutter Backdoor Checkin", "ET MALWARE Gasket Requesting Commands from CnC", "ET MALWARE SpyAgent C&C Activity (Request)", "ET MALWARE PoshC2 - Observed Default URI Structure M16", "ET MALWARE ELF/lizkebab CnC Activity (Flooding 1)", "ET MALWARE Patchwork Backdoor - Requesting Task", "ET MALWARE ELF/Roboto - Possible Encrypted Roboto P2P Payload Requested M2", "ET MALWARE W32/Armageddon CnC Checkin", "ET MALWARE Win32/Fujacks Variant CnC Activity", "ET MALWARE PoshC2 - Observed Default URI Structure M15", "ET MALWARE TA402/Molerats Pierogi CnC Response (Screenshot)", "ET MALWARE VNCStartServer BOT Variant CnC Beacon", "ET MALWARE Win32/Syndicasec Encoded Response Embedded in XML HTML Title Tags Inbound", "ET MALWARE Troxen Downloader Checkin", "ET MALWARE Win32/Rodecap/Travle/PYLOT CnC Checkin M2", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Microphone)", "ET MALWARE Linux/ShellshockCampaign.DDOSBot Terminate Process CnC Server Message", "ET MALWARE UsefulTyphon CnC Activity M2", "ET MALWARE Win32/Trickbot Data Exfiltration M4", "ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M2", "ET MALWARE Parallax CnC Response Activity M9", "ET MALWARE Unattributed CnC Domain in DNS Lookup (internal-message .app)", "ET MALWARE Suspected REDCURL CnC Activity M1", "ET MALWARE Observed

	linux.backdoor.wordpressexploit.2 Domain (lobbydesires .com) in TLS SNI", "ET MALWARE Win32/Dofoil.L Checkin", "ET MALWARE W32/Citadel Conf.bin Download From CnC Server", "ET MALWARE PowerShell Downloader CnC Activity", "ET MALWARE TeamTNT Gattling Gun AWS Creds Exfil", "ET MALWARE W32/DelfInject.A CnC Checkin 2", "ET MALWARE Win32/Cutwail.BE Checkin 2", "ET MALWARE Observed DNS Query to RisePro Domain (files-rate .com)", "ET MALWARE ProxyBox - HTTP CnC - proxy_info.php", "ET MALWARE TA402/Molerats Pierogi CnC Response (Command)", "ET MALWARE Win32/PSW.LdPinch CnC Checkin", "ET MALWARE Downloader.Win32.Geral Checkin", "ET MALWARE Possible Linux/Cdorked.A CnC", "ET MALWARE Delf Alms backdoor checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 41", "ET MALWARE W32/Jabberbot.A Trednet XMPP CnC Beacon", "ET MALWARE KINS/ZeusVM Variant CnC Beacon", "ET MALWARE RedControle Communicating with CnC", "ET MALWARE AlphaCrypt CnC Beacon 6", "ET MOBILE_MALWARE PHANTOMLANCE CnC Domain in DNS Lookup", "ET MALWARE Nemours/Proyecto RAT CnC Checkin", "ET MALWARE Win32.Troj.Cidox Checkin", "ET MALWARE [PTsecurity] Win32/SpyAgent.Raptor (realtime-spy) CnC activity 1", "ET MALWARE Hangover related campaign Checkin", "ET MALWARE Infostealer.Mysayad Checkin 1", "ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Lateral Movement Activity", "ET MALWARE Delf Checkin via HTTP (5)", "ET MALWARE Downloader.VB.TX/Backdoor.Win32.DSSdoor!IK Checkin", "ET MALWARE DoS.Linux/Elknot.G Checkin", "ET MALWARE AutoHotkey Downloader Checkin via IPLogger", "ET MALWARE ELF/MooBot Mirai DDoS Variant Server Response", "ET MALWARE Panchan Mining Rig CnC Activity (Inbound)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 2", "ET MALWARE Win32/Protux.B POST checkin", "ET MALWARE Blackenergy Bot Checkin to C&C (2)", "ET MALWARE Vidar/Arkei/Megumin/Oski Stealer Data Exfil", "ET MALWARE Possible Win32.Bicololo Checkin", "ET MALWARE Platinum APT - Titanium Payload CnC Checkin (x86)", "ET MALWARE IXWARE Stealer CnC Activity", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (ruciplbrxwjscyhtapvlfskoqqgnxevw .name)", "ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M2", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Capture)", "ET MALWARE Win32/Sabsik.FL.B!ml CnC Activity", "ET MALWARE Possible APT34 TONEDEAF 2.0 User-Agent Observed", "ET MALWARE W32/SecVerif.Downloader Initial Checkin", "ET MALWARE Win32/Retadup Success Response from CnC", "ET MALWARE Win32/Laturo Stealer CnC Checkin", "ET MALWARE PoshC2 - Observed Default URI Structure M2", "ET MALWARE Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5", "ET MALWARE Pteranodon Variant 3 Backdoor Checkin", "ET MALWARE FraudLoad.aww HTTP CnC Post", "ET MALWARE MSIL/Spy.Banker.DH Checkin", "ET MALWARE Trojan-Spy.Win32.Zbot.qgxi Checkin", "ET MALWARE Win32/Trickbot Data Exfiltration", "ET MALWARE Win32/WarHawk Checkin Activity", "ET MALWARE [PTsecurity] Remcos RAT Checkin 71", "ET MALWARE Win32.Runner/Bublik Checkin", "ET MALWARE Observed BatLoader Domain (logmeincloudss .com) in TLS SNI", "ET MALWARE W32/Taidoor.Backdoor CnC Checkin With Default Substitute MAC Address Field", "ET MALWARE Win32/Remcos RAT Checkin 109", "ET MALWARE LDPinch Checkin (3)", "ET MALWARE Knockbot Proxy Checkin", "ET MALWARE AutoHotKey offthewall Downloader Requesting Payload", "ET MALWARE DonBot Checkin", "ET MALWARE Uroburos/Turla CnC (OUTBOUND) 2", "ET MALWARE Lethic Spambot CnC Initial Connect", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.1)", "ET MALWARE CASHY200 Style DNS Query - Sending Command Results", "ET MALWARE KeyBase Keylogger Checkin", "ET MALWARE Baldr Stealer Checkin M2", "ET MALWARE Enfal CnC GET", "ET MALWARE Observed MongoLock Variant CnC Domain (s .rapid7 .xyz in TLS SNI)", "ET MALWARE ELF/STDbot CnC Activity (STD attack)", "ET MALWARE Win32/VictoryGate/Orchard Botnet CnC Checkin", "ET MALWARE Win32/Orion Logger SMTP Base64 Exfil", "ET MALWARE VBulletin Backdoor C2 URI Structure", "ET MALWARE W32/Witch.3FA0!tr CnC Actiivty", "ET MALWARE Backdoor Win32/Hupigon.CK Client Checkin", "ET MALWARE [PTsecurity] Win32/Remcos RAT Checkin 51", "ET MALWARE Backdoor.Darpapox/Jaku Initial C2 Checkin", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Services Listing)", "ET MALWARE Asprox Form

	Submission to C&C", "ET MALWARE Win32/AZORult V3.2 Client Checkin M15", "ET MALWARE Aveo C2 Response", "ET MALWARE StealerNeko CnC Checkin", "ET MALWARE Worm.Win32.Vobfus Checkin 3", "ET MALWARE W32/Citadel Content.php CnC POST", "ET MALWARE MSIL/EasyLocker Ransomware CnC Activity", "ET MALWARE TA402/Molerats Pierogi CnC Activity (Upload)", "ET MALWARE Win32/Pterodo.NG Checkin 2", "ET MALWARE Suspected USBFERRY CnC", "ET MALWARE W32/Bravix.Dropper CnC Beacon", "ET MALWARE Win32/Agent.RTQ CnC Activity", "ET MALWARE Fareit/Pony Downloader Checkin 3", "ET MALWARE Win32/Backdoor Sending Task Status (POST)", "ET MALWARE PoshC2 - Observed Default URI Structure M7", "ET MALWARE MSIL/Modi RAT CnC Command Outbound (aw)", "ET MALWARE njrat ver 0.7d Malware CnC Callback Response (File Manager)", "ET MALWARE Potential Sefnit C2 traffic (from server)", "ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (newsroom247 .xyz)", "ET MALWARE Suspected REDCURL CnC Activity M2", "ET MALWARE HAWKBALL CnC Initial Request", "ET MALWARE Backdoor.ADDNEW (DarKDdoser) CnC 3", "ET MALWARE ELF/Muhstik - IRC CnC Checkin", "ET MALWARE Win32/Jackpot Ransomware CnC Checkin", "ET MALWARE Playtech Downloader Online Gaming Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (best24-files .com)", "ET MALWARE W32/Hyteod.Downloader CnC Beacon", "ET MOBILE_MALWARE Android/xDrop Ransomware CnC Checkin", "ET MALWARE APT 41 LOWKEY Backdoor - Initalisation Bytes Received from CnC", "ET MALWARE ReverseRAT Activity (POST) M5", "ET MALWARE Win32.Raccoon Stealer - Telegram Mirror Checkin (generic)", "ET MALWARE Possible TickGroup Casper CnC Activity", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Upload Command Success", "ET MALWARE ELF/Mirai Variant CnC Activity", "ET MALWARE Win32/RisePro CnC Server Response M2", "ET MALWARE Foudre Checkin M2", "ET MALWARE Ransomware Locky CnC Beacon 2", "ET MALWARE Win32/Sarwent Initial Checkin", "ET MALWARE W32/Numnet.Downloader CnC Checkin 1", "ET MALWARE PowerTrick Task Answer", "ET MALWARE Backdoor.Win32.Fynloski.A/DarkRat Checkin Outbound", "ET MALWARE Possible OceanLotus CnC Heartbeat", "ET POLICY SSL Certificate IRC GEEKS Likely Encrypted IRC or CnC", "ET MALWARE Fbot/Satori CnC DNS Lookup (rippr .cc)", "ET MALWARE Gamaredon MalDoc CnC Exfil", "ET MALWARE Ursnif Variant CnC Beacon 4", "ET MALWARE Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected", "ET MALWARE DNS Query for known ShadowPad CnC 3", "ET MALWARE [eSentire] Win32/Spy.Banker.ADIO CnC Checkin", "ET MALWARE NuggetPhantom Module Download Request", "ET MALWARE Sakula/Mivast RAT CnC Beacon 1", "ET MALWARE JKDDOS Bot CnC Phone Home Message", "ET MALWARE Possible Turla Carbon Paper CnC Beacon (Fake User-Agent)", "ET MALWARE Observed DNS Query to RisePro Domain (pin-files .com)", "ET MALWARE W32/Spy.KeyLogger.OCI CnC Checkin", "ET MALWARE Patchwork Backdoor - Sending Task Results", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 56", "ET MALWARE Observed DNS Query to RisePro Domain (first-mirror .com)", "ET MALWARE Ransomware/Cerber Checkin M3 (10)", "ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (DISCONNECT)", "ET MALWARE PWS.Win32/Daceluw.A Checkin", "ET MALWARE SpyEye C&C Check-in URI", "ET MALWARE [PTsecurity] Remcos RAT Checkin 70", "ET MALWARE Dridex v2 POST Checkin", "ET MALWARE Mespinoza Ransomware - Pre-Encryption File Exfil to CnC", "ET MALWARE [TGI] Py.Machete HTTP CnC Exfil", "ET MALWARE Observed DNS Query to RisePro Domain (gs24softeasy .com)", "ET MALWARE Win.Backdoor.Kolobko-9950676-0 Retrieving CnC Commands", "ET MALWARE CoreDDRAT KeepAlive Message", "ET MALWARE [TGI] Cobalt Strike Malleable C2 Request (YouTube Profile)", "ET MALWARE Linux/BillGates Checkin", "ET MALWARE DTLoader Binary Request M2", "ET MALWARE PoetRAT Upload via HTTP", "ET MOBILE_MALWARE Android/Drinik Activity M2 (POST)", "ET MALWARE Parallax CnC Activity (set) M15", "ET MALWARE Vawtrak/NeverQuest CnC Beacon", "ET MALWARE zgRAT Activity M2", "ET MALWARE IndigoZebra APT xCaon/Textpadx Activity (POST)", "ET MALWARE Kuluoz/Asprox CnC Response", "ET MALWARE Mac Flashback Checkin 2", "ET MALWARE ZeroAccess/Max++ Rootkit C&C Activity 1", "ET MALWARE W32/AGENT.NXNX Checkin 2", "ET MALWARE

	Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 2", "ET MALWARE Win32/Valak Variant CnC", "ET MALWARE CrownAdPro CnC Activity M1", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M6", "ET MALWARE BigLock Ransomware CnC Activity (ext)", "ET MALWARE Patchwork APT CnC Beacon 2", "ET MALWARE Android/FakeKakao checkin", "ET MALWARE DEEP PANDA Checkin 3", "ET MALWARE Possible Pipka JS Skimmer CnC Request", "ET MALWARE Win32/IcedID Requesting Encoded Binary M4", "ET MALWARE Downloader General Bot Checking In via HTTP Post (bot_id push)", "ET MALWARE Possible DACLS RAT CnC (Log Server Reporting)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 57", "ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (politiaromana .bit in DNS Lookup)", "ET MALWARE Win32/BlackNET CnC Keep-Alive", "ET MALWARE JS/Agent.NZH CnC Response", "ET MALWARE Operation Mystery Baby syschk CnC Communication", "ET MALWARE W32/Iyus.H work_troy.php CnC Request", "ET MALWARE Diavol Communicating with CnC - Priority Request", "ET MALWARE Foudre Checkin M4", "ET MALWARE TURLA APT CnC Activity", "ET MALWARE PS/SunCrypt Ransomware CnC Activity", "ET MALWARE DNS Query for known ShadowPad CnC 11", "ET MALWARE APT/Donot Group Checkin Activity (GET)", "ET MALWARE ProxyBox - HTTP CnC - getiplist.php", "ET MALWARE ProxyBox - HTTP CnC - get_servers.php", "ET MALWARE MSIL/Agent.DNL CnC Activity M1", "ET MALWARE W32/Nutiliers.A Downloader CnC Checkin - Request Encrypted Response", "ET MALWARE MSUpdater alt checkin to CnC", "ET MALWARE Bitter RAT TCP CnC Beacon", "ET MALWARE MSIL/Modi RAT CnC Command Outbound (ds)", "ET MALWARE Win32/WarHawk Activity (filemgr) M2", "ET MALWARE ELF/RedXOR CnC Response", "ET MALWARE Observed DNS Query to RisePro Domain (files-sender .com)", "ET MALWARE Amadey Stealer CnC", "ET JA3 Hash - Remcos 3.x TLS Connection", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Sleep Command Success", "ET MALWARE Win32.Pony Variant FOX Checkin", "ET MOBILE_MALWARE Android GolfSpy (services4me .net in TLS SNI)", "ET MALWARE MedusaHTTP Variant CnC Checkin", "ET MALWARE Soraya C2 User-Agent (slayer)", "ET MALWARE MSIL/Black Hat Worm Server Response", "ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 5", "ET MALWARE Win32/Urausy.C Checkin 3", "ET MALWARE MAGICHOUND.FETCH CnC Beacon", "ET MALWARE AZORult v3.3 Server Response M3", "ET MALWARE BlackMatter CnC Activity", "ET MALWARE FrameworkPOS Covert DNS CnC Initial Check In", "ET MALWARE JavaScriptBackdoor HTTP GET CnC Beacon", "ET MALWARE Win32/Emotet CnC Activity (POST) M5", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 86", "ET MOBILE_MALWARE Android Joker CnC Configuration Retrieval", "ET MALWARE OSX/Leverage.A Checkin", "ET MALWARE Miras C2 Activity", "ET MALWARE Backdoor.Win32.Xyligan Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (2)", "ET MALWARE Win32/Dorv Stealer Exfiltrating Data to CnC", "ET MALWARE TURLA NETFLASH CnC", "ET MALWARE SNIcat - Detected C2 Commands (LIST)", "ET MALWARE Possible Hiloti DNS Checkin Message explorer_exe", "ET MALWARE Gh0st Remote Access Trojan Encrypted Session To CnC Server", "ET MALWARE FakeAV.EGZ Checkin 1", "ET MALWARE Operation Baby Coin syschk CnC Communication", "ET MALWARE Sakula/Mivast C2 Activity", "ET MALWARE Suspected Fancy Bear (APT28) Maldoc CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 20", "ET MALWARE Turkojan C&C Info Command (MINFO)", "ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)", "ET MALWARE TinyLoader.B1 Checkin x86", "ET MALWARE Pteranodon Variant 1 Backdoor Checkin", "ET MALWARE Linux/Moose NAT Traversal CnC Beacon - Multiple Tunnel", "ET MALWARE Hangover Campaign Keylogger Checkin", "ET MALWARE Win32.ChinaZ.DDoSClient Checkin", "ET MALWARE eleethub botnet CnC Domain in DNS Lookup (ghost.eleethub .com)", "ET MALWARE Win32/Ponmocup.A Checkin", "ET MALWARE Win32/Qbot CnC Activity M2", "ET MALWARE Win32/Rarog Stealer CnC Checkin", "ET MALWARE OSX/Mokes.A CnC Heartbeat Request (set)", "ET MALWARE Win32/Backdoor.Agent.qweydh CnC Checkin M1", "ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (JPEG)", "ET MALWARE Cobalt Strike Malleable C2 Profile (bg)", "ET MALWARE DDoS Win32/Nitol.A Checkin", "ET MALWARE DNSChanger

	CnC Domain in DNS Lookup", "ET MALWARE MargulasRAT Checkin M1", "ET MALWARE ReflectiveGnome Download Activity", "ET MALWARE Possible Red October proxy CnC 2", "ET MALWARE Win32/PivNoxy CnC Activity", "ET MALWARE TA505 P2P CnC Checkin", "ET MALWARE Win32/AZORult V3.2 Client Checkin M24", "ET MALWARE Cobalt Strike Malleable C2 Profile (btn_bg)", "ET MALWARE Win32/Rovnix.J Checkin 2", "ET MALWARE Trojan:Win32/Sabsik.FL.B!ml CnC Activity", "ET MALWARE W32/Dexter Infostealer CnC POST", "ET MALWARE Win32.ServStart.D Checkin", "ET MALWARE Win32/Valak <v9 Checkin", "ET MALWARE Cobalt Strike Malleable C2 (WooCommerce Profile)", "ET MALWARE Win32/Termite Agent Implant CnC Checkin", "ET MALWARE Nyanw0rm CnC Keep-Alive (Outbound) M2", "ET MALWARE W32/Neverquest.InfoStealer Configuration Request CnC Beacon", "ET MALWARE Observed MAZE Ransomware CnC Domain (checksoffice .me in TLS SNI)", "ET MALWARE r0 CnC Report GET", "ET MALWARE Shifr Ransomware CnC DNS Query (v5t5z6a55ksmt3oh)", "ET MALWARE Kimsuky WildCommand CnC Activity", "ET MALWARE Fodcha Bot CnC Client Heartbeat", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 8", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.GWO Checkin", "ET MALWARE AgentTesla Communicating with CnC Server", "ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 3", "ET MALWARE Win32/Autophyte.F C2 Domain (www .anlway .com in TLS SNI)", "ET MALWARE Win32.Androm.gnlb Checkin", "ET MALWARE Worm.VBS.ayr Checkin 2", "ET MALWARE W32/Snojan.BNQKZQH CnC Activity", "ET MALWARE APT34 TONEDEAF 2.0 Uploading to CnC", "ET MALWARE LYCEUM CnC Domain Observed in DNS Query", "ET MALWARE APT Lazarus Nukesped Downloader", "ET MALWARE PurpleFox Backdoor/Rootkit Download Request M1", "ET MALWARE Win32/AZORult V3.3 Client Checkin M22", "ET MALWARE W32/Mnless Checkin", "ET MALWARE EvilNum CnC Checkin", "ET MALWARE Linux.Mumblehard Spam Command CnC", "ET MALWARE W32/Qakbot.Bot Version 8 CnC Beacon", "ET MALWARE Ruskill/Palevo CnC PONG", "ET MALWARE Qarallax RAT Keepalive C2 (set)", "ET MALWARE Win32/TrojanDownloader.Delf.BVP Win32/BioData CnC Beacon", "ET MALWARE AHK/BKDR_HTV.ZKGD-A CnC Checkin", "ET MALWARE Havex RAT CnC Server Response", "ET MALWARE Observed Win32/Orion Logger SMTP Exfil Subject Line", "ET MALWARE Win32/TrojanDropper.Agent.RLO CnC Acitivty", "ET MALWARE Win32/AZORult V3.2 Client Checkin M6", "ET MALWARE LDPinch Checkin Post", "ET MALWARE Dialer-715 Install Checkin", "ET MALWARE Win32/Kryptik.HNBU CryptoMiner - Report Request", "ET MALWARE Emotet Post Drop C2 Comms M2", "ET MALWARE ELF/Win32 Lucky Ransomware CnC Checkin", "ET MALWARE Win32/Unk.BrowserStealer CnC Keep-Alive", "ET MALWARE Win32/Swrort.A Checkin 2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 91", "ET MALWARE Sakula/Mivast RAT CnC Beacon 2", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (count .trackstatisticsss .com) in DNS Lookup", "ET MALWARE Ransomware Locky CnC Beacon 4 21 May", "ET MALWARE WORM_VOBFUS Checkin Generic 2", "ET MALWARE XcodeGhost CnC M2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 63", "ET MALWARE Zbot POST Request to C2", "ET MALWARE Win32/CHIP Ransomware CnC Checkin", "ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (gabriellalovecats .com) in TLS SNI", "ET MALWARE Generic Downloader Checkin - HTTP GET", "ET MALWARE VBS/TrojanDownloader.Agent.SEB Keep-Alive", "ET MALWARE MalDoc Exfil (2019-12-12)", "ET MALWARE Generic Dropper/Clicker Checkin", "ET MALWARE EVILNUM CnC Host Checkin", "ET MALWARE Go/PSW.Agent_AGen.A Data Exfil", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 24", "ET MALWARE W32/Mentory CnC Server Providing Update Details", "ET MALWARE hacker87 checkin", "ET MALWARE Naoinstalad Checkin", "ET MALWARE Pontoeb CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 11", "ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (WAIT)", "ET MALWARE Lucifer CnC Checkin", "ET MALWARE Piptea.a Related Trojan Checkin (1)", "ET MALWARE Wonton-JH Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (jojo-files .com)", "ET MALWARE [GIGAMON_ATR] FIN8 BADHATCH CnC Checkin", "ET MALWARE

	Mermaid Ransomware Variant CnC Activity M3", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.2)", "ET MALWARE FrameworkPOS Covert DNS CnC Beacon 1", "ET MALWARE MagikPOS CnC Beacon", "ET MALWARE PoshC2 - Observed Default URI Structure M3", "ET MALWARE Click Fraud Checkin", "ET MALWARE W32/Farfli.BHQ!tr Dropper CnC Beacon 2", "ET MALWARE TA450 Nagual CnC Activity", "ET MALWARE Win32/RaaLoader CnC Activity", "ET MALWARE SEASALT HTTP Checkin", "ET MALWARE Win32/GandCrab Ransomware CnC Activity", "ET MALWARE MSUpdater POST checkin to CnC", "ET MALWARE PoshC2 - Observed Default URI Structure M4", "ET MALWARE Unknown Actor Targeting Minority Groups CnC Activity", "ET MALWARE MSIL/DataMilk Stealer Communicating with CnC", "ET MALWARE Win32/BlackNET CnC Checkin", "ET MALWARE Observed DNS Query to RisePro Domain (rate-files .com)", "ET MALWARE Win32/Cridex Checkin", "ET MALWARE Bladabindi/njrat CnC Command (Registry)", "ET MALWARE [PTsecurity] Botnet Nitol.B Checkin", "ET MALWARE Ousaban Banker Server Response M2", "ET MALWARE Operation Buhtrap CnC Beacon 2", "ET MALWARE Observed BatLoader Domain (cloudsteamview .com) in TLS SNI", "ET MALWARE W32/LockscreenBEI.Scareware Cnc Beacon", "ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M3", "ET MALWARE FoggyWeb Backdoor Incoming Request (GET)", "ET MALWARE HAWKBALL CnC Activity", "ET MALWARE Win32/Nuclear Checkin", "ET MOBILE_MALWARE Android/Comll.Banker RAT CnC Beacon", "ET MALWARE Banker/Banbra Related HTTP Post-infection Checkin", "ET MALWARE Bladabindi/njrat CnC Keep-Alive (INBOUND)", "ET MALWARE Tibs Checkin", "ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.2)", "ET MALWARE Win32/WarHawk Activity (ping)", "ET MALWARE Win32/InfoTester Checkin", "ET MALWARE Cayosin/Mirai CnC Domain in DNS Lookup", "ET MALWARE Likseput.B Checkin", "ET MALWARE Win32/FakeSysdef Rogue AV Checkin", "ET MALWARE H1N1 Loader CnC Beacon M2", "ET MALWARE Possible TickGroup Coolbee/Avenger CnC Activity", "ET MALWARE Glupteba CnC Observed in DNS Query", "ET MALWARE Winsoft.E Checkin 1", "ET MALWARE Win32/Remcos RAT Checkin 29", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Registry Listing)", "ET MALWARE DonotGroup CnC Domain in DNS Lookup (drivethrough .top)", "ET MALWARE SuperCMD CnC Beacon", "ET MALWARE Trojan.Win32.Codenox.gyezu CnC Activity", "ET MALWARE Win32/TrojanProxy.JpiProx.B CnC Beacon 2", "ET MALWARE Smurf2 CnC Checkin", "ET MALWARE Win32/Ropest.H CnC - INBOUND set", "ET MALWARE Arechclient2 Backdoor CnC Keep-Alive", "ET MALWARE Emotet CnC Beacon", "ET MALWARE Dropper.Win32.Agent.bpxo Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (9)", "ET MALWARE Nitlove POS CnC", "ET MALWARE Observed TrumpHead Ransomware CnC Domain (6bbsjnrzv2uvp7bp .onion .pet in TLS SNI)", "ET MALWARE Win32/Enchanim Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 79", "ET MALWARE General Downloader Checkin URL (GUID+)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 25", "ET MALWARE Suspected Stitch Variant Backdoor CnC", "ET MALWARE MegalodonHTTP CnC Checkin", "ET MALWARE Win32/Zacom.A CnC Beacon 1", "ET MALWARE Observed DNS Query to RisePro Domain (teleportsoft .com)", "ET MOBILE_MALWARE Android/HeHe.Spy LoginRequest CnC Beacon", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/nt/sk", "ET MALWARE Observed BatLoader Domain (105105105015 .com) in TLS SNI", "ET MALWARE Bladabindi/njrat CnC Checkin", "ET MALWARE Taidoor Checkin", "ET MALWARE W32/Symmi Remote File Injector Initial CnC Beacon", "ET MALWARE MSIL/Heracles Variant CnC Activity", "ET MALWARE ELF/Freakout IRC Checkin", "ET MALWARE W32/Asprox.ClickFraudBot CnC Beacon Acknowledgement", "ET MALWARE Trojan.FakeMS Checkin", "ET MALWARE MirrorBlast KiXtart Downloader Server Response", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 14", "ET MALWARE Possible Ransomware HTTP POST to Onion Link Domain", "ET MALWARE Backdoor.Win32/Momibot Ping Checkin", "ET MALWARE Mirai/OMG Proxy Variant CnC in DNS Lookup (ccnew.mm .my)", "ET MALWARE Locky CnC checkin Nov 21 M2", "ET MALWARE Lemon_Duck Powershell - Install Tracking", "ET MALWARE OSX/OceanLotus.D Requesting Commands from CnC", "ET MALWARE NightfallGT

	Discord Token Grabber", "ET MALWARE Zeoticus Ransomware CnC Activity", "ET MALWARE Win32/Urausy.C Checkin 4", "ET MALWARE Enfal CnC POST", "ET MALWARE PoshC2 - Observed Default URI Structure M23", "ET MALWARE Ponmocup C2 Post-infection Checkin", "ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M2", "ET MALWARE Suspected APT32/Oceanlotus Maldoc CnC", "ET MALWARE BalkanDoor CnC Checkin", "ET MALWARE AlinaPOS Exfiltration via DNS", "ET MALWARE VBS/TrojanDownloader.Agent.SEB Reporting Network Info", "ET MALWARE Theoreon.com Related Trojan Checkin", "ET MALWARE Malicious Browser Installer Checkin (POST)", "ET MALWARE MSIL.Zapchast Checkin", "ET MALWARE APT39/Chafer Payload - CnC Checkin M2", "ET ADWARE_PUP Win32/RiskWare.YouXun.X CnC Server Response", "ET MALWARE Win32.Banload.BTQP Checkin 1", "ET MALWARE IceRat CnC Acitivty M2", "ET MALWARE Possible Gamaredon HEAD Request for .dot file on ddns.net", "ET MALWARE Unattributed CnC Domain in DNS Lookup (encrypt-email .online)", "ET MALWARE Felismus CnC Beacon 1", "ET MALWARE Gh0st Trojan CnC 2", "ET MALWARE Mirai pTea Variant - Info Submission Inbound", "ET MOBILE_MALWARE Android/SMSThief.F Banker CnC Beacon", "ET MALWARE HCRootkit CnC Domain in DNS Lookup (ywbgrcrupasdiqxknwgceatlnbvmezti .com)", "ET MALWARE Unruy Downloader Checkin", "ET MALWARE Win32/AZORult V3.2 Client Checkin M1", "ET MALWARE PunkeyPOS HTTP CnC Beacon 1", "ET MALWARE StrifeWater RAT CnC Activity M2", "ET MALWARE Win32.VBKrypt.vquj Checkin", "ET MALWARE Possible PrivateLoader Payload Request (GET)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M21", "ET MALWARE ABUSE.CH Locky C2 Domain (uxwavkmttywsuynt in DNS Lookup)", "ET MALWARE Lop.gfr/Swizzor HTTP Update/Checkin (usually host-domain-lookup.com related)", "ET MALWARE Win32/Remcos RAT Checkin 63", "ET MALWARE PoshC2 - Observed Default URI Structure M12", "ET MALWARE Win32/SVCReady Loader CnC Activity M2", "ET MALWARE Win32/Backdoor Retrieving Task (POST)", "ET MALWARE DCRat CnC Activity M12", "ET MALWARE Georbot initial checkin", "ET MALWARE Win32/Emotet CnC Activity (POST) M4", "ET MALWARE Downloader.Win32.Small CnC Beacon", "ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M3", "ET MALWARE Project Plague CnC Activity", "ET MALWARE Banload HTTP Checkin", "ET MALWARE Ransomware/Cerber Checkin M3 (14)", "ET MALWARE ProxyBox - HTTP CnC - botinfo.php", "ET MALWARE DeathStalker/Powersing CnC Checkin", "ET MALWARE Win32/SuperBOT CnC Checkin", "ET WORM W32/Njw0rm CnC Beacon", "ET MALWARE FakeAV checkin", "ET MALWARE Socelars Stealer CnC Activity", "ET MALWARE Win32/Snatch Ransomware - Encryption Started", "ET MALWARE Win32/MillionLoader CnC Activity (Inbound)", "ET MALWARE PurpleFox Backdoor/Rootkit Download Request M2", "ET MALWARE Parallax CnC Activity M8 (set)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 77", "ET MALWARE W32/Gaudox Checkin", "ET MALWARE ELF/Chacha.DDoS/Xor.DDoS Stage 2 CnC Checkin", "ET MALWARE GoBrut/StealthWorker Service Bruter CnC Activity", "ET MALWARE Win32/Autophyte.F C2 Domain (tpddata .com in DNS Lookup)", "ET MALWARE Win32.Cerberus RAT Checkin Response", "ET MALWARE W32/ZxShell Server Checkin Response", "ET MALWARE MSIL/Hidden-Tear Variant Ransomware CnC Checkin", "ET MALWARE Possible Fake AV Checkin", "ET MALWARE W32 Bamital or Backdoor.Win32.Shiz CnC Communication", "ET MALWARE Taurus Stealer CnC Exfil", "ET MALWARE MICROPSIA HTTP Failover CnC Checkin", "ET MALWARE W32/TRCrypt.ULPM Downloader CnC Beacon", "ET MALWARE Win32/Denisca.A CnC Beacon 2", "ET MALWARE Rogue.Win32/Winwebsec Checkin", "ET MALWARE FighterPOS CnC Beacon 2", "ET MALWARE W32/Hicrazyk.A Downloader Install CnC Beacon", "ET MALWARE Win32/WarHawk Sending Windows System Information (POST)", "ET MOBILE_MALWARE Android/Revive Banking Trojan Initial Checkin Activity (POST)", "ET MALWARE CobianRAT Checkin to CnC", "ET MALWARE FakeAvCn-A Checkin 3", "ET MALWARE MSIL/Crimson CnC Server Command (info) M3", "ET MALWARE Platinum APT - Titanium Hardcoded String Observed", "ET MALWARE Win32.Sality-GR Checkin", "ET MOBILE_MALWARE Android PHONEMONITOR RAT CnC (getsettings)", "ET MALWARE TickGroup Datper CnC Checkin M2", "ET MALWARE Win32/Wacapew.C!ml Checkin", "ET MALWARE Worm.Win32.Balucaf.A Checkin", "ET MALWARE

	OSX/KeRanger Ransomware CnC DNS Request 3", "ET MALWARE [PTsecurity] Win32/Randrew!rfn CnC Activity", "ET MALWARE Win32/Autophyte.F C2 Domain (www .ap8898 .com in TLS SNI)", "ET MALWARE MSIL/Spy.Keylogger.ENJ Variant CnC Activity", "ET MALWARE IceRat Backdoor Checkin", "ET MALWARE Lemon_Duck Powershell CnC Checkin M6", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 88", "ET MALWARE Generic Bot Checkin", "ET DNS Hiloti DNS CnC Channel Successful Install Message", "ET MALWARE 44Calibar Variant Exfil via Telegram", "ET MALWARE Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1", "ET MALWARE [PTsecurity] Remcos RAT Checkin 87", "ET MALWARE Observed DNS Query to RisePro Domain (get-files24 .com)", "ET MALWARE Antinum WebSockets Start", "ET MALWARE Observed Buran Ransomware UA", "ET MALWARE Win32/Tofsee Covid19 Spam Template 1 Active - Outbound Email Spam", "ET MALWARE COMRAT CnC", "ET MALWARE Nuke Ransomware Checkin", "ET MALWARE MSIL/Black Hat Worm Checkin", "ET MALWARE Win32/AnteFrigus Ransomware Activity", "ET MALWARE GET to Google with specific HTTP lib likely Cycbot/Bifrose/Kryptic checking Internet connection", "ET MALWARE Cobalt Strike Malleable C2 (jquery Profile)", "ET MALWARE Ransomware/Cerber Checkin M3 (13)", "ET MALWARE CobianRAT Screenshot Exfil to CnC", "ET MALWARE Uroburos/Turla CnC (OUTBOUND) 1", "ET MALWARE Lampion CnC Activity", "ET MALWARE ABUSE.CH Locky C2 Domain (dyoravdkiavfkbkx in DNS Lookup)", "ET MALWARE PoshC2 - Observed Default URI Structure M22", "ET MALWARE WORM_VOBFUS Checkin Generic", "ET MALWARE Observed Lazarus Related Domain (share .bloomcloud .org in TLS SNI)", "ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Anatsa Checkin", "ET MALWARE Dmechant Exfil Cryptowallets via SMTP", "ET MALWARE ICEFOG-P Variant CnC Checkin M2", "ET MALWARE Win32.Trojan.Agent.U3D7V0 Checkin", "ET MALWARE Sidewinder CnC DNS Query", "ET MALWARE Unattributed CnC Domain in DNS Lookup (encrypted-message .cloud)", "ET MALWARE Win32/Remcos RAT Checkin 58", "ET MALWARE Hupigon.DF Checkin", "ET MALWARE Virusremover2008.com Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 22", "ET MALWARE FindPOS Checkin", "ET MALWARE DNSG - Data Exfiltration via DNS", "ET MALWARE Trojan.NSIS.Comame.A Checkin", "ET MALWARE ConPtyShell Client Response", "ET MALWARE W32/PointOfSales.Misc CnC Beacon", "ET MALWARE DDoS.Win32/Nitol.B Checkin", "ET MALWARE Win32.Raccoon Stealer Data Exfil Attempt", "ET MALWARE MedusaHTTP Variant CnC Checkin M2", "ET MALWARE Criptobit/Mobef Ransomware Checkin", "ET MALWARE Observed MageCart CnC Domain (mcdnn .me in TLS SNI)", "ET MALWARE Win32/Farfli.CUY KeepAlive M2", "ET MALWARE NSIS/TrojanDownloader.Agent.NZK CnC Activity M2", "ET MALWARE Win32/AZORult V3.3 Client Checkin M5", "ET MALWARE Win32/Colibri Loader Activity M2", "ET MALWARE SNIcat - Detected C2 Commands (ALIVE)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 101", "ET MALWARE Sakula/Mivast RAT CnC Beacon 3", "ET MALWARE Tinba Banker CnC Response", "ET MALWARE Buer Loader Update Request", "ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M2", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 36", "ET MALWARE CollectorStealer CnC Exfil", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Get Passwords)", "ET MALWARE Zyklon CnC Activity", "ET MALWARE MSIL/Crimson Rat CnC Server Response", "ET MALWARE Win32/AZORult V3.3 Client Checkin M10", "ET MALWARE DTLoader Encoded Binary - Server Response", "ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST)", "ET MALWARE MICROPSIA Screenshot Upload M2", "ET MALWARE Generic Spambot (often Tibs) Post-Infection Checkin (justcount.net likely)", "ET MALWARE W32/Liftoh.Downloader Feed404 CnC Beacon", "ET MALWARE Win32/Spy.Agent.PZE Variant CnC Activity", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 7", "ET MALWARE lu0bot Loader HTTP Request M2", "ET MALWARE f0xy Checkin", "ET MOBILE_MALWARE Android/BasBanke CnC Checkin", "ET MALWARE Mermaid Ransomware Variant CnC Activity M1", "ET MALWARE Win32/Unknown Stealer Command (filegrab) (Outbound)", "ET MALWARE Sysget/HelloBridge HTTP GET CnC Beacon", "ET MALWARE Joanap CnC Checkin", "ET MALWARE MSIL/Firebird RAT CnC

	Checkin", "ET MALWARE Winsoft.E Checkin 3", "ET MALWARE ELF/Mirai Botnet CnC Activity", "ET MALWARE CrownAdPro CnC Activity M5", "ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (xipxesip .design in TLS SNI)", "ET MALWARE Banload HTTP Checkin Detected (envia.php)", "ET MALWARE W32/Downvision.A Initial Checkin", "ET MALWARE AZORult v3.3 Server Response M2", "ET MALWARE HTTPCore CnC Task Request", "ET MALWARE FoggyWeb Backdoor Incoming Request (POST)", "ET MALWARE MSIL/Agent.PYO Possible net.tcp CnC Beacon (stat)", "ET MALWARE r0 CnC Architecture GET 1", "ET MALWARE Turkojan C&C Initial Checkin (ams)", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 61", "ET MALWARE MSIL/Agent.BIC Variant CnC Checkin", "ET MALWARE MSIL/Khonsri Ransomware CnC Activity", "ET MALWARE Bladabindi/njrat CnC Command (File Manager)", "ET MALWARE Backdoor.Win32.Pushdo.s Checkin", "ET MALWARE FTCode Stealer CnC Activity", "ET MALWARE CoreDDRAT Initial Checkin", "ET MALWARE Generic Trojan Checkin (UA VBTagEdit)", "ET MALWARE Golang/Kaos/YamaBot CnC Activity", "ET MALWARE W32/SchwSonne CnC Beacon M2", "ET MALWARE Qadars CnC DNS Lookup (zkdef09i7ola.net)", "ET MALWARE AHK Bot Domain Profiler CnC Activity", "ET MALWARE SuperKillerX Checkin Activity", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 26", "ET MALWARE [TGI] Cobalt Strike Malleable C2 Response (YouTube Profile)", "ET MALWARE Zbot CnC POST /common/versions.php", "ET MALWARE APT34 TONEDEAF 2.0 Requesting Commands from CnC", "ET MALWARE MSIL/Small.FU Variant CnC Activity M3", "ET MALWARE ApolloLocker Ransomware CnC Checkin", "ET MALWARE Win32/1xxbot CnC Checkin", "ET MALWARE BabyShark CnC Domain in SNI", "ET MALWARE Poweliks Clickfraud CnC M1", "ET MALWARE Matanbuchus Loader CnC M3", "ET MALWARE Ransomware Locky CnC Beacon", "ET MALWARE TickGroup ABK Backdoor CnC Check-in", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 30", "ET MALWARE Ransomware/Cerber Checkin M3 (6)", "ET MALWARE [PTsecurity] Kuriyama Loader Checkin", "ET MALWARE PS/Beapy CnC Checkin", "ET MALWARE ELF Linux/Dnsamp.AB Variant CnC", "ET MALWARE Win32/RisePro CnC Server Response M3", "ET MALWARE Linux/MayhemBruter Inbound Ping From CnC", "ET MALWARE Win32/Valak <v20 Checkin - Server Response", "ET MALWARE DNS Query for known ShadowPad CnC 6", "ET MALWARE Backdoor.Win32.Trup.CX Checkin 1", "ET MALWARE ELF/lizkebab CnC Activity (Server Banner)", "ET MALWARE Ransomware/Cerber Checkin M3 (1)", "ET MOBILE_MALWARE Android/Opfake.A Country CnC Beacon", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 90", "ET MALWARE JsOutProx Variant CnC Activity", "ET MALWARE Possible GhostMiner CCBOT Component - CnC Checkin", "ET MALWARE Grandoreiro CnC Activity (iso)", "ET MALWARE Hitpop.AG/Pophot.az HTTP Checkin", "ET MOBILE_MALWARE ITW Android Post-Exploit Downloader CnC Activity", "ET MALWARE Backdoor.Win32.Xtrat Checkin 2", "ET MALWARE Vidar Stealer - FaceIt Checkin Response", "ET MALWARE Panda Banker C2 Domain (uiaoduiiej .chimkent .su in TLS SNI)", "ET MALWARE NAZAR EYService Pong response", "ET MALWARE W32.Geodo/Emotet Checkin", "ET MALWARE GratefulPOS Covert DNS CnC Initial Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 21", "ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (deliverygoodstrategies .com) in TLS SNI", "ET MALWARE W32/Adrom.Backdoor CnC Beacon", "ET MALWARE Win32/Colibri Loader Activity M3", "ET MALWARE Trojan-PSW.Win32.Stealer.sb CnC", "ET MALWARE W32/Downloader.Mevade.FBV CnC Beacon", "ET MALWARE MSIL.L4L Stealer Screenshot Exfiltration", "ET MALWARE Qadars CnC DNS Lookup (websecuranalityc.com)", "ET MALWARE Turkojan C&C Info Command Response (MINFO)", "ET MALWARE Win32/AZORult V3.3 Client Checkin M23", "ET MALWARE Fullz House Credit Card Skimmer JavaScript Inbound", "ET MALWARE JavaRAT CnC Init Activity", "ET MALWARE Trojan.BlackRev Botnet Command Request CnC Beacon", "ET MALWARE Mirai Variant Checkin Response", "ET MALWARE Win32/Agent.AETZ CnC Checkin", "ET MALWARE ELF/Emptiness v1.1 CnC Checkin", "ET MOBILE_MALWARE Android/Opfake.A GetTask CnC Beacon", "ET MALWARE Downloader General Bot Checking In - Possible Win32.Small.htz related", "ET MALWARE Backdoor.Elise CnC Beacon 2", "ET MALWARE ServHelper CnC Domain", "ET

	MALWARE Lazarus FALLCHILL Fake SSL Checkin 2", "ET MALWARE ZAccess/Sirefef/MAX++/Jorik/Smadow Checkin", "ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Checkin", "ET MALWARE Possible Konni Encrypted Stage 2 Payload Inbound via HTTP", "ET MALWARE Win32/Unknown Stealer CnC Log Exfil", "ET MALWARE Asprox Data Post to C&C", "ET MALWARE Win32/Spy.Banker.AAQD Checkin", "ET MALWARE Databack CnC", "ET MALWARE MirrorBlast KiXtart Downloader Client Request M2", "ET MALWARE MirrorBlast Checkin", "ET MALWARE Patchwork Backdoor Checkin", "ET MALWARE OilRig APT PowDesk Powershell Check", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 73", "ET MALWARE Win32/Milum CnC", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 67", "ET MALWARE Observed DNS Query to RisePro Domain (boost-files .com)", "ET MALWARE FakeYak or Related Infection Checkin 1", "ET MALWARE Win32/LockScreen CnC HTTP Pattern", "ET MALWARE W32/Eclipse.DDOSBot CnC Beacon Response", "ET MALWARE DEEP PANDA Checkin 2", "ET MALWARE Overtoolbar.net Backdoor ICMP Checkin Response", "ET MALWARE DDoS.XOR Checkin", "ET MALWARE Kelihos/Hlux GET jucheck.exe from CnC", "ET MALWARE Backdoor.Win32.RShot HTTP Checkin", "ET MALWARE Chafer CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Android Brunhilda Dropper (flowdivison .club in TLS SNI)", "ET MALWARE DNS Query for Known Chewbacca CnC Server", "ET MALWARE Cobalt Strike Malleable C2 (Custom Profile)", "ET MALWARE CerberTear Ransomware CnC Checkin", "ET MALWARE Win32/Autophyte.F C2 Domain (tpddata .com in TLS SNI)", "ET MALWARE Banker Trojan CnC AddNew Command", "ET MALWARE Win32/Pift Checkin 2", "ET MALWARE WORM_VOBFUS Checkin 1", "ET MALWARE MirrorBlast KiXtart Downloader Client Request", "ET MALWARE Manjusaka C2 Client Heartbeat", "ET MALWARE Win32/MailerBot CnC Activity", "ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (s3 .hiahornber .com)", "ET MALWARE Win32/AZORult V3.2 Client Checkin M4", "ET MALWARE BatLoader CnC Domain (105105105015 .com) in DNS Lookup", "ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 1", "ET MALWARE Linux/KDefend Checkin", "ET MALWARE CenterPOS CnC", "ET MALWARE DarkGate CNC Checkin", "ET MALWARE Parallax CnC Activity M9 (set)", "ET MALWARE Kraken C2 Domain Observed (kraken656kn6wyyx in DNS Lookup)", "ET MALWARE BatLoader CnC Domain (installationsoftware1 .com) in DNS Lookup", "ET MALWARE SNIcat - Detected C2 Commands (CB)", "ET MALWARE MSIL/Runsome Ransomware CnC Checkin", "ET MALWARE ELF.SystemdMiner C2 Domain in DNS Lookup", "ET MALWARE Webshell Execute Command Inbound - Possibly Iran-based M1", "ET MALWARE Win32/AZORult V3.3 Client Checkin M2", "ET MALWARE Unattributed CnC Domain in DNS Lookup (microsoftonline-secure-login .com)", "ET MALWARE Win32/Remcos RAT Checkin 26", "ET MALWARE Athena DDoS Bot Checkin", "ET MALWARE L0rdix Stealer CnC Sending Screenshot", "ET MALWARE Win32/CryptInject.BE!MTB Stealer CnC Checkin", "ET MALWARE Win32/GandCrab Ransomware CnC Activity M2", "ET MALWARE Possible FoggyWeb Backdoor Server Response", "ET MALWARE Win32/Tesch.B CnC Beacon", "ET MALWARE PoshC2 - Observed Default URI Structure M13", "ET MALWARE P2P Zeus or ZeroAccess Request To CnC", "ET MALWARE Bladabindi/njrat CnC Command Response (Get Passwords)", "ET MALWARE Aveo Checkin", "ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 4", "ET MALWARE Win32/Autophyte.F C2 Domain (www .anlway .com in DNS Lookup)", "ET MALWARE Hiloti/Mufanom CnC Response", "ET MALWARE Spora Ransomware Checkin", "ET MALWARE FRat WebSocket Request M1", "ET MALWARE Mermaid Ransomware Variant CnC Activity M4", "ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Receive Data", "ET MALWARE PureCrypter Requesting Injector M2", "ET MALWARE Win32/Remcos RAT Checkin 66", "ET MALWARE Potential FakePAV Checkin", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 54", "ET MALWARE BBSRAT POST request CnC", "ET MALWARE FIN6 StealerOne CnC Domain in SNI", "ET MALWARE zgRAT Activity", "ET MALWARE VirRansom/VirLock Checkin Response", "ET MALWARE Win32/Sarwent Variant CnC Activity", "ET MALWARE Win32/InnaputRAT CnC DNS Lookup (ninjagames .top)", "ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 3", "ET MALWARE Teslarvng

	Ransomware CnC Activity M1", "ET MALWARE Ransomware Win32/WinPlock.A Successfully Installed CnC Beacon", "ET JA3 Hash - Suspected Cobalt Strike Malleable C2 M1 (set)", "ET MALWARE Backdoor.Egobot Checkin", "ET MALWARE Win32/Kaicone.A Checkin via HTTP POST", "ET MALWARE Win32/Vundo.OD Checkin", "ET MALWARE ELF/Muhstik Bot Reporting Vulnerable Server to CnC", "ET MALWARE PowerTrick Task Checkin M2", "ET MALWARE Win32.MSUpdater C&C traffic GET", "ET MALWARE Parallax CnC Response Activity M17", "ET MALWARE Win32/Scieron-A Checkin via HTTP POST", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (letsmakeparty3 .ga) in DNS Lookup", "ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M3", "ET MALWARE Observed BatLoader Domain (installationupgrade6 .com) in TLS SNI", "ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/win/wcx", "ET MALWARE MSIL/Agent.TRM Task Command", "ET MALWARE Trojan-Dropper.Win32.Sysn.cdjy CnC Activity", "ET MALWARE Jasper URI Path Observed M2", "ET MALWARE PoshC2 - Observed Default URI Structure M19", "ET MALWARE Win32.Datamaikon Checkin myAgent", "ET MALWARE Smoke Loader Checkin r=gate", "ET MALWARE Sharik/Smoke CnC Beacon 3", "ET MALWARE Kimsuky Related CnC", "ET MALWARE Downloader.Win32.Adload (KaiXin Payload) Checkin Response", "ET MALWARE Revcode RAT CnC 2", "ET MALWARE Sarwent CnC Command (powershell)", "ET MALWARE Py/MechaFlounder CnC Activity - Reporting Upload Command Error", "ET MALWARE ELF/MooBot Mirai DDoS Variant Server Keep Alive", "ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 49", "ET MALWARE Win32/RisePro CnC Server Response M1", "ET MALWARE njrat ver 0.7d Malware CnC Callback Response (Remote Desktop)", "ET MALWARE RouteX CnC Domain (322ffbbc7c1b312c2f9d942f20422f8d .com) in DNS Lookup", "ET MALWARE [PTsecurity] Win32/Ramnit Stage 0 Communicating with CnC", "ET MALWARE TrueBot/Silence.Downloader CnC Checkin", "ET MALWARE [CISA AA21-291A] Possible BlackMatter Ransomware Lateral Movement", "ET MALWARE W32/Siggen.Dropper CnC Beacon", "ET MALWARE [PTsecurity] TR/Spy.Banker.agdtw Checkin", "ET MALWARE njrat ver 0.7d Malware CnC Callback (Keylogging)", "ET MALWARE UsefulTyphon CnC Activity M1", "ET MALWARE RedLine - GetArguments Request", "ET MALWARE Possible NGLite Backdoor C2 Traffic (NKN)", "ET MALWARE Win32/Denisca.A CnC Beacon", "ET MALWARE TAIDOOR CnC Domain in DNS Lookup (www.infonew.dubya .net)", "ET MALWARE Win32/CollectorStealer CnC Exfil M3", "ET MALWARE Wrapper/Gholee/Wedex Checkin", "ET MALWARE ViperSoftX CnC Activity M2", "ET MALWARE Win32/MillionLoader CnC Activity (Outbound)", "ET MOBILE_MALWARE Android/HeHe.Spy ReportRequest CnC Beacon", "ET MALWARE MSIL/Agent.PYO Possible net.tcp CnC Beacon (control)", "ET MALWARE Possible DEEP PANDA C2 Activity", "ET MALWARE Win32/LODEINFO v0.4.x CnC Checkin", "ET MALWARE Yayih.A Checkin", "ET MALWARE Ursnif Variant CnC Data Exfil", "ET MALWARE SuperFish CnC Beacon 2", "ET MALWARE Win32/Agent.UHC CnC Activity", "ET MALWARE Win32/Ketrican CnC Activity", "ET MALWARE ProjectSauron Remsec/HTTPBrowser/Pisloader Covert DNS CnC Channel TXT Lookup", "ET MALWARE W32/GameThief Initial CnC Beacon", "ET MALWARE Teslarvng Ransomware CnC Activity M3", "ET MALWARE W32/Gagolino Banking Trojan Reporting to CnC", "ET MALWARE Win32/Fosniw CnC Checkin Style 2", "ET MALWARE Win32/XRat.AT Variant CnC Activity"
GeoIP Южная Америка и зависимые территории	"GeoIP Уругвай", "GeoIP Парагвай", "GeoIP Аргентина", "GeoIP Бразилия", "GeoIP Французская Гвиана", "GeoIP Суринам", "GeoIP Боливия", "GeoIP Перу", "GeoIP Фолклендские о-ва", "GeoIP Гайана", "GeoIP Венесуэла", "GeoIP Чили", "GeoIP Эквадор", "GeoIP Колумбия"
Блокирование крупных утечек информации	"ET WEB_SPECIFIC_APPS WordPress DB XML dump successful leakage"
Эксплойты	"ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 1", "ET EXPLOIT_KIT Suspicious GitHack TLS SNI Request - Possible PurpleFox EK", "ET EXPLOIT_KIT Capesand EK Landing", "ET EXPLOIT_KIT Unknown EK Landing (Payload Downloaded Via Dropbox)", "ET EXPLOIT_KIT DRIVEBY Incognito Payload Requested /getfile.php by Java Client", "ET EXPLOIT_KIT Possible Router EK Landing Page Inbound 2019-05-24", "ET

	EXPLOIT_KIT SunDown EK RIP Landing M1 B642", "ET EXPLOIT_KIT SunDown EK Slight Sep 22 2016 (b642)", "ET EXPLOIT_KIT Styx Exploit Kit Secondary Landing", "ET EXPLOIT_KIT Terror EK Payload Download", "ET EXPLOIT_KIT Sibhost/FlimKit/Glazunov Jar with lowercase class names", "ET EXPLOIT_KIT GrandSoft PDF Payload Download", "ET EXPLOIT_KIT Underminer EK Resource File Download M1", "ET EXPLOIT_KIT Redirect to driveby sid=mix", "ET EXPLOIT_KIT Possible Red Dot Exploit Kit Single Character JAR Request", "ET EXPLOIT_KIT Sakura obfuscated javascript Jun 1 2013", "ET EXPLOIT_KIT Watering Hole applet name AppletHigh.jar", "ET EXPLOIT_KIT Terror EK Landing M1 Feb 07 2016 M2", "ET EXPLOIT_KIT TDS Sutra - page redirecting to a SutraTDS", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - TH3BUG and Non-Targetted Groups Watering Hole Deobfuscation function", "ET EXPLOIT_KIT RIG EK URI struct Oct 24 2016 (RIG-v)", "ET EXPLOIT_KIT Possible Underminer EK Landing", "ET EXPLOIT_KIT Unknown_MM - Payload Download", "ET EXPLOIT_KIT KaiXin Exploit Kit Landing Page parseInt Javascript Replace", "ET EXPLOIT_KIT CottonCastle EK URI Struct", "ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 2 M1", "ET EXPLOIT_KIT Java UA Requesting Numeric.ext From Base Dir (Observed in Redkit/Sakura)", "ET EXPLOIT_KIT SunDown EK Slight Sep 22 2016 (b643)", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole iframe", "ET EXPLOIT_KIT Cool PDF July 15 2013", "ET EXPLOIT_KIT PluginDetect Observed - Possible EK Activity", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64", "ET EXPLOIT_KIT Lucky7 EK Landing Encoded Plugin-Detect", "ET EXPLOIT_KIT Terror EK Landing T1 Jun 02 2017 M1", "ET EXPLOIT_KIT Disdain EK Flash Exploit M3 Aug 23 2017", "ET EXPLOIT_KIT Underminer EK SWF Request", "ET EXPLOIT_KIT Yszz JS/Encryption (Used in KaiXin Exploit Kit)", "ET EXPLOIT_KIT Download file with Powershell via LNK file (observed in Sundown EK)", "ET EXPLOIT_KIT Fragus Exploit jar Download", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox and Targetted Watering Holes PDF", "ET EXPLOIT_KIT SofosFO/GrandSoft landing applet plus class Mar 03 2013", "ET EXPLOIT_KIT Possible PurpleFox EK Framework Landing", "ET EXPLOIT_KIT Observed LordEK HTTP POST Request", "ET EXPLOIT_KIT Powershell Download Command Observed within Flash File - Probable EK Activity", "ET EXPLOIT_KIT DRIVEBY EL8 EK Landing", "ET EXPLOIT_KIT SWF filename used in IE 2014-0322 Watering Hole Attacks", "ET EXPLOIT_KIT Possible Malicious Redirect Leading to EK Oct 29", "ET EXPLOIT_KIT Possible Keitaro TDS Redirect", "ET EXPLOIT_KIT Terror EK Landing T1 Jun 02 2017 M2", "ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 2 M2", "ET EXPLOIT_KIT Possible Malvertising EK Redirect to EK M2", "ET EXPLOIT_KIT Spelevo EK Landing M1", "ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 3", "ET EXPLOIT_KIT Possible MSFVenom Exploit via Browser", "ET EXPLOIT_KIT SunDown EK CVE-2015-0016 Sep 22 2016 (b643)", "ET EXPLOIT_KIT Terror EK Payload URI T1 Jun 02 2017", "ET EXPLOIT_KIT KaiXin Landing M5 1 Oct 05 2015", "ET EXPLOIT_KIT SunDown EK NOP Sled Sep 22 2016 (b643)", "ET EXPLOIT_KIT Possible PurpleFox EK Framework Landing - Various Exploits", "ET EXPLOIT_KIT RIG EK Landing March 20 2015", "ET EXPLOIT_KIT Probable Sakura Java applet with obfuscated URL Sep 21 2012", "ET EXPLOIT_KIT SUSPICIOUS Grey Advertising Often Leading to EK", "ET EXPLOIT_KIT WindowBase64.atob Function In Edwards Packed JavaScript - Possible iFrame Injection Detected", "ET EXPLOIT_KIT ScanBox Framework used in WateringHole Attacks Initial (POST)", "ET EXPLOIT_KIT Probable Sakura exploit kit landing page obfuscated applet tag Mar 1 2013", "ET EXPLOIT_KIT Evil Redirector Leading To EK Sep 30 2015", "ET JA3 Hash - Possible Malware - FiestaEK", "ET EXPLOIT_KIT JDB Exploit Kit Landing Page", "ET EXPLOIT_KIT Styx Landing Page Oct 25 2013", "ET EXPLOIT_KIT GoonEK encrypted binary (3)", "ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack payload request (exploit successful!)", "ET EXPLOIT_KIT TDS - in.php", "ET EXPLOIT_KIT Magnitude EK JSE", "ET EXPLOIT_KIT BottleEK Payload Request", "ET EXPLOIT_KIT SNET EK Encoded VBS 3", "ET EXPLOIT_KIT FlimKit hex.zip Java Downloading Jar", "ET EXPLOIT_KIT Terror EK CVE-2016-0189 Exploit M2", "ET EXPLOIT_KIT DoSWF Flash Encryption (Used in KaiXin Exploit Kit)", "ET EXPLOIT_KIT RedKit/Sakura/CritX/SafePack/FlashPack applet + obfuscated URL Apr 10 2013", "ET EXPLOIT_KIT DNSChanger EK Secondary Landing May 12 2015 M2", "ET EXPLOIT_KIT Terror EK Payload Download M2 Mar 14 2017", "ET

	EXPLOIT_KIT Safe/CritX/FlashPack URI Struct .php?id=Hex", "ET EXPLOIT_KIT FlimKit Post Exploit Payload Download", "ET EXPLOIT_KIT Styx Exploit Kit Jerk.cgi TDS", "ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017 M2", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b646)", "ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack exploit request", "ET EXPLOIT_KIT RIG encrypted payload M1 Feb 02 2016", "ET EXPLOIT_KIT Cool Exploit Kit Plugin-Detect July 08 2013", "ET EXPLOIT_KIT TDS Sutra - cookie set", "ET EXPLOIT_KIT Possible Sweet Orange redirection 21 July 2014", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b641)", "ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct Sept 15 2015", "ET EXPLOIT_KIT RedKit applet + obfuscated URL Apr 7 2013", "ET EXPLOIT_KIT Unknown Exploit Kit Java Archive Request (Java-SPLOIT.jar)", "ET EXPLOIT CVE-2015-2419 As observed in Magnitude EK", "ET EXPLOIT_KIT TDS Sutra - cookie is set RULEZ", "ET EXPLOIT_KIT SunDown EK RIP Landing M3 B643", "ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 1 M1", "ET EXPLOIT_KIT Double-Encoded Reverse Base64/Dean Edwards Packed JavaScript Observed in Unknown EK Feb 16 2015 b64 1 M2", "ET EXPLOIT_KIT DRIVEBY Router DNS Changer Apr 07 2015 M2", "ET EXPLOIT_KIT g01pack exploit pack /mix/ payload", "ET EXPLOIT_KIT Obfuscated LordEK Landing M2", "ET EXPLOIT_KIT CritXPack PDF Request", "ET EXPLOIT_KIT Magnitude EK (formerly Popads) Java Exploit 32-32 byte hex java payload request Oct 16 2013", "ET EXPLOIT_KIT Nuclear EK Gate Injected iframe Oct 22 2014", "ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack payload download", "ET EXPLOIT_KIT StyX Landing Page (2)", "ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 2", "ET EXPLOIT_KIT Sakura Exploit Kit Landing Page Request", "ET EXPLOIT_KIT Obfuscated LordEK Landing M1", "ET EXPLOIT_KIT WinHttpRequest Downloading EXE Non-Port 80 (Likely Exploit Kit)", "ET EXPLOIT_KIT KaiXin Exploit Kit Landing Page NOP String", "ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 12 2016", "ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M2", "ET EXPLOIT_KIT DRIVEBY SPL - Java Exploit Requested - /spl_data/", "ET EXPLOIT_KIT SunDown EK RIP Landing M4 B641", "ET EXPLOIT_KIT KaiXin Landing Page Nov 25 2014", "ET EXPLOIT_KIT Possible Internet Explorer CVE-2014-6332 Common Construct b64 1 (Observed in Archie EK)", "ET EXPLOIT_KIT Gondad Exploit Kit Post Exploitation Request", "ET EXPLOIT_KIT RIG Exploit URI Struct March 20 2015", "ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 3 M2", "ET EXPLOIT_KIT Unknown EK Landing URL", "ET EXPLOIT_KIT ScanBox Jun 06 2015 M2 T1", "ET EXPLOIT_KIT Possible PurpleFox EK Framework Flash HEAD Request", "ET EXPLOIT_KIT CritXPack Landing Pattern", "ET EXPLOIT_KIT Possible Unknown TDS /top2.html", "ET EXPLOIT_KIT %Hex Encoded Applet (Observed in Sakura)", "ET EXPLOIT_KIT Redkit Exploit Kit Three Numerical Character Naming Convention PDF Request", "ET EXPLOIT_KIT BottleEK Landing", "ET EXPLOIT_KIT DRIVEBY SweetOrange - Java Exploit Downloaded", "ET EXPLOIT_KIT Magnitude EK Landing M2 Aug 05 2017", "ET EXPLOIT_KIT BottleEK Plugin Check Response", "ET EXPLOIT_KIT CritXPack - Landing Page - Received", "ET EXPLOIT_KIT CirtXPack - No Java URI - /a.Test", "ET EXPLOIT_KIT DRIVEBY Java Atomic Exploit Downloaded", "ET EXPLOIT_KIT Unknown EK Landing Page", "ET EXPLOIT_KIT Nuclear SilverLight Exploit", "ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b641)", "ET EXPLOIT_KIT Terror EK CVE-2016-0189 Exploit", "ET EXPLOIT_KIT Redirection to driveby Page Home index.php", "ET EXPLOIT_KIT Fiesta Flash Exploit Download", "ET EXPLOIT_KIT Likely Evil JS used in Unknown EK Landing", "ET EXPLOIT_KIT DRIVEBY EgyPack Exploit Kit Cookie Set", "ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Payload Request M1", "ET EXPLOIT_KIT BegOpEK - TDS - icon.php", "ET EXPLOIT_KIT SunDown EK RIP Landing M3 B642", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 (Reversed)", "ET EXPLOIT_KIT KaiXin Landing Page M2", "ET EXPLOIT_KIT SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs", "ET EXPLOIT_KIT Likely Scalaxy Exploit Kit URL template download", "ET EXPLOIT_KIT CritXPack - No Java URI - Dot.class", "ET EXPLOIT_KIT DRIVEBY EgyPack Exploit Kit Cookie Present", "ET WEB_CLIENT SUSPICIOUS Microsoft-Edge protocol in use (Observed in Magnitude EK)", "ET MALWARE Cryptowall docs campaign Aug 2015 encrypted binary (1)", "ET EXPLOIT_KIT Possible Malvertising Redirect to EK M1", "ET EXPLOIT_KIT KaiXin Secondary Landing

	Page", "ET EXPLOIT_KIT DRIVEBY Styx - TDS - Redirect To Landing Page", "ET EXPLOIT_KIT Flash Exploit Likely SunDown EK", "ET EXPLOIT_KIT Possible Evil Redirector Leading to EK June 10 2015", "ET EXPLOIT_KIT Likely TDS redirecting to exploit kit", "ET EXPLOIT_KIT Possible PurpleFox/RIG EK Flash Request M2", "ET EXPLOIT_KIT Sweet Orange Landing with Applet Oct 4 2013", "ET EXPLOIT_KIT Fiesta EK Landing Apr 23 2015", "ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b642)", "ET MALWARE Win32/Agent.RDE Checkin", "ET EXPLOIT_KIT Disdain EK URI Struct Aug 23 2017 M2", "ET EXPLOIT_KIT Spelevo EK Flash Exploit Attempt", "ET EXPLOIT_KIT RedKit - Potential Payload Requested - /2Digit.html", "ET EXPLOIT_KIT CoolEK - Landing Page - FlashExploit", "ET EXPLOIT_KIT Unknown Exploit Kit Exploit Request", "ET EXPLOIT_KIT CoolEK Payload Download (9)", "ET EXPLOIT_KIT DRIVEBY Java Rhino Scripting Engine Exploit Downloaded", "ET EXPLOIT_KIT Sutra TDS /simmetry", "ET EXPLOIT_KIT Incognito Exploit Kit PDF request to images.php?t=81118", "ET EXPLOIT_KIT RIG EK URI Struct Feb 26 2017", "ET EXPLOIT_KIT exploit kit x/load/svchost.exe", "ET EXPLOIT_KIT HoeflerText Chrome Popup DriveBy Download Attempt 2", "ET EXPLOIT_KIT KaiXin EK Jar URI Struct", "ET EXPLOIT_KIT KaiXin Secondary Landing Page M2", "ET EXPLOIT_KIT Internet Explorer Information Disclosure Vuln as Observed in RIG EK Prefilter M2 Dec 06", "ET EXPLOIT_KIT SunDown EK RIP Landing M1 B641", "ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Landing Request", "ET EXPLOIT_KIT Incognito Exploit Kit Java request to images.php?t=", "ET EXPLOIT_KIT Dadong Exploit Kit Downloaded", "ET EXPLOIT_KIT JDB Exploit Kit JAR Download", "ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct M2 Feb 06 2015", "ET EXPLOIT_KIT CritXPack Jar Request", "ET EXPLOIT_KIT KaiXin Landing Page Oct 05 2015", "ET EXPLOIT_KIT Underminer EK IE Exploit", "ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Jpg Request", "ET EXPLOIT_KIT Possible Glazunov Java payload request /5-digit", "ET EXPLOIT_KIT Underminer EK Resource File Download M2", "ET EXPLOIT_KIT Bingo EK Payload Download", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole Content form tag appended to head", "ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 3 M1", "ET EXPLOIT_KIT Sakura exploit kit exploit download request /nano.php", "ET EXPLOIT_KIT SNET EK Encoded VBS 1", "ET EXPLOIT_KIT Unknown Bleeding EK Variant Landing Sep 06 2013", "ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 05 2016", "ET EXPLOIT_KIT Terror EK Landing M1 Feb 07 2016 M1", "ET EXPLOIT_KIT Probable Sakura exploit kit landing page obfuscated applet tag Mar 28 2013", "ET EXPLOIT_KIT RIG EK Rip Sep 05 2017", "ET EXPLOIT_KIT Neutrino Exploit Kit Redirector To Landing Page", "ET INFO Serialized Java Applet (Used by some EKs in the Wild)", "ET EXPLOIT_KIT Capesand EK Visitor Tracking", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 2 (Reversed)", "ET EXPLOIT_KIT Fiesta SilverLight Exploit Download", "ET EXPLOIT_KIT Redirect on ActiveXObject support", "ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M1", "ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017", "ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b643)", "ET EXPLOIT_KIT Possible Magnitude IE EK Payload Nov 8 2013", "ET EXPLOIT_KIT Unknown_gmf EK - pdfx.html", "ET EXPLOIT_KIT Suspicious GitHack DNS Request - Possible PurpleFox EK", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated Click To Run Bypass", "ET EXPLOIT_KIT Nuclear Exploit Kit exe.exe Payload", "ET EXPLOIT_KIT LightsOut EK POST Compromise POST", "ET EXPLOIT_KIT Sibhost Zip as Applet Archive July 08 2013", "ET EXPLOIT_KIT Spelevo EK Landing M3", "ET EXPLOIT_KIT Possible Spartan/Nuclear EK Payload", "ET EXPLOIT_KIT Possible Astrum EK URI Struct", "ET EXPLOIT_KIT Disdain EK Flash Exploit M1 Aug 23 2017", "ET EXPLOIT_KIT EITest Evil Redirect Leading to EK Feb 01 2016", "ET EXPLOIT_KIT SunDown EK CVE-2016-0189 Sep 22 2016 (b643)", "ET EXPLOIT_KIT EITest Inject July 25 2017", "ET INFO JAR Sent Claiming To Be Text Content - Likely Exploit Kit", "ET EXPLOIT_KIT suspicious VBE-encoded script (seen in Sundown EK)", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b645)", "ET EXPLOIT_KIT Possible RedDotv2 applet with 32hex value Landing Page", "ET EXPLOIT_KIT TDS Sutra - HTTP header redirecting to a SutraTDS", "ET EXPLOIT_KIT NuclearPack - Landing Page Received - applet archive=32CharHex", "ET EXPLOIT_KIT DRIVEBY Possible Goon/Infinity/Magnitude EK SilverLight Exploit", "ET EXPLOIT_KIT

	Magnitude EK (formerly Popads) Flash Exploit Requested", "ET EXPLOIT_KIT Underminer EK Key POST", "ET EXPLOIT_KIT Terror EK Payload URI T1 Jun 02 2017 M2", "ET EXPLOIT_KIT Spelevo EK Post-Compromise Data Dump", "ET EXPLOIT_KIT HanJuan EK Current Campaign Landing URI Struct Jul 10 2015", "ET EXPLOIT_KIT Redkit Landing Page URL March 03 2013", "ET EXPLOIT_KIT NeoSploit Jar with three-letter class names", "ET EXPLOIT_KIT Sakura Exploit Kit Version 1.1 Archive Request", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 3", "ET EXPLOIT_KIT Possible PurpleFox EK Framework Payload", "ET EXPLOIT_KIT RIG EK Landing Sep 12 2016 T2", "ET EXPLOIT_KIT Possible Dynamic Dns Exploit Pack Java exploit", "ET EXPLOIT_KIT Base64 http argument in applet (Neutrino/Angler)", "ET EXPLOIT_KIT DRIVEBY FlashPack Plugin-Detect May 13 2014", "ET EXPLOIT_KIT RIG EK Rip Sep 05 2017 M2", "ET EXPLOIT_KIT Unkown exploit kit pdf download", "ET EXPLOIT_KIT RIG Payload URI Struct March 20 2015", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole function return value", "ET EXPLOIT_KIT Evil Redirector Leading to EK Dec 09", "ET EXPLOIT_KIT RIG EK Payload Jul 05 2016", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b642)", "ET INFO JAR Sent Claiming To Be Image - Likely Exploit Kit", "ET EXPLOIT_KIT TDS Sutra - redirect received", "ET EXPLOIT_KIT SSL Cert Used In Unknown Exploit Kit (ashburn)", "ET WEB_CLIENT Injected iframe leading to Redkit Jan 02 2013", "ET EXPLOIT_KIT Nuclear EK PDF URI Struct", "ET EXPLOIT_KIT Unknown EK Secondary Landing Page May 01 2015 M1", "ET EXPLOIT_KIT Unknown EK Fake Microsoft Security Update Applet Sep 16 2013", "ET EXPLOIT_KIT [PTsecurity] Grandsoft EK Payload", "ET EXPLOIT_KIT TDS Sutra - request in.cgi", "ET EXPLOIT_KIT DRIVEBY Incognito Payload Download /load/*exe", "ET EXPLOIT_KIT phoenix exploit kit - admin login page detected", "ET EXPLOIT_KIT Unknown EK Secondary Landing Page May 01 2015 M2", "ET EXPLOIT_KIT Zuponcic Hostile JavaScript", "ET EXPLOIT_KIT SunDown EK RIP Landing M1 B643", "ET EXPLOIT_KIT Styx Exploit Kit Payload Download", "ET EXPLOIT_KIT CoolEK Payload Download (5)", "ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 08", "ET EXPLOIT_KIT Evil Redirector Leading to EK Mon Dec 21 2015 5", "ET EXPLOIT_KIT Nuclear EK Gate Sep 16 2014", "ET EXPLOIT_KIT DotkaChef EK initial landing from Oct 02 2013 mass-site compromise EK campaign", "ET EXPLOIT_KIT Phoenix Exploit Kit VBscript download", "ET EXPLOIT_KIT Probable Sakura exploit kit landing page with obfuscated URLs", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 3 (Reversed)", "ET EXPLOIT_KIT Fiesta EK Landing Nov 05 2014", "ET EXPLOIT_KIT Sakura Landing with Applet Aug 30 2013", "ET EXPLOIT_KIT NeoSploit - Version Enumerated - Java", "ET EXPLOIT_KIT GrandSoft EK IE Exploit Jan 30 2018", "ET EXPLOIT_KIT DRIVEBY Generic - 8Char.JAR Naming Algorithm", "ET EXPLOIT_KIT Redirect to DotkaChef EK Landing", "ET EXPLOIT_KIT ScanBox Jun 06 2015 M3 T1", "ET EXPLOIT_KIT Nuclear SilverLight URI Struct (noalert)", "ET EXPLOIT_KIT JDB Exploit Kit Fake Adobe Download", "ET EXPLOIT_KIT Java File Sent With X-Powered By HTTP Header - Common In Exploit Kits", "ET EXPLOIT_KIT Disdain EK URI Struct Aug 23 2017 M1", "ET MALWARE PurpleFox EK Landing Page Domain in SNI", "ET EXPLOIT_KIT SUSPICIOUS Request for Grey Advertising Often Leading to EK", "ET EXPLOIT_KIT Possible Nicepack EK Landing (Anti-VM)", "ET EXPLOIT_KIT Sweet Orange Landing Page Dec 09 2013", "ET EXPLOIT_KIT Magnitude/Hunter EK IE Exploit Aug 23 2015", "ET EXPLOIT_KIT Possible PurpleFox EK Framework Flash GET Request", "ET EXPLOIT_KIT Fiesta EK Flash Exploit Apr 23 2015", "ET EXPLOIT_KIT RIG encrypted payload M1 Aug 01 2017", "ET EXPLOIT_KIT Possible Broken/Filtered RIG EK Payload Download", "ET EXPLOIT_KIT Evil Redirect Leading to EK Mar 18 2016", "ET EXPLOIT_KIT Terror EK CVE-2015-2419 Exploit", "ET EXPLOIT_KIT Disdain EK Flash Exploit M2 Aug 23 2017", "ET EXPLOIT_KIT Unknown Java Exploit Kit 32-32 byte hex initial landing", "ET EXPLOIT_KIT Fiesta EK SilverLight Exploit Apr 23 2015", "ET HUNTING suspicious embedded zip file in web page", "ET EXPLOIT_KIT Terror EK Payload RC4 Key M1 Mar 14 2017", "ET MALWARE Cryptowall docs campaign Sept 2015 encrypted binary (1)", "ET EXPLOIT_KIT Unknown Malvertising Exploit Kit Hostile Jar app.jar", "ET EXPLOIT_KIT Disdain EK Landing Aug 23 2017", "ET EXPLOIT_KIT Possible Sundown EK Payload Struct T2 M1 Apr 24 2015", "ET EXPLOIT_KIT Spelevo EK Landing M2", "ET EXPLOIT_KIT Magnitude EK

	Landing M1 Aug 05 2017", "ET EXPLOIT_KIT RIG EK - Unexpected Victim Location Server Response", "ET EXPLOIT_KIT Possible PurpleFox EK Redirect M2", "ET EXPLOIT_KIT CritXPack Landing Page", "ET EXPLOIT_KIT BegOpEK - Landing Page", "ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 28 2016", "ET EXPLOIT_KIT Disdain EK Payload Aug 23 2017", "ET EXPLOIT_KIT Internet Explorer Information Disclosure Vuln as Observed in RIG EK Prefilter M1 Dec 06", "ET EXPLOIT_KIT Sakura/RedKit obfuscated URL", "ET EXPLOIT_KIT HellSpawn EK Landing 1 May 24 2013", "ET EXPLOIT_KIT Cool Java Exploit Recent Jar (1)", "ET EXPLOIT_KIT Terror EK Payload Download M1 Mar 14 2017", "ET EXPLOIT_KIT RIG EK encrypted payload Sept 11 (1)", "ET MALWARE Karagany encrypted binary (3)", "ET EXPLOIT_KIT Underminer EK Flash/WAV Loader", "ET EXPLOIT_KIT SofosFO obfuscator string 19 Dec 12 - possible landing", "ET EXPLOIT_KIT StyX Landing Page", "ET EXPLOIT_KIT RIG EK Landing Feb 26 2016", "ET EXPLOIT_KIT Fiesta EK IE Exploit Apr 23 2015", "ET EXPLOIT_KIT Incognito Exploit Kit Checkin", "ET EXPLOIT_KIT Possible JDB Exploit Kit Class Request", "ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017", "ET EXPLOIT_KIT DRIVEBY Nuclear EK IE Exploit CVE-2013-2551 March 12 2014", "ET EXPLOIT_KIT Exploit Kit Delivering JAR Archive to Client", "ET EXPLOIT_KIT Bingo Exploit Kit Landing May 08 2017", "ET EXPLOIT_KIT Fiesta SilverLight 5.x Exploit URI Struct", "ET EXPLOIT_KIT KaiXin Landing M3", "ET EXPLOIT_KIT DRIVEBY SPL - Landing Page Received", "ET EXPLOIT_KIT Sakura Exploit Kit Binary Load Request", "ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated Click To Run Bypass (Reversed)", "ET EXPLOIT_KIT Evil Redirector Leading to EK September 04 2015", "ET EXPLOIT_KIT - Landing Page Requested - 15Alpha1Digit.php", "ET EXPLOIT_KIT TDS Sutra - cookie set RULEZ", "ET EXPLOIT_KIT Fiesta URI Struct", "ET EXPLOIT_KIT Evil Redirect Leading to EK Jul 28 2016", "ET EXPLOIT_KIT RIG Landing URI Struct March 20 2015", "ET EXPLOIT_KIT RIG EK Payload Jun 26 2016", "ET EXPLOIT_KIT Suspicious JS Observed in Unknown EK Landing", "ET EXPLOIT_KIT Document.write Long Backslash UTF-16 Encoded Content - Exploit Kit Behavior Flowbit Set", "ET EXPLOIT_KIT BottleEK Plugin Check JS", "ET EXPLOIT_KIT Sundown EK Secondary Landing Apr 20 2015", "ET EXPLOIT_KIT Sweet Orange Landing with Applet Sep 30 2013", "ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing May 05 2014", "ET EXPLOIT_KIT Hostile Gate landing seen with pamdql/Sweet Orange base64", "ET EXPLOIT_KIT KaiXin Landing M4", "ET EXPLOIT_KIT Possible Sakura Exploit Kit Version 1.1 document.write Fake 404 - Landing Page", "ET EXPLOIT_KIT SNET EK Encoded VBS 2", "ET EXPLOIT_KIT RIG EK Broken/Filtered Payload Download Jun 19 2017", "ET EXPLOIT_KIT Evil Redirector Leading to EK March 15 2017", "ET EXPLOIT_KIT ElTest Exploit Kit Redirection Script", "ET EXPLOIT_KIT Unknown_MM EK - Landing Page", "ET EXPLOIT_KIT Possible PurpleFox EK Redirect", "ET EXPLOIT_KIT SunDown EK RIP Landing M4 B642", "ET EXPLOIT_KIT Possible Archie/Metasploit SilverLight Exploit", "ET EXPLOIT_KIT Possible Styx EK SilverLight Payload", "ET EXPLOIT_KIT SunDown EK RIP Landing M3 B641", "ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Flash Request", "ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox and Targetted Watering Holes ActiveX Call", "ET EXPLOIT_KIT SUSPICIOUS DNS Request for Grey Advertising Often Leading to EK", "ET EXPLOIT_KIT DRIVEBY Generic - Redirection to Kit - BrowserDetect with var stopit", "ET EXPLOIT_KIT Underminer EK Plugin Check", "ET EXPLOIT_KIT Possible Dynamic DNS Exploit Pack Landing Page /de/sN", "ET EXPLOIT_KIT Wordpress timthumb look-alike domain list RFI", "ET HUNTING SUSPICIOUS Java Lang Runtime in Response", "ET EXPLOIT_KIT - Possible Redkit 1-4 char JNLP request", "ET EXPLOIT_KIT ScanBox Jun 06 2015 M1 T1", "ET EXPLOIT_KIT Spelevo VBS Payload Downloaded", "ET EXPLOIT_KIT Evil Flash Redirector to RIG EK Dec 17 2014", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b643)", "ET EXPLOIT_KIT Possible Internet Explorer CVE-2014-6332 Common Construct b64 2 (Observed in Archie EK)", "ET EXPLOIT_KIT MWI Maldoc Exploit Kit Stats Callout", "ET EXPLOIT_KIT BHEK Payload Download (java only alternate method may overlap with 2017454)", "ET EXPLOIT_KIT Fiesta Flash Exploit URI Struct", "ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b644)"
PT Open	"ATTACK [pt-open] Drupalgeddon2 <8.3.9 <8.4.6 <8.5.1 RCE through registration form (CVE-2018-7600)", "MALWARE [pt-open] Pegasus (Buhtrap/Ratopak) domain

	replication remote pipe check", "MALWARE [PTsecurity] Backdoor.Java.Adwind.cu", "ATTACK [pt-open] WordPress Plugin LearnDash LMS <2.5.4 Arbitrary file upload", "ATTACK [pt-open] Apache Struts 2.3.20-2.3.28.1 Privilege Escalation attempt", "ATTACK [pt-open] Apache2 <2.2.34 <2.4.27 Optionsbleed (CVE-2017-9798) Attempt", "ATTACK [pt-open] ISC BIND DNS TSIG authentication bypass successful (CVE-2017-3143)", "MALWARE [pt-open] Bayrob pkt checker #0", "ATTACK [pt-open] DHCP Client Script WPAD option OS Command Injection (CVE-2018-1111)", "ATTACK [pt-open] Omnivista 8770 UnAuth RCE (AddJobSet)", "MALWARE [pt-open] RemoteAdmin.RemoteUtilities pkt checker #0", "ATTACK [pt-open] Mikrotik <6.42 Password disclosure path traversal (CVE-2018-14847)", "ATTACK [pt-open] Exim <4.90.1 Base64 Overflow RCE (CVE-2018-6789)", "SCAN [pt-open] Neutrino shell probing die(@md5(", "MALWARE [pt-open] Tofsee.bot connection detected", "MALWARE [pt-open] RemoteAdmin.RemoteUtilities pkt checker #1", "ATTACK [pt-open] Exim 4.88, 4.89 UAF RCE Attempt (CVE-2017-16943)", "MALWARE [pt-open] Tofsee.bot pkt57 connection", "SCAN [pt-open] Neutrino shell probing die(md5(", "MALWARE [pt-open] Win32.Backdoor.Zegost.Auto connection pkt checker #0", "ATTACK [pt-open] Dnsmasq <2.78 Heap Based Buffer Overflow (CVE-2017-14492)", "ATTACK [pt-open] Nagios Core < 4.2.2 Curl Command Injection (CVE-2016-9565) RSS Request", "MALWARE [pt-open] Bayrob pkt checker #3", "ATTACK [pt-open] FreePBX 13/14 Remote Command Execution", "MALWARE [pt-open] Babylon RAT pkt checker #0", "MALWARE [pt-open] REMCOS pkt checker 1", "MALWARE [pt-open] Linux/BillGates pkt checker #0", "ATTACK [pt-open] Magento < 2.0.6 Arbitrary write file", "ATTACK [pt-open] Nfcapd DoS attempt caused inifinite loop", "ATTACK [pt-open] Mikrotik <6.41.3 <6.42rc27 RCE Attempt (CVE-2018-7445)", "ATTACK [pt-open] MS IIS 6.0 BO RCE (CVE-2017-7269)", "MALWARE [pt-open] Babylon RAT pkt checker #1", "ATTACK [pt-open] Nfcapd buffer overflow via incorrect flowset_length field attempt", "ATTACK [pt-open] MS RDP CredSSP Remote Code Execution MitM (CVE-2018-0886)", "ATTACK [pt-open] Mikrotik Router OS 6.38.4 Stack Clash RCE", "MALWARE [PTsecurity] Dyre/Trickbot/Dridex SSL connection #2", "MALWARE [pt-open] Cybergate/Rebhip/Spyrat Backdoor", "MALWARE [pt-open] LanternVPN connection pkt checker #1", "ATTACK [pt-open] Arbitrary PHP RCE in Drupal 8 < 8.5.11,8.6.10 (CVE-2019-6340)", "ATTACK [pt-open] ShellCode Upload Mikrotik <6.41.3 <6.42rc27 RCE (CVE-2018-7445)", "MALWARE [pt-open] Win32.Backdoor.Zegost.Auto connection", "ATTACK [pt-open] SMB2 Create PSEXESVC.EXE", "MALWARE [PTsecurity] Dyre/Trickbot/Dridex SSL connection #0", "MALWARE [pt-open] Backdor.W32/Virut", "MALWARE [PTsecurity] Silent Trinity pkt checker #0", "ATTACK [PTsecurity] Spring Core RCE aka Spring4Shell Attempt", "MALWARE [pt-open] REMCOS pkt checker 2", "ATTACK [pt-open] FreePBX 13/14 Remote Command Execution attempt", "MALWARE [pt-open] Bayrob pkt checker #1", "MALWARE [pt-open] Ozone RAT connection", "MALWARE [pt-open] LanternVPN connection pkt checker #0", "MALWARE [pt-open] Cybergate/Rebhip/Spyrat pkt checker #3", "ATTACK [pt-open] NT Trans Response", "MALWARE [PTsecurity] Silent Trinity RAT (post-exploitation agent)", "MALWARE [pt-open] Pegasus (Buhtrap/Ratopak) C2 connection", "MALWARE [pt-open] REMCOS pkt checker 3", "ATTACK [pt-open] EpicBanana Exploitation", "MALWARE [pt-open] Bayrob", "ATTACK [pt-open] Possible Dnsmasq <2.78 DHCPv6 Link Layer Address Stack Overflow (CVE-2017-14493)", "ATTACK [pt-open] Attempt to crash named using malformed RNDC packet", "ATTACK [pt-open] Spring AMQP <1.7.4, 1.6.11, 1.5.7 Java Object Deserialization RCE (CVE--2017-8045)", "MALWARE [pt-open] Backdor.W32/Virut pkt checker #1", "MALWARE [pt-open] AMMYY RAT pkt checker #0", "MALWARE [pt-open] LanternVPN connection pkt checker #4", "ATTACK [pt-open] Metasploit MS17-010 ETERNALCHAMPION Successful kernel data leak (CVE-2017-0146)", "MALWARE [pt-open] Win32/Lethic.AF", "ATTACK [pt-open] PHP7 x86 heap overflow attempt via crafted zip archive", "ATTACK [pt-open] Raisecom GPON RCE via command injection (CVE-2019-7384)", "MALWARE [pt-open] Cybergate/Rebhip/Spyrat pkt checker #0", "ATTACK [pt-open] DHCP Client Script WPAD option Exploit (CVE-2018-1111)", "MALWARE [pt-open] Backdor.W32/Virut pkt checker #0", "MALWARE [pt-open] Pegasus (Buhtrap/Ratopak) credentials broadcast via Mailslot", "MALWARE [PTsecurity]

	Backdoor.Java.Adwind.cu pkt Checker flowbit set 4", "ATTACK [pt-open] FreePBX 13/14 Malicious Filename Upload attempt", "ATTACK [pt-open] PHPMyAdmin web shell planting with log redirection", "ATTACK [pt-open] Petya ransomware perfc.dat component", "ATTACK [pt-open] Apple macOS 10.12.1/iOS 10 OCSP DDoS Attempt (CVE-2016-7636)", "MALWARE [pt-open] AMMYY RAT pkt checker #1", "ATTACK [pt-open] Buffer Overflow via Negative HTTP Chunk size number (FFMPEG CVE-2016-10190, WGET CVE-2017-13089, CVE-2017-13090)", "ATTACK [pt-open] Metasploit MS17-010 ETERNALBLUE Exploitation (CVE-2017-0144)", "ATTACK [PTsecurity] log4j RCE aka Log4Shell successful. Malicious LDAP response (CVE-2021-44228)", "ATTACK [pt-open] Cisco Adaptive Security Appliance 8.x SNMP overflow RCE Attempt", "ATTACK [pt-open] Modx Revolution CMS < 2.6.4 RCE by PoC (CVE-2018-1000207)", "ATTACK [pt-open] Drupalgeddon2 <7.5.9 <8.4.8 <8.5.3 RCE (CVE-2018-7602)", "MALWARE [pt-open] Bunitu.Proxy pkt checker #0", "ATTACK [PTsecurity] log4j RCE aka Log4Shell attempt (CVE-2021-44228)", "MALWARE [pt-open] PowerShell Empire Request HTTP Pattern", "MALWARE [pt-open] Linux/BillGates pkt checker #1", "MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 3", "ATTACK [pt-open] MySQL <= 5.7.15, 5.6.33, 5.5.53 root RCE/Privilege Escalation attempt", "ATTACK [PTSecurity] Cisco ASA and Cisco FTD possible DoS (CVE-2018-15454)", "MALWARE [pt-open] RemoteAdmin.RemoteUtilities pkt checker #3", "MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 2", "MALWARE [pt-open] Bunitu.Proxy", "ATTACK [pt-open] MikroTik Firewall & NAT Bypass (CVE-2019-3924)", "MALWARE [pt-open] LanternVPN connection pkt checker #2", "MALWARE [pt-open] Babylon RAT (Dodiw.A VT) Check-in", "MALWARE [pt-open] Backdoor.Win32/Remcos RAT connection", "ATTACK [pt-open] Webexservice remote priveleged command execution (CVE-2018-15442)", "MALWARE [pt-open] Babylon RAT C2 conversation pkt checker #2", "MALWARE [pt-open] Babylon RAT C2 Client Request", "MALWARE [pt-open] Babylon RAT unset", "MALWARE [pt-open] Neutrino Bot Check-in", "ATTACK [pt-open] Apache Portals Pluto 3.0.0 RCE (CVE-2018-1306)", "ATTACK [pt-open] ISC BIND DNS TSIG authentication bypass attempt (CVE-2017-3143, HMAC_SHA256)", "ATTACK [pt-open] GitHub Electron <1.8.2-beta.4, <1.7.11, <1.6.16 protocol handler RCE (CVE-2018-1000006)", "ATTACK [pt-open] Nfcapd buffer overflow with large scope_field_count field attempt", "ATTACK [pt-open] GraphicsMagick popen shell vulnerability", "MALWARE [pt-open] Tofsee.bot pkt200 connection", "ATTACK [pt-open] SVN/Git Remote Code Execution through malicious (svn+,git+)ssh:// URL (Multiple CVEs)", "ATTACK [pt-open] SAP NetWeaver AS Java UDDI 7.11-7.50 SQL Injection (CVE-2016-2386)", "ATTACK [pt-open] Successful Mikrotik <6.41.3 <6.42rc27 RCE (CVE-2018-7445)", "MALWARE [pt-open] Tofsee.bot pkt97 sequence", "ATTACK [pt-open] Cisco Adaptive Security Appliance 8.x SNMP overflow RCE Probe", "ATTACK [pt-open] Nagios Core < 4.2.2 Curl Command Injection (CVE-2016-9565) Attempt", "ATTACK [pt-open] MS Edge WScript Command Injection RCE (CVE-2018-8495)", "ATTACK [pt-open] Cisco Smart Install 15.2(5)E RCE (CVE-2018-0171)", "MALWARE [pt-open] Bayrob detected ", "MALWARE [pt-open] Bayrob pkt checker #2", "MALWARE [PTsecurity] Silent Trinity pkt checker #1", "ATTACK [pt-open] LSASS Remote Memory Corruption Successful LSASS Inf. loop (MS16-137)", "ATTACK [pt-open] Apache2 <2.2.34 <2.4.27 Optionsbleed (CVE-2017-9798) Leak", "ATTACK [pt-open] GitStack Arbitrary PHP upload RCE (CVE-2018-5955)", "MALWARE [pt-open] Babylon RAT C2 Server Response", "ATTACK [pt-open] Metasploit MS17-010 ETERNALCHAMPION. Non-Fragmented NT Trans Request with command NT Rename (CVE-2017-0146)", "ATTACK [pt-open] Jenkins sandbox bypassing RCE (CVE-2019-1003000/1/2)", "ATTACK [pt-open] Samba RCE exploitation attempt (SambaCry)", "ATTACK [pt-open] Nagios Core < 4.2.2 Curl Command Injection (CVE-2016-9565) Remote Script Execution", "ATTACK [pt-open] iOS 10.1.x Remote memory corruption through certificate file Attempt", "MALWARE [pt-open] Bunitu.Proxy pkt checker #1", "ATTACK [pt-open] Kibana < 6.4.3 <5.6.13 Arbitrary File Inclusion/Disclosure/RCE attempt (CVE-2018-17245)", "MALWARE [pt-open] Win32/Lethic.AF connection pkt checker #0", "MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 5", "ATTACK [pt-open] LSASS Remote Memory Corruption Attempt (MS16-137)", "ATTACK [pt-open] BadTunnel NBNS

	response after NBSTAT query", "ATTACK [pt-open] Omnivista 8770 UnAuth RCE (AddJob)", "ATTACK [pt-open] Raisecom GPON RCE via command injection (CVE-2019-7385)", "ATTACK [pt-open] Remote WMI Win32_Process create", "MALWARE [PTsecurity] Backdoor.Java.Adwind.cu Certificate flowbit set 1", "INFO [pt-open] DNS RRSIG without covered RR (CVE-2016-9147)", "ATTACK [pt-open] Metasploit MS17-010 ETERNALROMANCE exploitation (CVE-2017-0143)", "ATTACK [pt-open] Webexservice Service Probe (CVE-2018-15442)", "MALWARE [pt-open] Cybergate/Rebhip/Spyrat pkt checker #1", "ATTACK [pt-open] Cisco Prime Infrastructure < 3.4.1 & 3.3.1 TFTP RCE (CVE-2018-15379)", "MALWARE [pt-open] RemoteAdmin.RemoteUtilities pkt checker #2", "MALWARE [pt-open] PowerShell Empire stager receive over HTTP", "ATTACK [pt-open] Mismatch URI and Host header. Possible Squid cache poisoning", "MALWARE [pt-open] Cybergate/Rebhip/Spyrat pkt checker #2", "MALWARE [pt-open] Trojan.Ranapama.JH", "MALWARE [pt-open] REMCOS pkt checker 0", "MALWARE [pt-open] Backdor.W32/Virut pkt checker #2", "ATTACK [pt-open] Omnivista 8770 UnAuth RCE (ExecuteNow)", "ATTACK [pt-open] Apache Continuum <= v1.4.2 CMD Injection", "MALWARE [pt-open] Win32/Lethic.AF connection pkt checker #1", "ATTACK [pt-open] Suspicious Remote WMI Win32_Process create", "ATTACK [pt-open] Possible Mikcrotik Router OS 6.38.4 Stack Clash RCE", "ATTACK [pt-open] Flowbits for SMB NTTrans Request", "MALWARE [pt-open] Bayrob pkt sequence detected set", "ATTACK [pt-open] Possible HTTPoxy HTTP_PROXY value spoofing", "ATTACK [pt-open] PHP Object Deserialization RCE POP Chain (Guzzle/RCE1)", "ATTACK [pt-open] Apache Struts < 2.3.32 < 2.5.10.1 RCE through Jakarta Multipart parser Attempt", "ATTACK [pt-open] Safari 10.0.3 UAF RCE (CVE-2017-2491)", "MALWARE [pt-open] Win32/RemoteAdmin.RemoteUtilities pkt checker #4", "ATTACK [pt-open] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool", "MALWARE [pt-open] Ozone RAT connection pkt#0", "MALWARE [PTsecurity] Dyre/Trickbot/Dridex SSL connection #1", "ATTACK [pt-open] GNU Wget < 1.18 Arbitrary File Upload / Potential Remote Code Execution", "ATTACK [pt-open] GNU Wget http request", "MALWARE [pt-open] Trojan.Ranapama.JH pkt checker #0", "MALWARE [pt-open] Trojan.Ranapama.JH pkt checker #1", "MALWARE [pt-open] LanternVPN connection pkt checker #3", "ATTACK [pt-open] Metasploit MS17-010 ETERNALCHAMPION Race Condition Exploit. NT Trans Secondary packet follows NT Trans Req (CVE-2017-0146)", "ATTACK [pt-open] Possible Dnsmasq <2.78 DHCPv6 Sensitive info leak (CVE-2017-14494)", "ATTACK [PTsecurity] Windows Server DNS RCE aka SIGRed (CVE-2020-1350) - Query response", "ATTACK [pt-open] MS Exchange 2010-2019 Possible privilege escalation (CVE-2018-8581)", "MALWARE [pt-open] Linux/BillGates", "MALWARE [pt-open] Linux/BillGates pkt checker #2"
GeoIP защита от удаленных подключений	"GeoIP TCP remote connect to 443 from DE", "GeoIP TCP remote connect to 443 from NL", "GeoIP TCP remote connect to 2443 from AU", "GeoIP TCP remote connect to 3443 from RO", "GeoIP TCP remote connect to 4443 from ES", "GeoIP UDP remote connect to 500 from DE", "GeoIP TCP remote connect to 3443 from TW", "GeoIP UDP remote connect to 4500 from NL", "GeoIP TCP remote connect to 22 from TW", "GeoIP TCP remote connect to 3443 from CN", "GeoIP UDP remote connect to 4500 from AU", "GeoIP UDP remote connect to 4500 from PT", "GeoIP UDP remote connect to 4500 from TW", "GeoIP TCP remote connect to 2443 from UA", "GeoIP UDP remote connect to 4500 from ES", "GeoIP TCP remote connect to 1443 from JP", "GeoIP TCP remote connect to 22 from RO", "GeoIP TCP remote connect to 1723 from PT", "GeoIP TCP remote connect to 1723 from NL", "GeoIP TCP remote connect to 3443 from PT", "GeoIP TCP remote connect to 1443 from AU", "GeoIP TCP remote connect to 3443 from NL", "GeoIP TCP remote connect to 443 from CN", "GeoIP TCP remote connect to 22 from JP", "GeoIP TCP remote connect to 4443 from DE", "GeoIP TCP remote connect to 2443 from DE", "GeoIP TCP remote connect to 22 from ES", "GeoIP TCP remote connect to 1443 from NL", "GeoIP TCP remote connect to 1723 from AU", "GeoIP UDP remote connect to 4500 from DE", "GeoIP UDP remote connect to 4500 from CN", "GeoIP UDP remote connect to 500 from RO", "GeoIP TCP remote connect to 2443 from RO", "GeoIP TCP remote connect to 4443 from NL", "GeoIP TCP remote connect to 4443 from PT", "GeoIP TCP remote connect to 3443 from DE", "GeoIP TCP remote

	connect to 22 from NL", "GeoIP TCP remote connect to 2443 from JP", "GeoIP UDP remote connect to 500 from TW", "GeoIP UDP remote connect to 4500 from UA", "GeoIP TCP remote connect to 22 from UA", "GeoIP TCP remote connect to 1443 from TW", "GeoIP TCP remote connect to 1443 from RO", "GeoIP TCP remote connect to 443 from UA", "GeoIP TCP remote connect to 443 from PT", "GeoIP TCP remote connect to 1723 from ES", "GeoIP TCP remote connect to 2443 from CN", "GeoIP TCP remote connect to 3443 from JP", "GeoIP TCP remote connect to 1723 from TW", "GeoIP TCP remote connect to 1723 from RO", "GeoIP TCP remote connect to 2443 from TW", "GeoIP TCP remote connect to 1443 from PT", "GeoIP UDP remote connect to 500 from JP", "GeoIP UDP remote connect to 500 from PT", "GeoIP TCP remote connect to 443 from AU", "GeoIP TCP remote connect to 1443 from ES", "GeoIP UDP remote connect to 4500 from RO", "GeoIP UDP remote connect to 500 from AU", "GeoIP TCP remote connect to 1723 from DE", "GeoIP TCP remote connect to 443 from JP", "GeoIP TCP remote connect to 3443 from ES", "GeoIP UDP remote connect to 4500 from JP", "GeoIP TCP remote connect to 4443 from AU", "GeoIP TCP remote connect to 22 from CN", "GeoIP TCP remote connect to 443 from ES", "GeoIP TCP remote connect to 1443 from UA", "GeoIP UDP remote connect to 500 from NL", "GeoIP TCP remote connect to 22 from PT", "GeoIP UDP remote connect to 500 from CN", "GeoIP TCP remote connect to 1443 from CN", "GeoIP TCP remote connect to 1443 from DE", "GeoIP TCP remote connect to 3443 from UA", "GeoIP TCP remote connect to 4443 from TW", "GeoIP TCP remote connect to 2443 from ES", "GeoIP TCP remote connect to 3443 from AU", "GeoIP TCP remote connect to 4443 from JP", "GeoIP TCP remote connect to 1723 from JP", "GeoIP TCP remote connect to 443 from RO", "GeoIP UDP remote connect to 500 from UA", "GeoIP TCP remote connect to 4443 from CN", "GeoIP TCP remote connect to 2443 from PT", "GeoIP UDP remote connect to 500 from ES", "GeoIP TCP remote connect to 1723 from CN", "GeoIP TCP remote connect to 443 from TW", "GeoIP TCP remote connect to 22 from AU", "GeoIP TCP remote connect to 2443 from NL", "GeoIP TCP remote connect to 4443 from RO", "GeoIP TCP remote connect to 1723 from UA", "GeoIP TCP remote connect to 22 from DE", "GeoIP TCP remote connect to 4443 from UA"
Попытки сканирования сети	"ET SCAN RDP Connection Attempt from Nmap", "ET SCAN NETWORK Incoming Masscan detected", "ET WEB_SERVER IIS 8.3 Filename With Wildcard (Possible File/Dir Bruteforce)", "GPL SCAN SSH Version map attempt", "ET SCAN SSH BruteForce Tool with fake PUTTY version", "ET SCAN WordPress HelloThinkCMF Scan", "ET SCAN Grim's Ping ftp scanning tool", "ET WEB_SERVER Fake Googlebot UA 2 Inbound", "ET SCAN crimscanner User-Agent detected", "ET SCAN DNS Query for allports.exposed", "GPL SCAN SolarWinds IP scan attempt", "ET SCAN WordPress Scanner Performing Multiple Requests to Windows Live Writer XML", "ET SCAN NYU Internet Census UA Inbound", "ET SCAN ICMP =XXXXXXXX Likely Precursor to Scan", "ET SCAN Zmap User-Agent (Inbound)", "ET POLICY ASafaWeb Scan User-Agent (asafaweb.com)", "SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)", "ET SCAN NETWORK Outgoing Masscan detected", "ET SCAN H.323 Scanning device", "ET INFO NYU Internet HTTP/SSL Census Scan"
GeoIP Территории Африки и зависимые территории	"GeoIP Территорий Африки и зависимые src,территории", "GeoIP Территорий Африки и зависимые dst,территории"
Атаки на web-приложения	"ET WEB_SPECIFIC_APPS Apache Archive deleteArtifact script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress Contact Form Maker Plugin - SQL Injection 1", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In UPDATE", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id UPDATE", "ET WEB_SPECIFIC_APPS TCExam tce_xml_user_results.php script SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- meal_rest.asp mealid ASCII", "ET WEB_SPECIFIC_APPS WHCMS banco Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id DELETE", "ET WEB_SPECIFIC_APPS 2z Project SQL

	Injection Attempt -- rating.php rating INSERT", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS Kalptaru Infotech Automated Link Exchange Portal cat_id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid UNION SELECT", "ET WEB_SPECIFIC_APPS DaFun Spirit lgsl_players.php lgsl_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country UPDATE", "ET WEB_SPECIFIC_APPS User Agent (SQLi Injection / Scanning)", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-trackback.php INSERT", "ET WEB_SPECIFIC_APPS WordPress Video Lead Form plugin errMsg parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id DELETE", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category UPDATE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite ASCII", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id INSERT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_jshop pid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! JoomlaFacebook Component DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS vtiger CRM service parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid DELETE", "ET WEB_SPECIFIC_APPS phpBMS invoices_discount_ajax.php id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page UNION SELECT", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv DELETE", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category SELECT", "ET WEB_SPECIFIC_APPS SERWeb main_prepend.php functionsdir Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id UPDATE", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id SELECT", "ET WEB_SPECIFIC_APPS joomla com_edir controller parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid INSERT", "ET WEB_SERVER Possible HTTP 503 XSS Attempt (Internal Source)", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id ASCII", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid SELECT", "ET WEB_SPECIFIC_APPS IBM Possible Lotus Domino readme.nsf Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l DELETE", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details SELECT", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- index.php p_skin UNION SELECT", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id UNION SELECT", "ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli)", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php UPDATE", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name INSERT", "ET WEB_SPECIFIC_APPS PhotoSmash action Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS RecordPress rp-menu.php sess_user Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick INSERT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid UNION SELECT", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id SELECT", "ET WEB_SERVER Possible DROP SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas SELECT", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc SELECT", "ET WEB_SPECIFIC_APPS

	Aktueldownload Haber script SQL Injection Attempt -- rss.asp kid UNION SELECT", "ET WEB_SPECIFIC_APPS phpRS id parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter UNION SELECT SQL Injection Attempt", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (41)", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid DELETE", "ET WEB_SPECIFIC_APPS Jenkins Chained Exploits CVE-2018-1000861 and CVE-2019-1003000 M2", "ET WEB_SPECIFIC_APPS Joomla GoogleMaps Plugin Open Proxy Access", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title UNION SELECT", "ET WEB_SPECIFIC_APPS Interactive Web Solutions site_info.php UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer DELETE", "ET WEB_SPECIFIC_APPS HP System Management Homepage Input Validation Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Design4Online UserPages2 SQL Injection Attempt -- page.asp art_id INSERT", "ET WEB_SPECIFIC_APPS Design4Online UserPages2 SQL Injection Attempt -- page.asp art_id UNION SELECT", "ET WEB_SPECIFIC_APPS WeBid active_auctions.php lan Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- index.php p_skin DELETE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id INSERT", "ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (1)", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text ASCII", "ET WEB_SPECIFIC_APPS iGaming CMS reviews.php browse parameter SQL injection", "ET WEB_SPECIFIC_APPS NewSolved newsscript.php idneu Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid SELECT", "ET WEB_SPECIFIC_APPS MODx CMS snippet.reflect.php reflect_base Remote File Inclusion", "ET WEB_SPECIFIC_APPS Joomla portalid Component DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php UPDATE", "ET WEB_SPECIFIC_APPS Nuke Evolution Xtreme pid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre INSERT", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php template INSERT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid ASCII", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action SELECT", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType SELECT", "ET WEB_SERVER Joomla Component SQLi Attempt", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID DELETE", "ET WEB_SPECIFIC_APPS coRED CMS rubID Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat INSERT", "ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID INSERT", "ET WEB_SPECIFIC_APPS Joomla SQL Reports user_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod INSERT", "ET WEB_SPECIFIC_APPS Ideal MooFAQ Joomla Component file_includer.php file Parameter Local File Inclusion", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (44)", "ET WEB_SPECIFIC_APPS DVD Rental Software cat_id parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear UPDATE", "ET WEB_SPECIFIC_APPS Joomla Component com_jmsfileseller view Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS McAfee Email Gateway QtnType Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp INSERT", "ET

	WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct DELETE", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt -- cp_menu_data_file.php menu UPDATE", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id UNION SELECT", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-Old_Articles.php cat SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort INSERT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail SELECT", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- meal_rest.asp mealid INSERT", "ET WEB_SERVER Likely Malicious Request for /proc/<pid>/cmdline", "ET WEB_SPECIFIC_APPS Easebay Resources Login Manager SQL Injection Attempt -- memberlist.php init_row UNION SELECT", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id DELETE", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq UPDATE", "ET WEB_SPECIFIC_APPS WordPress Thinkun Remind Plugin dirPath Remote File Disclosure Vulnerability", "ET WEB_SPECIFIC_APPS RoseOnline CMS LFI Attempt", "ET PHISHING Apple Phishing Panel Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Shape Web Solutions imprimir.php UNION SELECT SQL Injection Attempt", "ET WEB_CLIENT Generic WSO Webshell Password Prompt Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp ASCII", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password UNION SELECT", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy UPDATE", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp year SELECT", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id INSERT", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php ASCII", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid UPDATE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat DELETE", "ET WEB_SPECIFIC_APPS Celepar module for Xoops aviso.php codigo SQL injection", "ET WEB_SPECIFIC_APPS Joomla com_jshop component pid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id SELECT", "ET WEB_SPECIFIC_APPS Fatwiki monatsblatt.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id UPDATE", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q ASCII", "ET WEB_SPECIFIC_APPS MyFusion last_seen_users_panel.php settings Parameter Local File Inclusion Attempt", "ET WEB_SERVER Possible Apache Struts OGNL Expression Injection", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass UNION SELECT", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id UNION SELECT", "ET WEB_SERVER HP LaserJet Printer Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke Surveys pollID parameter INSERT INTO SQL Injection Attempt", "ET WEB_SERVER PHP Possible data Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS VTiger CRM module_name parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf SELECT", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username UPDATE", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby INSERT", "ET WEB_SPECIFIC_APPS evision cms addnewsletter.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id UPDATE", "ET WEB_SERVER ImageMagick CVE-2016-3715 File Deletion Inbound (ephermeral:+ mvg)", "ET WEB_SPECIFIC_APPS WordPress Tune

	Library Plugin letter parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat DELETE", "ET WEB_SPECIFIC_APPS FireStats window-add-excluded-ip.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Possible Apache Tomcat Host Manager Cross Site Scripting Attempt", "ET ACTIVEX Gesytec ElonFmt ActiveX Component GetItem1 member Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent UNION SELECT", "ET WEB_SPECIFIC_APPS Easyedit CMS news.php intPageID parameter sql injection", "ET WEB_SPECIFIC_APPS PunBB profile_send.php pun_user language Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat SELECT", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Relocate Upload plugin abspath parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder DELETE", "ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id ASCII", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-trackback.php SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid SELECT", "ET WEB_SPECIFIC_APPS Amateur Photographer Image Gallery file parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage INSERT", "ET WEB_SPECIFIC_APPS Immophp annonce parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DirectNews menu_layers.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass SELECT", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic SELECT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid DELETE", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid SELECT", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php by DELETE", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid ASCII", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname DELETE", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id ASCII", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp INSERT", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_job Component id_job Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id DELETE", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id UNION SELECT", "ET WEB_SPECIFIC_APPS I-Escorts Directory country_id parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword DELETE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id UNION SELECT", "ET WEB_SPECIFIC_APPS rgboard _footer.php skin_path parameter local file inclusion", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd ASCII", "ET WEB_SPECIFIC_APPS PowerPHPBoard footer.inc.php settings Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage DELETE", "ET ACTIVEX ChilkatHttp ActiveX 2.3 Arbitrary Files Overwrite", "ET WEB_SPECIFIC_APPS eGroupware loaddetails.php script SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL

	Injection Attempt -- forgotpass.asp id INSERT", "ET WEB_SPECIFIC_APPS Joomla com_videogallery controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l SELECT", "ET WEB_SPECIFIC_APPS Joomla com_zoomportfolio component SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla morfeoshow morfeoshow.html.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode UNION SELECT", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID INSERT", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id ASCII", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id DELETE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid ASCII", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id SELECT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id INSERT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID UNION SELECT", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id DELETE", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx UPDATE", "ET WEB_SPECIFIC_APPS Joomla Seyret Video com_seyret Component Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id SELECT", "ET WEB_SPECIFIC_APPS Pranian Group e107 page Parameter Cross Site Scripting Vulnerability Attempt", "ET WEB_SERVER Possible HP OpenView Network Node Manager ovalarm.exe CGI Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id UNION SELECT", "ET WEB_CLIENT Generic Mailer Check Accessed on External Server", "ET WEB_SPECIFIC_APPS JCE Joomla Extension", "ET WEB_SERVER Suspected Webshell systeminfo Command (Inbound)", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat SELECT", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id INSERT", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID INSERT", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username SELECT", "ET WEB_SPECIFIC_APPS impressCMS dhtmltextarea root_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS WordPress Copperleaf Photolog postid Parameter UNION SELECT SQL Injection Attempt", "ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id ASCII", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent UNION SELECT", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld INSERT", "ET ACTIVEX Softek Barcode Reader Toolkit ActiveX Control Buffer Overflow Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 15", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat UPDATE", "ET WEB_SPECIFIC_APPS Vlog System note parameter SQL Injection", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID DELETE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eMates SQL Injection Attempt -- newsdetail.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did INSERT", "ET WEB_SPECIFIC_APPS TinyWebGallery install_path parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 ASCII", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id ASCII", "ET WEB_SPECIFIC_APPS phpCow skin_file Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country SELECT", "ET

	WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid SELECT", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection Attempt -- detail.asp ID SELECT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug DELETE", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id DELETE", "ET WEB_SPECIFIC_APPS T-Content Management System id_novedad Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby SELECT", "ET WEB_SPECIFIC_APPS LogAnalyzer asktheoracle.php file XSS Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code DELETE", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) (Content-Disposition) M1", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID DELETE", "ET WEB_SPECIFIC_APPS MODx CMS snippet.reflect.php reflect_base Local File Inclusion", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details UPDATE", "ET WEB_SPECIFIC_APPS WordPress Audio showfile Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS gravity-gtd rpc.php objectname parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS asaher pro emailsender.php row_y5_site_configuration Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key DELETE", "ET WEB_SERVER ColdFusion Path Traversal (locale 5/5)", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf ASCII", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user DELETE", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup UPDATE", "ET WEB_SPECIFIC_APPS joomla com_connect controller parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php ASCII", "ET WEB_SERVER Possible SQL Injection Attempt INSERT INTO", "ET WEB_SPECIFIC_APPS DirectNews remote.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Wordpress Google Doc Embedder plugin file parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS QUICKTEAM qte_result.php title Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email INSERT", "ET WEB_SERVER ATTACKER WebShell - Zehir4.asp", "ET WEB_SPECIFIC_APPS Dolphin BxDolGzip.php file Disclosure Attempt", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_Type_ID ASCII", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id INSERT", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid SELECT", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id SELECT", "ET EXPLOIT Possible Microsoft Exchange Server OWA GetWacUrl Information Disclosure Attempt (CVE-2020-17143)", "ET WEB_SPECIFIC_APPS web wiz forums ForumID Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Apache Tomcat Possible CVE-2017-12617 JSP Upload Bypass Attempt", "ET WEB_SPECIFIC_APPS playSMS function.php apps_path libs parameter local file inclusion", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id UPDATE", "GPL EXPLOIT xp_filelist attempt", "ET WEB_SPECIFIC_APPS Orlando CMS stage1.php GLOBALS Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id DELETE", "ET WEB_SPECIFIC_APPS Horde XSS attempt passwd/main.php", "ET WEB_SPECIFIC_APPS DiY-CMS lang Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS WB News comments.php config Parameter Remote File Inclusion - 1", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi UNION SELECT", "ET WEB_SERVER Possible HTTP 405 XSS Attempt (Local Source)", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id UNION SELECT", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq UNION SELECT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection

	Attempt -- add_comment.php i UPDATE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position UNION SELECT", "ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php by UPDATE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start ASCII", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id DELETE", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa SELECT", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id DELETE", "ET WEB_SPECIFIC_APPS XAMPP xamppsecurity.phpp TEXT Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent SELECT", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp UNION SELECT", "ET WEB_SPECIFIC_APPS YouTube Blog cuerpo.php base_archivo Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where UNION SELECT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici ASCII", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php blogid INSERT", "ET EXPLOIT Possible Telerik UI CVE-2019-18935 File Upload Attempt M2", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 SELECT", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id INSERT", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro DELETE", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img ASCII", "ET WEB_SPECIFIC_APPS WebSense Email security viewHeaders.asp FileName XSS Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass ASCII", "ET WEB_SERVER JAWS Webserver Unauthenticated Shell Command Execution", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id INSERT", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor DELETE", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin INSERT", "ET WEB_SPECIFIC_APPS digiSHOP cart.php UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ZyXEL ZyWALL LoginPassword/HiddenPassword Cross Site Scripting Attempt", "GPL ATTACK_RESPONSE del attempt", "ET WEB_SPECIFIC_APPS phpMyAdmin Remote Code Execution Proof of Concept (c=)", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID UPDATE", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list ASCII", "ET WEB_SPECIFIC_APPS Plogger plog-download.php checked Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id SELECT", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews UNION SELECT", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor INSERT", "ET WEB_SPECIFIC_APPS Papoo CMS message_class.php pfadhier Local File Inclusion", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from ASCII", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id SELECT", "ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent ASCII", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id DELETE", "ET WEB_SPECIFIC_APPS OBOphiX fonctions_racine.php chemin_lib parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid ASCII", "ET WEB_SPECIFIC_APPS Plogger phpThumb.php w Parameter Remote File Disclosure Attempt", "ET WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page SELECT", "ET WEB_SPECIFIC_APPS SuperNews valor.php noticia Parameter SQL

	Injection", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username DELETE", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details ASCII", "ET WEB_SPECIFIC_APPS IBBY nouvelles.php id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id UPDATE", "ET WEB_SPECIFIC_APPS WordPress Download Monitor plugin uploader.php Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x INSERT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php ASCII", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 9", "ET WEB_SPECIFIC_APPS Contenido idart Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start DELETE", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id SELECT", "ET WEB_SPECIFIC_APPS Campsite article_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SERVER AntSword Webshell Commands Inbound", "ET WEB_SPECIFIC_APPS CiscoWorks Help Servlet Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS TurnkeyForms Local Classifieds listtest.php r parameter SQL Injection", "ET WEB_SPECIFIC_APPS Possible JBoss/JMX EJBInvokerServlet RCE Using Marshalled Object", "ET WEB_SPECIFIC_APPS Softsaurus CMS subHeader.php objects_path Parameter Remote File Inclusion -1", "ET WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category UPDATE", "ET WEB_SPECIFIC_APPS DokuWiki target parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password ASCII", "ET WEB_SPECIFIC_APPS Multi SEO phpBB pfad parameter local file inclusion", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm ASCII", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query INSERT", "ET WEB_SPECIFIC_APPS asaher pro left_menu.php row_y5_site_configuration Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass ASCII", "ET WEB_SPECIFIC_APPS QUICKTEAM qte_result.php title Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user ASCII", "ET ACTIVEX SoftCab Sound Converter ActiveX SaveFormat File overwrite Attempt", "ET WEB_SPECIFIC_APPS Rematic CMS produkte.php id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp AD_ID UPDATE", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php qid UNION SELECT", "GPL EXPLOIT .cmd executable file parsing attack", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position UPDATE", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL Injection Attempt -- haberoku.asp id UPDATE", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid UPDATE", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id SELECT", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from DELETE", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id UPDATE", "ET WEB_SPECIFIC_APPS WordPress WP Publication file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail INSERT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- email.php id ASCII", "ET WEB_SERVER PHP Possible https Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WordPress WP Custom Pages url parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS Helpdesk Pilot Knowledge Base SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp DELETE", "ET WEB_SPECIFIC_APPS cpCommerce SQL

	Injection Attempt -- category.php id_category INSERT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid DELETE", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php mcname INSERT", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code UPDATE", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_recent.asp currentpage SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search UPDATE", "ET WEB_SERVER PHP Possible ssh2 Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 30", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email UNION SELECT", "ET WEB_SPECIFIC_APPS TinyButStrong bs_us_examples_0view.php script Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids UPDATE", "ET WEB_SPECIFIC_APPS webEdition CMS shop_artikelid Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id DELETE", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt -- dsp_page.cfm pageid UPDATE", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id SELECT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid ASCII", "ET WEB_SPECIFIC_APPS OTRS Installation Dialog (after auth) attempt", "ET WEB_SPECIFIC_APPS Joomla com_avosbillets Component id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SERVER SHOW CHARACTER SET SQL Injection Attempt in URI", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid SELECT", "ET MALWARE BroBot POST", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat INSERT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id UNION SELECT", "ET WEB_SPECIFIC_APPS MyForum centre.php padmin Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms INSERT", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd UPDATE", "ET WEB_SERVER MINI MO Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp SELECT", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp author UPDATE", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id INSERT", "ET WEB_SERVER WSO 4.2.5 Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid UNION SELECT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass INSERT", "ET WEB_SPECIFIC_APPS Fatwiki datumscalc.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS BetMore Site Suite mainx_a.php bid Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid UPDATE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board katid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_profile controller parameter Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID SELECT", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id SELECT", "ET WEB_SPECIFIC_APPS Joomla com_quicknews Component newsid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid SELECT", "ET WEB_SPECIFIC_APPS Joomla com_photoblog component category Parameter DELETE FROM SQL Injection Attempt", "ET EXPLOIT TP-Link TL-WR840N/TL-WR841N -

	Authentication Bypass (WiFi Password Change)", "ET WEB_CLIENT WSO 4.2.6 Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Web Edition mod parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area DELETE", "ET WEB_SPECIFIC_APPS Wordpress Plugin PICA Photo Gallery imgname parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id DELETE", "ET WEB_SERVER PHP Possible ftps Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS T-Content Management System id_novedad Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid UPDATE", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password UNION SELECT", "ET WEB_SPECIFIC_APPS SFS EZ Hotscripts-like Site software-description.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w UNION SELECT", "ET WEB_SPECIFIC_APPS Manage Engine Service Desk Plus WorkOrder.do UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass INSERT", "ET WEB_SPECIFIC_APPS PHPNuke general SQL injection attempt", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID INSERT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola ASCII", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password DELETE", "ET WEB_SPECIFIC_APPS Joomla Frontend-User-Access controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi UNION SELECT", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php ASCII", "ET WEB_SPECIFIC_APPS Joomla com_blog Component id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary ASCII", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did UNION SELECT", "ET WEB_SPECIFIC_APPS Wordpress yousaytoo-auto-publishing plugin submit Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod UPDATE", "ET WEB_SPECIFIC_APPS Apache Archive addLegacyArtifactPath script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url INSERT", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php mcname SELECT", "ET WEB_SPECIFIC_APPS PHP-fusion Team Structure Infusion team_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid ASCII", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id SELECT", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp UNION SELECT", "ET WEB_SPECIFIC_APPS WebSense Email security viewHeaders.asp Queue XSS Attempt", "ET WEB_SPECIFIC_APPS webEdition CMS openBrowser.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id DELETE", "ET WEB_SERVER SQL Injection Attempt (Agent CZ32ts)", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat DELETE", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx SELECT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent UNION SELECT", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname SELECT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt --

	view_recent.asp currentpage ASCII", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo ASCII", "ET WEB_SPECIFIC_APPS 4images global.php db_servertype Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id INSERT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page UPDATE", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_quicknews Component newsid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS pfile file.php id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id DELETE", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php rating ASCII", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft ASCII", "ET WEB_SPECIFIC_APPS ITechBids productid Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id DELETE", "ET WEB_SPECIFIC_APPS PHP-Lance show.php catid SQL Injection", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id UPDATE", "ET SCAN PHP Attack Tool Morfeus F Scanner", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp ASCII", "ET WEB_SPECIFIC_APPS WebSense Email security viewHeaders.asp IsolatedMessageID XSS Attempt", "ET WEB_SPECIFIC_APPS Joomla com_photoblog component category Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort UPDATE", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid INSERT", "ET WEB_SPECIFIC_APPS ChillyCMS mod Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear UNION SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id INSERT", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex DELETE", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy SELECT", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID UNION SELECT", "ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID UNION SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php website DELETE", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder ASCII", "ET WEB_SPECIFIC_APPS Manage Engine Service Desk Plus WorkOrder.do UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_rwcards mosConfig_absolute_path Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wordpress disclosure policy plugin Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid SELECT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id INSERT", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent INSERT", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 DELETE", "ET WEB_SPECIFIC_APPS Joomla! JBudgetsMagic 'bid' Parameter DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid DELETE", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf UNION SELECT", "ET WEB_SPECIFIC_APPS PRADO PHP Framework functional_tests.php

	Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob ASCII", "ET WEB_SPECIFIC_APPS WB News archive.php config Parameter Remote File Inclusion -1", "ET EXPLOIT MMCS service (Big Endian)", "ET SCAN DirBuster Web App Scan in Progress", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id INSERT", "ET WEB_SPECIFIC_APPS WordPress Copperleaf Photolog postid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat ASCII", "ET WEB_SPECIFIC_APPS YourFreeWorld Reminder Service tr.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo DELETE", "ET WEB_SPECIFIC_APPS HP Insight Diagnostics Online Edition search.php XSS Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php login SELECT", "ET WEB_SPECIFIC_APPS Oracle E-Business Suite Financials jtfwcpnt.jsp INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout DELETE", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key UPDATE", "ET WEB_SPECIFIC_APPS Orlando CMS stage4.php GLOBALS Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-Old_Articles.php cat UPDATE", "ET WEB_SPECIFIC_APPS phpRS id parameter UPDATE SET SQL Injection Attempt", "ET WEB_SERVER PHP Generic Remote File Include Attempt (FTP)", "ET WEB_SPECIFIC_APPS Possible Rentventory SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpSkelSite TplSuffix parameter local file inclusion", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant DELETE", "ET WEB_SPECIFIC_APPS Joomla Community Builder Enhenced Component Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Barracuda Web Application Firewall 600 XSS attempt (backup_password)", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code ASCII", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php SELECT", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php ASCII", "ET WEB_SPECIFIC_APPS ActivDesk cid Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_quicknews Component newsid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent DELETE", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id ASCII", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course DELETE", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php DELETE", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp INSERT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId ASCII", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php catid ASCII", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id DELETE", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php so ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp SELECT", "ET SCAN Havij SQL Injection Tool User-Agent Outbound", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic UPDATE", "ET WEB_SPECIFIC_APPS Piwik Backdoor Access", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user INSERT", "ET WEB_SPECIFIC_APPS Abtp Portal Project skel_null.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id DELETE", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name INSERT", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt --

	cp_menu_data_file.php menu SELECT", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID UPDATE", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id DELETE", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language INSERT", "ET WEB_SPECIFIC_APPS Mambo N-Myndir INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant INSERT", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text UPDATE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id INSERT", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id SELECT", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid SELECT", "ET WEB_SPECIFIC_APPS Tinderbox.mozilla.org showbuilds.cgi Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent UPDATE", "ET WEB_SPECIFIC_APPS iScripts MultiCart orderid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID UPDATE", "ET WEB_SPECIFIC_APPS Joomla 3.7.0 - Sql Injection (CVE-2017-8917)", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php qid DELETE", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (3)", "ET WEB_SPECIFIC_APPS Joomla virtuemart Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id INSERT", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search INSERT", "ET WEB_SPECIFIC_APPS Joomla com_photoblog component category Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS SimpleInvoices having parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp year INSERT", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid UPDATE", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent UPDATE", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 16", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt -- dsp_page.cfm pageid DELETE", "ET WEB_SERVER SELECT SUBSTR/ING in URI Possible Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id UPDATE", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order INSERT", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- category.php id_category UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! Foobla RSS Feed Creator Component 'id' Parameter DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id ASCII", "ET WEB_SPECIFIC_APPS WordPress PHP Speedy Plugin title parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id SELECT", "ET WEB_SPECIFIC_APPS YourFreeWorld Classifieds Blaster tr.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS IBM Lotus Sametime Server stconf.nsf Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id DELETE", "ET WEB_SPECIFIC_APPS Joomla! SportFusion Component SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection Attempt -- print.asp id DELETE", "ET WEB_SPECIFIC_APPS Joomla component smartformer Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id UNION SELECT", "ET WEB_SPECIFIC_APPS

	Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS Reversed Pastebin Injection in Magento DB", "ET WEB_SPECIFIC_APPS Cyphor show.php SQL injection attempt", "ET WEB_SERVER Tilde in URI - potential .php~ source disclosure vulnerability", "ET WEB_SPECIFIC_APPS OSClass file Parameter Remote File Access Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text UNION SELECT", "ET WEB_SPECIFIC_APPS PHP Aardvark Topsites PHP CONFIG PATH Remote File Include Attempt", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft DELETE", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username INSERT", "ET WEB_CLIENT WSO 2.6 Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS WordPress CommentLuv Plugin _ajax_nonce Parameter XSS Attempt", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid UNION SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID UPDATE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin INSERT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId DELETE", "ET WEB_SPECIFIC_APPS Wikiwig spell-check-savedicts.php to_p_dict Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp IsolatedMessageID XSS Attempt", "ET WEB_SERVER PHP Possible file Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Script Toko Online shop_display_products.php cat_id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt -- dsp_page.cfm pageid UNION SELECT", "ET WEB_SPECIFIC_APPS Interactive Web Solutions site_info.php UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text DELETE", "ET WEB_SPECIFIC_APPS Horde XSS attempt colorpicker.php (2)", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci ASCII", "ET WEB_SPECIFIC_APPS VidShare Pro listing_video.php catid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS DBHcms editmenu Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board UNION SELECT", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id SELECT", "ET WEB_SPECIFIC_APPS WP Cost Estimator Plugin AFI Vulnerability", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId UNION SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email DELETE", "ET WEB_SPECIFIC_APPS Check New findoffice.php search parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik SELECT", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id SELECT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc ASCII", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id UPDATE", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay ASCII", "ET WEB_SPECIFIC_APPS GaziYapBoz Game Portal SQL Injection Attempt -- kategori.asp kategori UNION SELECT", "ET WEB_SPECIFIC_APPS Oracle JSF2 Path Traversal Attempt", "ET WEB_SPECIFIC_APPS SoftMP3 search Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS SHOP-INET show_cat2.php grid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_Type_ID INSERT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w UPDATE", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id UPDATE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass UNION SELECT", "ET WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country DELETE", "ET WEB_SPECIFIC_APPS Joomla com_picasa2gallery controller parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id DELETE", "ET WEB_SPECIFIC_APPS Joomla com_dshop Component UPDATE SET SQL Injection

	Attempt", "ET WEB_SPECIFIC_APPS VBulletin 4.0.1 SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id SELECT", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary UNION SELECT", "ET WEB_SPECIFIC_APPS Wordpress PingBack Possible GHOST attempt", "ET WEB_SPECIFIC_APPS E-Xoopport Samsara Sections module secid Parameter Blind SQL Injection Exploit", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x DELETE", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x UPDATE", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id SELECT", "ET WEB_SPECIFIC_APPS Bugzilla token.cgi HPP e-mail validation bypass Attempt Client Body", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID UPDATE", "ET WEB_SPECIFIC_APPS Potential Cewolf DOS attempt", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl SELECT", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass DELETE", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid UPDATE", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p SELECT", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php ASCII", "ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword SELECT", "ET WEB_SPECIFIC_APPS Joomla com_rsgallery2 Component catid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Tunngavik CMS id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text SELECT", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla SQL Reports user_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection Attempt -- default.asp id INSERT", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php INSERT", "ET WEB_SPECIFIC_APPS gpEasy CMS index.php file XSS Attempt", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid UPDATE", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick SELECT", "ET WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page DELETE", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id ASCII", "ET WEB_SPECIFIC_APPS WordPress flash-album-gallery plugin i Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id SELECT", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid ASCII", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id SELECT", "ET WEB_SPECIFIC_APPS Joomla Incapsula component Performance.php file XSS Attempt", "ET WEB_SPECIFIC_APPS Openconstructor CMS keyword Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Possible Joomla Game Server Component id Parameter INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SERVER WEBSHELL K-Shell/ZHC Shell 1.0/Aspx Shell Backdoor NetCat_Listener", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user UPDATE", "ET WEB_SPECIFIC_APPS Publishing Technology id Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Immophp annonce parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class ASCII", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id UPDATE", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor UPDATE", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress updateAJAX.php

	post_id Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where DELETE", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid DELETE", "ET WEB_SPECIFIC_APPS Joomla com_musicgallery Component Id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt -- show_webfeed.php wcHeadlines UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php ASCII", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno DELETE", "GPL EXPLOIT CodeRed v2 root.exe access", "ET SCAN ZmEu exploit scanner", "ET WEB_SPECIFIC_APPS OrangeHRM recruitcode parameter Cross Site Script Attempt", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete INSERT", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid UPDATE", "ET WEB_SPECIFIC_APPS Joomla Pro Desk Component include_file Local File Inclusion", "ET WEB_SPECIFIC_APPS PHP-Nuke Surveys pollID parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w INSERT", "ET WEB_SPECIFIC_APPS OpenX OpenFlashChart Remote Exploit - possible Access to uploaded Files", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item UPDATE", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which ASCII", "ET WEB_SPECIFIC_APPS Possible Joomla! Game Server Component 'id' Parameter UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php UNION SELECT", "ET WEB_SPECIFIC_APPS PowerEasy ComeUrl Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Aigaion ID Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where ASCII", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid DELETE", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic INSERT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php UPDATE", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php UPDATE", "ET WEB_SPECIFIC_APPS V-EVA Classified Script clsid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Bexfront sid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress Vodpod Video Gallery Plugin gid Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name INSERT", "ET WEB_SPECIFIC_APPS Possible Mambo MOStlyCE Module Image Manager Utility Arbitrary File Upload Attempt", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc INSERT", "ET WEB_SPECIFIC_APPS Joomla Community component userid parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid SELECT", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- compare_product.php id ASCII", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id ASCII", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID UPDATE", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num SELECT", "ET WEB_SPECIFIC_APPS PEAR_PHPDIR Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS SnippetMaster vars.inc.php _SESSION Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id DELETE", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php ASCII", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid ASCII", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php i INSERT", "ET WEB_SPECIFIC_APPS WordPress Download Monitor thumbnail parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID SELECT", "ET WEB_SPECIFIC_APPS Constructr CMS SQL Injection Attempt -- constructrXmlOutput.content.xml.php page_id INSERT", "ET WEB_SPECIFIC_APPS Campsite article_id Parameter SELECT FROM SQL Injection Attempt", "ET

	WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter UPDATE SET SQL Injection Attempt", "ET ACTIVEX Dart Communications PowerTCP FTP for ActiveX DartFtp.dll Control Buffer Overflow", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category ASCII", "ET SCAN Simple Slowloris Flooder", "ET WEB_SPECIFIC_APPS ea-gBook index_inc.php inc_ordner parameter local file inclusion", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL Injection Attempt -- haberoku.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_wisroyq controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Awstats Apache Tomcat Configuration File Remote Arbitrary Command Execution Attempt", "ET WEB_SPECIFIC_APPS Possible eFront database.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WordPress WP Survey and Quiz Tool plugin rowcount Cross-Site Scripting Attempt", "ET WEB_SERVER Kageyama Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id INSERT", "ET WEB_SPECIFIC_APPS ClipShare Pro channel_detail.php chid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- index.php p_skin ASCII", "ET WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id UPDATE", "ET EXPLOIT Cisco ASA XSS Attempt (CVE-2020-3580)", "ET PHISHING Apple Phishing Panel Accessed on Internal Server", "ET WEB_SPECIFIC_APPS vBulletin cChatBox messageid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id UPDATE", "ET WEB_SPECIFIC_APPS Joomla! Foobla RSS Feed Creator Component 'id' Parameter SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id UNION SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no ASCII", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid SELECT", "ET WEB_SPECIFIC_APPS Wordpress NextGEN Gallery plugin test-head parameter XSS Attempt", "ET WEB_SPECIFIC_APPS Jetik.net ESA sayfalar.php KayitNo Parameter SQL Injection", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice UPDATE", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did ASCII", "ET WEB_SPECIFIC_APPS Possible APC Network Management Card Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod SELECT", "ET WEB_SPECIFIC_APPS Joomla! CB Resume Builder 'group_id' Parameter UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Barracuda Web Application Firewall 600 XSS attempt (backup_path)", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php ASCII", "ET EXPLOIT Attempted D-Link ShareCenter (DNS-320/325) RCE (Inbound)", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid INSERT", "ET WEB_SERVER Bot Search RFI Scan (ByroeNet/Casper-Like sun4u)", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod UNION SELECT", "ET WEB_SPECIFIC_APPS Zen Cart loader_file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS NotFTP config.php languages Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa DELETE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- usermgr.php gid UPDATE", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id SELECT", "ET WEB_SPECIFIC_APPS Interactive Web Solutions site_info.php INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress FeedList Plugin i Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID UNION SELECT", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID SELECT", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat ASCII", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt --

	show_webfeed.php wcHeadlines UPDATE", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid UPDATE", "ET WEB_SPECIFIC_APPS Google Urchin session.cgi Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID DELETE", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_media file parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_jshop pid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID INSERT", "ET WEB_SPECIFIC_APPS Joomla mediaslide component viewer.php path Local File Inclusion Attempt", "ET WEB_CLIENT Generic Stolen Credentials Accessed on External Server", "ET WEB_SERVER Generic Mini Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps UPDATE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id INSERT", "ET WEB_SPECIFIC_APPS phPortal gunaysoft.php icerikyolu Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass ASCII", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id SELECT", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id DELETE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite SELECT", "ET WEB_SPECIFIC_APPS Horde XSS attempt test.php", "ET WEB_SERVER Attempt To Access MSSQL xp_enumerrorlogs Stored Procedure Via URI to View Error Logs", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID UPDATE", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID UPDATE", "ET WEB_SPECIFIC_APPS coRED CMS rubID Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 1024 CMS filename Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SportFusion Component DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date DELETE", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp secondgroup SELECT", "ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP GET 1)", "ET WEB_SPECIFIC_APPS eNdonesia artid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id UPDATE", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id UPDATE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id UPDATE", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid SELECT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start UNION SELECT", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp UPDATE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat ASCII", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- moscomment.php mcname ASCII", "ET WEB_SPECIFIC_APPS Mp3 Online Id Tag Editor getid3.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer INSERT", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre ASCII", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email SELECT", "ET WEB_SPECIFIC_APPS Nucleus server.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ClanSphere CurrentFolder Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid ASCII", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci ASCII", "ET WEB_SPECIFIC_APPS Bexfront sid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS SiteGo get_templet.php of green

	Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country ASCII", "ET WEB_SPECIFIC_APPS vBulletin cChatBox messageid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS ViArt Shop Evaluation previews_functions.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id SELECT", "ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci INSERT", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid UNION SELECT", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field SELECT", "ET WEB_SPECIFIC_APPS ODARS resource_categories_view.php CLASSES_ROOT parameter local file inclusion", "ET WEB_SPECIFIC_APPS Enthrallweb eMates SQL Injection Attempt -- newsdetail.asp ID SELECT", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code INSERT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby ASCII", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username DELETE", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat SELECT", "ET WEB_SPECIFIC_APPS evision cms addpolling.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID UNION SELECT", "ET WEB_SPECIFIC_APPS WP Jetpack/Twentyfifteen Possible XSS Request", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID UPDATE", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid SELECT", "ET WEB_SPECIFIC_APPS DirectNews lib.panier.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic UNION SELECT", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id INSERT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare SELECT", "ET ACTIVEX winhlp32 ActiveX control attack - phase 1", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php INSERT", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv INSERT", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer UNION SELECT", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Facebook-Page-Promoter-Lightbox settings-updated Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us DELETE", "ET WEB_SPECIFIC_APPS Cacti SQL Injection Vulnerability tree.php leaf_id DELETE", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail UPDATE", "ET WEB_SERVER ColdFusion Path Traversal (locale 3/5)", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php UNION SELECT", "ET WEB_SPECIFIC_APPS Job2C detail.php adtype Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS DynPG CMS PathToRoot Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS ARISg errmsg Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WordPress LiveGrounds plugin uid parameter Cross-Site Script Attempt", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php UNION SELECT", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid INSERT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp secondgroup INSERT", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid INSERT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort ASCII", "ET

	WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country INSERT", "ET WEB_SPECIFIC_APPS OTManager ADM_Pagina.php Tipo Local File Inclusion", "ET WEB_SPECIFIC_APPS WordPress Chocolate WP Theme src Remote File Inclusion Attempt", "ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M4", "ET WEB_SPECIFIC_APPS Joomla Component com_zcalendar (eid) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q DELETE", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID UPDATE", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php DELETE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 27", "ET WEB_SPECIFIC_APPS WordPress Mingle Forum groupid parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank ASCII", "ET WEB_SPECIFIC_APPS Constructr CMS SQL Injection Attempt -- constructrXmlOutput.content.xml.php page_id UNION SELECT", "ET WEB_SPECIFIC_APPS pHNews comments.php template Local File Inclusion", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid UPDATE", "ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M3", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id ASCII", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php SELECT", "ET PHISHING Apple Phishing Panel Accessed on External Server", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt -- news.php id INSERT", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode UNION SELECT", "ET WEB_SPECIFIC_APPS Wordpress wp-livephp plugin wp-live.php Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Download Monitor tags parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Possible IBM Rational RequisitePro ReqWebHelp Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month SELECT", "ET WEB_SPECIFIC_APPS WordPress XCloner Plugin index2.php option Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid UPDATE", "ET WEB_SPECIFIC_APPS WordPress Tune Library Plugin letter parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew UNION SELECT", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID ASCII", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username SELECT", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid SELECT", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID UNION SELECT", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity DELETE", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod UPDATE", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin UNION SELECT", "ET WEB_SPECIFIC_APPS Blogplus block_right.php Local File Inclusion", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user UNION SELECT", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id DELETE", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid UPDATE", "ET WEB_SPECIFIC_APPS Gazi Download Portal SQL Injection Attempt -- down_indir.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter UPDATE", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat UPDATE", "ET WEB_SPECIFIC_APPS N-13 News default_login_language Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt --

	process.php login UNION SELECT", "ET WEB_SPECIFIC_APPS KLINK txtCodiInfo parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-3", "ET WEB_SPECIFIC_APPS Joomla Bsadv controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS OSClass id parameter data access Attempt 2", "ET WEB_SPECIFIC_APPS OvBB admincp.php smilieid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID UPDATE", "ET WEB_SPECIFIC_APPS ManageEngine Applications Manager attributeToSelect parameter Cross-Site Script Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id ASCII", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword UNION SELECT", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear DELETE", "ET WEB_SPECIFIC_APPS I-Escorts Directory country_id parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS asaher pro view_blog_archives.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi INSERT", "ET WEB_SPECIFIC_APPS RS-CMS rscms_mod_newsview.php key Parameter Processing Remote SQL Injection", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate UPDATE", "ET WEB_SPECIFIC_APPS Jenkins Chained Exploits CVE-2018-1000861 and CVE-2019-1003000 M1", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id INSERT", "GPL EXPLOIT echo command attempt", "ET WEB_SPECIFIC_APPS Cacti SQL Injection Vulnerability tree.php leaf_id UPDATE", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php ASCII", "ET WEB_SPECIFIC_APPS RecordPress header.php titledesc Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Immophp annonce parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id UPDATE", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid UPDATE", "ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country DELETE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik UPDATE", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q SELECT", "ET WEB_SPECIFIC_APPS vBulletin cChatBox messageid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-Old_Articles.php cat UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla Component com_banners banners.class.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_acmis (Itemid) SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board DELETE", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 SELECT", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-Old_Articles.php cat ASCII", "ET WEB_SPECIFIC_APPS joomla com_djcatalog component INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Telephone Directory 2008 edit1.php code Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct INSERT", "ET WEB_SPECIFIC_APPS Wordpress Token Manager Plugin tokenmanagertypeedit page XSS Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 UNION SELECT", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img SELECT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did UNION SELECT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav UNION SELECT", "ET

	WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk DELETE", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor SELECT", "ET WEB_SPECIFIC_APPS Joomla com_jshop component pid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id INSERT", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete UPDATE", "ET WEB_SERVER Casper Bot Search RFI Scan", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID SELECT", "ET WEB_SPECIFIC_APPS OpenX OpenFlashChart Remote Exploit Attempt", "ET WEB_SPECIFIC_APPS Joomla com_hdflvplayer Component id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHPNuke SQL injection attempt", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki wgDekiPluginPath parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_hdflvplayer Component id Parameter DELETE FROM SQL Injection Attempt", "ET MALWARE Polaris Botnet User-Agent (Outbound)", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid UNION SELECT", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode INSERT", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php by INSERT", "ET WEB_SERVER Antsword Related Webshell Activity (Inbound)", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid DELETE", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection Attempt -- print.asp id SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id DELETE", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID INSERT", "ET WEB_SPECIFIC_APPS MassMirror Uploader example_1.php Remote File Inclusion attempt", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip ASCII", "ET WEB_SPECIFIC_APPS DMXReady Multiple Products upload_image_category.asp cid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName INSERT", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno UNION SELECT", "ET WEB_SERVER Microsoft SharePoint Server 2007 _layouts/help.aspx Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id UPDATE", "ET WEB_SPECIFIC_APPS Million Pixel Ad Script tops_top.php id_cat parameter SQL Injection", "ET WEB_SPECIFIC_APPS Joomla com_perchagallery Component id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS My PHP Dating id parameter SQL Injection", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php SELECT", "ET WEB_SPECIFIC_APPS JBoss JMX Console Beanshell Deployer .WAR File Upload and Deployment Cross Site Request Forgery Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model ASCII", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style SELECT", "ET WEB_SPECIFIC_APPS Joomla Appointment Booking Pro view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i DELETE", "ET WEB_SPECIFIC_APPS X-BLC get_read.php section Parameter SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID SELECT", "ET WEB_SPECIFIC_APPS Comtrend ADSL Router srvName parameter XSS attempt", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id UNION SELECT", "ET WEB_SPECIFIC_APPS ArdeaCore pathForArdeaCore Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PNphpBB2 admin_groups_reapir.php ModName parameter Local File inclusion", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id SELECT", "ET WEB_SPECIFIC_APPS Joomla MyRemote Video Gallery (user_id) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL

	Injection Attempt -- massedit_album.php gall_id UPDATE", "ET WEB_SPECIFIC_APPS ProdLer prodler.class.php sPath Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WordPress Lazyest Gallery Plugin image Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi DELETE", "ET SCAN Nikto Web App Scan in Progress", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid UPDATE", "ET WEB_SPECIFIC_APPS MyOWNspace getfeed.php file Parameter Local File Inclusion Attempt(2)", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id DELETE", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id INSERT", "ET WEB_SPECIFIC_APPS phpAddEdit editform parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS CSSTidy css_optimiser.php url Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area ASCII", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp UNION SELECT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID UNION SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no INSERT", "ET WEB_SPECIFIC_APPS cfagcms right.php title Parameter SQL Injection", "ET WEB_SERVER PHP Generic Remote File Include Attempt (FTPS)", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID SELECT", "ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (2)", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 DELETE", "ET WEB_SPECIFIC_APPS Possible Joomla Com_joomlub Component Union Select SQL Injection", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php catid DELETE", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager eventmon Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id SELECT", "ET WEB_SPECIFIC_APPS The Uploader download_launch.php Remote File Disclosure Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php SELECT", "ET WEB_SPECIFIC_APPS evision cms addplain.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS SaurusCMS com_del.php class_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS AdaptBB latestposts.php forumspath Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Multiple Membership Script id parameter SQL injection", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model INSERT", "ET WEB_SPECIFIC_APPS Ektron CMS400.NET medialist.aspx selectids Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid INSERT", "ET WEB_SPECIFIC_APPS Apache Archive addLegacyArtifactPath.action Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS V-EVA Classified Script clsid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID DELETE", "ET WEB_SPECIFIC_APPS Automne upload-controler.php Arbitrary File Upload Vulnerability", "ET WEB_SPECIFIC_APPS Joomla com_blog Component id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID UPDATE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID UNION SELECT", "ET WEB_SPECIFIC_APPS WebSense Email security msgForwardToRiskFilter.asp FileName XSS Attempt", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids INSERT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php SELECT", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid UNION SELECT", "ET EXPLOIT AsusWRT RT-AC750GF Cross-Site Request Forgery", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat UNION SELECT", "ET WEB_SPECIFIC_APPS Softbiz Article Directory Script sbiz_id Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php rating DELETE", "ET

	WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php blogid DELETE", "ET WEB_SPECIFIC_APPS Wazzum Dating Software profile_view.php userid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Softsaurus CMS subHeader.php objects_path Parameter Remote File Inclusion -2", "ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WHMCompleteSolution templatefile Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Greenpeace.fr filter_dpt Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DeltaScripts PHP Classifieds siteid parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid INSERT", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID UPDATE", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod DELETE", "ET WEB_SPECIFIC_APPS Joomla! Soundset Component 'cat_id' Parameter INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url UPDATE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang UPDATE", "ET EXPLOIT Xiongmai/HiSilicon DVR - Request for Product Details Possible CVE-2017-7577 Exploit Attempt", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id UPDATE", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy DELETE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla Component Event Manager 1.5 (id) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Lantern CMS intPassedLocationID Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS z1exchange edit.php site parameter SQL injection", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php ASCII", "ET WEB_SPECIFIC_APPS Joomla com_rsgallery2 Component catid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area INSERT", "ET WEB_SPECIFIC_APPS e107 HANDLERS_DIRECTORY Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid UNION SELECT", "ET WEB_SPECIFIC_APPS Plogger phpThumb.php h Parameter Remote File Disclosure Attempt", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php UNION SELECT", "ET WEB_SERVER Anonymous Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS TinyBrowser tinybrowser.php file Script Execution Attempt", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid DELETE", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice UPDATE", "ET WEB_SPECIFIC_APPS Joomla! Foobla RSS Feed Creator Component 'id' Parameter INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS JE Ajax Event Calendar view Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MyioSoft EasyBookMarker Parent parameter SQL Injection", "ET WEB_SPECIFIC_APPS SnippetMaster pcltar.lib.php g_pcltar_lib_dir Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php login INSERT", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity INSERT", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php template SELECT", "ET WEB_SPECIFIC_APPS IBM Rational RequisitePro ReqWebHelp scope Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre ASCII", "ET WEB_SPECIFIC_APPS GetSimple CMS path parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS XAMPP showcode.php TEXT Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search SELECT", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum UPDATE", "ET WEB_SPECIFIC_APPS EasySiteNetwork Riddles Complete Website riddle.php

	riddleid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre ASCII", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active DELETE", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent ASCII", "ET WEB_SPECIFIC_APPS impressCMS FCKeditor root_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS PunBB Functions_navlinks.php pun_user language Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla com_dshop Component INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text UNION SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active UNION SELECT", "ET WEB_SPECIFIC_APPS Aigaion ID Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage ASCII", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id INSERT", "ET EXPLOIT Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)", "ET WEB_SPECIFIC_APPS WordPress PDF and Print Button Joliprint plugin opt parameter Cross-Site Scripting Attempt", "ET EXPLOIT BlueCoat CAS v1.3.7.1 Report Email Command Injection attempt", "ET WEB_SPECIFIC_APPS iScripts MultiCart orderid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php DELETE", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month INSERT", "ET WEB_SPECIFIC_APPS Wordpress Plugin Page Flip Image Gallery getConfig.php book_id parameter Remote File Disclosure", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent DELETE", "ET WEB_SPECIFIC_APPS Joomla Foobla Suggestions Component idea_id UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort SELECT", "ET WEB_SPECIFIC_APPS PHP link Directory sbcat_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer SELECT", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid SELECT", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item INSERT", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id UPDATE", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password UPDATE", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id UPDATE", "ET WEB_SPECIFIC_APPS Joomla Jotloader component section parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla Dada Mail Manager Component config.dadamail.php GLOBALS Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did ASCII", "ET WEB_SERVER Suspected Webshell directory listing Command (Inbound)", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID INSERT", "ET WEB_SPECIFIC_APPS Possible WP CuckooTap Arbitrary File Download", "ET WEB_SPECIFIC_APPS impressCMS tinymce root_path Parameter Remote File inclusion Attempt", "ET WEB_SERVER ATTACKER WebShell - PHP Offender - POST Command", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id UNION SELECT", "ET WEB_SPECIFIC_APPS F5 Data Manager DiagCaptureFileListActionBody.do capture parameter LFI Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid UNION SELECT", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did DELETE", "ET WEB_SERVER PIWIK Backdoored Version calls home", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username UNION SELECT", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img DELETE", "ET WEB_SPECIFIC_APPS Aigaion ID Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PMB Services id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_hello UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS pragmaMx img_url parameter Cross-Site Scripting

	Attempt", "ET WEB_SPECIFIC_APPS SoftExpert Excellence Suite 2.0 SQL Injection", "ET WEB_SPECIFIC_APPS PHP-fusion Team Structure Infusion team_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id UNION SELECT", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id INSERT", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid SELECT", "ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id INSERT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php i SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice UNION SELECT", "ET WEB_SPECIFIC_APPS T-Content Management System id_novedad Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id DELETE", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic DELETE", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url ASCII", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID ASCII", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer ASCII", "ET WEB_SPECIFIC_APPS jbShop e107 CMS plugin item_id parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS epay a_affil.php _REQUEST Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name UPDATE", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id INSERT", "ET SCAN Acunetix scan in progress acunetix variable in http_uri", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php categoryid INSERT", "ET WEB_SPECIFIC_APPS TECHNOTE shop_this_skin_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS RecordPress header.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID ASCII", "ET WEB_SPECIFIC_APPS Opencadastre soustab.php script Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php user_login_cookie UPDATE", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name UNION SELECT", "ET WEB_SPECIFIC_APPS Mp3 Online Id Tag Editor module.archive.gzip.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list SELECT", "ET WEB_SPECIFIC_APPS LightOpenCMS smarty.php cwd Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user UPDATE", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- rss.asp kid DELETE", "ET WEB_SERVER Suspected Webshell ipconfig Command (Inbound)", "ET WEB_SPECIFIC_APPS Woltlab Burning Board katid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Mole Group Vacation Estate Listing Script Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce UNION SELECT", "ET WEB_SPECIFIC_APPS McAfee Email Gateway queueMsgType Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS CAT2 spaw_control.class.php spaw_root Parameter Local File Inclusion", "ET WEB_SERVER Generic File Upload Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style UNION SELECT", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 ASCII", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- usermgr.php gid ASCII", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP DELETE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid ASCII", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password ASCII", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection

	Attempt -- usermgr.php gid UNION SELECT", "ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword UPDATE", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php UNION SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 28", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids UNION SELECT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni SELECT", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id INSERT", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews UPDATE", "ET WEB_SPECIFIC_APPS phpBMS invoices_discount_ajax.php id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType DELETE", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname INSERT", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php login ASCII", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug ASCII", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id UNION SELECT", "ET WEB_SPECIFIC_APPS WebPhotoPro galeri_info.php lang Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id DELETE", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php DELETE", "ET WEB_SPECIFIC_APPS MoinMoin twikidraw Action Traversal File Upload", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date INSERT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- email.php id SELECT", "GPL EXPLOIT ISAPI .ida attempt", "ET WEB_SPECIFIC_APPS ColdUserGroup LibraryID Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php sqlcmd ASCII", "ET WEB_SPECIFIC_APPS WordPress Dynamic Widgets plugin id parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! JBudgetsMagic 'bid' Parameter UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch UNION SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category UPDATE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 18", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage UNION SELECT", "ET WEB_SPECIFIC_APPS Apache Archive useredit script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Sahana Agasti dao.php approot Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID DELETE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id UPDATE", "ET WEB_SPECIFIC_APPS Wordpress Plugin Newsletter data parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username ASCII", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category DELETE", "ET WEB_SERVER Predator the Thief Password Prompt Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Interleave basicstats.php AjaxHandler Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id DELETE", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut SELECT", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php SELECT", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid DELETE", "ET WEB_SPECIFIC_APPS

	Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid SELECT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid UNION SELECT", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection Attempt -- detail.asp ID UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text INSERT", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid DELETE", "ET WEB_SPECIFIC_APPS Snipsnap search Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id INSERT", "ET WEB_SPECIFIC_APPS PHP-Daily add_postit.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection Attempt -- detail.asp ID INSERT", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice UNION SELECT", "ET WEB_SERVER WebResource.axd access without t (time) parameter - possible ASP padding-oracle exploit", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl ASCII", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp year UPDATE", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass DELETE", "ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear SELECT", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id SELECT", "ET ACTIVEX SaschArt SasCam Webcam Server ActiveX Control Head Method Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa ASCII", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid ASCII", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand SELECT", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL Injection Attempt -- massedit_album.php gall_id ASCII", "ET WEB_SERVER MongoDB Negated Parameter Server Side JavaScript Injection Attempt", "ET WEB_SPECIFIC_APPS Zimplit CMS file Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-trackback.php DELETE", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent DELETE", "ET WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area INSERT", "ET WEB_SPECIFIC_APPS JobHut browse.php pk Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area DELETE", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id UNION SELECT", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id SELECT", "ET WEB_SPECIFIC_APPS Joomla Community component userid parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS GeekLog filemgt INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vBulletin vBTube uname Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Mambo N-Myndir DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID UNION SELECT", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main DELETE", "ET WEB_SPECIFIC_APPS myBloggie mybloggie_root_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent UPDATE", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id DELETE", "ET WEB_SPECIFIC_APPS WordPress PDF and Print Button Joliprint plugin type parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! JoomlaFacebook

	Component SELECT FROM SQL Injection", "ET WEB_SERVER Suspected Webshell netstat Command (Inbound)", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- rss.asp kid SELECT", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen DELETE", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID ASCII", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery output Parameter Remote Command Execution Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_hello DELETE FROM SQL Injection Attempt", "ET WEB_SERVER 16Shop Phishing Kit Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId UNION SELECT", "ET WEB_SPECIFIC_APPS BibCiter contacts.php idc Parameter SQL Injection", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname SELECT", "ET WEB_SPECIFIC_APPS Easyedit CMS subcategory.php intSubCategoryID parameter sql injection", "ET WEB_SERVER Possible INSERT VALUES SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Possible HP Power Manager Management Web Server Login Remote Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS e107 BLOG Engine macgurublog.php uid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc UPDATE", "ET WEB_SERVER Suspicious PHP UNZIP Tool Accessed on Internal Possibly Compromised Server", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo UNION SELECT", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa ASCII", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite UPDATE", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder INSERT", "ET WEB_SPECIFIC_APPS V-EVA Classified Script clsid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare DELETE", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id INSERT", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q UNION SELECT", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID UNION SELECT", "ET WEB_SPECIFIC_APPS SocialEngine browse_classifieds.php Remote SQL Injection", "ET WEB_SPECIFIC_APPS Shape Web Solutions imprimir.php INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Ve-EDIT debug_php.php _GET Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici SELECT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-trackback.php ASCII", "ET WEB_SPECIFIC_APPS WordPress Simple Download Button Shortcode Plugin Arbitrary File Disclosure Vulnerability", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 22", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid INSERT", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname DELETE", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut ASCII", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 26", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp INSERT", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- compare_product.php id DELETE", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php DELETE", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UNION SELECT", "ET EXPLOIT Local File Inclusion with Shell Execution via proc/self/environ", "ET WEB_SPECIFIC_APPS PHP-Nuke Module

	Emporium SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Lanoba Social plugin action parameter Cross-Site Script Attempt", "ET WEB_SPECIFIC_APPS Pre Online Tests Generator Pro SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS TEDE Simplificado processaPesquisa.php script DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id UNION SELECT", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SportFusion Component UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp UPDATE", "ET WEB_SPECIFIC_APPS Joomla! CB Resume Builder 'group_id' Parameter DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx UNION SELECT", "ET EXPLOIT TIBCO JasperReports Directory Traversal Attempt (CVE-2018-18809)", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- category.php id_category DELETE", "ET WEB_SPECIFIC_APPS Cisco Prime Infrastruture RCE - CVE-2019-1821", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php ASCII", "ET WEB_SERVER Possible SQL injection obfuscated via REVERSE function", "ET WEB_SPECIFIC_APPS Xt-News SQL Injection Attempt -- show_news.php id_news UPDATE", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order UNION SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php t SELECT", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode SELECT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId INSERT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid UNION SELECT", "GPL EXPLOIT cmd32.exe access", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt -- dsp_page.cfm pageid ASCII", "ET WEB_SPECIFIC_APPS SoftMP3 search Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id INSERT", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi ASCII", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare ASCII", "ET WEB_SPECIFIC_APPS jQuery Mega Menu Wordpress Plugin Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS DevelopItEasy Photo Gallery photo_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Fusion Members CV(job) Module members.php sortby parameter SQL injection", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup INSERT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_recent.asp currentpage UNION SELECT", "ET WEB_SPECIFIC_APPS TotalCalendar config.php inc_dir Parameter Local File Inclusion", "ET WEB_SERVER Generic Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Joomla Component com_hello UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id ASCII", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php mcname UNION SELECT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni INSERT", "ET WEB_SPECIFIC_APPS ReVou Micro Blogging user_updates.php user Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Cyberfolio css.php theme Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla! JoomlaFacebook Component INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type INSERT", "ET WEB_SPECIFIC_APPS I-Escorts Directory country_id parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp author DELETE", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p DELETE", "ET WEB_SPECIFIC_APPS F5 Data Manager

	ViewInventoryErrorReport.do Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Inventory newinventario.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid UPDATE", "ET WEB_SERVER Likely Malicious Request for /proc/self/environ", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice DELETE", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID INSERT", "ET WEB_SPECIFIC_APPS Mambo component com_zoom Blind SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid DELETE", "ET WEB_SPECIFIC_APPS eNdonesia artid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity UPDATE", "ET WEB_SPECIFIC_APPS WordPress Featured Content param Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Profi Einzelgebots Auktions System auktion_text.php Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment UNION SELECT", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field DELETE", "ET WEB_CLIENT Generic Webshell Accessed on External Server", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa DELETE", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id UPDATE", "ET WEB_SPECIFIC_APPS ThWboard SQL Injection Attempt -- index.php board DELETE", "ET WEB_SPECIFIC_APPS Flash Quiz answers.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id ASCII", "ET WEB_SPECIFIC_APPS f-fileman direkt Parameter Directory Traversal Vulnerability", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity ASCII", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch ASCII", "ET WEB_SPECIFIC_APPS WordPress Plugin Pie Register SQL Injection", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID DELETE", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt -- show_webfeed.php wcHeadlines SELECT", "ET WEB_SPECIFIC_APPS e107 trackback_url Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS LoCal Calendar System LIBDIR Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid INSERT", "ET WEB_SPECIFIC_APPS Pre Podcast Portal tour.php id SQL Injection", "ET WEB_SPECIFIC_APPS Oracle E-Business Suite Financials jtfwcpnt.jsp UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php SELECT", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid INSERT", "ET WEB_SPECIFIC_APPS Magento Shoplift Exploit Inbound", "ET WEB_SPECIFIC_APPS Barracuda Web Application Firewall 600 XSS attempt (backup_username)", "ET WEB_SPECIFIC_APPS PEAR include_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id SELECT", "ET WEB_CLIENT Generic Mailer Accessed on External Server", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat INSERT", "ET WEB_SPECIFIC_APPS iPortal X gallery_show.asp GID parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board INSERT", "ET WEB_SPECIFIC_APPS Jetik.net ESA diger.php KayitNo Parameter SQL Injection", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id ASCII", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php DELETE", "ET WEB_SERVER Generic PHP Uploader Accessed on Internal Server", "ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli) M2", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl UNION SELECT", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi DELETE",

	"ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword UNION SELECT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_recent.asp currentpage INSERT", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID ASCII", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID UNION SELECT", "ET WEB_SPECIFIC_APPS Possible OpenSiteAdmin pageHeader.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php DELETE", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse ASCII", "ET WEB_SPECIFIC_APPS OSSIM repository_attachment.php DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS OrangeHRM uri Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick ASCII", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php t UPDATE", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid SELECT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id INSERT", "ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WikyBlog which Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s UPDATE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id ASCII", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug SELECT", "ET WEB_SERVER Gootkit Website Infection Request for FTP Credentials from Control Server", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage SELECT", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id SELECT", "ET WEB_SPECIFIC_APPS SaurusCMS captcha_image.php script Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php mcname UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname UNION SELECT", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout ASCII", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- category.php id_category SELECT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category SELECT", "ET WEB_SPECIFIC_APPS Zabbix popup.php SELECT FROM SQL Injection Vulnerability", "ET WEB_SERVER ColdFusion path disclosure to get the absolute path", "ET WEB_SPECIFIC_APPS DVD Rental Software cat_id parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id UPDATE", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp FileName XSS Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid DELETE", "ET WEB_SPECIFIC_APPS Webspell wCMS-Clanscript staticID Parameter SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid UNION SELECT", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key SELECT", "ET WEB_SPECIFIC_APPS Joomla com_br controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS DVD Rental Software cat_id parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat ASCII", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid UNION SELECT", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php template DELETE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php UNION SELECT", "ET WEB_SPECIFIC_APPS TEDE Simplificado processaPesquisa.php script UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS Quantum Game Library smarty.inc.php CONFIG Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Xt-

	News SQL Injection Attempt -- show_news.php id_news ASCII", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID UNION SELECT", "ET WEB_SPECIFIC_APPS Mole viewsource.php dirn Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids DELETE", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id INSERT", "ET WEB_CLIENT Possible HTTP 405 XSS Attempt (External Source)", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID SELECT", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum SELECT", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld SELECT", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id UPDATE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat SELECT", "ET WEB_SPECIFIC_APPS Wordpress WPsc-MijnPress plugin rwflush parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w SELECT", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order INSERT", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum UNION SELECT", "ET WEB_SERVER Tilde in URI - potential .aspx source disclosure vulnerability", "ET WEB_SPECIFIC_APPS Zimplit CMS client Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS FCMS familynews.php current_user_id Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId ASCII", "ET WEB_SPECIFIC_APPS Possible Zenoss Cross Site Request Forgery Attempt", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 INSERT", "ET WEB_SPECIFIC_APPS Joomla com_jvb_bridge Itemid Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Horde 3.3.12 Backdoor Attempt", "ET WEB_SERVER Possible SQL Injection Attempt UPDATE SET", "ET WEB_SPECIFIC_APPS Joomla portalid Component UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID ASCII", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user ASCII", "ET EXPLOIT Possible Telerik UI CVE-2019-18935 File Upload Attempt M1", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from UNION SELECT", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid UNION SELECT", "ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS PozScripts Classified Auctions id parameter SQL Injection", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id SELECT", "ET WEB_SPECIFIC_APPS WordPress LeagueManager plugin season parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid ASCII", "ET WEB_SPECIFIC_APPS PHPmyGallery lang parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid INSERT", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user ASCII", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID UNION SELECT", "ET WEB_SPECIFIC_APPS Possible Zenoss Network Monitoring Application INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke viewslink module sid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID SELECT", "ET ACTIVEX winhlp32 ActiveX control attack - phase 2", "ET WEB_SPECIFIC_APPS joomla com_djcatalog component DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l UNION SELECT", "ET WEB_SPECIFIC_APPS joomla com_djcatalog component SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php

	sqlcmd UNION SELECT", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp UPDATE", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id UPDATE", "ET WEB_SPECIFIC_APPS Joomla! Soundset Component 'cat_id' Parameter DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS Possible Zenoss Network Monitoring Application INTO OUTFILE SQL Injection Attempt", "ET WEB_SERVER Suspected Webshell query Command (Inbound)", "ET WEB_SPECIFIC_APPS WHM filtername Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user UPDATE", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id SELECT", "ET WEB_SPECIFIC_APPS NewsOffice news_show.php newsoffice_directory Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke Surveys pollID parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Cisco Unified Communications Manager xmldirectorylist.jsp SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup UPDATE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID UNION SELECT", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType UPDATE", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id INSERT", "ET WEB_SPECIFIC_APPS Joomla! CB Resume Builder 'group_id' Parameter INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where SELECT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php UPDATE", "ET WEB_SPECIFIC_APPS KR-Web krgourl.php DOCUMENT_ROOT Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_universal Component Remote File Inclusion", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment INSERT", "ET WEB_SPECIFIC_APPS Possible Drupal Object Unserialize Exploit Attempt", "ET WEB_SERVER Suspected Webshell del Command (Inbound)", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd UNION SELECT", "ET WEB_SPECIFIC_APPS Open Web Analytics owa_action Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php DELETE", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid INSERT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In INSERT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld DELETE", "ET WEB_SPECIFIC_APPS F3Site2009 LFI Exploit Attempt (poll.php)", "ET WEB_SPECIFIC_APPS DEDECMS feedback_js.php arcurl Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Tours Manager cityview.php cityid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Nuke Surveys pollID parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Community component userid parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rematic CMS referenzdetail.php id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Immophp annonce parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname DELETE", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum INSERT", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq SELECT", "ET WEB_SERVER ImageMagick CVE-2016-3714 Inbound (mvg)", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid ASCII", "ET WEB_SPECIFIC_APPS webEdition CMS we_transaction Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID ASCII", "ET WEB_SERVER ColdFusion administrator access", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid ASCII", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt --

	vehiclelistings.asp year DELETE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin UNION SELECT", "ET WEB_SPECIFIC_APPS Orlando CMS init.php GLOBALS Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS ClaSS export.php ftype parameter Information Disclosure", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php website UNION SELECT", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (1)", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID UPDATE", "ET WEB_SPECIFIC_APPS Wordpress featurific-for-wordpress plugin snum parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS CubeCart loc parameter Local File Inclusion Attempt", "ET WEB_SERVER SELECT USER SQL Injection Attempt in URI", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp UPDATE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl INSERT", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID ASCII", "ET WEB_SPECIFIC_APPS PHP Volunteer Management id parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid DELETE", "ET WEB_SPECIFIC_APPS W-Agora search.php bn Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID SELECT", "ET WEB_SPECIFIC_APPS Joomla Component com_xmovie file Parameter Local File Inclusion Attempt", "ET WEB_SERVER Possible Cisco PIX/ASA HTTP Web Interface HTTP Response Splitting Attempt", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail UPDATE", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby DELETE", "ET WEB_SPECIFIC_APPS Jenkins RCE CVE-2019-1003000", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id UPDATE", "ET WEB_SPECIFIC_APPS pfile file.php id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID UPDATE", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id DELETE", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid DELETE", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID SELECT", "ET WEB_SPECIFIC_APPS Flash Quiz num_questions.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php rating SELECT", "ET WEB_SPECIFIC_APPS WordPress Annonces Remote File inclusion Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 4", "ET WEB_SPECIFIC_APPS WordPress XCloner Plugin cloner.cron.php config Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip SELECT", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order SELECT", "ET WEB_SPECIFIC_APPS Piwik Backdoor Access 2", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class INSERT", "ET WEB_SERVER /bin/ksh In URI Possible Shell Command Execution Attempt", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-7", "ET WEB_SPECIFIC_APPS Dros core.write_compiled_include.php smarty Remote File Inclusion Attempt", "ET SCAN SQL Injection Attempt (Agent uil2pn)", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat SELECT", "ET WEB_SPECIFIC_APPS All In One Control Panel poll_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id SELECT", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid UNION SELECT", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id DELETE", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- rss.asp kid INSERT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text UPDATE", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eMates

	SQL Injection Attempt -- newsdetail.asp ID DELETE", "ET WEB_SPECIFIC_APPS Joomla Redirect Component view Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid ASCII", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php DELETE", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID ASCII", "ET WEB_SPECIFIC_APPS Slooze Web Photo Album file Parameter Command Execution Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass UNION SELECT", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID INSERT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew INSERT", "ET WEB_SPECIFIC_APPS Mambo AHS Shop component UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent SELECT", "ET WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex ASCII", "ET WEB_SPECIFIC_APPS Simple Machines Forum ssi_function parameter path disclosure vulnerability", "ET WEB_SPECIFIC_APPS Loggix Project RFI Attempt", "ET WEB_SERVER ColdFusion scheduletasks access", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did SELECT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id INSERT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc INSERT", "ET WEB_SPECIFIC_APPS Possible Docebo DELETE FROM SQL Injection Attempt", "ET WEB_SERVER Suspected Webshell net Command (Inbound)", "ET WEB_SPECIFIC_APPS QUICKTEAM qte_result.php title Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID SELECT", "ET WEB_SPECIFIC_APPS Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat INSERT", "ET WEB_SPECIFIC_APPS FCMS settings.php current_user_id Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid ASCII", "ET WEB_SERVER HP OpenView /OvCgi/Toolbar.exe Accept Language Heap Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id DELETE", "ET WEB_SPECIFIC_APPS cpCommerce _functions.php GLOBALS Parameter Local File Inclusion", "ET PHISHING Generic Phishing Panel Accessed on Internal Server", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id DELETE", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id ASCII", "ET WEB_SPECIFIC_APPS WordPress FSML Plugin fsml-admin.js.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic UNION SELECT", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla component Simple File Lister sflDir Parameter directory traversal attempt", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Hedgehog CMS header.php c_temp_path Remote File Inclusion", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code SELECT", "ET WEB_SPECIFIC_APPS eGroupware loaddetails.php script DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit ASCII", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order INSERT", "ET ACTIVEX Ask.com Toolbar askBar.dll ActiveX ShortFormat Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id DELETE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby UNION SELECT", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps INSERT", "ET

	WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category UNION SELECT", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID SELECT", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id INSERT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak INSERT", "ET EXPLOIT NB8-02 - Possible Unauthed RCE via nbbsdtar", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language UNION SELECT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid UPDATE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id UPDATE", "ET WEB_SPECIFIC_APPS Rakhi Software Price Comparison Script product.php subcategory_id SQL Injection", "ET WEB_SERVER HP OpenView Network Node Manager CGI Directory Traversal", "ET WEB_SERVER Attempt To Access MSSQL xp_enumdsn/xp_enumgroups/xp_ntsec_enumdomains Stored Procedure Via URI", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent UPDATE", "ET WEB_SPECIFIC_APPS Possible APC Switched Rack PDU Web Administration Interface Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage ASCII", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen ASCII", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id SELECT", "ET SCAN Tomcat Auth Brute Force attempt (manager)", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id UPDATE", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid INSERT", "ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user UPDATE", "ET WEB_SPECIFIC_APPS SiteGo file parameter Local File Inclusion Attempt", "ET WEB_SERVER Oracle Secure Enterprise Search 10.1.8 search Script XSS attempt", "ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA Authentication Bypass (management) (CVE-2021-20016)", "ET WEB_SPECIFIC_APPS Joomla mod_virtuemart_featureprod module Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp UPDATE", "ET WEB_SPECIFIC_APPS Wordpress Token Manager Plugin tokenmanageredit page XSS Attempt", "ET WEB_SPECIFIC_APPS Joomla com_g2bridge controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke Surveys pollID parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId INSERT", "ET WEB_SPECIFIC_APPS ViArt Shop Evaluation ajax_list_tree.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php INSERT", "ET EXPLOIT Cisco SD-WAN vManage Software Directory Traversal (CVE-2020-26073)", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- ipsearch.admin.php SELECT", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv UPDATE", "ET WEB_SPECIFIC_APPS Froxlor customer_ftp.php id Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft UNION SELECT", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id SELECT", "ET WEB_SPECIFIC_APPS Openfire Jabber-Server type Parameter INSERT INTO SQL Injection Attempt", "GPL WEB_SPECIFIC_APPS PHPNuke Forum viewtopic SQL insertion attempt", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id DELETE", "ET WEB_SPECIFIC_APPS BaconMap updatelist.php filepath Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid SELECT", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id UPDATE", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php by UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla FaceBook Component face_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS OrangeHRM path Parameter Local File Inclusion Attempt", "ET

	WEB_SPECIFIC_APPS Nagios XI view parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection Attempt -- print.asp id ASCII", "ET WEB_SERVER ImageMagick CVE-2016-3717 Local File Read Inbound (label: + mvg)", "ET WEB_SPECIFIC_APPS Blogplus block_center_down.php Local File Inclusion", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID INSERT", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids SELECT", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid UPDATE", "ET SCAN JCE Joomla Scanner", "ET WEB_SPECIFIC_APPS iScripts MultiCart orderid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch UPDATE", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno DELETE", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php INSERT", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id INSERT", "GPL EXPLOIT ISAPI .idq attempt", "ET WEB_SPECIFIC_APPS ASPApps.com Template Creature media_level.asp mcatid parameter SQL Injection", "ET WEB_SPECIFIC_APPS DEDECMS feedback_js.php arcurl Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Nucleus PLUGINADMIN.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat DELETE", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month ASCII", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand ASCII", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid DELETE", "ET WEB_SPECIFIC_APPS Thyme export.php export_to Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection Attempt -- print.asp id INSERT", "ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M4", "ET WEB_SPECIFIC_APPS Joomla com_ckforms controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid ASCII", "ET WEB_CLIENT WSO 4.2.5 Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Joomla com_zoomportfolio component UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Openscrutin utilisateur.class.php path_om Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat UPDATE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code INSERT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid DELETE", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order UNION SELECT", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php UNION SELECT", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id INSERT", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank DELETE", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id DELETE", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang ASCII", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID INSERT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id SELECT", "ET WEB_SPECIFIC_APPS WordPress Copperleaf Photolog postid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect INSERT", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid UPDATE", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection Attempt -

	- default.asp id DELETE", "ET WEB_SPECIFIC_APPS A Better Member-Based ASP Photo Gallery view.asp entry parameter SQL injection", "ET WEB_CLIENT ALFA TEaM Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS PHP-Fusion mguser fotoalbum album_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID DELETE", "ET WEB_SPECIFIC_APPS Openads row Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni ASCII", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url UNION SELECT", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS WHCMS smarty Parameter Remote File inclusion Attempt 2", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat UPDATE", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username INSERT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail ASCII", "ET WEB_SPECIFIC_APPS Informacion General informacion_general.php UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum UNION SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID DELETE", "ET WEB_SPECIFIC_APPS programsrating postcomments.php id XSS attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent INSERT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic SELECT", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s DELETE", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id SELECT", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid DELETE", "ET WEB_SPECIFIC_APPS eGroupware loaddetails.php script UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid UPDATE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang SELECT", "ET WEB_SPECIFIC_APPS DeluxeBB misc.php qorder Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img UNION SELECT", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-5", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID SELECT", "ET WEB_SPECIFIC_APPS phpDatingClub website.php page Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS AvailScript Photo Album Script pics.php sid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID UPDATE", "ET WEB_SPECIFIC_APPS bug_actiongroup_page.php script Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category INSERT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick INSERT", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key UNION SELECT", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php categoryid DELETE", "ET WEB_SPECIFIC_APPS Mambo Component com_viewfulllisting SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress Mini Mail Dashboard Widget abspath Remote File inclusion Attempt", "ET EXPLOIT Attempted ThinkPHP < 5.2.x RCE Outbound (CVE-2018-20062)", "ET WEB_SPECIFIC_APPS Nagios Expand Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id DELETE", "ET WEB_SPECIFIC_APPS Rails Arbitrary File Disclosure Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre SELECT", "ET WEB_SPECIFIC_APPS Joomla! Soundset Component 'cat_id' Parameter UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS

	Concrete DIR_FILES_BLOCK_TYPES_CORE Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id UPDATE", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id SELECT", "ET WEB_SPECIFIC_APPS OSSIM repository_attachment.php UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PointComma pctemplate.php pcConfig Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id INSERT", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id SELECT", "ET WEB_SPECIFIC_APPS jSchool Advanced id_gallery Parameter SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list UPDATE", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id UPDATE", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name ASCII", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i SELECT", "ET WEB_SPECIFIC_APPS Web File Browser file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS jbShop e107 CMS plugin item_id parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid INSERT", "ET WEB_SPECIFIC_APPS Constructr CMS SQL Injection Attempt -- constructrXmlOutput.content.xml.php page_id ASCII", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa ASCII", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids ASCII", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id ASCII", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat ASCII", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id UPDATE", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id SELECT", "ET WEB_SPECIFIC_APPS asaher pro view_blog_comments.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id UPDATE", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php sqlcmd DELETE", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php UNION SELECT", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk SELECT", "ET WEB_CLIENT Suspicious PHP UNZIP Tool Accessed on External Possibly Compromised Server", "ET MALWARE D-Link ShareCenter (DNS-320/325) RCE (Outbound)", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action UPDATE", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id UNION SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat UPDATE", "ET WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order UNION SELECT", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor ASCII", "ET WEB_SPECIFIC_APPS V-EVA Classified Script clsid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice SELECT", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP UPDATE", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic INSERT", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment UPDATE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby SELECT", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- archives.php month UNION SELECT", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID ASCII", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id ASCII", "ET WEB_SPECIFIC_APPS artmedic weblog artmedic_print.php date Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Sonicwall NSA E7500 XSS attempt (fwReg parameter)", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic UNION SELECT", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp author INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt --

	ad.asp AD_ID INSERT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid DELETE", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile UNION SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite UNION SELECT", "ET WEB_SPECIFIC_APPS phpRS id parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite UPDATE", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm UNION SELECT", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id DELETE", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did UPDATE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page SELECT", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp SELECT", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid SELECT", "ET WEB_SPECIFIC_APPS Joomla! Survey Manager Component UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk UPDATE", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id UNION SELECT", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy ASCII", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id UPDATE", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid DELETE", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat SELECT", "ET WEB_SPECIFIC_APPS Wiki Web Help configpath parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid ASCII", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id DELETE", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID DELETE", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid INSERT", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id ASCII", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick ASCII", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp UPDATE", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course INSERT", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php INSERT", "ET WEB_SPECIFIC_APPS Hubscript XSS Attempt", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity UNION SELECT", "ET WEB_SPECIFIC_APPS Horde XSS attempt test.php (2)", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 20", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id SELECT", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did UPDATE", "ET DOS LOIC GET", "ET WEB_SPECIFIC_APPS Joomla com_rsgallery2 Component catid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid INSERT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid DELETE", "ET WEB_SPECIFIC_APPS Gallery2 adodb-error.inc.php ADODB_LANG Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id INSERT", "ET WEB_SPECIFIC_APPS Joomla Jimtawl Component task Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL Injection Attempt -- haberoku.asp id ASCII", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl ASCII", "ET WEB_SERVER Bot Search RFI Scan (ByroeNet/Casper-Like planetwork)", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen UNION SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail INSERT", "ET WEB_SPECIFIC_APPS Mambo SQL

	Injection Attempt -- moscomment.php mcname UNION SELECT", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page DELETE", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid SELECT", "ET WEB_SERVER Generic Stolen Credentials Accessed on Internal Server", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID DELETE", "ET WEB_SERVER PHP Generic Remote File Include Attempt (HTTPS)", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_jphoto Component Id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_CLIENT Generic File Upload Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp year ASCII", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 INSERT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick UPDATE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID ASCII", "ET WEB_SPECIFIC_APPS Joomla NoticeBoard Component controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort UNION SELECT", "ET WEB_SPECIFIC_APPS Mu Perspectives Cms id parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid INSERT", "ET WEB_SPECIFIC_APPS Joomla com_blog Component id Parameter INSERT INTO SQL Injection Attempt", "ET SCAN JAWS Webserver Unauthenticated Shell Command Execution", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id UPDATE", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa INSERT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- users.php id ASCII", "ET WEB_SERVER ColdFusion scheduleedit access", "ET WEB_SPECIFIC_APPS Joomla com_zoomportfolio component INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PozScripts Business Directory Script cid parameter SQL Injection", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username DELETE", "ET WEB_SPECIFIC_APPS LetoDMS lang Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa SELECT", "ET WEB_SPECIFIC_APPS digiSHOP cart.php UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp MessagePart XSS Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter INSERT", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke viewslink module sid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)", "ET WEB_SPECIFIC_APPS OSClass id parameter data access Attempt 1", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id DELETE", "ET WEB_SPECIFIC_APPS Joomla FaceBook Component face_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_job Component id_job Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent INSERT", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id INSERT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start INSERT", "ET WEB_SPECIFIC_APPS phpRS id parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id UPDATE", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id SELECT", "ET WEB_SPECIFIC_APPS Joomla com_joaktree Component treeId Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection

	Attempt -- detail.asp ID ASCII", "ET WEB_SPECIFIC_APPS PHP link Directory sbcat_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass DELETE", "ET WEB_SPECIFIC_APPS Dell OpenManage Server Administrator topic parameter XSS Attempt", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id UNION SELECT", "ET WEB_SERVER X-Sec Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php ASCII", "ET WEB_SPECIFIC_APPS Joomla com_some controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id ASCII", "ET WEB_SPECIFIC_APPS WordPress Tune Library Plugin letter parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id UPDATE", "ET WEB_SPECIFIC_APPS asaher pro downloads.php row_y5_site_configuration Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Appointment Hour Booking - WordPress Plugin - Stored XSS (CVE-2019-13505)", "ET WEB_SERVER PHP Possible zlib Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla Component Media Mall Factory Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which SELECT", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list INSERT", "ET WEB_SPECIFIC_APPS Aigaion ID Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp secondgroup ASCII", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary DELETE", "ET WEB_SPECIFIC_APPS Joomla Component Billy Portfolio catid Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID INSERT", "ET SCAN abdullkarem Wordpress PHP Scanner", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod SELECT", "ET WEB_SPECIFIC_APPS Mambo AHS Shop component INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre SELECT", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id DELETE", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre DELETE", "ET WEB_SPECIFIC_APPS Wordpress whois search domain Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare INSERT", "ET WEB_SPECIFIC_APPS Possible IBM Lotus Connections simpleSearch.do Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id ASCII", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat UPDATE", "ET ACTIVEX AoA Audio Extractor ActiveX Control Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS PHP Classified ads software cid parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Worksystems linkbar.php cfile Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wordpress eShop plugin viewemail parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_musicgallery Component Id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email ASCII", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName UPDATE", "ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id INSERT INTO SQL Injection Attempt", "ET WEB_SERVER Generic Mailer Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro ASCII", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url INSERT", "ET WEB_SPECIFIC_APPS Dompdf dompdf.php input_file Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area UPDATE", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id SELECT", "ET SCAN Nmap Scripting Engine User-Agent Detected

	(Nmap NSE)", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M3", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country INSERT", "ET WEB_SPECIFIC_APPS Joomla com_eventcal mosConfig_absolute_path Parameter Remote File inclusion Attempt", "ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key ASCII", "ET WEB_SPECIFIC_APPS Potential Wordpress local file disclosure vulnerability", "ET WEB_SPECIFIC_APPS ispCP Omega admin1.template.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS e107 imgp Parameter Remote File inclusion Attempt", "GPL EXPLOIT cmd? access", "ET WEB_SPECIFIC_APPS Oracle Event Processing FileUploadServlet Arbitrary File Upload", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass UPDATE", "ET WEB_SPECIFIC_APPS e107 123 FlashChat Module 123flashchat.php e107path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID UNION SELECT", "ET WEB_SPECIFIC_APPS Simple Customer contact.php SQL injection", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler ASCII", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course UNION SELECT", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num INSERT", "GPL WEB_SERVER Tomcat null byte directory listing attempt", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand UNION SELECT", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user ASCII", "ET WEB_SPECIFIC_APPS Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat DELETE", "ET WEB_SPECIFIC_APPS x10 Automatic MP3 Script layout_lyrics.php web_root Parameter Local file Inclusion", "ET WEB_SPECIFIC_APPS Joomla com_quicknews Component newsid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Possible Zenoss Network Monitoring Application UNTION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS OTManager ADM_Pagina.php Tipo Remote File Inclusion", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id SELECT", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp UPDATE", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position ASCII", "ET WEB_SPECIFIC_APPS Amateur Photographer Image Gallery albumid parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId SELECT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did UPDATE", "ET WEB_SPECIFIC_APPS WebSense Email security msgForwardToRiskFilter.asp Queue XSS Attempt", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite DELETE", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq DELETE", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk DELETE", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user DELETE", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid SELECT", "ET WEB_SPECIFIC_APPS CultBooking lang Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id UPDATE", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci SELECT", "ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (3)", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId ASCII", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id INSERT", "ET WEB_SPECIFIC_APPS Wordpress NextGEN Gallery Plugin Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id ASCII", "ET

	WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter ASCII", "ET WEB_SPECIFIC_APPS WordPress Mailing List plugin wpabspath parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID ASCII", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic ASCII", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username SELECT", "ET WEB_SERVER Bot Search RFI Scan (Casper-Like Jcomers Bot scan)", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms UNION SELECT", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode DELETE", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate SELECT", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list DELETE", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass ASCII", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid UPDATE", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id UPDATE", "ET WEB_SPECIFIC_APPS WebSense Email security viewHeaders.asp ServerName XSS Attempt", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID UNION SELECT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 ASCII", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno SELECT", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id ASCII", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f SELECT", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id UPDATE", "ET MALWARE JAWS Webserver Unauthenticated Shell Command Execution", "ET WEB_SPECIFIC_APPS DBHcms editmenu Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 DELETE", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message INSERT", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date SELECT", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id DELETE", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid SELECT", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo INSERT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp ASCII", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid UPDATE", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid ASCII", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query UNION SELECT", "ET WEB_SPECIFIC_APPS Bugzilla token.cgi HPP e-mail validation bypass Attempt URI", "ET WEB_SPECIFIC_APPS Possible JBoss/JMX InvokerServlet RCE Using Marshalled Object", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php DELETE", "ET WEB_SPECIFIC_APPS Joomla com_avosbilletsy Component id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick DELETE", "ET WEB_SPECIFIC_APPS iGaming CMS previews.php browse parameter SQL injection", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type UPDATE", "ET WEB_SPECIFIC_APPS joomla com_djcatalog component UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS BLOG CMS nsextt parameter Cross Site Scripting Vulnerability", "ET WEB_SPECIFIC_APPS Possible Achievo userid= Variable UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress SocialGrid Plugin default_services Cross-

	Site Scripting Vulnerability", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number INSERT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID UNION SELECT", "ET WEB_SERVER Attempt To Access MSSQL xp_fileexist Stored Procedure Via URI to Locate Files On Disk", "ET WEB_SPECIFIC_APPS TCExam tce_xml_user_results.php script UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Apache Archive editAppearance script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username ASCII", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message SELECT", "ET WEB_SERVER Tilde in URI - potential .conf source disclosure vulnerability", "ET WEB_SPECIFIC_APPS Dolibarr ERP CRM PHP Code Injection", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx ASCII", "ET WEB_SPECIFIC_APPS Basebuilder main.inc.php mj_config Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla com_jomestate Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout UPDATE", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite ASCII", "ET WEB_SPECIFIC_APPS WordPress Cloudsafe365 file parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Auto Listings Script moreinfo.php itemno Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id INSERT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id SELECT", "ET WEB_SPECIFIC_APPS p-Table for WordPress wptable-tinymce.php ABSPATH Parameter RFI Attempt", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat INSERT", "ET WEB_SPECIFIC_APPS Dokeos and Chamilo open_document.php file Parameter File Disclosure Attempt", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode DELETE", "ET WEB_SPECIFIC_APPS SaurusCMS class.writeexcel_workbook.inc.php class_path Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp AD_ID SELECT", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid DELETE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order UPDATE", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id UPDATE", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id ASCII", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php UPDATE", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp SELECT", "ET WEB_SPECIFIC_APPS Joomla Component com_kkcontent Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID INSERT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_Type_ID UPDATE", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from INSERT", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo SELECT", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa UNION SELECT", "ET WEB_SPECIFIC_APPS Nagios Expand Parameter XSS Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid DELETE", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- inlinemod.php postids UNION SELECT", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id DELETE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf DELETE", "GPL WEB_SERVER perl post attempt", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_Type_ID UNION SELECT", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass DELETE", "ET WEB_SPECIFIC_APPS e107 IMAGES_DIRECTORY Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id SELECT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user SELECT", "ET

	WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex UPDATE", "ET WEB_CLIENT Generic Webshell Accessed on Compromised External Server", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews INSERT", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which UPDATE", "ET WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order INSERT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id UNION SELECT", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid SELECT", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order ASCII", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date UPDATE", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID SELECT", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid UPDATE", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm INSERT", "ET WEB_SPECIFIC_APPS Aj Square RSS Reader url SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Fusion mguser fotoalbum album_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp id UPDATE", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID ASCII", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 19", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id INSERT", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id SELECT", "ET WEB_SERVER Suspected Webshell wmic Command (Inbound)", "ET WEB_SPECIFIC_APPS Joomla com_zoomportfolio component DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Informacion General informacion_general.php INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Cacti cacti/utilities.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php by SELECT", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid INSERT", "ET WEB_SPECIFIC_APPS Joomla component com_jinc (newsid) Blind SQL Injection Attempt", "ET WEB_CLIENT WSO 2.5 Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat ASCII", "ET WEB_SPECIFIC_APPS Joomla techfolio component INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms UPDATE", "ET WEB_SPECIFIC_APPS e107 resetcore.php SQL Injection attempt", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user ASCII", "ET WEB_SPECIFIC_APPS Zabbix popup.php DELETE FROM SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort DELETE", "ET WEB_SPECIFIC_APPS Joomla Component joomlaXplorer admin.joomlaxplorer.php File Inclusion Attempt", "ET WEB_SPECIFIC_APPS IBBY nouvelles.php id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Wordpress plugin Flash Album Gallery pid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_CLIENT Generic Cpanel Cracker Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS I-

	Escorts Directory country_id parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Possible Joomla! Game Server Component 'id' Parameter SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby UNION SELECT", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id SELECT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav DELETE", "ET WEB_SPECIFIC_APPS LightNEasy File Manager language Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php ASCII", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit UPDATE", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id INSERT", "ET WEB_SPECIFIC_APPS Joomla com_jshop pid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Gazi Download Portal SQL Injection Attempt -- down_indir.asp id ASCII", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew DELETE", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp SELECT", "ET WEB_SPECIFIC_APPS phpProfiles topic_title parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id ASCII", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password UPDATE", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id SELECT", "ET WEB_SPECIFIC_APPS WordPress 1-jquery-photo-gallery-slideshow-flash plugin page Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID ASCII", "ET WEB_SPECIFIC_APPS XOOPS Module dictionary 2.0.18 (detail.php) SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php UPDATE", "ET EXPLOIT NB8-04 - Possible Unauthed RCE via whitelist bypass", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php INSERT", "ET WEB_SPECIFIC_APPS Possible AWStats awstats.pl Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType INSERT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id UPDATE", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp UPDATE", "ET WEB_SPECIFIC_APPS Openfoncier bible.class.php script Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eMates SQL Injection Attempt -- newsdetail.asp ID UPDATE", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id ASCII", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 29", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids DELETE", "ET WEB_SPECIFIC_APPS Bandwebsite lyrics.php id parameter Sql Injection", "ET WEB_SPECIFIC_APPS GeekLog filemgt UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci DELETE", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup DELETE", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent UPDATE", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did INSERT", "ET WEB_SPECIFIC_APPS Joomla Component com_doqment Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id ASCII", "ET WEB_SPECIFIC_APPS WordPress Tune Library Plugin letter parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text DELETE", "ET WEB_SERVER Generic Cpanel Cracker Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS DAMICMS Cross-Site Request Forgery (Add Admin)", "ET WEB_SPECIFIC_APPS RIPS function.php Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt --

	search.asp author ASCII", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid SELECT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_mailchimpccnewsletter controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID DELETE", "ET WEB_SPECIFIC_APPS Constructr CMS Injection Attempt -- constructrXmlOutput.content.xml.php page_id DELETE", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola SELECT", "ET WEB_SPECIFIC_APPS Consona Products n6plugindestructor.asp Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WordPress Browser Rejector Plugin wppath Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Group Office json.php fingerprint Parameter Remote Command Execution Attempt", "ET WEB_SPECIFIC_APPS Campsite article_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik DELETE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code UNION SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID INSERT", "ET WEB_SPECIFIC_APPS Joomla com_obsuggest controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid ASCII", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id UPDATE", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php UNION SELECT", "ET WEB_SPECIFIC_APPS Guestbook guestbook.php mes_id SQL Injection attempt", "ET WEB_CLIENT Owl PHPMailer Accessed on External Server", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod UNION SELECT", "ET WEB_SPECIFIC_APPS PMB Services id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms ASCII", "ET WEB_SPECIFIC_APPS RealtyListings type.asp iType Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email SELECT", "ET WEB_SPECIFIC_APPS DvBBS boardrule.php groupboardid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id DELETE", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum INSERT", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm UPDATE", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id SELECT", "ET WEB_SERVER /bin/bash In URI, Possible Shell Command Execution Attempt Within Web Exploit", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no DELETE", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid ASCII", "ET WEB_SPECIFIC_APPS MyOWNspace getfeed.php file Parameter Local File Inclusion Attempt(1)", "ET WEB_SPECIFIC_APPS bug_actiongroup_ext_page.php script Local File Inclusion Attempt", "GPL WEB_SERVER Tomcat directory traversal attempt", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order ASCII", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant ASCII", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid ASCII", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id INSERT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page DELETE", "ET WEB_SERVER Generic Email Spoofing Tool Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent ASCII", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid ASCII", "GPL EXPLOIT iissamples access", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp SELECT", "ET WEB_SERVER Oracle BEA

	Weblogic Server 10.3 searchQuery XSS attempt", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id ASCII", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp AD_ID UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress PHP Speedy Plugin page Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country UPDATE", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode INSERT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID SELECT", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id INSERT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug UNION SELECT", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp Dictionary XSS Attempt", "ET WEB_SPECIFIC_APPS AstroSPACES profile.php SQL Injection", "ET WEB_SPECIFIC_APPS MantisBT db_type Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS KingCMS menu.php CONFIG Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id ASCII", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- usermgr.php gid DELETE", "ET WEB_SPECIFIC_APPS Joomla com_job Component id_job Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid DELETE", "ET WEB_SPECIFIC_APPS Informacion General informacion_general.php DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid ASCII", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- compare_product.php id INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 UPDATE", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup UNION SELECT", "ET WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex INSERT", "ET WEB_SPECIFIC_APPS Joomla com_perchagallery Component id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc UPDATE", "ET WEB_SPECIFIC_APPS EasySiteEdit langval Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Simplis CMS download_file Parameter Local File Inclusion Attempt", "ET SCAN NMAP SQL Spider Scan", "ET WEB_SERVER Possible IIS Integer Overflow DoS (CVE-2015-1635)", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field UNION SELECT", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen INSERT", "ET WEB_SPECIFIC_APPS vBulletin sortorder parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent ASCII", "ET WEB_SERVER Likely Malicious Request for /proc/self/fd/", "ET WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct UNION SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name UPDATE", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name SELECT", "ET WEB_SPECIFIC_APPS PHPOF DB_AdoDB.Class.PHP PHPOF_INCLUDE_PATH parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids ASCII", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php website ASCII", "ET WEB_SPECIFIC_APPS Joomla com_ztautolink controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id DELETE", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL Injection Attempt -- haberoku.asp id SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code UPDATE", "ET WEB_SPECIFIC_APPS PHPStore Wholesales id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Joomla Component Ek rishta 2.10 - SQL Injection 1", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection

	Attempt -- default.asp id SELECT", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby INSERT", "ET WEB_SPECIFIC_APPS TorrentTrader Classic delreq.php categ Parameter Sql Injection", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid UNION SELECT", "ET WEB_SPECIFIC_APPS Openfoncier action.class.php script Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid SELECT", "ET WEB_SPECIFIC_APPS Manage Engine Service Desk Plus WorkOrder.do SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola DELETE", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p INSERT", "ET WEB_SPECIFIC_APPS WordPress Copperleaf Photolog postid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS iBrowser Plugin dir Parameter Cross Site Scripting Attempt-2", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod ASCII", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID SELECT", "ET WEB_SPECIFIC_APPS BASE base_stat_common.php remote file include", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler UNION SELECT", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder UNION SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active ASCII", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail DELETE", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i INSERT", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id DELETE", "ET WEB_SPECIFIC_APPS TFTgallery adminlangfile Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ UPDATE", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id ASCII", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php INSERT", "ET WEB_SERVER SHOW CURDATE/CURTIME SQL Injection Attempt in URI", "ET WEB_SPECIFIC_APPS Informacion General informacion_general.php SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id ASCII", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic DELETE", "ET WEB_SPECIFIC_APPS Possible Docebo UPDATE SET SQL Injection Attempt", "ET WEB_SERVER Tilde in URI - potential .cgi source disclosure vulnerability", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid ASCII", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage DELETE", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete ASCII", "ET WEB_SPECIFIC_APPS WordPress Safe Search Plugin v1 Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl UPDATE", "ET WEB_SPECIFIC_APPS Bexfront sid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas ASCII", "ET WEB_SPECIFIC_APPS WordPress Download Manager cid parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick UPDATE", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id ASCII", "ET WEB_SPECIFIC_APPS Joomla Foobla Suggestions Component idea_id UPDATE SET SQL Injection Attempt", "ET WEB_SERVER Likely Malicious Request for /proc/<pid>/smaps", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent UPDATE", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid ASCII", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent SELECT", "ET

	EXPLOIT [ConnectWise CRU] Potential Sonicwall SRA SQLi (CVE-2019-7481)", "ET WEB_SPECIFIC_APPS Horde XSS attempt passwd/main.php (2)", "ET WEB_SPECIFIC_APPS coRED CMS rubID Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PRADO PHP Framework functional.php Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS Flatchat pmscript.php with Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla com_perchagallery Component id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld UPDATE", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email INSERT", "ET WEB_SPECIFIC_APPS Unique Ads (UDS) SQL Injection Attempt -- banner.php bid SELECT", "ET WEB_SPECIFIC_APPS Joomla com_jeauto view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country UNION SELECT", "ET WEB_SPECIFIC_APPS Sisplet CMS komentar.php site_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak ASCII", "ET WEB_SPECIFIC_APPS Blogplus window_down.php Local File Inclusion", "ET WEB_SPECIFIC_APPS RSS Simple News news.php pid parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id UPDATE", "ET WEB_SPECIFIC_APPS Havalite userId parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS SFS EZ BIZ PRO track.php id Parameter Remote SQL Injection", "ET WEB_CLIENT MINI MO Webshell Accessed on External Compromised Server", "ET EXPLOIT Possible ELEFANTE/ElephantBeetle WebShell Access Inbound", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main INSERT", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-2", "ET WEB_SPECIFIC_APPS Mambo Cache_Lite Class mosConfig_absolute_path Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid INSERT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic INSERT", "ET WEB_SPECIFIC_APPS Horde IMP fetchmailprefs.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp INSERT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid UPDATE", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce INSERT", "ET WEB_SPECIFIC_APPS DaFun Spirit lgsl_settings.php lgsl_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay DELETE", "ET WEB_SPECIFIC_APPS Community CMS view.php article_id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type DELETE", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php categoryid ASCII", "ET WEB_SPECIFIC_APPS Design4Online UserPages2 SQL Injection Attempt -- page.asp art_id SELECT", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic UPDATE", "ET WEB_SPECIFIC_APPS Nuke Evolution Xtreme pid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat INSERT", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category ASCII", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak SELECT", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname SELECT", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType UNION SELECT", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID ASCII", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection

	Attempt -- email.php id DELETE", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut UPDATE", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid DELETE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active INSERT", "ET WEB_SERVER Possible Cisco ASA Appliance Clientless SSL VPN HTML Rewriting Security Bypass Attempt/Cross Site Scripting Attempt", "GPL WEB_SERVER /scripts/iisadmin/default.htm access", "ET WEB_SPECIFIC_APPS AjaxPortal ajaxp_backend.php page Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Shape Web Solutions imprimir.php DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid SELECT", "ET ACTIVEX Awingsoft Web3D Player Remote Buffer Overflow", "ET WEB_SPECIFIC_APPS Car Portal car Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter DELETE", "ET WEB_SPECIFIC_APPS HotNews hnmain.inc.php3 incdir Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img INSERT", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id INSERT", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft UPDATE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass UPDATE", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie SELECT", "ET WEB_SPECIFIC_APPS WordPress CataBlog plugin category parameter Cross-Site Scripting Attempt", "ET WEB_SERVER Possible Perl Shell in HTTP POST", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip DELETE", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php user_login_cookie UNION SELECT", "ET WEB_SERVER jQuery File Upload Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname SELECT", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state INSERT", "ET WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_perchagallery Component id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName DELETE", "ET WEB_SPECIFIC_APPS Wordpress plugin Flash Album Gallery pid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_jr_questionnaire Directory Traversal Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid INSERT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie INSERT", "ET WEB_SPECIFIC_APPS Joomla Foobla Suggestions Component idea_id DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi SELECT", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass INSERT", "ET WEB_SPECIFIC_APPS Wordpress Plugins Wp-ImageZoom file parameter Remote File Disclosure Vulnerability", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search DELETE", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType DELETE", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num UNION SELECT", "ET WEB_SPECIFIC_APPS WebPhotoPro rub.php idr Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Apache Archive userlist script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS jbShop e107 CMS plugin item_id parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 UPDATE", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main UPDATE", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main ASCII", "ET WEB_SPECIFIC_APPS coRED CMS rubID Parameter

	INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS LightOpenCMS smarty.php cwd Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php blogid SELECT", "ET WEB_SPECIFIC_APPS Joomla Component com_personel (id) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno UPDATE", "GPL SQL Oracle iSQLPlus login.uix username overflow attempt", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php template UNION SELECT", "ET WEB_SPECIFIC_APPS TurnkeyForms Business Survey Pro id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id UPDATE", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp DELETE", "ET WEB_SPECIFIC_APPS OpenX phpAdsNew phpAds_geoPlugin Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Mambo Zorder zorder Parameter UPDATE SET SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS phpMiniAdmin db Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id UPDATE", "ET WEB_SPECIFIC_APPS SaurusCMS class.writeexcel_worksheet.inc.php class_path Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID UPDATE", "ET WEB_SPECIFIC_APPS CafeEngine id Remote SQL Injection (menu.php)", "ET WEB_SPECIFIC_APPS Joomla SQL Reports user_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Barracuda Web Application Firewall 600 XSS attempt (backup_server)", "ET WEB_SPECIFIC_APPS Possible Achievo userid= Variable SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce INSERT", "ET WEB_SPECIFIC_APPS Joostina CMS users component Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS pfile file.php id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_phocadownload folder Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp orderby UPDATE", "ET WEB_SPECIFIC_APPS Boonex Dolphin explain Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user ASCII", "ET WEB_SPECIFIC_APPS MAXcms RFI attempt (3)", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod INSERT", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID UPDATE", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id SELECT", "ET WEB_SPECIFIC_APPS Joomla! JBudgetsMagic 'bid' Parameter INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Joomla com_yelp Component cid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf INSERT", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username UPDATE", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID ASCII", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class UNION SELECT", "ET WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct ASCII", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid UNION SELECT", "ET MALWARE Dark Nexus IoT Variant User-Agent (Outbound)", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id INSERT", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php UPDATE", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-

	trackback.php UNION SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id ASCII", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)", "ET WEB_SPECIFIC_APPS TinyBrowser upload.php file Script Execution Attempt", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id DELETE", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant UPDATE", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user ASCII", "ET WEB_SPECIFIC_APPS Joomla com_musicgallery Component Id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id SELECT", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album UPDATE", "ET WEB_SERVER Possible SQL Injection Using MSSQL sp_configure Command", "ET WEB_SPECIFIC_APPS WordPress Zotpress citation Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Sonicwall Global Management System XSS attempt (scrn_name parameter)", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname UPDATE", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id ASCII", "ET WEB_SPECIFIC_APPS Openfire Jabber-Server type Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress Count Per Day Plugin page parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text ASCII", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id SELECT", "ET WEB_SPECIFIC_APPS GeekLog filemgt SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- members.asp sent UNION SELECT", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user INSERT", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id UPDATE", "ET WEB_SPECIFIC_APPS PHP Realty dpage.php docID parameter SQL Injection", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id ASCII", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username INSERT", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user UNION SELECT", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url ASCII", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie UPDATE", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf SELECT", "ET WEB_SPECIFIC_APPS Mahara query Parameter Cross Site Scripting Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 21", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x ASCII", "ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA User-Level Authentication Bypass (portal) (CVE-2021-20016)", "ET WEB_SPECIFIC_APPS webEdition CMS edit_shop_editorFrameset.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId UPDATE", "ET WEB_SPECIFIC_APPS e107 permLink Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id UPDATE", "ET WEB_SPECIFIC_APPS iScripts MultiCart orderid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_joomportfolio (secid) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS GaziYapBoz Game Portal SQL Injection Attempt -- kategori.asp kategori DELETE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state DELETE", "ET WEB_SPECIFIC_APPS Joomla com_pinboard option Parameter Remote File inclusion

	Attempt", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page UPDATE", "ET WEB_SERVER Generic Webshell Accessed", "ET WEB_SPECIFIC_APPS Mamboleto Joomla component mamboleto.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin ASCII", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did DELETE", "ET WEB_SPECIFIC_APPS jbShop e107 CMS plugin item_id parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail SELECT", "ET WEB_SPECIFIC_APPS Informacion General informacion_general.php UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WP Forum Server wordpress plugin SQL Injection Attempt -- feed.php topic SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id UNION SELECT", "ET WEB_SPECIFIC_APPS YACS update_trailer.php context Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username UNION SELECT", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id UNION SELECT", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id INSERT", "ET WEB_SPECIFIC_APPS Wikiwig spell-check-savedicts.php to_r_list Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid UPDATE", "ET WEB_SERVER Generic Webshell Activity", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id UNION SELECT", "GPL EXPLOIT unicode directory traversal attempt", "ET WEB_SPECIFIC_APPS DVD Rental Software cat_id parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat ASCII", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue UNION SELECT", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf UPDATE", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id SELECT", "ET WEB_SPECIFIC_APPS evision cms addcontact.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi SELECT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_Type_ID SELECT", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid UNION SELECT", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid ASCII", "ET WEB_SERVER Generic Webshell Accessed on Internal Server", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user SELECT", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php UNION SELECT", "ET WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order SELECT", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre SELECT", "ET WEB_SPECIFIC_APPS Joomla! Soundset Component 'cat_id' Parameter SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS Mole viewsource.php fname Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp ASCII", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment ASCII", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php so DELETE", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro SELECT", "ET WEB_SPECIFIC_APPS PHPizabi dac.php sendChatData Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType UNION SELECT", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer INSERT", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID INSERT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category UNION SELECT", "ET

	WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword ASCII", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php so UPDATE", "ET WEB_SERVER Possible SQL Injection INTO OUTFILE Arbitrary File Write Attempt", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut INSERT", "ET WEB_SPECIFIC_APPS DS CMS DetailFile.php nFileId Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id SELECT", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail UPDATE", "ET WEB_SPECIFIC_APPS F3Site2009 LFI Exploit Attempt (new.php)", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php ASCII", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php SELECT", "ET WEB_SPECIFIC_APPS Flash Quiz question.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup INSERT", "ET WEB_SPECIFIC_APPS 724CMS section.php Module Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname ASCII", "ET WEB_SPECIFIC_APPS ClanSphere 'CKEditorFuncNum' parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS F5 Data Manager DiagCaptureFileListActionBody.do Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name DELETE", "ET WEB_SPECIFIC_APPS Joomla Component Ek rishta 2.10 - SQL Injection 2", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID DELETE", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user SELECT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user DELETE", "ET WEB_SPECIFIC_APPS T-Content Management System id_novedad Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS maxxweb Cms kategorie parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS 212cafe Board view.php qID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Flash Quiz high_score_web.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile ASCII", "ET WEB_SPECIFIC_APPS Joomla mod_currencyconverter from Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Possible Joomla! Game Server Component 'id' Parameter DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS Nuke Evolution Xtreme pid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Achievo debugger.php config_atkroot parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla EZ Realty id Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS B-Cumulus tagcloud-ru.swf Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid UNION SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid DELETE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id SELECT", "ET WEB_SPECIFIC_APPS WB News SendFriend.php config Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS phpCow skin_file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search ASCII", "ET WEB_SPECIFIC_APPS Wordpress Custom Contact Forms DB Upload/Download Auth Bypass", "ET WEB_SPECIFIC_APPS Joomla techfolio component UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent ASCII", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id UPDATE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 24", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s ASCII", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php login DELETE", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID DELETE", "ET

	WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id INSERT", "ET WEB_SPECIFIC_APPS Joomla Component com_hello INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Xt-News SQL Injection Attempt -- show_news.php id_news SELECT", "ET WEB_SPECIFIC_APPS Jenkins Pre-auth User Information Leakage", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro UPDATE", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID INSERT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola UNION SELECT", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order DELETE", "ET WEB_SPECIFIC_APPS 29o3 CMS layoutParser.php LibDir Parameter Remote File Inclusion Attempt", "ET WEB_SERVER PHP Possible expect Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Mambo Zorder zorder Parameter INSERT INTO SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Pre Online Tests Generator Pro DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id UNION SELECT", "ET WEB_SERVER ElasticSearch Directory Traversal Attempt (CVE-2015-3337)", "ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id UPDATE", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- HaberDetay.asp id INSERT", "GPL EXPLOIT Alternate Data streams ASP file access attempt", "ET WEB_SPECIFIC_APPS GaziYapBoz Game Portal SQL Injection Attempt -- kategori.asp kategori SELECT", "ET WEB_SPECIFIC_APPS Grady Levkov id Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- category.php id_category ASCII", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where SELECT", "ET WEB_SPECIFIC_APPS Ektron CMS400.NET reterror.aspx info Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php catid UPDATE", "ET WEB_SPECIFIC_APPS Snitz Forums 2000 SQL Injection Attempt -- pop_profile.asp id UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi DELETE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite DELETE", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id ASCII", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_recent.asp currentpage DELETE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid ASCII", "ET WEB_SPECIFIC_APPS Apache Archive addRepository script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_mgm Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS phpBMS invoices_discount_ajax.php id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage INSERT", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode ASCII", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class UPDATE", "ET WEB_SPECIFIC_APPS Immophp secteur parameter Cross Site Scripting Attempt", "ET EXPLOIT ADB Broadband Authorization Bypass", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat DELETE", "ET WEB_SPECIFIC_APPS Joomla Component com_hello SELECT FROM SQL Injection Attempt", "ET WEB_SERVER Cisco IOS HTTP Server Exec Command Execution Attempt", "ET WEB_SPECIFIC_APPS Apache Tomcat Sort Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action DELETE", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp listing_price DELETE", "ET WEB_SPECIFIC_APPS Joomla com_hdflvplayer Component id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SERVER PHP Possible php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId UNION

	SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID ASCII", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id SELECT", "ET WEB_CLIENT Cpanel Cracker Accessed on External Server", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid INSERT", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat UPDATE", "ET WEB_SPECIFIC_APPS digiSHOP cart.php INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DevelopItEasy Photo Gallery cat_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- manufacturer.php id_manufacturer SELECT", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id INSERT", "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi INSERT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear INSERT", "ET WEB_SPECIFIC_APPS DEDECMS feedback_js.php arcurl Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language UPDATE", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup ASCII", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php mcname ASCII", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid ASCII", "ET WEB_SPECIFIC_APPS Softwebs Nepal Ananda Real Estate SQL Injection Attempt -- list.asp agent DELETE", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID DELETE", "ET WEB_SPECIFIC_APPS Zabbix popup.php INSERT INTO SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Cartweaver 3 Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection Attempt -- detail.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS evision cms addtour.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat UNION SELECT", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent UNION SELECT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID ASCII", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid UPDATE", "ET WEB_SERVER Apache Tomcat Boundary Overflow DOS/File Upload Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID DELETE", "ET WEB_SERVER 3Com Intelligent Management Center Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id ASCII", "ET WEB_SPECIFIC_APPS Turuncu Portal SQL Injection Attempt -- h_goster.asp id UNION SELECT", "ET WEB_SERVER MYSQL Benchmark Command in URI to Consume Server Resources", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum.asp baslik ASCII", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci DELETE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us UNION SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name ASCII", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid ASCII", "ET WEB_SPECIFIC_APPS TEMENOS T24 skin parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid SELECT", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID SELECT", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue SELECT", "ET WEB_SPECIFIC_APPS playSMS init.php apps_path themes parameter local file inclusion", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt --

	news.php id SELECT", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname ASCII", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId DELETE", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki deki_plugin.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- printarticle.asp DELETE", "ET EXPLOIT TIBCO JasperReports Authenticated Arbitrary File Read Attempt (CVE-2018-5430)", "ET WEB_SPECIFIC_APPS Possible Joomla! Game Server Component 'id' Parameter UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS PHP Membership Site Manager Script key Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer UNION SELECT", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id INSERT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s INSERT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp id SELECT", "ET WEB_SPECIFIC_APPS Invision Community Blog Mod SQL Injection Attempt -- entry_reply_entry.php eid DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids SELECT", "ET WEB_SPECIFIC_APPS Enthusiast path parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us INSERT", "ET WEB_SPECIFIC_APPS ACGVannu SQL Injection Attempt -- modif.html id_mod DELETE", "ET MALWARE ELF/Mirai Variant User-Agent (Outbound)", "ET WEB_SPECIFIC_APPS XOOPS Makale Module id SQL Injection", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id DELETE", "ET WEB_SPECIFIC_APPS MAXcms fm_includes_special Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Possible Adobe Flex SDK index.template.html Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID SELECT", "ET WEB_SPECIFIC_APPS WordPress Skysa Official submit parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email UPDATE", "ET WEB_SPECIFIC_APPS Mambo N-Myndir UPDATE SET SQL Injection Attempt", "ET WEB_SERVER Generic Mailer Check Accessed on Internal Server", "ET WEB_SPECIFIC_APPS Joomla com_joaktree Component treeId Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq ASCII", "ET WEB_SPECIFIC_APPS SonicWALL SonicOS searchStr XML Tag Script Insertion Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler DELETE", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip INSERT", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- DisplayResults.php iSearchID ASCII", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki link.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp id DELETE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang UNION SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo UPDATE", "ET WEB_SPECIFIC_APPS eNdonesia artid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse DELETE", "ET WEB_SPECIFIC_APPS Realtor v_cat SQL Injection", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank SELECT", "ET WEB_SPECIFIC_APPS asaher pro add_comments.php row_y5_site_configuration Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass UNION SELECT", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch DELETE", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp Scoring XSS Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType INSERT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup ASCII", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php rating UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_collector

	Component Arbitrary File Upload Vulnerability", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid DELETE", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki wgDekiPluginPath parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php template UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword SELECT", "ET WEB_SPECIFIC_APPS Redaxo CMS specials.inc.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Exponent file parameter Local File Inclusion Attempt", "ET WEB_SERVER /bin/tsh In URI Possible Shell Command Execution Attempt", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id UPDATE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID DELETE", "ET WEB_SPECIFIC_APPS PHP phpMyAgenda rootagenda Remote File Include Attempt", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id ASCII", "ET WEB_SPECIFIC_APPS Free Blog Arbitrary File Deletion Attempt", "ET WEB_SERVER HP Intelligent Management Java Deserialization RCE Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce DELETE", "ET WEB_SPECIFIC_APPS Joomla DS-Syndicate Component feed_id SQL Injection", "ET WEB_SPECIFIC_APPS Joomla Component com_jphone Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Possible Joomla! com_album Component Local File Inclusion Attempt", "ET WEB_SERVER Suspected Generic Webshell Activity (Outbound)", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID DELETE", "ET WEB_SPECIFIC_APPS Mxmania File Upload Manager (FUM) SQL Injection Attempt -- detail.asp ID DELETE", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php website INSERT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where UNION SELECT", "ET WEB_SERVER SQL Injection Attempt (Agent NV32ts)", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch INSERT", "ET WEB_SPECIFIC_APPS WordPress LeagueManager plugin group parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla Dada Mail Manager Component config.dadamail.php GLOBALS Parameter Local File Inclusion", "ET WEB_SERVER Suspected Webshell arp Command (Inbound)", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid INSERT", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id DELETE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps SELECT", "ET ACTIVEX winhlp32 ActiveX control attack - phase 3", "ET WEB_SPECIFIC_APPS QuickTeam qte_web.php qte_web_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid DELETE", "ET WEB_SPECIFIC_APPS Tunngavik CMS id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code DELETE", "ET WEB_SPECIFIC_APPS fystyq Duyuru Scripti SQL Injection Attempt -- goster.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id SELECT", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat DELETE", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid UNION SELECT", "ET WEB_SPECIFIC_APPS WeBid ST_browsers.php include_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid ASCII", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ SELECT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language SELECT", "ET WEB_SPECIFIC_APPS DeZine DZcms products.php pcat parameter SQL injection", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php

	categoryid SELECT", "ET WEB_SPECIFIC_APPS millionpixel payment.php order_id XSS attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id UPDATE", "ET WEB_SPECIFIC_APPS Joomla eZine Component d4m_ajax_pagenav.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id INSERT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name UNION SELECT", "ET WEB_SPECIFIC_APPS ndCMS editor.aspx index Parameter SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer DELETE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area UNION SELECT", "ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WP Generic revslider Arbitrary File Download", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew UPDATE", "ET WEB_SERVER Generic WSO Webshell Password Prompt Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module power_management_policy_options.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id SELECT", "ET WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct SELECT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni UNION SELECT", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user DELETE", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp ASCII", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt -- news.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Openscrutin droit.class.php path_om Parameter Remote File inclusion Attempt", "ET WEB_SERVER possible IBM Rational Directory Server (RDS) Help system href browser redirect", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id SELECT", "ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusion", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki link.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla wgPicasa Component controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php UPDATE", "ET WEB_SPECIFIC_APPS Oracle E-Business Suite Financials jtfwcpnt.jsp SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay UPDATE", "ET WEB_SPECIFIC_APPS WebPhotoPro galeri_info.php ida Parameter SQL Injection", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 23", "ET WEB_SPECIFIC_APPS V-EVA Classified Script clsid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w DELETE", "ET WEB_SERVER PHP Possible ogg Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS dirLIST thumb_gen.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort DELETE", "ET WEB_SPECIFIC_APPS gpEasy CMS section parameter XSS Attempt", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp DELETE", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php UPDATE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board katid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid UNION SELECT", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order DELETE", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password INSERT", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk INSERT", "ET WEB_SPECIFIC_APPS X-Ice News System SQL Injection Attempt -- devami.asp id INSERT", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id ASCII", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum DELETE", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt --

	archive.php blogid UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Fusion maincore.php folder_level Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did DELETE", "ET WEB_SPECIFIC_APPS Blogplus block_left.php Local File Inclusion", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php INSERT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId DELETE", "ET WEB_SERVER Possible HTTP 401 XSS Attempt (Local Source)", "ET WEB_SPECIFIC_APPS SurgeFTP surgeftpmgr.cgi classid Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Free PHP photo gallery script path parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid DELETE", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid INSERT", "ET WEB_SPECIFIC_APPS Falcon Series One sitemap.xml.php dir Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-Old_Articles.php cat INSERT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup UPDATE", "ET WEB_SERVER Possible ALTER SQL Injection Attempt", "ET WEB_SERVER WPScan User Agent", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f INSERT", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout INSERT", "ET WEB_SPECIFIC_APPS Invision Gallery SQL Injection Attempt -- post.php img UPDATE", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- viewlinks.asp CategoryID INSERT", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id DELETE", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate DELETE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid UPDATE", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php UNION SELECT", "ET WEB_SPECIFIC_APPS Mambo Component com_smf smf.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Possible JBoss/JMX InvokerServlet Auth Bypass Attempt", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url UNION SELECT", "ET WEB_SPECIFIC_APPS ViArt Shop Evaluation admin_header.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid INSERT", "ET WEB_SPECIFIC_APPS Sourdough neededFiles Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID ASCII", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php INSERT", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid INSERT", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID UNION SELECT", "ET WEB_SERVER Generic PHP Mailer Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic DELETE", "ET WEB_SPECIFIC_APPS Joomla com_rsgallery2 Component catid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_rule controller Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat INSERT", "GPL WEB_SERVER python access attempt", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID UPDATE", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse UPDATE", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid INSERT", "ET WEB_SPECIFIC_APPS PHP-fusion Team Structure Infusion team_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress WP-Cumulus Plugin tagcloud.swf Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Mambo N-Myndir SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary UPDATE", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname INSERT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid

	UPDATE", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c UPDATE", "ET WEB_SPECIFIC_APPS MAXcms RFI attempt (2)", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid INSERT", "ET WEB_SPECIFIC_APPS Apache Archive configureAppearance script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Immophp annonce parameter INSERT INTO SQL Injection Attempt", "GPL WEB_SERVER viewcode access", "ET WEB_SPECIFIC_APPS People Joomla Component controller Parameter Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID SELECT", "ET WEB_SPECIFIC_APPS WebAuction lang parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! Survey Manager Component UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Planex Mini-300PU & Mini100s Cross-site Scripting Attempt", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre INSERT", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text DELETE", "ET WEB_SPECIFIC_APPS DevelopItEasy News And Article aid parameter SQL Injection", "ET WEB_SPECIFIC_APPS Fork-CMS js.php module parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order SELECT", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php SELECT", "ET WEB_SPECIFIC_APPS Cisco Collaboration Server LoginPage.jhtml Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Constructr CMS SQL Injection Attempt -- constructrXmlOutput.content.xml.php page_id SELECT", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user SELECT", "ET WEB_SERVER ALFA TEaM Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce UPDATE", "ET EXPLOIT Possible Local Active Directory Federation Services (AD FS) Replication Attempt", "ET WEB_SPECIFIC_APPS WordPress church_admin Plugin id parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id UPDATE", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat ASCII", "ET WEB_SPECIFIC_APPS Joomla com_jphoto Component Id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS playSMS init.php apps_path plug parameter local file inclusion", "ET WEB_SPECIFIC_APPS Possible Achievo userid= Variable UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno ASCII", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user DELETE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id SELECT", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search ASCII", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie ASCII", "ET WEB_SPECIFIC_APPS WordPress Tune Library Plugin letter parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail ASCII", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php so UNION SELECT", "ET WEB_SPECIFIC_APPS Wordpress Audio Player Plugin playerID parameter XSS attempt in swf", "ET WEB_SERVER PHP tags in HTTP POST", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat UPDATE", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field ASCII", "ET WEB_SPECIFIC_APPS beLive arch.php arch Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id UPDATE", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent INSERT", "ET WEB_SPECIFIC_APPS Easebay Resources Login Manager SQL Injection Attempt -- memberlist.php init_row INSERT", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id UPDATE", "ET WEB_SPECIFIC_APPS KLINK txtCodiInfo parameter UPDATE SET SQL Injection Attempt", "ET

	WEB_SPECIFIC_APPS DVD Rental Software cat_id parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- mainfile.php lang INSERT", "ET WEB_SERVER Possible MySQL SQLi User-Dump Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp aminprice INSERT", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style INSERT", "ET WEB_SPECIFIC_APPS Apache Archive networkProxies script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name ASCII", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php url DELETE", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid INSERT", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode UPDATE", "ET WEB_SPECIFIC_APPS WordPress Newsletter Plugin newsletter Parameter SQL Injection", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid INSERT", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand INSERT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici UNION SELECT", "ET WEB_SPECIFIC_APPS AlstraSoft AskMe que_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q UPDATE", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item SELECT", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item ASCII", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp listing_price SELECT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav INSERT", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url DELETE", "ET WEB_SPECIFIC_APPS Joomla intuit component intuit.php approval Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php user UPDATE", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id DELETE", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_musicgallery Component Id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SERVER PHP System Command in HTTP POST", "ET WEB_SPECIFIC_APPS DEDECMS feedback_js.php arcurl Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id ASCII", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID UPDATE", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php DELETE", "ET WEB_CLIENT APT/Hafnium SPORTSBALL Webshell Observed Outbound", "ET EXPLOIT Possible Microsoft SQL RCE Attempt (CVE-2020-0618)", "ET WEB_SPECIFIC_APPS Wordpress Zingiri webshop plugin Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eMates SQL Injection Attempt -- newsdetail.asp ID ASCII", "ET WEB_SPECIFIC_APPS dB Masters Curium CMS SQL Injection Attempt -- news.php c_id UNION SELECT", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen SELECT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick UNION SELECT", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php UPDATE", "ET WEB_SERVER possible SAP Crystal Report Server 2008 path parameter Directory Traversal vulnerability", "ET WEB_SPECIFIC_APPS Unclassified NewsBoard forum.php __tplCollection Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl UPDATE", "ET WEB_SPECIFIC_APPS Easebay Resources Login

	Manager SQL Injection Attempt -- memberlist.php init_row ASCII", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID INSERT", "GPL WEB_SERVER iisadmin access", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php INSERT", "ET SCAN Acunetix scan in progress acunetix_wvs_security_test in http_uri", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Simplemachines view parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt -- news.php id UPDATE", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php categoryid UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_dshop Component UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID ASCII", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici UPDATE", "ET WEB_SPECIFIC_APPS vBulletin cChatBox messageid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area ASCII", "ET WEB_SPECIFIC_APPS evision cms addproduct.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS phpBazar picturelib.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did ASCII", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email UPDATE", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php sqlcmd SELECT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail UNION SELECT", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum DELETE", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP ASCII", "ET WEB_SPECIFIC_APPS Bexfront sid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid ASCII", "ET WEB_SPECIFIC_APPS DM Albums album.php SECURITY_FILE Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us SELECT", "ET WEB_SPECIFIC_APPS Joomla PollXT component Itemid parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS TCExam tce_xml_user_results.php script INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id UPDATE", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id ASCII", "ET WEB_SPECIFIC_APPS Joomla com_musicgallery Component Id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla XGallery com_xgallery Component Local File Inclusion Attempt", "ET WEB_SERVER Generic Website Ransomnote Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order DELETE", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID UPDATE", "ET WEB_SPECIFIC_APPS WB News news.php config Parameter Remote File Inclusion -1", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id INSERT", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- news.php item UNION SELECT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s SELECT", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc UNION SELECT", "ET WEB_SPECIFIC_APPS BbZL.PhP lien_2 Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID ASCII", "ET WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category DELETE", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details UNION SELECT", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp

	UPDATE", "ET WEB_SPECIFIC_APPS OneFileCMS f parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php INSERT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo UNION SELECT", "ET WEB_SPECIFIC_APPS OvBB admincp.php smilieid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid UNION SELECT", "ET WEB_SPECIFIC_APPS Bexfront sid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp author SELECT", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which DELETE", "ET WEB_SPECIFIC_APPS XRMS CRM workflow-activities.php include_directory Remote File Inclusion", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id INSERT", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp DELETE", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity INSERT", "ET WEB_SPECIFIC_APPS Joomla com_blog Component id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php id UPDATE", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews DELETE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby DELETE", "ET WEB_SPECIFIC_APPS Galerie ShowGallery.php SQL Injection attempt", "ET WEB_SPECIFIC_APPS Adobe JRun Directory Traversal", "ET WEB_SPECIFIC_APPS CultBooking lang parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Ve-EDIT edit_htmlarea.php highlighter Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module blade_leds.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS 29o3 CMS layoutManager.php LibDir Parameter Remote File Inclusion Attempt", "ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M2", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search UPDATE", "ET EXPLOIT Ubiquiti Networks UniFi Cloud Key Firm v0.6.1 Host Remote Command Execution attempt", "ET DOS LOIC POST", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt -- cp_menu_data_file.php menu UNION SELECT", "ET WEB_SPECIFIC_APPS phpBB2 Plus SQL Injection Attempt -- admin_acronyms.php id ASCII", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd INSERT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 6", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php DELETE", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup SELECT", "ET WEB_SPECIFIC_APPS DirectNews uploadBigFiles.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Campsite article_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- courseLog.php scormcontopen UPDATE", "ET WEB_SPECIFIC_APPS QUICKTEAM qte_result.php title Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- contacts.php text SELECT", "ET WEB_SPECIFIC_APPS PNphpBB2 admin_smilies.php ModName parameter Local File inclusion", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- table_broken.php lid UNION SELECT", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id UNION SELECT", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse UNION SELECT", "ET WEB_SPECIFIC_APPS Possible Mambo/Joomla! com_koesubmit Component 'koesubmit.php' Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text UNION SELECT", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordNew ASCII", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP SELECT", "ET WEB_SPECIFIC_APPS BtitTracker

	SQL Injection Attempt -- torrents.php by ASCII", "ET WEB_SPECIFIC_APPS CMSQLITE id parameter Cross Site Scripting Attempt", "ET WEB_CLIENT Generic Email Spoofing Tool Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID INSERT", "ET WEB_SERVER SQL Injection BULK INSERT in URI to Insert File Content into Database Table", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- category.php catid DELETE", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- moscomment.php mcname UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat UPDATE", "ET MALWARE ELF/Mirai User-Agent Observed (Outbound)", "ET WEB_SPECIFIC_APPS PHool mainnav Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS WHCMS smarty Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id ASCII", "ET WEB_SPECIFIC_APPS Open Source Support Ticket System module.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Digiappz DigiAffiliate SQL Injection Attempt -- visu_user.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS WeBid ST_platforms.php include_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Possible CactuShop User Invoices Persistent XSS Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email DELETE", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- moscomment.php mcname DELETE", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php UNION SELECT", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid SELECT", "ET WEB_SERVER Tilde in URI - potential .pl source disclosure vulnerability", "ET WEB_SPECIFIC_APPS KLINK txtCodiInfo parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS F5 Data Manager DiagLogListActionBody.do Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PMB Services id Parameter SELECT FROM SQL Injection Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 31", "ET WEB_SPECIFIC_APPS WebMoney html.php page Remote File Inclusion", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_joaktree Component treeId Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page SELECT", "ET WEB_SERVER PHP Possible phar Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS gpEasy CMS key parameter XSS Attempt", "ET WEB_SPECIFIC_APPS AvailScript Article Script articles.php aIDS Parameter SQL Injection", "ET WEB_SPECIFIC_APPS WordPress Chocolate WP Theme src Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk UPDATE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 8", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid UPDATE", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id SELECT", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout SELECT", "ET WEB_SPECIFIC_APPS Reversed Pastebin Injection in Magento DB 2", "ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp grup SELECT", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_forum ASCII", "ET WEB_SERVER Cpanel Cracker Accessed on Internal Server", "ET WEB_SPECIFIC_APPS Eric GUILLAUME uploader&downloader SQL Injection Attempt -- administre2.php id_user UNION SELECT", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass SELECT", "ET WEB_SPECIFIC_APPS ProNews SQL Injection Attempt -- lire-avis.php aa INSERT", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci INSERT", "ET WEB_SPECIFIC_APPS TotalCalendar cms_detect.php include Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke

	viewslink module sid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AjaxPortal di.php pathtoserverdata Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position INSERT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup UNION SELECT", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user UNION SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model UNION SELECT", "ET WEB_SPECIFIC_APPS Wbstreet show.php id parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AJDating SQL Injection Attempt -- view_profile.php user_id ASCII", "ET WEB_SPECIFIC_APPS PozScripts Classified Ads 'store_info.php' SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WEB-PHP RCE PHPBB 2004-1315", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid UPDATE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id INSERT", "ET WEB_SPECIFIC_APPS KLINK txtCodiInfo parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthusiast path parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid UNION SELECT", "ET WEB_SPECIFIC_APPS American Bankers Association Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- index.php p_skin SELECT", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob UPDATE", "ET WEB_SERVER PHP Possible glob Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup INSERT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- wp-trackback.php UPDATE", "ET WEB_SPECIFIC_APPS Podcast Generator themes.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla com_jmsfileseller view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Possible bloofoxCMS 'search' Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS IBM Rational RequisitePro ReqWebHelp maxHits Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa UNION SELECT", "ET WEB_SPECIFIC_APPS Sepcity Lawyer Portal deptdisplay.asp ID parameter SQL Injection", "ET WEB_SPECIFIC_APPS IBBY nouvelles.php id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user DELETE", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id SELECT", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php UNION SELECT", "ET WEB_SPECIFIC_APPS CMScontrol 7.x (index.php id_menu) SQL Injection Vulnerability", "ET WEB_SERVER PUT Website Defacement Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php UNION SELECT", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user DELETE", "ET WEB_SERVER HTTP 414 Request URI Too Large", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p UPDATE", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- types.asp TYPE_ID ASCII", "ET WEB_SPECIFIC_APPS Joomla com_jradio controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS eNdonesia artid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_jcalpro cal_popup.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id ASCII", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f UPDATE", "ET WEB_SPECIFIC_APPS e-Vision CMS SQL Injection Attempt -- style.php

	template ASCII", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname UPDATE", "ET WEB_SPECIFIC_APPS Sahana Agasti AccessController.php approot Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Harlandscripts Pro Traffic One mypage.php trg Parameter SQL Injection", "ET WEB_SPECIFIC_APPS WarHound General Shopping Cart SQL Injection Attempt -- item.asp ItemID INSERT", "ET WEB_SPECIFIC_APPS WebPhotoPro art.php idm Parameter SQL Injection", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay SELECT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id ASCII", "ET WEB_SPECIFIC_APPS Mambo N-Myndir UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid ASCII", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php INSERT", "ET WEB_SERVER Possible HTTP 406 XSS Attempt (Local Source)", "ET WEB_SPECIFIC_APPS IBBY nouvelles.php id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php sqlcmd UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat ASCII", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id INSERT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id DELETE", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where INSERT", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php DELETE", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id UNION SELECT", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- update_profile.php username UPDATE", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id ASCII", "ET WEB_SPECIFIC_APPS WordPress Pretty Link plugin url Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS SFS EZ Hotscripts-like Site showcategory.php cid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Fusion mguser fotoalbum album_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SERVER Nagios statuswml.cgi Remote Arbitrary Shell Command Injection attempt", "ET WEB_SPECIFIC_APPS PHP link Directory sbcat_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat DELETE", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp password INSERT", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php UNION SELECT", "ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (web.config) (CVE-2020-10148)", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id UNION SELECT", "ET WEB_SPECIFIC_APPS SAPID get_infochannel.inc.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP-Fusion mguser fotoalbum album_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_blog Component id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text UPDATE", "ET WEB_SPECIFIC_APPS eGroupware loaddetails.php script INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id INSERT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country ASCII", "ET WEB_SPECIFIC_APPS Wordpress Plugin Tinymce Thumbnail Gallery href parameter Remote File Disclosure Attempt", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course ASCII", "ET WEB_SPECIFIC_APPS Tiki Wiki CMS Groupware language Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid UPDATE", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id ASCII", "ET WEB_SPECIFIC_APPS AdaptWeb a_index.php CodigoDisciplina Parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id DELETE", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection

	Attempt -- print.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area SELECT", "ET WEB_SPECIFIC_APPS Kalptaru Infotech Product Sale Framework customer.forumtopic.php forum_topic_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage UNION SELECT", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php catid INSERT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id SELECT", "ET WEB_SPECIFIC_APPS WebPhotoPro rubrika.php idr Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice INSERT", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php ipadd SELECT", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id INSERT", "ET WEB_SPECIFIC_APPS Openscrutin courrier.class.php path_om Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak DELETE", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId INSERT", "ET WEB_SPECIFIC_APPS Mambo AHS Shop component SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php so SELECT", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid SELECT", "ET SCAN GET with HTML tag in start of URI seen with PHPMyAdmin scanning", "ET WEB_SPECIFIC_APPS Oracle E-Business Suite Financials jtfwcpnt.jsp DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla RokQuickCart view Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- prodList.asp brand UPDATE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id SELECT", "ET WEB_SPECIFIC_APPS ButorWiki service Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_communitypolls controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id SELECT", "ET WEB_SPECIFIC_APPS TCExam tce_xml_user_results.php script UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS nicLOR CMS-School showarticle.php aID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- mesajkutum.asp mesajno SELECT", "ET WEB_SPECIFIC_APPS Joomla techfolio component UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant UNION SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort INSERT", "ET WEB_SPECIFIC_APPS WebSense Email security msgForwardToRiskFilter.asp IsolatedMessageID XSS Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name UNION SELECT", "ET WEB_SERVER possible IBM Rational Directory Server (RDS) Help system href Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Expinion.net iNews SQL Injection Attempt -- articles.asp ex SELECT", "ET PHISHING Apple Phishing Panel Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Experts answer.php question_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS starCMS q parameter Cross Site Scripting Attempt", "ET WEB_SERVER Leaf PHPMailer Accessed on Internal Server", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id DELETE", "ET WEB_SPECIFIC_APPS Inventory newtransact.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id UPDATE", "ET EXPLOIT NB8-01 - Unauthed RCE via bprd", "ET WEB_SPECIFIC_APPS Joomla component img Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Nucleus action.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php website SELECT", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did UNION SELECT", "ET WEB_SPECIFIC_APPS Keynect Ecommerce SQL Injection Attempt -- products.php ctf ASCII", "ET ACTIVEX Microsoft DirectX 9 msvidctl.dll ActiveX Control Code Execution Attempt", "ET ACTIVEX Visagesoft eXPert PDF Viewer ActiveX Control Arbitrary File Overwrite", "ET WEB_SPECIFIC_APPS

	Glossword gw_admin.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp parentid DELETE", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid UPDATE", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid DELETE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php Itemid UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id UNION SELECT", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php user_login_cookie ASCII", "ET WEB_SPECIFIC_APPS Joomla com_jphoto Component Id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv ASCII", "ET WEB_SPECIFIC_APPS Demium CMS urheber.php name Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id DELETE", "ET WEB_SPECIFIC_APPS Horde XSS attempt colorpicker.php", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp manufacturer UPDATE", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid INSERT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewBugs.php s UNION SELECT", "ET EXPLOIT SaltStack Salt Exploitation Inbound (CVE-2020-16846)", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- usermgr.php gid SELECT", "ET WEB_SPECIFIC_APPS SoftMP3 search Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Community component userid parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail INSERT", "ET WEB_SPECIFIC_APPS Zabbix popup.php UNION SELECT SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Audins Audiens SQL Injection Attempt -- index.php PHPSESSID DELETE", "ET WEB_SPECIFIC_APPS Michelles L2J Dropcalc SQL Injection Attempt -- i-search.php itemid UPDATE", "ET WEB_CLIENT FiercePhish Password Prompt Accessed on External Server", "ET WEB_SPECIFIC_APPS WordPress PHP Speedy Plugin page Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user SELECT", "ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp ASCII", "ET WEB_SPECIFIC_APPS Autos catid SQL Injection", "ET WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category SELECT", "ET WEB_SPECIFIC_APPS NewSolved newsscript.php jahr Parameter SQL Injection", "ET WEB_SERVER SQL Injection Local File Access Attempt Using LOAD_FILE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby ASCII", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName ASCII", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat UPDATE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id UNION SELECT", "ET WEB_SPECIFIC_APPS Ban SQL Injection Attempt -- connexion.php id SELECT", "ET WEB_SPECIFIC_APPS WordPress 2 Click Social Media Buttons plugin pinterest-url parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- group.php id UPDATE", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid UPDATE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword UPDATE", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id ASCII", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- email.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id UPDATE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid UNION SELECT", "ET WEB_SERVER PHP Possible rar Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL

	Injection Attempt -- rss.asp kid ASCII", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id SELECT", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat DELETE", "ET WEB_SPECIFIC_APPS x10 Automatic MP3 Script function_core.php web_root Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS B-Cumulus tagcloud.swf Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS programsrating rate.php id XSS attempt", "ET WEB_SPECIFIC_APPS Real Estate Manager realestate-index.php cat_id SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id INSERT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 32", "ET WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id ASCII", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id DELETE", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username INSERT", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php UPDATE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite SELECT", "ET WEB_SPECIFIC_APPS tinyCMS templater.php Local File Inclusion", "ET WEB_SPECIFIC_APPS Wordpress Myflash path parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- email.php id UPDATE", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- page.asp NewsID SELECT", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In ASCII", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid UPDATE", "ET WEB_SPECIFIC_APPS Joomla Foobla Suggestions Component idea_id INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Possible Docebo SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk INSERT", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user SELECT", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which UNION SELECT", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id ASCII", "ET WEB_SPECIFIC_APPS JiRos FAQ Manager SQL Injection Attempt -- index.asp tID INSERT", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board katid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php UPDATE", "ET WEB_SPECIFIC_APPS mcRefer SQL Injection Attempt -- install.php bgcolor UNION SELECT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail SELECT", "ET WEB_SPECIFIC_APPS Joomla com_dshop Component SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS evision cms add3rdparty.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS phpMyAdmin Remote Code Execution Proof of Concept (p=)", "ET WEB_SPECIFIC_APPS Joomla Component com_ccnewsletter controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla SQL Reports user_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id UNION SELECT", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f DELETE", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity DELETE", "ET WEB_SPECIFIC_APPS Modx Revolution < 2.6.4 phpthumb.php RCE Attempt", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID INSERT", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php DELETE", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc UNION SELECT", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile SELECT", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- com_comment.php

	mcname DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat UPDATE", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id SELECT", "ET WEB_SERVER Owl PHPMailer Accessed on Internal Server", "ET WEB_SPECIFIC_APPS PHP Classifieds class.phpmailer.php lang_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp loc DELETE", "ET WEB_SPECIFIC_APPS Joomla com_visa controller Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS TEDE Simplificado processaPesquisa.php script INSERT INTO SQL Injection Attempt", "ET WEB_CLIENT Possible HTTP 503 XSS Attempt (External Source)", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp SELECT", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode ASCII", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp INSERT", "ET WEB_SPECIFIC_APPS Joomla com_avosbillets Component id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Blogplus window_top.php Local File Inclusion", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt -- cp_menu_data_file.php menu INSERT", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID INSERT", "ET EXPLOIT D-Link DCS-930L Remote Command Execution attempt", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php UPDATE", "ET WEB_SPECIFIC_APPS Possible VBulletin Unauthorized Admin Account Creation", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt dsp_page.cfm pageid SELECT", "ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS evision cms addbrandnews.php module parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS WordPress Advanced Text Widget plugin page parameter Cross-Site Script Attempt", "ET WEB_SERVER PHP Possible ftp Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage UPDATE", "ET WEB_SPECIFIC_APPS DBHcms editmenu Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid INSERT", "ET WEB_SPECIFIC_APPS Joomla com_rsgallery2 Component catid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Manage Engine Service Desk Plus WorkOrder.do INSERT INTO SQL Injection Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 17", "ET WEB_SPECIFIC_APPS PhreeBooks js_include.php form Parameter Cross Site Scripting Attempt 2", "ET WEB_SPECIFIC_APPS CF_Calendar calid parameter SQL Injection", "ET WEB_SPECIFIC_APPS MyStats SQL Injection Attempt -- mystats.php details INSERT", "ET EXPLOIT Websense Content Gateway submit_net_debug.cgi cmd_param Param Buffer Overflow Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid INSERT", "ET WEB_SPECIFIC_APPS eGroupware loaddetails.php script UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Comersus Shop Cart SQL Injection Attempt -- comersus_optReviewReadExec.asp idProduct UPDATE", "ET WEB_SPECIFIC_APPS ShopNx - Arbitrary File Upload", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID UNION SELECT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id ASCII", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module pm_temp.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php UNION SELECT", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID UNION SELECT", "ET WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id DELETE", "ET PHISHING ANTIBOT Phishing Panel Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x SELECT", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did ASCII", "ET

	WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- meal_rest.asp mealid DELETE", "ET WEB_SERVER Suspected Webshell tasklist Command (Inbound)", "ET WEB_SPECIFIC_APPS SiteloomCMS mailform_1 variable Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS pliggCMS src parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_adsmanager mosConfig_absolute_path Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank UNION SELECT", "ET WEB_SPECIFIC_APPS Interactive Web Solutions site_info.php SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model UPDATE", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course SELECT", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa UPDATE", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp ASCII", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode ASCII", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL Injection Attempt -- massedit_album.php gall_id UNION SELECT", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt -- news.php id DELETE", "ET WEB_SPECIFIC_APPS iGaming CMS loadplugin.php load Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! JoomlaFacebook Component UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id SELECT", "ET WEB_SPECIFIC_APPS Possible Computer Associates SiteMinder Web Agent Smpwservices.FCC Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp AD_ID ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler INSERT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup DELETE", "ET WEB_SPECIFIC_APPS Scripts For Sites EZ e-store searchresults.php where Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id INSERT", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album ASCII", "ET WEB_SPECIFIC_APPS TinyWebGallery workaround_dir parameter Local File Inclusion Attempt", "ET PHISHING Lucy Phishing Panel Accessed on Internal Server", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId DELETE", "ET WEB_SPECIFIC_APPS AJ Classifieds SQL Injection Attempt -- postingdetails.php postingid UPDATE", "ET WEB_SPECIFIC_APPS AWCM window_top.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS joomla com_djcatalog component UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps DELETE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newname INSERT", "ET WEB_SPECIFIC_APPS phpRS id parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre UPDATE", "ET PHISHING 16Shop Phishing Kit Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id INSERT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ ASCII", "ET WEB_SPECIFIC_APPS WEB-PHP Wordpress enable-latex plugin url Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType ASCII", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid SELECT", "ET WEB_SERVER ImageMagick CVE-2016-3716 Move File Inbound (msl: + mvg)", "ET WEB_SPECIFIC_APPS Nitrotech members.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt --

	product_review.php so INSERT", "ET ACTIVEX DjVu DjVu_ActiveX_MSOffice.dll ActiveX Component Heap Buffer Overflow", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order UNION SELECT", "ET WEB_SPECIFIC_APPS myEvent viewevent.php SQL Injection", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php DELETE", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid DELETE", "ET WEB_SERVER Possible HTTP 403 XSS Attempt (Local Source)", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce SELECT", "ET WEB_SPECIFIC_APPS TEDE Simplificado processaPesquisa.php script UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl INSERT", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id DELETE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id SELECT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl UNION SELECT", "ET WEB_SPECIFIC_APPS Dog Pedigree Online Database managePerson.php personId Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id UPDATE", "ET WEB_SPECIFIC_APPS Orbis editor-body.php script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID UNION SELECT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod UNION SELECT", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID INSERT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare UNION SELECT", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID UPDATE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- cat.asp cat ASCII", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user UNION SELECT", "ET WEB_SPECIFIC_APPS SiteGo OpenFolder parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php UNION SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid INSERT", "ET WEB_SPECIFIC_APPS pfile file.php id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid INSERT", "ET EXPLOIT Lexmark Printer RDYMSG Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id INSERT", "ET WEB_SERVER ScriptResource.axd access without t (time) parameter - possible ASP padding-oracle exploit", "ET WEB_SPECIFIC_APPS Golem Gaming Portal root_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity SELECT", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname DELETE", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate UNION SELECT", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id UPDATE", "ET WEB_SPECIFIC_APPS University Of Vermont intro Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text ASCII", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery retva Parameter Remote Command Execution Attempt", "ET ACTIVEX EasyMail Object IMAP4 Component Buffer Overflow Function call Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce DELETE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where DELETE", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php UNION SELECT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php blogid UPDATE", "ET WEB_SPECIFIC_APPS GaziYapBoz Game

	Portal SQL Injection Attempt -- kategori.asp kategori UPDATE", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob INSERT", "ET WEB_SPECIFIC_APPS Openfoncier architecte.class.php script Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS phpBMS invoices_discount_ajax.php id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp listing_price UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp squarefeet1 DELETE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid UNION SELECT", "ET WEB_SPECIFIC_APPS GS Real Estate Portal email.php AgentID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid UNION SELECT", "ET WEB_SPECIFIC_APPS Venalsur Booking Centre HotelID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Possible ZOHO ManageEngine ADSelfService Captcha Bypass Attempt", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid UPDATE", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page INSERT", "ET WEB_SPECIFIC_APPS xNews SQL Injection Attempt -- xNews.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug UPDATE", "ET WEB_CLIENT Generic Mini Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Joomla com_bch controller Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eMates SQL Injection Attempt -- newsdetail.asp ID INSERT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search SELECT", "ET WEB_SPECIFIC_APPS Joomla com_yelp Component cid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AWCM header.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce UNION SELECT", "ET WEB_SPECIFIC_APPS Digitizing Quote And Ordering System SQL Injection Attempt -- search.asp ordernum ASCII", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id DELETE", "ET WEB_SPECIFIC_APPS Mambo AHS Shop component DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PhpTax Possible Remote Code Exec", "ET WEB_SPECIFIC_APPS Andromeda Streaming MP3 Server andromeda.php Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm newsId SELECT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i ASCII", "ET WEB_SERVER Generic Uploader Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php SELECT", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid UPDATE", "ET WEB_SPECIFIC_APPS PHP JackKnife SQL Injection Attempt -- G_Display.php iCategoryUnq INSERT", "ET WEB_SPECIFIC_APPS ECSHOP user.php SQL INJECTION via Referer", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id ASCII", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state ASCII", "ET WEB_SPECIFIC_APPS Joomla mod_virtuemart_latestprod module Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publications_list.asp vjob SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- order-track.php orderNo INSERT", "ET WEB_SPECIFIC_APPS Joomla! JoomlaFacebook Component UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id UPDATE", "ET WEB_SPECIFIC_APPS Joomla! Survey Manager Component INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection

	Attempt -- product_review.php t DELETE", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID UPDATE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php imageurl DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage DELETE", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album DELETE", "ET WEB_SPECIFIC_APPS Joomla XCloner Component index2.php mosmsg Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType UPDATE", "ET WEB_SPECIFIC_APPS com_if_nexus controller Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS X7 Chat mini.php help_file Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName INSERT", "ET WEB_SPECIFIC_APPS Mathis Dirksen-Thedens ZephyrSoft Toolbox Address Book Continued (ABC) SQL Injection Attempt -- functions.php id SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID INSERT", "ET WEB_SPECIFIC_APPS Campsite article_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Redaxo CMS index.inc.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat ASCII", "ET WEB_SPECIFIC_APPS IBM Rational RequisitePro ReqWebHelp searchWord Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS OneFileCMS p parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php defaultLetter SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid DELETE", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID UPDATE", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module power_module.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- compare_product.php id UNION SELECT", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas DELETE", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- moscomment.php mcname SELECT", "ET WEB_SPECIFIC_APPS Achievo atknodetype parameter Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-1", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In UNION SELECT", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt -- show_webfeed.php wcHeadlines DELETE", "ET WEB_SPECIFIC_APPS Bahar Download Script aspkat.asp SQL Injection", "ET WEB_SERVER Possible Cisco Subscriber Edge Services Manager Cross Site Scripting/HTML Injection Attempt", "ET WEB_SPECIFIC_APPS Built2go Real Estate Listings event_id SQL Injection", "ET WEB_SPECIFIC_APPS Joomla mojoBlog wp-comments-post.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid DELETE", "ET EXPLOIT Cisco Viptela vManage Directory Traversal (CVE-2020-27128)", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php i UNION SELECT", "ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp id ASCII", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id INSERT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category DELETE", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i UPDATE", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- modules.php active SELECT", "ET WEB_SPECIFIC_APPS Joomla com_photoblog component category Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname DELETE", "ET

	WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page ASCII", "ET WEB_SPECIFIC_APPS Joomla com_job Component id_job Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent DELETE", "ET WEB_SPECIFIC_APPS SunByte e-Flower popupproduct.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id DELETE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID SELECT", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_catalogue controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- user.php email UNION SELECT", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid SELECT", "ET WEB_SPECIFIC_APPS PowerPHPBoard header.inc.php settings Parameter Local File Inclusion", "ET WEB_SERVER /bin/csh In URI Possible Shell Command Execution Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat INSERT", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid DELETE", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php qid UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id ASCII", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model DELETE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName UPDATE", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id ASCII", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- index.asp ID UNION SELECT", "ET WEB_SERVER Possible CREATE SQL Injection Attempt in URI", "ET WEB_SERVER Magento XMLRPC-Exploit Attempt", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm langId ASCII", "ET WEB_SPECIFIC_APPS Turnkeyforms Software Directory showcategory.php cid parameter SQL Injection", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id UPDATE", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment ASCII", "ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID UNION SELECT", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php qid ASCII", "ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php t UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Huge IT Image Gallery 1.0.0 SQL Injection", "ET WEB_SPECIFIC_APPS Joomla techfolio component DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce ASCII", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- pfs.edit.inc.php INSERT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci INSERT", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id UNION SELECT", "ET WEB_SPECIFIC_APPS 29o3 CMS layoutHeaderFuncs.php LibDir Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title DELETE", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk SELECT", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt -- show_webfeed.php wcHeadlines ASCII", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi SELECT", "ET WEB_SPECIFIC_APPS Gallo gfw_smarty.php gfwroot Parameter Remote File Inclusion Attempt", "ET

	WEB_SPECIFIC_APPS eFiction toplists.php list Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid UNION SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect ASCII", "ET WEB_SPECIFIC_APPS eyeOS file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid SELECT", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id SELECT", "ET WEB_SERVER SHOW TABLES SQL Injection Attempt in URI", "ET WEB_SPECIFIC_APPS MantisBT db_type Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Jasmine CMS SQL Injection Attempt -- login.php login_username DELETE", "ET WEB_SERVER Possible Oracle Reports Forms RCE CVE-2012-3152", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search DELETE", "ET WEB_SPECIFIC_APPS Synactis All_IN_THE_BOX ActiveX SaveDoc Method Arbitrary File Overwrite", "ET WEB_SPECIFIC_APPS I-Escorts Directory country_id parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection Attempt -- default.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid ASCII", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id INSERT", "ET WEB_SPECIFIC_APPS Inventory consulta_fact.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS BibCiter projects.php idp Parameter SQL Injection", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo DELETE", "ET WEB_SPECIFIC_APPS Online Grades parents.php ADD Parameter SQL Injection", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID DELETE", "ET WEB_SPECIFIC_APPS DBHcms editmenu Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password SELECT", "ET WEB_SPECIFIC_APPS Cacti SQL Injection Vulnerability tree.php leaf_id INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic ASCII", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_categories.asp catID DELETE", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid UNION SELECT", "ET WEB_SPECIFIC_APPS Invalid/Suspicious User-Agent (PHP)", "ET WEB_SPECIFIC_APPS Motionborg Web Real Estate SQL Injection Attempt -- admin_check_user.asp txtUserName DELETE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newemail ASCII", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! Foobla RSS Feed Creator Component 'id' Parameter UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS WordPress Custom Contact Forms options-general.php Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Calendar SQL Injection Attempt -- user.php id ASCII", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp clear ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid ASCII", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid ASCII", "ET WEB_SPECIFIC_APPS jbShop e107 CMS plugin item_id parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID UPDATE", "ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M2", "ET WEB_SPECIFIC_APPS WSN Guest search.php search parameter SQL Injection", "ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php sid SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board ASCII", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection

	Attempt -- compare_product.php id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_quicknews Component newsid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SERVER SELECT INSTR in URI Possible ORACLE Related Blind SQL Injection Attempt", "ET WEB_SERVER Generic WSO Webshell Accessed on Internal Compromised Server", "ET WEB_CLIENT WSO Webshell Password Prompt Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp DELETE", "ET WEB_SPECIFIC_APPS Joomla Community component userid parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l UPDATE", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete SELECT", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid INSERT", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS PowerNews news.php newsid parameter SQL Injection", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id ASCII", "ET WEB_SPECIFIC_APPS phpscripte24 Vor und Ruckwarts Auktions System Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id DELETE", "ET WEB_CLIENT Java Web Start Command Injection (.jar)", "ET WEB_SPECIFIC_APPS WebMplayer SQL Injection Attempt -- filecheck.php id SELECT", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid DELETE", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni DELETE", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id INSERT", "ET WEB_SPECIFIC_APPS GaziYapBoz Game Portal SQL Injection Attempt -- kategori.asp kategori INSERT", "ET WEB_SPECIFIC_APPS PHP-Fusion mguser fotoalbum album_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo UPDATE", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id ASCII", "ET WEB_SPECIFIC_APPS Joomla Component com_jcollection controller Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci UNION SELECT", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id UNION SELECT", "ET WEB_SPECIFIC_APPS PunBB viewtopic_PM-link.php pun_user language Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp page ASCII", "ET WEB_SPECIFIC_APPS phPortal gunaysoft.php sayfaid Parameter Remote File Inclusion", "ET PHISHING Lucy Phishing Panel Accessed on External Server", "ET WEB_SPECIFIC_APPS WordPress WP-Property Plugin uploadify.php Arbitrary File Upload Vulnerability", "ET WEB_SPECIFIC_APPS Xt-News SQL Injection Attempt -- show_news.php id_news UNION SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp uid INSERT", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id DELETE", "ET WEB_SPECIFIC_APPS RecordPress header.php rp-menu.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat SELECT", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-functions.php ASCII", "ET WEB_SPECIFIC_APPS eyeOS callback parameter Cross Site Scripting Attempt", "ET WEB_SERVER Bot Search RFI Scan (Casper-Like MaMa Cyber/ebes)", "ET WEB_SPECIFIC_APPS ZABBIX locales.php srclang Parameter Local File Inclusion", "ET WEB_SERVER Local Website Infected By Gootkit", "ET WEB_CLIENT Predator the Thief Password Prompt Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- dispimage.asp id DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id DELETE", "ET WEB_SPECIFIC_APPS

	Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class DELETE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 11", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid ASCII", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php password DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position SELECT", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx DELETE", "ET WEB_SPECIFIC_APPS Apache Archive legacyArtifactPath script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl DELETE", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id UNION SELECT", "ET WEB_SPECIFIC_APPS Quantum Game Library server_request.php CONFIG Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Joomla com_dshop Component DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword DELETE", "ET WEB_SPECIFIC_APPS QuickTeam qte_init.php qte_root Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid UPDATE", "ET WEB_SPECIFIC_APPS Joomla FaceBook Component face_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress wp-admin/admin.php Module Configuration Security Bypass Attempt", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete UNION SELECT", "ET PHISHING ANTIBOT Phishing Panel Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS cPanel fileop Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WebRCSdiff viewver.php File Inclusion Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id ASCII", "ET WEB_SPECIFIC_APPS MAXcms RFI attempt (4)", "ET EXPLOIT Microsoft Exchange Server Exploitation Inbound (CVE-2020-17141)", "ET WEB_CLIENT Possible HTTP 500 XSS Attempt (External Source)", "ET WEB_SPECIFIC_APPS Volusion Chat ID Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 INSERT", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci SELECT", "ET WEB_SPECIFIC_APPS FreeWebShop startmodules.inc.php lang_file Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Possible WP Plug-in MailPoet Arbitrary File Upload/Auth Bypass Vulnerability", "ET WEB_SPECIFIC_APPS phPortal gunaysoft.php uzanti Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- index.cfm SELECT", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName UNION SELECT", "ET WEB_SPECIFIC_APPS Hedgehog CMS footer.php c_temp_path Remote File Inclusion", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid UNION SELECT", "ET WEB_SPECIFIC_APPS Tiki Wiki CMS ajax parameter XSS Vulnerability", "ET WEB_SPECIFIC_APPS Zabbix popup.php UPDATE SET SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Joomla Onguma Time Sheet Component onguma.class.php mosConfig_absolute_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery (CPG) SQL Injection Attempt -- thumbnails.php cpg131_fav UPDATE", "ET SCAN Tomcat Auth Brute Force attempt (admin)", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- index.php blogid DELETE", "ET WEB_SPECIFIC_APPS 2FLY Gift Delivery 2fly_gift.php gameid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid UNION SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 ASCII", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile INSERT", "ET WEB_SPECIFIC_APPS GeekLog filemgt UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 29o3 CMS pageDescriptionObject.php LibDir Parameter Remote File Inclusion Attempt", "ET

	WEB_SPECIFIC_APPS vBulletin vBTube vidid Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Digirez SQL Injection Attempt -- info_book.asp book_id INSERT", "ET WEB_SPECIFIC_APPS PHP link Directory sbcat_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Vizayn Haber SQL Injection Attempt -- haberdetay.asp id UPDATE", "ET WEB_SPECIFIC_APPS WebSense Email security msgAnalyse.asp ServerName XSS Attempt", "ET WEB_SPECIFIC_APPS Manhali download.php Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS bizdir.cgi f_srch Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip UPDATE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number UNION SELECT", "ET WEB_SPECIFIC_APPS Easebay Resources Login Manager SQL Injection Attempt -- memberlist.php init_row UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid ASCII", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode UPDATE", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php INSERT", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- dlwallpaper.php wallpaperid DELETE", "ET WEB_SPECIFIC_APPS BibCiter users.php idu Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass SELECT", "ET WEB_SERVER Tilde in URI - potential .asp source disclosure vulnerability", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id UNION SELECT", "ET WEB_SPECIFIC_APPS Openscrutin collectivite.class.php path_om Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area UPDATE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us ASCII", "ET WEB_SPECIFIC_APPS Dros core.process_compiled_include.php smarty Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id UNION SELECT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id DELETE", "ET WEB_SPECIFIC_APPS Seo Panel file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Nuke Evolution Xtreme pid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query DELETE", "ET WEB_SPECIFIC_APPS Jelsoft vBulletin SQL Injection Attempt -- attachment.php SELECT", "ET WEB_SPECIFIC_APPS Free Directory Script 1.1.1 API_HOME_DIR Local File Inclusion", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id SELECT", "ET WEB_SERVER ColdFusion Path Traversal (locale 2/5)", "ET WEB_SPECIFIC_APPS Tyger Bug Tracking System (TygerBT) SQL Injection Attempt -- ViewReport.php bug INSERT", "ET WEB_SPECIFIC_APPS BaglerCMS articleID parameter Cross-Site Script Attempt", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no SELECT", "ET WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page UNION SELECT", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-4", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP id UNION SELECT", "ET WEB_SPECIFIC_APPS PWP Technologies The Classified Ad System SQL Injection Attempt -- default.asp main SELECT", "ET WEB_SPECIFIC_APPS PHPCMS modelid Parameter SQL Injection Attempt", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php cat_id DELETE", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid ASCII", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID DELETE", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID UPDATE", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id SELECT", "ET WEB_SPECIFIC_APPS WebSense Email security msgForwardToRiskFilter.asp ServerName XSS Attempt", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num DELETE", "ET WEB_SPECIFIC_APPS PHPAccounts SQL

	Injection Attempt -- index.php Outgoing_Type_ID DELETE", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid INSERT", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager deviceInstanceName Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname ASCII", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_downloads.php did SELECT", "ET WEB_SERVER SHOW VARIABLES SQL Injection Attempt in URI", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activeNews_comments.asp articleID INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp abedrooms DELETE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id ASCII", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi UPDATE", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod ASCII", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup DELETE", "ET WEB_SPECIFIC_APPS cpCommerce SQL Injection Attempt -- category.php id_category UPDATE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp AlphaSort ASCII", "ET WEB_SERVER WSO Webshell Password Prompt Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId UPDATE", "ET WEB_CLIENT Generic PHP Uploader Accessed on External Server", "ET WEB_SPECIFIC_APPS Joomla Component JE Story Submit view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php SELECT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola INSERT", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php newsid DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname ASCII", "ET WEB_SPECIFIC_APPS vBulletin cChatBox messageid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php i ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- forgotpass.asp id ASCII", "ET WEB_SPECIFIC_APPS Demium CMS tracking.php follow_kat Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp area UNION SELECT", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php catid UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp ASCII", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- email.php id INSERT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp UPDATE", "ET WEB_SERVER Attempt To Access MSSQL xp_cmdshell Stored Procedure Via URI", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user UPDATE", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp did INSERT", "ET WEB_SPECIFIC_APPS Pre Online Tests Generator Pro INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp secondgroup UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid INSERT", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user UNION SELECT", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- showfile.asp fid INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number UPDATE", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id DELETE", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass SELECT", "ET WEB_SPECIFIC_APPS AdaptCMS sitepath parameter Remote File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php product_id UPDATE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Emerson Network AllResults.aspx Cross Site Scripting Attempt",

	"ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id ASCII", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c UNION SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre UNION SELECT", "ET EXPLOIT Joomla RCE M2 (Serialized PHP in UA)", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid SELECT", "ET WEB_SPECIFIC_APPS Xt-News SQL Injection Attempt -- show_news.php id_news DELETE", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat UNION SELECT", "ET WEB_CLIENT SmailMax PHPMailer Accessed on External Server", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi UPDATE", "ET EXPLOIT phpMyAdmin 4.8.1 - Local File Inclusion", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id INSERT", "ET WEB_SPECIFIC_APPS DuWare DuClassmate SQL Injection Attempt -- default.asp iCity SELECT", "ET WEB_SPECIFIC_APPS Contra Haber Sistemi SQL Injection Attempt -- haber.asp id ASCII", "ET WEB_SPECIFIC_APPS Portel patron Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite INSERT", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- index.php p_skin UPDATE", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp category INSERT", "ET WEB_SPECIFIC_APPS bbPress SQL Injection Attempt -- formatting-functions.php INSERT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword SELECT", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid UNION SELECT", "ET WEB_SPECIFIC_APPS A6MamboHelpDesk Admin.a6mambohelpdesk.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php goTo ASCII", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID UPDATE", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod INSERT", "ET WEB_SPECIFIC_APPS GlobalMegaCorp dvddb SQL Injection Attempt -- common.php user INSERT", "ET WEB_SERVER Attempt To Access MSSQL xp_servicecontrol Stored Procedure Via URI", "ET WEB_SPECIFIC_APPS CitusCMS filePath Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f UNION SELECT", "ET WEB_SPECIFIC_APPS YapBB class_yapbbcooker.php cfgIncludeDirectory Parameter Remote File Inclusion", "ET WEB_SERVER ATTACKER WebShell - PHP Offender - Title", "ET WEB_SPECIFIC_APPS Acute Control Panel header.php theme_directory parameter local file inclusion", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id INSERT", "ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP GET 2)", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- mezungiris.asp pass UPDATE", "ET WEB_SPECIFIC_APPS Openfire Jabber-Server type Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID INSERT", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php SELECT", "ET WEB_SPECIFIC_APPS Dokeos SQL Injection Attempt -- my_progress.php course UPDATE", "ET WEB_SPECIFIC_APPS Mambo LaiThai SQL Injection Attempt -- mambo.php DELETE", "ET WEB_SERVER ImageMagick CVE-2016-3718 SSRF Inbound (mvg + fill + url)", "ET PHISHING Generic Phishing Panel Accessed on External Server", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci UPDATE", "ET WEB_SPECIFIC_APPS PMB Services id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk UNION SELECT", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode UPDATE", "ET WEB_SPECIFIC_APPS TinyBrowser edit.php file Script Execution Attempt", "ET WEB_SPECIFIC_APPS TEDE Simplificado processaPesquisa.php script SELECT FROM SQL Injection Attempt", "ET

	WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order DELETE", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids UPDATE", "ET WEB_SPECIFIC_APPS Pligg check_url.php url parameter SQL Injection", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary INSERT", "ET WEB_SPECIFIC_APPS Openfire Jabber-Server type Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style UPDATE", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php ASCII", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id DELETE", "GPL WEB_SERVER .htpasswd access", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php post_id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_joaktree Component treeId Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php UPDATE", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat DELETE", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp ASCII", "ET WEB_SPECIFIC_APPS DirectNews rootpath parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci ASCII", "ET WEB_SPECIFIC_APPS TECHNOTE shop_this_skin_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp INSERT", "ET WEB_SPECIFIC_APPS Super Link Exchange Script SQL Injection Attempt -- directory.php cat INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentwebsite INSERT", "ET WEB_SPECIFIC_APPS Ixprim SQL Injection Attempt -- ixm_ixpnews.php story_id INSERT", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php pid INSERT", "ET WEB_SPECIFIC_APPS Dros function.config_load.php _compile_file Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Nagios XI div parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Help Center Live file parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS Abtp Portal Project skel_null.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Adiscon LogAnalyzer viewid Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit DELETE", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id INSERT", "ET WEB_SPECIFIC_APPS WebMoney html2.php page Remote File Inclusion", "ET WEB_SPECIFIC_APPS Admidio headline parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php from UPDATE", "ET WEB_SPECIFIC_APPS WordPress jRSS Widget url parameter Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id DELETE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language DELETE", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity ASCII", "ET WEB_SPECIFIC_APPS Joomla! CB Resume Builder 'group_id' Parameter UNION SELECT SQL Injection", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 13", "ET WEB_SPECIFIC_APPS Weekly Drawing Contest SQL Injection Attempt -- check_vote.php order UPDATE", "ET WEB_SPECIFIC_APPS RealtyListings detail.asp iPro Parameter SQL Injection", "ET WEB_SPECIFIC_APPS vBulletin vbBux vbplaza.php Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp keyword INSERT", "ET WEB_SPECIFIC_APPS Manage Engine Service Desk Plus WorkOrder.do DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id UPDATE", "ET WEB_SPECIFIC_APPS Wordpress Plugin Is-human type Parameter Remote Code Execution Attempt", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp orderby UPDATE", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id UPDATE", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL

	Injection Attempt -- haberoku.asp id INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin UPDATE", "ET WEB_SPECIFIC_APPS Openconstructor CMS result Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! Survey Manager Component SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS PHP-Nuke viewslink module sid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Philboard SQL Injection Attempt -- philboard_forum.asp forumid UNION SELECT", "ET WEB_SPECIFIC_APPS Noname Media Photo Galerie Standard SQL Injection Attempt -- view.php id ASCII", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type SELECT", "ET WEB_SPECIFIC_APPS b2evolution inc_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Coupon Script bus parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Mambo Zorder zorder Parameter SELECT FROM SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- process.php login UPDATE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 1", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage ASCII", "ET WEB_SPECIFIC_APPS Fixit iDMS Pro Image Gallery SQL Injection Attempt -- filelist.asp show_id DELETE", "ET WEB_SPECIFIC_APPS MiNT Haber Sistemi SQL Injection Attempt -- duyuru.asp id INSERT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php x UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla! Foobla RSS Feed Creator Component 'id' Parameter UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Boonex Dolphin relocate Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId UPDATE", "ET WEB_SERVER ColdFusion Path Traversal (locale 1/5)", "ET WEB_SPECIFIC_APPS LWS php User Base unverified.inc.php template Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS DUware DUpaypal SQL Injection Attempt -- detail.asp iType SELECT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin ASCII", "ET WEB_SPECIFIC_APPS digiSHOP cart.php SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- letterman.class.php id INSERT", "ET WEB_SPECIFIC_APPS ShopStoreNow E-commerce Shopping Cart SQL Injection Attempt -- orange.asp CatID SELECT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- artreplydelete.asp username UPDATE", "ET WEB_SPECIFIC_APPS NewsOffice news_show.php newsoffice_directory Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id DELETE", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid DELETE", "ET WEB_SPECIFIC_APPS CandyPress Store SQL Injection Attempt -- openPolicy.asp policy UNION SELECT", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp INSERT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- send_password_preferences.asp DELETE", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c DELETE", "ET WEB_SPECIFIC_APPS QUICKTEAM qte_result.php title Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid UNION SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID SELECT", "ET WEB_SPECIFIC_APPS Joomla! SportFusion Component UPDATE SET SQL Injection", "ET WEB_SPECIFIC_APPS Connectix Boards SQL Injection Attempt -- admin.php uploadimage UPDATE", "ET WEB_SPECIFIC_APPS Lito Lite CMS cate.php cid parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp author UNION SELECT", "ET WEB_SPECIFIC_APPS b2evolution skins_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp uid UPDATE", "ET WEB_SERVER SmailMax PHPMailer Accessed on Internal Server", "ET WEB_SPECIFIC_APPS zeeproperty adid Parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS ZOHO ManageEngine ADSelfService Employee

	Search XSS Attempt", "ET WEB_SERVER Tilde in URI - potential .inc source disclosure vulnerability", "ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id DELETE", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id DELETE", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php t INSERT", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (2)", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp year UNION SELECT", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp harf UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- list.asp UNION SELECT", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci UNION SELECT", "ET WEB_SPECIFIC_APPS digiSHOP cart.php DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp UNION SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- fiche_membre.php idmembre UPDATE", "ET WEB_SPECIFIC_APPS Tunngavik CMS id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php user_login_cookie SELECT", "ET WEB_SPECIFIC_APPS Joomla mojoBlog wp-trackback.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_hdflvplayer Component id Parameter INSERT INTO SQL Injection Attempt", "ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP POST)", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id UPDATE", "ET WEB_SPECIFIC_APPS Mambo Zorder zorder Parameter DELETE FROM SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname UPDATE", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php email ASCII", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID SELECT", "ET WEB_SPECIFIC_APPS Wordpress plugin Flash Album Gallery pid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP NEWS SQL Injection Attempt -- news_detail.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_hello controller parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS aFAQ SQL Injection Attempt -- faqDsp.asp catcode INSERT", "ET WEB_SERVER Attack Tool Revolt Scanner", "ET WEB_SPECIFIC_APPS Fullaspsite Asp Hosting Sitesi SQL Injection Attempt -- windows.asp kategori_id ASCII", "ET ACTIVEX EasyMail Object SMTP Component Buffer Overflow Function call Attempt", "ET WEB_SPECIFIC_APPS Apache Archive confirmDeleteRepository script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Image Gallery with Access Database SQL Injection Attempt -- default.asp order UPDATE", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nukesentinel.php DELETE", "ET WEB_SPECIFIC_APPS DirectNews class.panier_article.php Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager eventmon_wrapper.jsp Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- phonemessage.asp num UPDATE", "ET WEB_SPECIFIC_APPS OvBB admincp.php smilieid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- sections.php text SELECT", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager advancedfind.do Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS phpBB SQL Injection Attempt -- admin_hacks_list.php hack_id UNION SELECT", "ET WEB_SPECIFIC_APPS WordPress Copperleaf Photolog postid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id INSERT", "ET WEB_SPECIFIC_APPS OSSIM repository_attachment.php SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID UPDATE", "ET WEB_SPECIFIC_APPS ParsBlogger blog.asp wr parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS dirLIST

	show_scaled_image.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Andy PHP Knowledgebase SQL Injection Attempt pdfgen.php pdfa UPDATE", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla com_yelp Component cid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp did SELECT", "ET WEB_SERVER Possible SQL Injection Attempt DELETE FROM", "ET WEB_SPECIFIC_APPS Future Internet SQL Injection Attempt -- index.cfm categoryid UNION SELECT", "ET WEB_SERVER ColdFusion password.properties access", "ET WEB_SPECIFIC_APPS WordPress Gallery Plugin filename_1 Parameter Remote File Access Attempt", "ET WEB_SPECIFIC_APPS Joomla YJ Contact Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS Joomla AjaxChat Component ajcuser.php GLOBALS Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_perchagallery Component id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- giris.asp kullaniciadi ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php id UNION SELECT", "ET WEB_SPECIFIC_APPS phpProfiles menu Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment SELECT", "ET WEB_SPECIFIC_APPS ClickTech Click Blog SQL Injection Attempt -- displayCalendar.asp date UNION SELECT", "ET WEB_SERVER Attempt To Access MSSQL xp_regread/xp_regwrite/xp_regdeletevalue/xp_regdeletekey Stored Procedure Via URI to Modify Registry", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass INSERT", "ET WEB_SPECIFIC_APPS Wordpress plugin Flash Album Gallery pid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost1 UNION SELECT", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid INSERT", "ET WEB_SPECIFIC_APPS AlstraSoft Video Share Enterprise album.php UID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Free Bible Search readbible.php SQL Injection", "ET WEB_SERVER Possible HTTP 500 XSS Attempt (Internal Source)", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- slideshow.asp ci UNION SELECT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user UNION SELECT", "ET EXPLOIT Intex Router N-150 Cross-Site Request Forgery", "ET SCAN Possible Scanning for Vulnerable JBoss", "ET WEB_SPECIFIC_APPS IBM Rational RequisitePro ReqWebHelp scopedSearch Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID DELETE", "ET WEB_SPECIFIC_APPS Plone and Zope cmd Parameter Remote Command Execution Attempt", "ET WEB_SPECIFIC_APPS ExBB threadstop.php exbb Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php sk ASCII", "ET WEB_SERVER Suspected Webshell Activity (Inbound)", "ET WEB_SPECIFIC_APPS WordPress 2 Click Social Media Buttons plugin xing-url parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc DELETE", "ET WEB_SPECIFIC_APPS W1L3D4 WEBmarket SQL Injection Attempt -- urunbak.asp id ASCII", "ET WEB_SPECIFIC_APPS Open Web Analytics owa_do Parameter Local File inclusion Attempt", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid SELECT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- userdetail.php id ASCII", "ET WEB_SPECIFIC_APPS Joomla com_job Component id_job Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection Attempt -- default.asp id ASCII", "ET WEB_SPECIFIC_APPS WordPress inline-gallery do parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS vSupport Integrated Ticket System SQL Injection Attempt -- vBSupport.php ticketid ASCII", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c ASCII", "ET WEB_SPECIFIC_APPS IBSng str Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS PHP-Daily delete.php id Parameter SQL Injection", "ET

	WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php message UNION SELECT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat INSERT", "ET ACTIVEX DB Software Laboratory VImpX.ocx ActiveX Control Multiple Insecure Methods", "ET WEB_SPECIFIC_APPS CommonSpot Server longproc.cfm Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid ASCII", "ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)", "ET WEB_SPECIFIC_APPS CMSQLITE mediaAdmin.php file Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Easebay Resources Login Manager SQL Injection Attempt -- memberlist.php init_row SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 25", "ET WEB_SERVER Attempt To Access MSSQL xp_readerrorlogs Stored Procedure Via URI to View Error Logs", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id UPDATE", "ET WEB_SPECIFIC_APPS Shape Web Solutions imprimir.php SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dirSub.asp sid ASCII", "ET WEB_SPECIFIC_APPS GeekLog filemgt DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClarkConnect Linux proxy.php XSS Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- repass.php nick_mod UPDATE", "ET WEB_SERVER SQL Injection Attempt (Agent CZxt2s)", "ET WEB_SPECIFIC_APPS AWStats Totals sort parameter Remote Code Execution Attempt", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php post_id DELETE", "ET WEB_SPECIFIC_APPS JoomSocial AvatarUpload RCE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php us UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_mscomment controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ScriptMate User Manager SQL Injection Attempt -- usermessages.asp mesid UPDATE", "ET WEB_SPECIFIC_APPS Vt-Forum Lite SQL Injection Attempt -- vf_memberdetail.asp user INSERT", "ET WEB_SPECIFIC_APPS Openfire Jabber-Server type Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WB News search.php config Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS PHP-Stats SQL Injection Attempt -- php-stats.recphp.php ip UNION SELECT", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id UPDATE", "ET WEB_SPECIFIC_APPS eNdonesia artid Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS IBM ENOVIA SmarTeam v5 LoginPage.aspx Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Just For Fun Network Management System (JFFNMS) SQL Injection Attempt -- auth.php pass INSERT", "ET WEB_SPECIFIC_APPS Mambo SQL Injection Attempt -- moscomment.php mcname INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment SELECT", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid ASCII", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- gmail.php INSERT", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp DELETE", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- ASPKAT.ASP kid UPDATE", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname UNION SELECT", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php productId INSERT", "ET WEB_SPECIFIC_APPS SiteGo get_templet.php of blue Remote File Inclusion Attempt", "ET MALWARE Mirai Variant User-Agent (Outbound)", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board SQL Injection Attempt -- usergroups.php DELETE", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid UPDATE", "ET WEB_SPECIFIC_APPS ClickTech ClickContact SQL Injection Attempt -- default.asp In SELECT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup SELECT", "ET WEB_SPECIFIC_APPS Apache Tomcat Orderby Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla Simple RSS Reader admin.rssreader.php mosConfig_live_site Parameter Remote File Inclusion", "ET

	WEB_SPECIFIC_APPS SourceBans ajaxargs Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS WB News Archive.php config Parameter Remote File Inclusion -2", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt -- cp_menu_data_file.php menu DELETE", "ET WEB_SERVER ImageMagick CVE-2016-3714 Inbound (svg)", "ET WEB_CLIENT Possible HTTP 406 XSS Attempt (External Source)", "ET WEB_SPECIFIC_APPS Oracle E-Business Suite Financials jtfwcpnt.jsp UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment UNION SELECT", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick_mod ASCII", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album INSERT", "ET WEB_SPECIFIC_APPS WeBid ST_countries.php include_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS AJ Auction SQL Injection Attempt -- subcat.php cate_id INSERT", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id DELETE", "ET WEB_SPECIFIC_APPS Oracle Business Process Management context Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-6", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue ASCII", "GPL SCAN nessus 1.X 404 probe", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre DELETE", "ET WEB_SPECIFIC_APPS Koan Software Mega Mall SQL Injection Attempt -- product_review.php t ASCII", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- meal_rest.asp mealid UPDATE", "ET WEB_SPECIFIC_APPS Wordpress Host Header Injection (CVE-2016-10033) M3", "ET WEB_SPECIFIC_APPS SlimCMS edit.php pageid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS ASP ListPics SQL Injection Attempt -- listpics.asp ID DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id UPDATE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php category_id UPDATE", "ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA User-Level Authentication Bypass (sslvpnclient) (CVE-2021-20016)", "ET WEB_SPECIFIC_APPS Autonomous LAN Party _bot.php master Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp model SELECT", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title INSERT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id INSERT", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_doc ASCII", "ET WEB_CLIENT Generic Uploader Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Joomla com_joomtouch controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php DELETE", "ET WEB_SPECIFIC_APPS SoftMP3 search Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS T-Content Management System id_novedad Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field UPDATE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php f ASCII", "ET WEB_SPECIFIC_APPS FireStats window-new-edit-site.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid UNION SELECT", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id DELETE", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id UNION SELECT", "ET WEB_SPECIFIC_APPS All In One Control Panel SQL Injection Attempt -- cp_menu_data_file.php menu ASCII", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p UNION SELECT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp maingroup ASCII", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp id DELETE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect DELETE", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment DELETE", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- block-

	Old_Articles.php cat DELETE", "ET WEB_SPECIFIC_APPS Fullaspsite GeometriX Download Portal SQL Injection Attempt -- down_indir.asp id INSERT", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin UPDATE", "ET WEB_SPECIFIC_APPS Nabopoll SQL Injection Attempt -- result.php surv SELECT", "ET WEB_SERVER Generic Webshell Password Prompt Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Joomla! Survey Manager Component DELETE FROM SQL Injection", "ET WEB_SPECIFIC_APPS Apache Archive addNetworkProxy script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS phpBMS invoices_discount_ajax.php id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vin DELETE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect UPDATE", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage SELECT", "ET SCAN Possible Nmap User-Agent Observed", "GPL EXPLOIT iisadmpwd attempt", "ET WEB_SPECIFIC_APPS Horde type Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id INSERT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- content.php where ASCII", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID DELETE", "ET WEB_SPECIFIC_APPS Possible Achievo userid= Variable INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_rssreader controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla JGrid Component File Inclusion Attempt", "ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M1", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid ASCII", "ET WEB_SPECIFIC_APPS Acute Control Panel container.php theme_directory parameter local file inclusion", "ET WEB_SPECIFIC_APPS BasicForum SQL Injection Attempt -- edit.asp id DELETE", "ET WEB_SPECIFIC_APPS Joomla com_jphoto Component Id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS pfile file.php id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UPDATE", "ET WEB_SPECIFIC_APPS DesktopOnNet don3_requiem.php app_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp compare UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice ASCII", "ET WEB_SPECIFIC_APPS Hunkaray Duyuru Scripti SQL Injection Attempt -- oku.asp id DELETE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- print.php news_id UNION SELECT", "ET WEB_CLIENT X-Sec Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS SERWeb load_lang.php configdir Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS CodeAvalanche News SQL Injection Attempt -- inc_listnews.asp CAT_ID UNION SELECT", "ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M3", "ET WEB_SPECIFIC_APPS RevokeSoft RevokeBB SQL Injection Attempt -- class_users.php UPDATE", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php user_login_cookie DELETE", "ET WEB_SPECIFIC_APPS WebC.be Fichier_a_telecharger Parameter Local File Disclosure Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) Lite SQL Injection Attempt -- pms.php pmid INSERT", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id ASCII", "ET WEB_SPECIFIC_APPS Joomla com_photoblog component category Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Ultrize TimeSheet timesheet.php include_dir Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Aktueldownload Haber script SQL Injection Attempt -- rss.asp kid UPDATE", "ET WEB_SPECIFIC_APPS Possible Zenoss Network Monitoring Application SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php INSERT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt --

	item_list.asp secondgroup DELETE", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp id INSERT", "ET WEB_SPECIFIC_APPS Joomla com_acooldebate controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- journal.php w ASCII", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtPas UNION SELECT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id ASCII", "ET WEB_SPECIFIC_APPS Joomla com_fundhelp controller Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url SELECT", "ET WEB_SPECIFIC_APPS Joomla Component Ek rishta 2.10 - SQL Injection 3", "ET WEB_SPECIFIC_APPS EvimGibi Pro Resim Galerisi kat_id parameter SQL Injection", "ET WEB_SPECIFIC_APPS Flash Quiz high_score.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS SpoonLabs Vivvo Article Management CMS (phpWordPress) SQL Injection Attempt -- show_webfeed.php wcHeadlines INSERT", "ET WEB_SPECIFIC_APPS Joomla com_hdflvplayer Component id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id DELETE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke viewslink module sid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla jfeedback Component controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla com_kp controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi UNION SELECT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user INSERT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla jwmmxtd Component mosConfig_absolute_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module cindefn.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- update.asp id UPDATE", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre UNION SELECT", "ET WEB_SPECIFIC_APPS Cacti SQL Injection Vulnerability tree.php leaf_id SELECT", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid UPDATE", "ET WEB_SPECIFIC_APPS Rapid Classified SQL Injection Attempt -- viewad.asp id ASCII", "ET EXPLOIT Joomla 3.2.1 SQL injection attempt 2", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp amaxprice DELETE", "ET WEB_SPECIFIC_APPS GDL gdl.php node Parameter SQL Injection", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id INSERT", "GPL EXPLOIT WEB-MISC JBoss RMI class download service directory listing attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID UPDATE", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID ASCII", "ET WEB_SPECIFIC_APPS Joomla Component com_digistore (pid) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp UNION SELECT", "ET WEB_SPECIFIC_APPS Kolayindir Download (Yenionline) SQL Injection Attempt -- down.asp id INSERT", "ET WEB_SPECIFIC_APPS ASP EDGE SQL Injection Attempt -- user.asp user UPDATE", "ET WEB_SPECIFIC_APPS WordPress WP ecommerce Shop Styling Plugin dompdf RFI Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php language ASCII", "ET WEB_SPECIFIC_APPS Cisco Unified Operations Manager clusterName Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword ASCII", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php name SELECT", "ET WEB_SPECIFIC_APPS Martyn Kilbryde Newsposter Script SQL Injection Attempt -- news_page.asp uid UPDATE", "ET WEB_SPECIFIC_APPS FormMailer formmailer.admin.inc.php BASE_DIR Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wordpress clickdesk-live-support-chat plugin cdwidgetid parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp

	listing_price UPDATE", "ET WEB_SPECIFIC_APPS Openfoncier avis.class.php script Remote File inclusion Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 10", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword UPDATE", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id INSERT", "ET WEB_SPECIFIC_APPS Design4Online UserPages2 SQL Injection Attempt -- page.asp art_id DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID ASCII", "ET WEB_SPECIFIC_APPS Maran PHP Shop id Parameter Remote SQL Injection", "ET SCAN Tomcat Auth Brute Force attempt (tomcat)", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserType ASCII", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage UPDATE", "ET WEB_SERVER eval/base64_decode Exploit Attempt Inbound", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID UNION SELECT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id UNION SELECT", "ET WEB_SPECIFIC_APPS Wordpress plugin Flash Album Gallery pid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS F5 Data Manager ViewSatReport.do Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid INSERT", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat SELECT", "ET WEB_SPECIFIC_APPS PHP-fusion Team Structure Infusion team_id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- detail.asp p ASCII", "ET WEB_SPECIFIC_APPS Pre Online Tests Generator Pro UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS VerliAdmin SQL Injection Attempt -- verify.php nick DELETE", "ET WEB_SPECIFIC_APPS IBBY nouvelles.php id Parameter UPDATE SET SQL Injection Attempt", "ET EXPLOIT Stored XSS and Webpass IoT devices CVE-2021-31643", "ET WEB_SPECIFIC_APPS Dragon Business Directory SQL Injection Attempt -- bus_details.asp ID INSERT", "ET WEB_SPECIFIC_APPS Joomla techfolio component SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_code SELECT", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id INSERT", "ET WEB_SPECIFIC_APPS KLINK txtCodiInfo parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Dance Studio Manager dailyview.php date Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS bitweaver SQL Injection Attempt -- edition.php tk ASCII", "ET WEB_SPECIFIC_APPS CreateAuction SQL Injection Attempt -- cats.asp catid UNION SELECT", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank UPDATE", "ET WEB_SPECIFIC_APPS evision cms addgame.php module parameter Local File Inclusion", "GPL EXPLOIT /msadc/samples/ access", "ET WEB_SPECIFIC_APPS PHP-Paid4Mail RFI attempt", "ET WEB_SPECIFIC_APPS Madirish Webmail basedir Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Dokuwiki doku.php config_cascade Local File Inclusion", "ET WEB_SERVER Suspected Webshell registry Command (Inbound)", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- weblinks.php where UPDATE", "ET WEB_SPECIFIC_APPS Tunngavik CMS id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id ASCII", "ET WEB_SPECIFIC_APPS Frontis aps_browse_sources.php source_class Parameter SQL Injection", "ET WEB_SERVER CRLF Injection - Newline Characters in URL", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- down.asp id SELECT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp l INSERT", "ET WEB_SPECIFIC_APPS Joomla! CB Resume Builder 'group_id' Parameter SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php SELECT", "ET WEB_SPECIFIC_APPS Joomla FaceBook Component face_id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS CMS Board site_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Wordpress Host Header Injection (CVE-2016-10033) M2", "ET WEB_SPECIFIC_APPS Neocrome Land Down Under (LDU) SQL Injection Attempt -- polls.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Beerwins PHPLinkAdmin

	edlink.php linkid Parameter SQL Injection", "ET WEB_SERVER Gootkit Website Infection Receiving FTP Credentials from Control Server", "ET WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName ASCII", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php q INSERT", "ET WEB_SPECIFIC_APPS iBrowser Plugin dir Parameter Cross Site Scripting Attempt-1", "ET WEB_SPECIFIC_APPS HIOX Star Rating System Script (HSRS) SQL Injection Attempt -- addrating.php url UPDATE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php topic_id UPDATE", "ET WEB_SPECIFIC_APPS ZyXEL P-660R-T1 HomeCurrent_Date Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Website Baker SQL Injection Attempt -- eWebQuiz.asp QuizID DELETE", "ET WEB_SPECIFIC_APPS MAXcms RFI attempt (1)", "ET WEB_SPECIFIC_APPS Joomla! SportFusion Component INSERT INTO SQL Injection", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp area SELECT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent DELETE", "ET WEB_SPECIFIC_APPS WordPress Contact Form Maker Plugin - SQL Injection 2", "ET WEB_SPECIFIC_APPS Zindizayn Okul Web Sistemi SQL Injection Attempt -- ogretmenkontrol.asp pass ASCII", "ET WEB_SPECIFIC_APPS Openscrutin profil.class.php path_om Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id ASCII", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid UNION SELECT", "ET WEB_SERVER DNS changer cPanel attempt", "ET WEB_SPECIFIC_APPS CMS Faethon info.php item Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- sendarticle.asp ASCII", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php DELETE", "ET WEB_SPECIFIC_APPS WB News Comments.php config Parameter Remote File Inclusion -2", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id UPDATE", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp grup UNION SELECT", "ET WEB_SPECIFIC_APPS ShopMaker product.php id Parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php UPDATE", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php pid UPDATE", "ET WEB_SPECIFIC_APPS My Datebook SQL Injection Attempt -- diary.php delete DELETE", "ET WEB_SERVER WSO 2.5 Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS axdcms aXconf Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS e107 Plugin lyrics_menu lyrics_song.php l_id Parameter Remote SQL Injection", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_search.asp query ASCII", "ET WEB_SPECIFIC_APPS evision cms addarticles.php module parameter Local File Inclusion", "ET WEB_SERVER Generic Webshell Accessed on Compromised Internal Server", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id DELETE", "ET WEB_SPECIFIC_APPS 2z Project SQL Injection Attempt -- rating.php rating UNION SELECT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id DELETE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp sale_type ASCII", "ET WEB_SPECIFIC_APPS X-dev xNews SQL Injection Attempt -- class.news.php id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_joaktree Component treeId Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS AWCM common.php Remote File Inclusion Attempt", "ET WEB_SERVER Generic Mailer Accessed on Internal Server", "ET WEB_SPECIFIC_APPS WordPress FSML Plugin fsml-hideshow.js.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Pet Listing Script type_id Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS EasyPage SQL Injection Attempt -- default.aspx docId UNION SELECT", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp INSERT", "ET WEB_SPECIFIC_APPS PHPKIT SQL Injection Attempt -- comment.php subid SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state UNION SELECT", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- display_review.php

	user_login_cookie INSERT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage UNION SELECT", "ET WEB_SPECIFIC_APPS PSY Auction SQL Injection Attempt -- item.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Possible AIOCP cp_html2xhtmlbasic.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp parola UPDATE", "ET WEB_SPECIFIC_APPS WordPress UnGallery pic Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid INSERT", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id UPDATE", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Fantastic News SQL Injection Attempt -- news.php id ASCII", "ET WEB_SPECIFIC_APPS PHP-Nuke SQL Injection Attempt -- modules.php cid UPDATE", "ET WEB_SPECIFIC_APPS web wiz forums ThreadPage Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Easebay Resources Paypal Subscription Manager SQL Injection Attempt -- memberlist.php keyword INSERT", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id INSERT", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- search.asp UPDATE", "ET WEB_SPECIFIC_APPS phpCC SQL Injection Attempt -- nickpage.php npid DELETE", "ET WEB_SPECIFIC_APPS ol bookmarks SQL Injection Attempt -- index.php id UPDATE", "ET WEB_SPECIFIC_APPS LiveCMS SQL Injection Attempt -- categoria.php cid DELETE", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ UNION SELECT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 14", "ET WEB_SPECIFIC_APPS Moodle PHPCOVERAGE_HOME Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page ASCII", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname INSERT", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id INSERT", "ET WEB_SPECIFIC_APPS fipsForum SQL Injection Attempt -- default2.asp kat DELETE", "ET WEB_SPECIFIC_APPS PNphpBB2 admin_words.php ModName parameter Local File inclusion", "ET WEB_SPECIFIC_APPS EzHRS HR Assist SQL Injection Attempt -- vdateUsr.asp ASCII", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity UPDATE", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid DELETE", "ET WEB_SPECIFIC_APPS GaziYapBoz Game Portal SQL Injection Attempt -- kategori.asp kategori ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp searchin DELETE", "ET WEB_SPECIFIC_APPS Apache Archive roleedit script Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla com_jphoto Component Id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ASP SiteWare autoDealer SQL Injection Attempt -- detail.asp iPro UNION SELECT", "ET WEB_SPECIFIC_APPS Nicola Asuni All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_functions_downloads.php download_category UNION SELECT", "ET WEB_SPECIFIC_APPS Possible Novell eDirectory 'dconserv.dlm' Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp order ASCII", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp menuSelect SELECT", "ET WEB_SPECIFIC_APPS CafeEngine id Remote SQL Injection (dish.php)", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php firstname UNION SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page INSERT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- list_comments.php i UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp UNION SELECT", "ET MALWARE AntSword Webshell User-Agent Observed", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail UNION SELECT", "ET WEB_SPECIFIC_APPS Banana Dance name Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla SQL Reports user_id Parameter SELECT

	FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- download_image.asp image_id UPDATE", "ET WEB_SPECIFIC_APPS Joomla com_boss controller Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Flash Quiz answers.php order_number Parameter SQL Injection", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler SELECT", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP id UNION SELECT", "ET WEB_SPECIFIC_APPS Joomla XCloner Component cloner.cron.php config Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Bookmark4U SQL Injection Attempt -- config.php sqlcmd INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp AD_ID DELETE", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid ASCII", "ET WEB_SPECIFIC_APPS wordpress thecartpress plugin loop parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Interactive Web Solutions site_info.php DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp INSERT", "ET SCAN DominoHunter Security Scan in Progress", "ET WEB_SPECIFIC_APPS Easyedit CMS page.php intpageID parameter sql injection", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search UNION SELECT", "ET WEB_SPECIFIC_APPS Possible Zenoss Cross Site Request Forgery Ping UserCommand Attempt", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- prikazInformacije.php IDStranicaPodaci UPDATE", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 UPDATE", "ET WEB_SPECIFIC_APPS WordPress XCloner Plugin index2.php mosmsg Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue DELETE", "ET WEB_SPECIFIC_APPS Joomla Component City Portal (Itemid) Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- save.php groupAddName SELECT", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id INSERT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 3", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak UNION SELECT", "ET WEB_SPECIFIC_APPS Hunkaray Okul Portaly SQL Injection Attempt -- haberoku.asp id DELETE", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserEmail DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb ePages SQL Injection Attempt -- actualpic.asp Biz_ID SELECT", "ET WEB_SERVER Possible Barracuda IM Firewall smtp_test.cgi Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Gazi Download Portal SQL Injection Attempt -- down_indir.asp id DELETE", "ET WEB_CLIENT Generic Mailer Accessed on Internal Server", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- printview.php topic UPDATE", "ET WEB_SPECIFIC_APPS FipsSHOP SQL Injection Attempt -- index.asp cat SELECT", "ET WEB_CLIENT Kageyama Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS nvisionix Roaming System sessions.php script Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS EZPX photoblog tpl_base_dir Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS MindTouch Deki Wiki deki_plugin.php Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Ublog Reload SQL Injection Attempt -- badword.asp DELETE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- aramayap.asp kelimeler UPDATE", "ET WEB_SPECIFIC_APPS Tunngavik CMS id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SERVER SQL Injection Select Sleep Time Delay", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL Injection Attempt -- massedit_album.php gall_id DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eCars SQL Injection Attempt -- Types.asp Type_id ASCII", "ET WEB_SPECIFIC_APPS Superfreaker Studios UPublisher SQL Injection Attempt -- preferences.asp ID ASCII", "ET WEB_SPECIFIC_APPS Burak Yylmaz Download Portal SQL Injection Attempt -- HABERLER.ASP kid DELETE", "ET WEB_SPECIFIC_APPS Possible Docebo UNION SELECT SQL Injection Attempt", "ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla! JBudgetsMagic 'bid' Parameter

	SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode DELETE", "ET WEB_SPECIFIC_APPS Pixel8 Web Photo Album AlbumID SQL Injection", "ET WEB_SPECIFIC_APPS dol storye SQL Injection Attempt -- dettaglio.asp id_aut DELETE", "ET EXPLOIT phpLDAPadmin LDAP Injection", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp categoryID_list UNION SELECT", "ET WEB_SPECIFIC_APPS uniForum SQL Injection Attempt -- wbsearch.aspx INSERT", "ET WEB_SPECIFIC_APPS Aspee and Dogantepe Ziyaretci Defteri SQL Injection Attempt -- giris.asp kullanici INSERT", "ET WEB_SERVER Possible PHP Remote Code Execution CVE-2019-11043 PoC (Inbound)", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie UNION SELECT", "ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION", "ET WEB_SPECIFIC_APPS Joomla com_yelp Component cid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cost2 SELECT", "ET WEB_SPECIFIC_APPS VS Panel showcat.php Cat_ID Parameter SQL Injection", "ET WEB_SPECIFIC_APPS YourFreeWorld Autoresponder hosting tr.php id Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp sub_id UPDATE", "ET WEB_SPECIFIC_APPS PHP Labs JobSitePro SQL Injection Attempt -- search.php salary SELECT", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php langue INSERT", "ET WEB_SPECIFIC_APPS Fullaspsite ASP Hosting Site SQL Injection Attempt -- listmain.asp cat UPDATE", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID UPDATE", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid UPDATE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listmain.asp cat UNION SELECT", "ET EXPLOIT php with eval/gzinflate/base64_decode possible webshell", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- DocPay.w2b listDocPay INSERT", "ET EXPLOIT MMCS service (Little Endian)", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchkey.asp Keyword INSERT", "ET WEB_SPECIFIC_APPS Pre Online Tests Generator Pro UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Okul Web Otomasyon Sistemi SQL Injection Attempt -- etkinlikbak.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- search.asp search UNION SELECT", "ET WEB_SPECIFIC_APPS PithCMS oldnews_reader.php lang Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp kullanici_ismi UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- menu.php UNION SELECT", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment UPDATE", "ET WEB_SPECIFIC_APPS Joomla Incapsula component Security.php XSS Attempt", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c SELECT", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- okvalannonce.php idannonce SELECT", "ET WEB_SPECIFIC_APPS ANGEL Learning Management Suite (LMS) SQL Injection Attempt -- default.asp id UPDATE", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- albmgr.php cat INSERT", "ET WEB_SPECIFIC_APPS PhreeBooks js_include.php form Parameter Cross Site Scripting Attempt 1", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- forums.php cat_id ASCII", "ET WEB_SPECIFIC_APPS Minerva mod SQL Injection Attempt -- forum.php c INSERT", "ET WEB_SPECIFIC_APPS WordPress Plugin iThemes Security SQL Injection", "ET WEB_SPECIFIC_APPS Event Calendar PHP cal_year Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board katid Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla Foobla Suggestions Component idea_id SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Nuke Evolution Xtreme pid Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WordPress SQL Injection Attempt -- admin-ajax.php cookie DELETE", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php

	website UPDATE", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name SELECT", "ET WEB_SPECIFIC_APPS Particle Soft Particle Gallery SQL Injection Attempt -- viewimage.php editcomment INSERT", "ET WEB_SERVER ColdFusion adminapi access", "ET WEB_SPECIFIC_APPS Webcat web_id Parameter Blind SQL Injection Vulnerability", "ET WEB_SPECIFIC_APPS Serendipity SQL Injection Attempt -- index.php serendipity UNION SELECT", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php boardids INSERT", "ET WEB_SPECIFIC_APPS WSN Guest SQL Injection Attempt -- comments.php id UNION SELECT", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid UNION SELECT", "ET WEB_SPECIFIC_APPS ProjectButler RFI attempt", "ET EXPLOIT Ecessa WANWorx WVR-30 Cross-Site Request Forgery", "ET WEB_SPECIFIC_APPS Woltlab Burning Board Lite SQL Injection Attempt -- thread.php threadvisit SELECT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_recent.asp currentpage UPDATE", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- ad.asp cat_id DELETE", "ET WEB_SERVER ATTACKER WebShell - Zehir4.asp - content", "ET WEB_SPECIFIC_APPS Newsletter MX SQL Injection Attempt -- admin_mail_adressee.asp ID INSERT", "ET WEB_SPECIFIC_APPS Pilot Online Training Solution news_read.php id SQL Injection", "ET WEB_SPECIFIC_APPS NewSolved newsscript.php newsid Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Comicsense SQL Injection Attempt -- index.php epi INSERT", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps UNION SELECT", "ET WEB_SPECIFIC_APPS SoftMP3 search Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Joomla com_avosbillets Component id Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php clickurl SELECT", "ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module ipmi_bladestatus.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- detail.asp property_id ASCII", "ET WEB_CLIENT Generic Website Ransomnote Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Forum Livre SQL Injection Attempt -- info_user.asp user DELETE", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Project_ID DELETE", "ET WEB_SPECIFIC_APPS Shape Web Solutions imprimir.php UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Particle Blogger SQL Injection Attempt -- post.php postid INSERT", "ET WEB_SPECIFIC_APPS cPanel dir Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS BtiTracker SQL Injection Attempt -- account_change.php style DELETE", "ET WEB_SPECIFIC_APPS gCards SQL Injection Attempt -- getnewsitem.php newsid UPDATE", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp vehicleID UPDATE", "ET WEB_SPECIFIC_APPS Simploo CMS x parameter Remote PHP Code Execution Attempt", "ET WEB_SPECIFIC_APPS LINK Content Management Server (CMS) SQL Injection Attempt -- navigacija.php IDMeniGlavni UPDATE", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- categories.php text INSERT", "ET WEB_SERVER LANDesk Command Injection Attempt", "ET WEB_SPECIFIC_APPS IWantOneButton Wordpress SQL Injection Attempt updateAJAX.php post_id UNION SELECT", "ET WEB_SPECIFIC_APPS MGinternet Property Site Manager SQL Injection Attempt -- listings.asp typ INSERT", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- changeannonce.php idannonce UPDATE", "ET WEB_SPECIFIC_APPS bcoos adresses module viewcat.php cid Parameter SQL injection", "ET WEB_SPECIFIC_APPS VP-ASP Shopping Cart SQL Injection Attempt -- shopgiftregsearch.asp LoginLastname ASCII", "ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .aspx Filename Extension Parsing File Upload Security Bypass Attempt (aspx)", "ET WEB_SPECIFIC_APPS Gazi Download Portal SQL Injection Attempt -- down_indir.asp id INSERT", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt --

	meal_rest.asp mealid SELECT", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp sort UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- login.asp sent SELECT", "ET WEB_SPECIFIC_APPS w-Agora SQL Injection Attempt -- search.php search_user INSERT", "ET WEB_SPECIFIC_APPS Openfoncier blocnote.class.php script Remote File inclusion Attempt", "ET EXPLOIT Xiongmai/HiSilicon DVR - Request for User Details - Possible CVE-2017-7577 Exploit Attempt", "ET WEB_CLIENT Leaf PHPMailer Accessed on External Server", "ET WEB_SPECIFIC_APPS BPG-InfoTech Content Management System SQL Injection Attempt -- publication_view.asp InfoID SELECT", "ET WEB_SERVER ColdFusion componentutils access", "ET WEB_SPECIFIC_APPS Hedgehog CMS header.php c_temp_path Local File Inclusion", "ET WEB_SPECIFIC_APPS LI-Guestbook SQL Injection Attempt -- guestbook.php country SELECT", "ET WEB_SPECIFIC_APPS W2B Online Banking SQL Injection Attempt -- mailer.w2b draft SELECT", "ET WEB_SPECIFIC_APPS Flash Quiz question.php order_number Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Solar Empire SQL Injection Attempt -- game_listing.php SELECT", "ET WEB_SPECIFIC_APPS Link Exchange Lite SQL Injection Attempt -- linkslist.asp psearch SELECT", "ET WEB_SPECIFIC_APPS EQdkp SQL Injection Attempt -- listmembers.php rank INSERT", "ET EXPLOIT TP-Link Technologies TL-WA850RE Wi-Fi Range Extender - Command Execution", "ET WEB_SPECIFIC_APPS Business Objects Crystal Reports Web Form Viewer Directory Traversal Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp listing_price INSERT", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid DELETE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id UNION SELECT", "ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field INSERT", "ET WEB_SPECIFIC_APPS Concrete CMS approveImmediately parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- listfull.asp ID ASCII", "ET WEB_SPECIFIC_APPS Joomla com_zoomportfolio component UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Fuzzylime Forum SQL Injection Attempt -- low.php topic ASCII", "ET WEB_SPECIFIC_APPS NukeSentinel SQL Injection Attempt -- nsbypass.php UNION SELECT", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile UPDATE", "ET WEB_SPECIFIC_APPS Joomla je-media-player view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS CubeCart SQL Injection Attempt -- cart.inc.php ASCII", "ET WEB_SPECIFIC_APPS Easebay Resources Login Manager SQL Injection Attempt -- memberlist.php init_row DELETE", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentmail DELETE", "ET WEB_SPECIFIC_APPS coRED CMS rubID Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DesktopOnNet frontpage.php app_path Parameter Remote File Inclusion", "ET WEB_SPECIFIC_APPS Joomla! JBudgetsMagic 'bid' Parameter UNION SELECT SQL Injection", "ET WEB_SPECIFIC_APPS Joomla com_bit controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp id DELETE", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID DELETE", "ET WEB_SPECIFIC_APPS Gbook MX newlangsel Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS FuseTalk SQL Injection Attempt -- autherror.cfm errorcode SELECT", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_joined.php cat UNION SELECT", "ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (SWNetPerfMon.db) (CVE-2020-10148)", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid INSERT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dirSub.asp sid SELECT", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php post_id ASCII", "ET WEB_SPECIFIC_APPS dev4u CMS SQL Injection Attempt -- index.php gruppe_id INSERT", "ET WEB_SPECIFIC_APPS Orlando CMS stage6.php GLOBALS Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Simple PHP Forum SQL Injection Attempt -- logon_user.php username UNION SELECT", "ET WEB_SPECIFIC_APPS Elxis CMS SQL Injection Attempt -- mod_banners.php DELETE", "ET WEB_SPECIFIC_APPS Cacti SQL

	Injection Vulnerability tree.php leaf_id UNION SELECT", "ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M1", "ET WEB_SPECIFIC_APPS Absolute Image Gallery SQL Injection Attempt -- gallery.asp categoryid UPDATE", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp DELETE", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- meal_rest.asp mealid UNION SELECT", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php did DELETE", "ET WEB_SPECIFIC_APPS RIPS code.php Local File Inclusion Vulnerability", "ET WEB_SPECIFIC_APPS WordPress Age Verification plugin redirect_to Parameter URI Redirection", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 UPDATE", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- list.php categoryid UPDATE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld UNION SELECT", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- db_ecard.php start UPDATE", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- a_register.asp DELETE", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage SELECT", "ET WEB_SPECIFIC_APPS PHPEcho CMS SQL Injection Attempt -- gallery.php id INSERT", "ET WEB_SPECIFIC_APPS Flash Quiz results_table_web.php quiz Parameter SQL Injection", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID ASCII", "ET WEB_SPECIFIC_APPS JiRos Links Manager SQL Injection Attempt -- openlink.asp LinkID ASCII", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- polls.php id SELECT", "ET WEB_SPECIFIC_APPS fipsGallery SQL Injection Attempt -- index1.asp which INSERT", "ET WEB_SPECIFIC_APPS LushiNews SQL Injection Attempt -- comments.php id DELETE", "ET WEB_SPECIFIC_APPS eNdonesia SQL Injection Attempt -- mod.php cid UNION SELECT", "ET WEB_SPECIFIC_APPS simple machines forum include parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- inc_secureloginmanager.asp sent INSERT", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- rating.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS DEDECMS feedback_js.php arcurl Parameter INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Uapplication UPhotoGallery SQL Injection Attempt -- thumbnails.asp ci DELETE", "ET WEB_SPECIFIC_APPS vSpin.net Classified System SQL Injection Attempt -- search.asp state SELECT", "ET WEB_SPECIFIC_APPS DMXReady Site Engine Manager SQL Injection Attempt -- index.asp mid ASCII", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchmain.asp cat DELETE", "ET WEB_SPECIFIC_APPS Gazi Download Portal SQL Injection Attempt -- down_indir.asp id UPDATE", "ET WEB_SPECIFIC_APPS ECShop user.php order_sn Parameter SQL Injection", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass DELETE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_cat_id ASCII", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- pop_up_member_search.asp name DELETE", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- kullanicilistesi.asp ak UPDATE", "ET WEB_SPECIFIC_APPS NetVIOS Portal SQL Injection Attempt -- page.asp NewsID DELETE", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php code ASCII", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid ASCII", "ET WEB_SPECIFIC_APPS XLAtunes SQL Injection Attempt -- view.php album SELECT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php comment DELETE", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass SELECT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id DELETE", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- search.php search INSERT", "ET WEB_SPECIFIC_APPS Virtuemart SQL Injection Attempt -- virtuemart_parser.php category_id SELECT", "ET WEB_SPECIFIC_APPS Services id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WeBid cron.php include_path Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS EasyMoblog SQL Injection Attempt -- add_comment.php i DELETE", "ET WEB_SERVER

	Possible AntSword Webshell Commands Inbound", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- admin.asp id UNION SELECT", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- gallery.php image_id INSERT", "ET WEB_SERVER Attempt To Access MSSQL sp_adduser Stored Procedure Via URI to Create New Database User", "ET WEB_SPECIFIC_APPS Jenkins Information Disclosure CVE-2017-1000395", "ET WEB_SPECIFIC_APPS Ultimate Survey Pro SQL Injection Attempt -- index.asp cat ASCII", "ET WEB_SPECIFIC_APPS Joomla com_jreactions mosConfig_absolute_path Parameter Remote File inclusion Attempt", "ET WEB_SPECIFIC_APPS E-Shop Shopping Cart Script search_results.php SQL Injection", "ET WEB_SPECIFIC_APPS Joomla com_jeformcr view parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP link Directory sbcat_id Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DuWare DuNews SQL Injection Attempt -- detail.asp iNews SELECT", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- example.php UPDATE", "ET WEB_SPECIFIC_APPS Metyus Okul Yonetim Sistemi SQL Injection Attempt -- uye_giris_islem.asp sifre INSERT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp stock_number DELETE", "ET WEB_SPECIFIC_APPS PHPKit SQL Injection Attempt -- include.php catid ASCII", "ET WEB_SERVER FiercePhish Password Prompt Accessed on Internal Server", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php position DELETE", "ET WEB_SPECIFIC_APPS AnnonceScriptHP SQL Injection Attempt -- voirannonce.php no UPDATE", "ET WEB_SPECIFIC_APPS vBSupport SQL Injection Attempt -- vBSupport.php SELECT", "ET WEB_SPECIFIC_APPS WebTester SQL Injection Attempt -- directions.php testID INSERT", "ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id ASCII", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent SELECT", "ET WEB_SPECIFIC_APPS Mambo AHS Shop component UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS FireStats window-add-excluded-url.php Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS icash Click&BaneX user_menu.asp ID parameter SQL Injection", "ET WEB_SPECIFIC_APPS Zenphoto date parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WordPress Sharebar plugin status parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Joomla swMenuPro ImageManager.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Cisco Common Services Framework Reflective XSS Attempt", "ET WEB_SPECIFIC_APPS Job2C windetail.php adtype Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS Coppermine Photo Gallery SQL Injection Attempt -- usermgr.php gid INSERT", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newwebsite UNION SELECT", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php newuserPass UPDATE", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp action ASCII", "ET WEB_SPECIFIC_APPS Portix-PHP SQL Injection Attempt -- archive.php blogid ASCII", "ET WEB_SPECIFIC_APPS Simple Web Content Management System SQL Injection Attempt -- page.php id INSERT", "ET WEB_SPECIFIC_APPS Online Web Building SQL Injection Attempt -- page.asp art_id UNION SELECT", "ET WEB_SPECIFIC_APPS DUware DUdownload SQL Injection Attempt -- detail.asp iFile DELETE", "ET WEB_SPECIFIC_APPS NetClassifieds Premium Edition SQL Injection Attempt -- ViewCat.php s_user_id UPDATE", "ET WEB_SPECIFIC_APPS Infinitytechs Restaurants CM SQL Injection Attempt -- res_details.asp resid DELETE", "ET WEB_SPECIFIC_APPS Joomla com_avosbillets Component id Parameter DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS DGNews SQL Injection Attempt -- news.php catid UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- content.asp sent INSERT", "ET WEB_SPECIFIC_APPS Neuron Blog SQL Injection Attempt -- addcomment2.php commentname UPDATE", "ET WEB_SPECIFIC_APPS OvBB admincp.php smilieid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp cat UNION SELECT", "ET WEB_SPECIFIC_APPS BP Blog SQL Injection Attempt -- default.asp layout UNION SELECT", "ET WEB_SPECIFIC_APPS Easynet4u Link Host directory.php cat_id parameter SQL Injection", "ET WEB_SERVER Possible D-Link Router HNAP Protocol Security Bypass Attempt", "ET WEB_SPECIFIC_APPS Xt-News SQL Injection

	Attempt -- show_news.php id_news INSERT", "ET WEB_SPECIFIC_APPS Xtreme ASP Photo Gallery SQL Injection Attempt -- displaypic.asp sortorder UPDATE", "ET WEB_SPECIFIC_APPS Joomla! SQL Injection Attempt -- ldap.php ASCII", "ET WEB_SPECIFIC_APPS E-SMARTCART SQL Injection Attempt -- productdetail.asp product_id ASCII", "ET WEB_SPECIFIC_APPS Joomla com_yelp Component cid Parameter UNION SELECT SQL Injection Attempt", "ET EXPLOIT Possible CVE-2017-12629 XXE Exploit Attempt (URI)", "ET WEB_SERVER PHP Scan Precursor", "ET WEB_SPECIFIC_APPS Joomla FaceBook Component face_id Parameter SELECT FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS BtitTracker SQL Injection Attempt -- torrents.php order SELECT", "ET WEB_SPECIFIC_APPS fipsCMS SQL Injection Attempt -- index.asp fid UPDATE", "ET WEB_SPECIFIC_APPS DynPage dynpage_load.php file Parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Joomla Component com_jbook (Itemid) Blind SQL Injection Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 2", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- news.php news_id UNION SELECT", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL Injection Attempt -- massedit_album.php gall_id SELECT", "ET WEB_SPECIFIC_APPS PHP Address Book from Parameter Cross Site Scripting Attempt", "ET WEB_SERVER WSO 2.6 Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS Joomla com_bulkenquery controller parameter Local File Inclusion Attempt", "ET WEB_SPECIFIC_APPS AJ Forum SQL Injection Attempt -- topic_title.php td_id SELECT", "ET WEB_SPECIFIC_APPS Hubscript PHPInfo Attempt", "ET WEB_SPECIFIC_APPS Woltlab Burning Board (wBB) SQL Injection Attempt -- search.php board UPDATE", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp gallery_id SELECT", "ET WEB_SPECIFIC_APPS YaPig last_gallery.php YAPIG_PATH Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS Website Designs For Less Click N Print Coupons SQL Injection Attempt -- coupon_detail.asp key INSERT", "ET WEB_SPECIFIC_APPS Savas Guestbook SQL Injection Attempt -- add2.php country UNION SELECT", "ET WEB_SPECIFIC_APPS iScripts MultiCart orderid Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS PHP-Update SQL Injection Attempt -- guestadd.php newmessage DELETE", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin folder.php type Parameter Cross Site Scripting Attempt", "ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM", "ET WEB_SPECIFIC_APPS Wordpress Easy Stats plugin homep Parameter Remote File inclusion Attempt", "GPL ATTACK_RESPONSE directory listing", "ET WEB_SPECIFIC_APPS ClearSite device_admin.php cs_base_path Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS While You Were Out (WYWO) InOut Board SQL Injection Attempt -- faqDsp.asp catcode SELECT", "ET WEB_SPECIFIC_APPS 20/20 Auto Gallery SQL Injection Attempt -- vehiclelistings.asp listing_price ASCII", "ET WEB_SPECIFIC_APPS Outfront Spooky Login SQL Injection Attempt -- register.asp UserUpdate ASCII", "ET WEB_SPECIFIC_APPS JGBBS SQL Injection Attempt -- search.asp title UPDATE", "ET WEB_SPECIFIC_APPS Sphider SQL Injection Attempt -- search.php category ASCII", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php lastname UPDATE", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id INSERT", "ET WEB_SPECIFIC_APPS SalesCart Shopping Cart SQL Injection Attempt -- reorder2.asp DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID INSERT", "ET WEB_SPECIFIC_APPS Design4Online UserPages2 SQL Injection Attempt -- page.asp art_id UPDATE", "ET WEB_SPECIFIC_APPS WORDPRESS Plugin Accept Signups email Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS ExoPHPDesk SQL Injection Attempt -- faq.php id ASCII", "ET WEB_SPECIFIC_APPS OvBB admincp.php smilieid Parameter UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.php id DELETE", "ET WEB_SPECIFIC_APPS Possible Docebo INSERT INTO Injection Attempt", "ET WEB_SPECIFIC_APPS Nakid CMS CKEditorFuncNum parameter Cross Site Scripting Attempt", "ET WEB_CLIENT Generic WSO Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS KLF-DESIGN (aka Kim L. Fraser) KLF-REALTY SQL Injection Attempt -- search_listing.asp agent SELECT", "ET WEB_SPECIFIC_APPS Euchia

	CMS catalogo.php id_livello Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Syntax Desktop preview.php synTarget Parameter Local File Inclusion", "ET WEB_SPECIFIC_APPS All In One Control Panel (AIOCP) SQL Injection Attempt -- cp_authorization.php xuser_name UPDATE", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 12", "ET WEB_SPECIFIC_APPS The Address Book SQL Injection Attempt -- user.php passwordOld ASCII", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- status.asp uid SELECT", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php id ASCII", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- user_confirm.asp pass INSERT", "ET WEB_SPECIFIC_APPS PollMentor SQL Injection Attempt -- pollmentorres.asp id ASCII", "ET WEB_SPECIFIC_APPS Wallpaper Complete Website SQL Injection Attempt -- wallpaper.php wallpaperid UNION SELECT", "ET WEB_SPECIFIC_APPS Concrete CMS btask parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS MaticMarket modulename Parameter Local File Inclusion Attempt-8", "ET WEB_SPECIFIC_APPS SOPHIA CMS SQL Injection Attempt -- dsp_page.cfm pageid INSERT", "ET WEB_SPECIFIC_APPS Francisco Burzi PHP-Nuke SQL Injection Attempt -- index.php ad_class SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- compareHomes.asp adID SELECT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_list.asp secondgroup UNION SELECT", "ET WEB_SPECIFIC_APPS Invision Power Board (IPB) SQL Injection Attempt -- class_session.php CLIENT_IP INSERT", "ET WEB_SPECIFIC_APPS asaher pro view_messages.php row_y5_site_configuration Remote File Inclusion Attempt", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 5", "ET WEB_SPECIFIC_APPS Symantec Endpoint Manager XXE RCE Attempt", "ET WEB_SPECIFIC_APPS Joomla portalid Component SELECT FROM SQL Injection", "ET WEB_SPECIFIC_APPS Omegasoft SQL Injection Attempt -- OmegaMw7.asp INSERT", "ET WEB_SPECIFIC_APPS Neocrome Seditio SQL Injection Attempt -- users.register.inc.php ASCII", "ET WEB_SPECIFIC_APPS SmE FileMailer SQL Injection Attempt -- dl.php ps ASCII", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id SELECT", "ET EXPLOIT Joomla 3.2.1 SQL injection attempt", "ET WEB_SPECIFIC_APPS WordPress CataBlog plugin category Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS OSSIM repository_attachment.php UNION SELECT SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Xoops SQL Injection Attempt -- print.php id UPDATE", "ET WEB_SPECIFIC_APPS Kartli Alisveris Sistemi SQL Injection Attempt -- news.asp news_id ASCII", "ET WEB_SPECIFIC_APPS Easypush Server Manager addressbook.cgi page Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS WB News News.php config Parameter Remote File Inclusion -2", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php galleryID UPDATE", "ET WEB_SPECIFIC_APPS Enthusiast SQL Injection Attempt -- show_owned.php cat UNION SELECT", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- default.asp page UNION SELECT", "ET WEB_SPECIFIC_APPS TCExam tce_xml_user_results.php script DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Wordpress eShop plugin action parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS EJBCA issuer Parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- jump.php id DELETE", "ET WEB_SPECIFIC_APPS LushiWarPlaner SQL Injection Attempt -- register.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Alan Ward A-Cart Pro SQL Injection Attempt -- product.asp productid ASCII", "ET WEB_SPECIFIC_APPS ActiveNews Manager SQL Injection Attempt -- activenews_view.asp articleID DELETE", "ET WEB_SPECIFIC_APPS Flash Gallery wordpress plugin SQL Injection Attempt -- massedit_album.php gall_id INSERT", "ET WEB_SPECIFIC_APPS Wordpress 2.2 SQL Injection Attempt -- xmlrpc.php UPDATE", "ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (42)", "ET WEB_SPECIFIC_APPS Doug Luxem Liberum Help Desk SQL Injection Attempt -- details.asp id ASCII", "ET WEB_SPECIFIC_APPS 8pixel.net simpleblog SQL Injection Attempt -- edit.asp id DELETE", "ET WEB_SPECIFIC_APPS phpx SQL Injection Attempt -- users.php user_id UPDATE", "ET WEB_SPECIFIC_APPS

	WordPress Leaflet plugin(leaflet_layer) id parameter Cross-Site Scripting Attempt", "ET SCAN Havij SQL Injection Tool User-Agent Inbound", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- printmain.asp ID ASCII", "ET WEB_SPECIFIC_APPS chatwm SQL Injection Attempt -- SelGruFra.asp txtUse INSERT", "ET WEB_SPECIFIC_APPS MGB OpenSource Guestbook SQL Injection Attempt -- email.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp pass DELETE", "ET WEB_SPECIFIC_APPS Kisisel Site 2007 SQL Injection Attempt -- forum.asp forumid SELECT", "ET WEB_SPECIFIC_APPS PHPWind SQL Injection Attempt -- admin.php UNION SELECT", "ET WEB_SPECIFIC_APPS Bluetrait SQL Injection Attempt -- bt-trackback.php ASCII", "ET WEB_SPECIFIC_APPS Calendar MX BASIC SQL Injection Attempt -- calendar_detail.asp ID DELETE", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- dircat.asp cid UNION SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp INSERT", "ET WEB_SPECIFIC_APPS MidiCart ASP Shopping Cart and ASP Plus Shopping Cart SQL Injection Attempt -- item_show.asp id2006quant SELECT", "ET WEB_SPECIFIC_APPS DMXReady Secure Login Manager SQL Injection Attempt -- set_preferences.asp SELECT", "ET WEB_SPECIFIC_APPS joomla com_jstore controller parameter Local File Inclusion vulnerability", "ET WEB_SPECIFIC_APPS Oxygen (O2PHP Bulletin Board) SQL Injection Attempt -- viewthread.php pid ASCII", "ET WEB_SPECIFIC_APPS TelebidAuctionScript aid Parameter Blind SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Rialto SQL Injection Attempt -- searchoption.asp acreage1 INSERT", "ET WEB_SPECIFIC_APPS Messageriescripthp SQL Injection Attempt -- lire-avis.php aa DELETE", "ET WEB_SPECIFIC_APPS ContentNow SQL Injection Attempt -- index.php pageid UNION SELECT", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- homeDetail.asp AD_ID UNION SELECT", "ET WEB_SPECIFIC_APPS Ezboxx Portal System Beta SQL Injection Attempt -- ShowAppendix.asp iid ASCII", "ET WEB_SPECIFIC_APPS webSPELL SQL Injection Attempt -- gallery.php picID DELETE", "ET WEB_SPECIFIC_APPS phpPollScript include_class Parameter Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS ASPMForum SQL Injection Attempt -- forum2.asp soruid DELETE", "ET WEB_SPECIFIC_APPS Web Wiz Forums SQL Injection Attempt -- functions_filters.asp SELECT", "ET WEB_SPECIFIC_APPS Blogplus block_center_top.php Local File Inclusion", "ET WEB_SPECIFIC_APPS Evolve shopping cart SQL Injection Attempt -- products.asp partno INSERT", "ET WEB_SPECIFIC_APPS OSSIM repository_attachment.php INSERT INTO SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Raymond BERTHOU script SQL Injection Attempt -- login.asp user INSERT", "ET WEB_SPECIFIC_APPS pHNews comments.php templates_dir Local File Inclusion", "ET WEB_SPECIFIC_APPS Enthrallweb eClassifieds SQL Injection Attempt -- dircat.asp cid SELECT", "ET WEB_SPECIFIC_APPS Recipes Complete Website SQL Injection Attempt -- recipe.php recipeid DELETE", "ET WEB_SPECIFIC_APPS Commentics id parameter Cross-Site Scripting Attempt", "ET WEB_SPECIFIC_APPS Plogger phpThumb.php src Parameter Remote File Disclosure Attempt", "ET WEB_SPECIFIC_APPS Nucleus media.php Remote File Inclusion Attempt", "ET WEB_SPECIFIC_APPS PHP Booking Calendar page_info_message parameter Cross-Site Scripting Vulnerability", "ET WEB_SPECIFIC_APPS RaXnet Cacti top_graph_header.php config Parameter Remote File Inclusion", "ET WEB_CLIENT Anonymous Webshell Accessed on External Compromised Server", "ET WEB_SPECIFIC_APPS Enthrallweb eHomes SQL Injection Attempt -- result.asp cat INSERT", "ET WEB_SPECIFIC_APPS Novell ZENworks Patch Management (ZPM) SQL Injection Attempt -- downloadreport.asp agentid DELETE", "ET WEB_SPECIFIC_APPS LocazoList SQL Injection Attempt -- main.asp subcatID INSERT", "ET WEB_SPECIFIC_APPS WordPress The-Welcomizer plugin page parameter Cross Site Scripting Attempt", "ET WEB_SERVER WSO 4.2.6 Webshell Accessed on Internal Compromised Server", "ET WEB_SPECIFIC_APPS PHP-fusion Team Structure Infusion team_id Parameter UPDATE SET SQL Injection Attempt", "ET WEB_SPECIFIC_APPS Grayscale Blog SQL Injection Attempt -- detail.php id UNION SELECT", "ET WEB_SPECIFIC_APPS Apache Archive deleteNetworkProxy script Cross Site Scripting Attempt", "ET ACTIVEX 4XEM

	VatDecoder VatCtrl Class ActiveX Control Url Property Buffer Overflow Vulnerability", "ET WEB_SPECIFIC_APPS PHPAccounts SQL Injection Attempt -- index.php Outgoing_ID SELECT", "ET WEB_SPECIFIC_APPS Lotfian Request For Travel SQL Injection Attempt -- ProductDetails.asp PID INSERT", "ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 7", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- view_gallery.asp currentpage UPDATE", "ET WEB_SPECIFIC_APPS Wordpress eShop plugin eshoptemplate parameter Cross Site Scripting Attempt", "ET WEB_SPECIFIC_APPS iGeneric iG Shop SQL Injection Attempt -- compare_product.php id SELECT", "ET WEB_SPECIFIC_APPS My Little Forum SQL Injection Attempt -- user.php id INSERT", "ET WEB_SPECIFIC_APPS Guo Xu Guos Posting System (GPS) SQL Injection Attempt -- print.asp id UPDATE", "ET WEB_SPECIFIC_APPS Possible Achievo userid= Variable DELETE FROM SQL Injection Attempt", "ET WEB_SPECIFIC_APPS WSPortal SQL Injection Attempt -- content.php page INSERT", "ET WEB_SPECIFIC_APPS ClickTech Click Gallery SQL Injection Attempt -- gallery.asp currentpage INSERT", "ET WEB_SPECIFIC_APPS Eclectic Designs CascadianFAQ SQL Injection Attempt -- index.php qid INSERT", "ET WEB_SPECIFIC_APPS WordPress Leaflet plugin(leaflet_marker) id parameter Cross-Site Scripting Attempt"
Попытки получения привилегий администратора	"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (24)", "ET EXPLOIT Supermicro BMC Password Disclosure 2", "ET EXPLOIT NetGear WNR2000v5 Buffer Overflow Attempt Inbound (CVE-2017-6862)", "ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M3", "ET EXPLOIT Apache log4j RCE Attempt - Nested upper (tcp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Possible CVE-2017-8759 Soap File DL", "GPL FTP SITE NEWER overflow attempt", "ET EXPLOIT TP-LINK DNS Change GET Request (DNSChanger EK)", "ET EXPLOIT Microsoft Exchange Server Exploitation Inbound (CVE-2020-17132)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - Possible Stack Buffer Overflow Attempt Outbound (Multiple CVE IDs)", "GPL NETBIOS SMB-DS CoGetInstanceFromFile overflow attempt", "GPL NETBIOS SMB NDdeSetTrustedShareW unicode overflow attempt", "ET EXPLOIT Trenda Router AC11 RCE Outbound (CVE-2021-31755)", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp corba) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Likely Struts S2-053-CVE-2017-12611 Exploit Attempt M2", "ET EXPLOIT 3Com Office Connect Remote Code Execution (Outbound)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - Possible Stack Buffer Overflow Attempt Inbound (Multiple CVE IDs)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (5)", "ET EXPLOIT Mikrotik Winbox RCE Attempt (CVE-2018-14847)", "ET EXPLOIT Apache log4j RCE Attempt (udp ldaps) (CVE-2021-44228)", "ET WEB_SERVER Access to /phppath/php Possible Plesk 0-day Exploit June 05 2013", "ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3", "ET EXPLOIT HiSilicon DVR - Buffer Overflow in Builtin Web Server", "ET EXPLOIT Possible Oracle Identity Manager Attempt to Logon with default account", "ET EXPLOIT Apache Solr RCE via Velocity Template M2 (CVE-2019-17558)", "ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M3", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nds) (Outbound) (CVE-2021-44228)", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode little endian andx overflow attempt", "ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Construct M2", "ET EXPLOIT CreateService via SMB to Reset-ComputerMachinePassword - Observed Post Zerologon Activity", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt M2", "ET EXPLOIT Microsoft Edge Chakra - InjectJsBuiltInLibraryCode Use-After-Free Inbound (CVE-2019-0568)", "ET EXPLOIT Apache2 Memory Corruption Inbound (CVE-2020-9490)", "ET MALWARE Possible Linux.Mirai Login Attempt (service)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M1", "ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040)", "ET EXPLOIT .NET Framework Remote Code Execution Injection (CVE-2020-0646)", "ET EXPLOIT Possible Postfix CVE-2014-6271 attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M3", "ET EXPLOIT Possible Microsoft Exchange ProxyLogon Activity - OABVirtualDirectory SetObject (CVE-2021-27065)", "ET EXPLOIT TerraMaster TOS Unauthenticated Command Injection Inbound M1 (CVE-

	2022-24989)", "ET MALWARE AllaKore RAT ID Command Observed", "ET WEB_SERVER BlackSquid JSP Webshell Outbound", "ET WEB_SPECIFIC_APPS Oracle WebLogic Deserialization (CVE-2018-2893)", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M2", "ET EXPLOIT Possible VMware Workspace ONE Access RCE via Server-Side Template Injection Inbound (CVE-2022-22954)", "ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1", "ET EXPLOIT Possible ManageEngine ADAudit Plus XXE (CVE-2022-28219)", "ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M1 (CVE-2021-31207)", "ET EXPLOIT Linksys WRT54G Version 3.1 Command Injection Attempt", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M3", "GPL MISC rsh root", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (29)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (12)", "ET HUNTING Suspicious PHP Code in HTTP POST (Inbound)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - tmpapp.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M2", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M4", "ET EXPLOIT Microsoft Exchange SUID Disclosure via SSRF Inbound M2 (CVE-2021-31207)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M8", "GPL MISC rsh froot", "ET WEB_SERVER Babydraco WebShell Activity", "ET EXPLOIT Sonicwall Unauthenticated Stack-Based Buffer Overflow (CVE-2021-20038)", "ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (web.xml) (CVE-2021-26085)", "ET EXPLOIT DynoRoot DHCP - Client Command Injection", "ET EXPLOIT MVPower DVR Shell UCE MSF Check", "ET EXPLOIT ARG-W4 ASDL Router DNS Changer Exploit Attempt M2", "ET EXPLOIT Samba Arbitrary Module Loading Vulnerability M2 (NT Create AndX .so) (CVE-2017-7494)", "ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Outbound - Attempt to clear logs", "ET EXPLOIT Possible Engineers Online Portal System Access Control Bypass (CVE-2021-42671)", "ET EXPLOIT TOTOLINK Realtek SDK RCE (CVE-2019-19824)", "ET EXPLOIT Cisco Data Center Network Manager Directory Traversal Inbound (CVE-2019-15980)", "ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Inbound (CVE-2019-7256)", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M3", "ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 1", "ET EXPLOIT Apache Solr RCE via Velocity Template M1 (CVE-2019-17558)", "ET EXPLOIT Possible NGINX Reference LDAP Query Injection Attack", "ET WEB_SPECIFIC_APPS Possible Joomla SQLi Attempt (CVE-2015-7297 CVE-2015-7857 CVE-2015-7858)", "ET EXPLOIT Technicolor TD5130.2 - Remote Command Execution", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M2", "ET EXPLOIT Possible SolarWinds Orion RCE Inbound (CVE-2021-31474)", "ET EXPLOIT Secutech Router DNS Changer Exploit Attempt", "ET EXPLOIT Online Scheduling System 1.0 - Authentication Bypass Attempt", "GPL NETBIOS SMB OpenKey unicode andx overflow attempt", "ET MALWARE AllaKore RAT Set Keep-Alive Observed", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (CVE-2021-44228)", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M3", "ET EXPLOIT TP-LINK TL-WR340G Router DNS Change GET Request", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW little endian overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M2 (Outbound) (CVE-2021-44228)", "ET EXPLOIT Fastweb Fastgate 0.00.81 - Remote Code Execution", "ET EXPLOIT Possible Cacti Unauthenticated RCE Inbound M1 (CVE-2022-46169)", "ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (udp) (CVE-2021-44228)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M7", "ET EXPLOIT Possible MySQL cnf overwrite CVE-2016-6662 Attempt", "ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781) M4", "ET EXPLOIT MetInfo 7.0 SQL Injection (CVE-2019-16997)", "ET EXPLOIT Possible Mirai Infection Attempt via OS Command Injection Outbound (CVE-2021-32305)", "ET EXPLOIT Apache log4j RCE Attempt (udp dns) (CVE-2021-44228)", "ET EXPLOIT Laravel

	Remote Code Execution (CVE-2021-3129) Outbound - Payload Execution Attempt", "GPL NETBIOS SMB-DS llsrconnect unicode little endian andx overflow attempt", "ET EXPLOIT Attempted Schneider Electric SpaceLogic C-Bus Home Controller 5200WHC2 Remote Code Execution (CVE-2022-34753)", "ET EXPLOIT Multiple Router RCE Routersploit", "ET EXPLOIT Genexis PLATINUM 4410 Command Injection Inbound (CVE-2021-29003)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (3)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance (2)", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M2", "ET INFO Suspicious POST to Axis OS (smtptest.cgi)", "ET EXPLOIT Apache log4j RCE Attempt (udp ldaps) (Outbound) (CVE-2021-44228)", "GPL NETBIOS SMB Session Setup AndX request username overflow attempt", "ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M1", "ET EXPLOIT Zyxel Command Injection RCE (CVE-2017-6884)", "ET EXPLOIT Linksys Auth Bypass override.cgi", "GPL NETBIOS SMB OpenKey overflow attempt", "GPL RPC snmpXdmi overflow attempt TCP", "ET EXPLOIT Possible SolarWinds Serv-U SSH RCE Inbound M2 (CVE-2021-35211)", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toserver M3", "ET EXPLOIT 3Com Office Connect Remote Code Execution (Inbound)", "ET EXPLOIT Zoho ManageEngine Desktop Central RCE Inbound (CVE-2020-10189)", "ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M1", "ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M2", "ET WEB_SERVER Possible attempt to enumerate MS SQL Server version", "ET WEB_SERVER Possible DD-WRT Metacharacter Injection Command Execution Attempt", "ET EXPLOIT D-Link DIR-825 R1 Web Interface RCE (CVE-2020-29557)", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)", "GPL FTP CWD overflow attempt", "ET MALWARE ftpchk3.php upload attempted", "ET EXPLOIT PCMan FTP Server 2.0.7 Remote Command Execution", "GPL POP3 APOP overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M2", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M1", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp nis) (CVE-2021-44228)", "GPL NETBIOS SMB OpenKey unicode overflow attempt", "ET INFO Common JSP WebShell String Observed in HTTP Header M2", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M1", "ET EXPLOIT VMware vCenter SSRF Inbound", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M2", "ET WEB_SERVER Possible SUPERMICRO IPMI url_redirect.cgi Directory Traversal Attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M3", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Intel AMT Login Attempt Detected (CVE 2017-5689)", "ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Inbound (CVE-2016-6255)", "ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M2", "ET EXPLOIT Apache Struts memberAccess and getWriter inbound OGNL injection remote code execution attempt", "ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis", "ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2", "ET WEB_SPECIFIC_APPS Jetty WEB-INF Information Leak Attempt Inbound (CVE-2021-34429)", "ET EXPLOIT ForgeRock Access Manager RCE (CVE-2021-35464)", "ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Outbound (CVE-2019-7256)", "ET MALWARE Possible Linux.Mirai Login Attempt (dreambox)", "ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-26186)", "ET EXPLOIT InoERP 0.7.2 Unauthenticated Remote Code Execution (Inbound)", "ET EXPLOIT Possible Apache log4j RCE Attempt - HTTP URI Obfuscation (CVE-2021-44228) (Inbound)", "ET EXPLOIT Apache log4j RCE Attempt - Nested upper (udp) (CVE-2021-44228)", "ET EXPLOIT Apache log4j RCE Attempt (tcp ldaps) (CVE-2021-44228)", "ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 3 Inbound - Execute Mal Config Trigger (CVE-2020-8260)", "ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M1", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M1", "GPL NETBIOS SMB-DS DCERPC Remote Activation bind attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M3",

	"ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation Inbound M2", "ET EXPLOIT Bonitasoft Authorization Bypass M1 (CVE-2022-25237)", "ET EXPLOIT Netlink GPON Remote Code Execution Attempt (Inbound)", "ET WEB_SERVER Possible SQL Injection Attempt char() Danmec related", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp nis) (Outbound) (CVE-2021-44228)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M1", "ET EXPLOIT D-Link DI-804HV DNS Changer Exploit Attempt", "GPL NETBIOS SMB-DS OpenKey little endian andx overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M1", "ET EXPLOIT Possible Apache log4j Uncontrolled Recursion Lookup (CVE-2021-45105)", "ET EXPLOIT Supermicro BMC Password Disclosure 3", "ET WEB_SERVER Possible SQL Injection (exec)", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW overflow attempt", "ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation - Responding with Superuser Credentials", "ET EXPLOIT Metasploit 2013-3346", "ET WEB_SPECIFIC_APPS rConfig ajaxArchiveFiles.php Command Injection Inbound (CVE-2019-19509)", "ET EXPLOIT VMware Spring Cloud Gateway Code Injection (CVE-2022-22947) (set)", "GPL POP3 XTND overflow attempt", "ET EXPLOIT Actiontec C1000A backdoor account M1", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (10)", "ET EXPLOIT QNAP Shellshock CVE-2014-6271", "ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M3", "ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Inbound)", "ET EXPLOIT Prestashop Supercheckout Module Arbitrary File Upload", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (23)", "ET EXPLOIT Attempted IDSVSE IP Camera RCE", "ET EXPLOIT D-Link DWR Command Injection Inbound (CVE-2018-10823)", "ET EXPLOIT Adobe ColdFusion 11 - LDAP Java Object Deserialization RCE (POST) CVE-2018-15957", "ET EXPLOIT Adobe ColdFusion 11 - LDAP Java Object Deserialization RCE (GET) CVE-2018-15957", "ET EXPLOIT Jenkins Plugin Script RCE Exploit Attempt (CVE-2019-1003001)", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M3 (CVE-2020-14882)", "ET EXPLOIT Possible MySQL CVE-2016-6662 Attempt", "ET WEB_SPECIFIC_APPS Apache Struts memberAccess inbound OGNL injection remote code execution attempt", "ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x0005 (CVE-2020-35225)", "ET EXPLOIT SonicWall SMA Stack-Based Buffer Overflow CVE-2021-20038 M1", "ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M2", "ET EXPLOIT Oracle BI Publisher Authentication Bypass (CVE-2019-2616)", "ET EXPLOIT Possible SolarWinds Serv-U SSH RCE Inbound M1 (CVE-2021-35211)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - Auth Bypass Attempt Outbound (CVE-2021-33543)", "ET WEB_SERVER CURL Command Specifying Output in HTTP Headers", "ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M2", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)", "ET EXPLOIT .NET Framework Remote Code Execution Injection (CVE-2020-1147)", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M1 (CVE-2021-44228)", "ET EXPLOIT Possible WordPress Plugin BBPress 2.5 - Unauthenticated Priv Esc Attempt (CVE-2020-13693)", "ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M1", "ET ATTACK_RESPONSE PHP script in OptimizePress Upload Directory Possible WebShell Access", "ET EXPLOIT NUUO OS Command Injection", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode andx overflow attempt", "ET EXPLOIT CVE-2016-1287 Public Exploit ShellCode", "ET EXPLOIT D-Link HNAP SOAPAction Command Injection (CVE-2015-2051)", "ET EXPLOIT Zerologon Phase 3/3 - Malicious NetrServerPasswordSet2 (CVE-2020-1472)", "ET EXPLOIT Linksys Auth Bypass fw_sys_up.cgi", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M2", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW andx overflow attempt", "ET EXPLOIT iRZ Mobile Router RCE Inbound M1 (CVE-2022-27226)", "ET EXPLOIT Possible Gitlab CE/EE Image Parser RCE Inbound (CVE-2021-22205)", "ET EXPLOIT CVE-2016-3210 Exploit Observed ITW M1 Nov 30", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M2", "ET EXPLOIT Equation Group ExtraBacon Cisco ASA PMCHECK Disable", "ET EXPLOIT Possible NSDP (Netgear) Unauthenticated Buffer Overflow (CVE-2020-35232)", "ET WEB_SERVER

	SLIGHTPULSE WebShell Access Inbound M1", "ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Outbound (CVE-2019-6277)", "ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M2 (CVE-2021-31207)", "ET EXPLOIT Scriptcase 9.7 Arbitrary File Upload Attempt", "ET EXPLOIT TikiWiki CMS Authentication Bypass (Forced Blank Admin Pass) Attempt Inbound (CVE-2020-15906)", "ET WEB_CLIENT Apple Quicktime RTSP Overflow (2)", "ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Outbound", "ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Inbound (CVE-2019-12780)", "ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Outbound", "ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M2", "ET EXPLOIT Zoho ManagedEngine Desktop Central Authentication Bypass - Administrator Password Reset Attempt (CVE-2021-44515)", "ET EXPLOIT Apache log4j RCE Attempt (tcp rmi) (CVE-2021-44228)", "ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Inbound)", "GPL NETBIOS SMB CoGetInstanceFromFile little endian overflow attempt", "ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)", "GPL SMTP RCPT TO overflow", "ET EXPLOIT Discourse SNS Webhook RCE Inbound (CVE-2021-41163)", "ET EXPLOIT Extreme Networks ExtremeWireless Aerohive HiveOS and IQ Engine (Log Poisoning) (CVE-2020-16152) M1", "ET EXPLOIT Possible Malicious NAT-PMP Response Successful TCP Map to External Network", "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M2 (Possible Staging for CVE-2022-25237)", "ET EXPLOIT Yealink RCE Attempt (CVE-2021-27561)", "ET EXPLOIT Mitsubishi Electric smartRTU RCE Inbound (CVE-2019-14931)", "ET EXPLOIT Quanta LTE Router RDE Exploit Attempt 2 (traceroute)", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M1", "ET EXPLOIT Xfinity Gateway - Remote Code Execution", "ET EXPLOIT LG SuperSign EZ CMS 2.5 Remote Code Execution CVE-2018-17173", "ET EXPLOIT Possible Zimbra Autodiscover Servlet XXE (CVE-2019-9670)", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Stack Overflow in Base64 Authorization Mechanism M1", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M3", "ET EXPLOIT Telesquare SDT-CW3B1 1.1.0 - OS Command Injection (CVE-2021-46422)", "ET EXPLOIT MetInfo 7.0 SQL Injection (CVE-2019-17418)", "ET SCAN Tomcat admin-admin login credentials", "ET EXPLOIT Apache log4j RCE Attempt (udp rmi) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Confluence Server Path Traversal Vulnerability (CVE-2019-3398)", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M1", "ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Outbound)", "ET EXPLOIT Possible Apache Text4shell RCE Attempt JEXL Path (CVE-2022-42889) (Outbound)", "ET EXPLOIT Possible EXIM DoS (CVE-2019-16928)", "ET EXPLOIT VMWare Server-side Template Injection RCE (CVE-2022-22954)", "ET EXPLOIT Potentially Malicious .cab Inbound (CVE-2020-1300)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - language.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Outbound)", "ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation Inbound M1", "ET EXPLOIT Possible TerraMaster TOS RCE Inbound (CVE-2020-28188 CVE-2020-35665)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M2", "ET EXPLOIT Apache CouchDB JSON Remote Privesc Attempt (CVE-2017-12636)", "ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack", "ET EXPLOIT Apache log4j RCE Attempt (http ldaps) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Firefox 0-day used against TOR browser Nov 29 2016 M1", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (28)", "ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3", "ET EXPLOIT UPnP UUID Password Change Exploit Attempt Inbound - R6700V3 PoC Gadgets (CVE-2021-34991)", "ET WEB_SPECIFIC_APPS Liferay Unauthenticated RCE via JSONWS Inbound (CVE-2020-7961)", "ET EXPLOIT Attempted VMware Authentication Bypass (CVE-2022-31656)", "ET EXPLOIT Likely Struts S2-053-CVE-2017-12611 Exploit Attempt M1", "ET EXPLOIT VMware Spring Cloud Directory Traversal (CVE-2020-5410)", "ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (seraph-config.xml) (CVE-2021-26085)", "GPL NETBIOS SMB NDdeSetTrustedShareW andx overflow attempt", "ET EXPLOIT Laravel Remote Code

	Execution (CVE-2021-3129) Inbound - Payload Execution Attempt", "ET EXPLOIT Netgear DGN1000/DGN2200 Unauthenticated Command Execution Outbound", "ET WEB_SERVER CVE-2014-6271 Attempt In HTTP Headers Line Continuation Evasion LF", "ET EXPLOIT VMware vCenter RCE Exploitation Attempt M2 (CVE-2021-22005)", "ET WEB_SPECIFIC_APPS e107 CMS backdoor access admin-access cookie and HTTP POST", "ET EXPLOIT WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion", "ET EXPLOIT MVPower DVR Shell UCE", "GPL NETBIOS SMB llsrconnect unicode andx overflow attempt", "ET EXPLOIT dotCMS Arbitrary File Upload Attempt (CVE-2022-26352) M1", "ET WEB_SPECIFIC_APPS Drupalgeddon2 <8.3.9 <8.4.6 <8.5.1 RCE Through Registration Form (CVE-2018-7600)", "ET EXPLOIT SonicWall SMA Stack-Based Buffer Overflow CVE-2021-20038 M2", "ET EXPLOIT SEOWON INTECH SLC-130/SLR-120S RCE Inbound M1 (CVE-2020-17456)", "ET EXPLOIT Apache Struts getWriter and opensymphony inbound OGNL injection remote code execution attempt", "ET EXPLOIT D-link DI604 Known Malicious Router DNS Change GET Request", "ET EXPLOIT Apache Ambari Default Credentials Attempt", "ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M2", "ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M3", "ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M1", "ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M2", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M2 (CVE-2020-14882)", "ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M3", "ET EXPLOIT Possible Apache Text4shell RCE Attempt URL Prefix (CVE-2022-42889) (Inbound)", "GPL FTP XMKD overflow attempt", "ET EXPLOIT ASUS RT-N56U/RT-AC66U Remote Code Execution", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower UDP Bypass) (CVE-2021-44228)", "GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian andx overflow attempt", "ET EXPLOIT Microsoft Exchange Delete User Configuration - xbit set 1 (CVE-2021-42321)", "ET WEB_SPECIFIC_APPS Nette Command Injection Attempt Inbound (CVE-2020-15227)", "ET MALWARE Possible Linux.Mirai Login Attempt (zlxx)", "ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M3", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M6", "ET EXPLOIT Furukawa Electric ConsciusMAP 2.8.1 Java Deserialization Remote Code Execution (CVE-2020-12133)", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M2", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M3", "ET EXPLOIT Fortinet FortiWeb OS Command Injection Inbound M1 (CVE-2021-22123)", "ET EXPLOIT D-Link and TRENDnet ncc2 Service Vulnerability (ping.ccp) 2015-1187", "ET EXPLOIT [NCC GROUP] Possible Bluekeep Inbound RDP Exploitation Attempt (CVE-2019-0708)", "ET HUNTING Possible Apache Airflow Experimental API Authentication Bypass Attempt (CVE-2020-13927)", "ET SCAN Tomato Router Default Credentials (root:admin)", "ET EXPLOIT Apache log4j RCE Attempt - AWS Access Key Disclosure (Outbound) (CVE-2021-44228)", "ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate2 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M1", "ET EXPLOIT Possible Saltstack Authentication Bypass CVE-2020-11651 M1", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections5/MozillaRhino1/Vaadin) M2", "ET EXPLOIT Outbound GPON Authentication Bypass Attempt (CVE-2018-10561)", "ET EXPLOIT Dataprobe iBoot-PDU Pre-Auth Remote Code Execution Attempt via git-update.php (CVE-2022-3184) M1", "ET WEB_SERVER [Cluster25] FortiOS Auth Bypass Attempt (CVE-2022-40684)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M3", "ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Inbound)", "ET HUNTING Suspicious Chmod Usage in URI (Outbound)", "ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Inbound", "GPL FTP ALLO overflow attempt", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M1 (CVE-2020-14882)", "ET EXPLOIT Equation Group EGREGIOUSBLUNDER Fortigate Exploit Attempt", "ET EXPLOIT Apache log4j RCE Attempt - Nested lower (tcp) (CVE-2021-44228)", "ET NETBIOS Microsoft Windows Server 2003 Active Directory Pre-Auth BROWSER ELECTION Heap Overflow Attempt", "ET WEB_SPECIFIC_APPS Apache Struts inbound .getClass OGNL injection remote code execution attempt", "GPL NETBIOS SMB OpenKey unicode little endian overflow

	attempt", "ET EXPLOIT FritzBox RCE GET Request", "ET EXPLOIT Possible Moxa MxView RCE Attempt (CVE-2021-38454)", "ET EXPLOIT SMB Null Pointer Dereference PoC Inbound (CVE-2018-0833)", "ET EXPLOIT Zyxel NWA-1100-NH Command Injection Attempt (CVE-2021-4039)", "ET EXPLOIT TP-LINK TL-WR841N Router DNS Change GET Request", "ET SNMP Attempted TCP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (CVE-2021-44228)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (22)", "ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 4 Prefix Set Inbound (CVE-2022-22965)", "ET EXPLOIT Mi TV Integration Remote Code Execution CVE-2018???16130", "ET INFO Netlink GPON Login Attempt (GET)", "ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228)", "ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Inbound)", "ET MALWARE Possible Linux.Mirai Login Attempt (meinsm)", "ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M2", "ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M3", "ET EXPLOIT Cisco ASA and Firepower Path Traversal Vulnerability M1 (CVE-2020-3452)", "ET EXPLOIT HP Printer Attempted Path Traversal via PJL", "ET INFO imPcRemote Download", "ET EXPLOIT HP Enterprise VAN SDN Controller Root Command Injection (Unix)", "ET INFO Possible NOP Sled Observed in Large DNS over TCP Packet M1", "ET WEB_SPECIFIC_APPS Metabase Local File Inclusion Inbound (CVE-2021-41277)", "ET EXPLOIT Apache Cocoon <= 2.1.x LFI (CVE-2020-11991)", "ET WEB_SERVER lolzilla WebSkimmer - Remote Code Execution Attempt M5", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp corba) (CVE-2021-44228)", "GPL POP3 APOP USER overflow attempt", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-30333) M1", "ET EXPLOIT Possible ImageMagick Malformed SVG Upload Leading to RCE", "ET EXPLOIT Netgear Multiple Router Auth Bypass", "ET EXPLOIT UDP Technology Firmware (IP Cam) - testcmd.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "ET EXPLOIT Cisco RV320/RV325 Debug Dump Disclosure Attempt Inbound (CVE-2019-1653)", "ET EXPLOIT Nagios XI OS Command Injection (CVE-2021-25297 & CVE-2021-25298)", "ET EXPLOIT QNAP Photo Station Path Traversal Attempt Inbound (CVE-2019-7195)", "ET EXPLOIT Nexus Repository Manager EL Injection to RCE Inbound (CVE-2020-10204)", "ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (No CVE)", "GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M3", "ET WEB_SPECIFIC_APPS Apache Kylin REST API DiagnosisService Command Injection Inbound (CVE-2020-13925)", "ET MALWARE Possible Linux.Mirai Login Attempt (Zte521)", "ET EXPLOIT Possible Spectre PoC Download In Progress", "ET EXPLOIT IBM Data Risk Manager Arbitrary File Download (CVE-2020-4430)", "GPL POP3 x86 SCO overflow", "ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Outbound)", "ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Outbound (CVE-2019-12780)", "ET EXPLOIT Possible EyesOfNetwork Remote File Upload with PHP WebShell Inbound (CVE-2021-27513)", "GPL SMTP EXPN overflow attempt", "ET EXPLOIT D-Link Related Command Injection Attempt Inbound (CVE-2013-7471)", "ET WEB_SPECIFIC_APPS PHP-Fusion Downloads.php Command Injection (CVE-2020-24949)", "ET EXPLOIT Linksys WRT54GL Router DNS Change POST Request", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M3", "ET EXPLOIT Apache log4j RCE Attempt (tcp ldaps) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Inbound VMware vCenter RCE Attempt M4 (CVE-2021-21972)", "ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M3", "ET EXPLOIT BlogEngine 3.3 - syndication.axd XXE Injection Attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M1", "ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M3", "ET EXPLOIT TP-LINK TL-WR840N RCE Inbound (CVE-2022-25064)", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M3", "ET EXPLOIT Possible GoldenPac Priv Esc in-use", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body

	(CommonsCollections5/MozillaRhino1/Vaadin) M3", "ET EXPLOIT GL iNet MTN300n Command Injection Attempt Inbound (CVE-2022-31898)", "GPL NETBIOS SMB-DS OpenKey unicode andx overflow attempt", "ET EXPLOIT FortiOS SSL VPN - Improper Authorization Vulnerability (CVE-2018-13382)", "ET WEB_SPECIFIC_APPS PeopleSoft Portal Command with Default Creds", "ET EXPLOIT Exim receive_msg Integer Overflow Attempt Inbound M1 (CVE-2020-28020)", "ET EXPLOIT Kramer VIAware Remote Code Execution (CVE-2021-35064 CVE-2021-36356)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (CVE-2021-44228)", "ET EXPLOIT Possible Zavio IP Camera OS Command Injection Attempt Inbound (CVE-2013-2568)", "ET EXPLOIT Apache log4j RCE Attempt (udp ldap) (CVE-2021-44228)", "ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-26210)", "ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M1", "ET WEB_SPECIFIC_APPS Apache Struts java.lang inbound OGNL injection remote code execution attempt", "ET EXPLOIT Possible OpenSSL Punycode Email Address Buffer Overflow Attempt Inbound (CVE-2022-3602)", "GPL NETBIOS SMB NDdeSetTrustedShareW little endian overflow attempt", "ET EXPLOIT OpenMRS Deserialization Vulnerability CVE-2018-19276 M2", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M3", "GPL NETBIOS SMB-DS CoGetInstanceFromFile andx overflow attempt", "ET WEB_SERVER Suspected SUPERNOVA Webshell Command (External)", "ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (CVE-2021-42013) M1", "ET WEB_SPECIFIC_APPS Joolma Simple File Upload Plugin Remote Code Execution (CVE-2011-5148)", "ET EXPLOIT Quanta LTE Router Information Disclosure Exploit Attempt", "ET SCAN Mirai Variant User-Agent (Inbound)", "GPL FTP NLST overflow attempt", "ET EXPLOIT Possible Cisco Jabber RCE Inbound (CVE-2020-3495)", "ET EXPLOIT Possible Vacron NVR Remote Command Execution M2", "ET EXPLOIT Jira Server/Data Center 8.4.0 Remote File Read Attempt (CVE-2021-26086) M2", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Remote Code Execution Inbound (CVE-2020-17530)", "ET EXPLOIT SEOWON INTECH SLC-130 RCE Inbound (No CVE)", "ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781) M2", "ET EXPLOIT Possible Apache Airflow DAG Example RCE Attempt - Create DAG (CVE-2020-11978)", "ET EXPLOIT Actiontec C1000A backdoor account M2", "ET EXPLOIT Possible Oracle WebLogic CVE-2020-2551 Scanning", "ET EXPLOIT [PwnedPiper] Exploitation Attempt - Large Malformed Translogic Packet (CVE-2021-37164)", "ET INFO Possible GoCD Authentication Bypass URI Path - cruise_config", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M1 (CVE-2021-44228)", "ET EXPLOIT Possible Cisco Data Center Network Manager - Unauthenticated File Upload (CVE-2019-1620)", "ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Outbound)", "ET EXPLOIT Citrix Application Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt - Server Response (CVE-2019-19781)", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Client Body 3", "ET MALWARE Possible Linux.Mirai Login Attempt (ubnt)", "ET EXPLOIT Exim/Dovecot Possible MAIL FROM Command Execution", "ET EXPLOIT Microsoft Exchange Remote Code Execution Attempt (CVE-2022-41040, CVE-2022-41082)", "ET EXPLOIT HiSilicon DVR - Application Credential Disclosure (CVE-2018-9995)", "ET SCAN ELF/Mirai User-Agent Observed (Inbound)", "ET EXPLOIT ManageEngine AdSelfService Plus - Authentication Bypass Attempt (CVE-2021-40539)", "GPL FTP CMD overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M1", "ET SCAN Possible WordPress xmlrpc.php wp.getUsersBlogs Flowbit Set", "ET EXPLOIT Possible Cisco Data Center Network Manager - Authenticated File Upload (CVE-2019-1620)", "ET EXPLOIT Apache log4j RCE Attempt (http dns) (CVE-2021-44228)", "ET EXPLOIT Yachtcontrol Webservers RCE CVE-2019-17270 (Inbound)", "ET MALWARE Possible Linux.Mirai Login Attempt (vizxv)", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M4", "ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M2", "ET TELNET busybox ECCHI hackers - Possible Brute Force Attack", "GPL NETBIOS SMB NDdeSetTrustedShareW unicode andx overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2", "ET EXPLOIT Possible

	NSDP (Netgear) Unauthenticated Write Access to DHCP Config (CVE-2020-35226)", "ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Inbound (CVE-2019-6277)", "ET MALWARE 404 Response with an EXE Attached - Likely Malware Drop", "GPL FTP RNTO overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M3", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (14)", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M2", "ET WEB_SPECIFIC_APPS KLOG Server RCE Public POC Inbound - Possible Scanning (CVE-2020-35729)", "ET EXPLOIT Possible Microsoft Exchange Mailbox Enumeration Inbound (CVE-2021-34473)", "ET EXPLOIT Quanta LTE Router RDE Exploit Attempt 1 (ping)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (CVE-2021-44228)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M1", "ET EXPLOIT Bonitasoft Authorization Bypass M2 (CVE-2022-25237)", "ET EXPLOIT Possible Zerologon Phase 1/3 - NetrServerReqChallenge with 0x00 Client Challenge (CVE-2020-1472)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (30)", "ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M1", "GPL FTP SITE ZIPCHK overflow attempt", "GPL FTP DELE overflow attempt", "ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Inbound)", "ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M1", "ET EXPLOIT Known Malicious Router DNS Change GET Request", "ET EXPLOIT Possible WatchGuard CVE-2022-26318 RCE Attempt M3", "ET EXPLOIT Possible SAP ICM MPI Desynchronization Scanning Activity (CVE-2022-22536) M2", "ET EXPLOIT IE MSHTML Out-of-Bounds Write Inbound (CVE-2021-33742)", "ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M1", "ET EXPLOIT Ruckus vRIoT Authentication Bypass Attempt Inbound (CVE-2020-26879)", "ET EXPLOIT Netgear Seventh Inferno Vulnerability (post-auth shell injection)", "ET EXPLOIT SonicWall SMA Authenticated Command Injection Attempt CVE-2021-20039", "ET WEB_SPECIFIC_APPS Citrix XenMobile Server Directory Traversal Attempt Inbound (CVE-2020-8209)", "ET WEB_SERVER Possible SQL Injection (varchar2)", "ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Inbound)", "ET SCAN Tomato Router Default Credentials (admin:admin)", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M2", "ET EXPLOIT Dell KACE Attempted Remote Command Injection Outbound", "ET EXPLOIT Possible NSDP (Netgear) Remote Authentication Bypass with Factory Reset (CVE-2020-35231)", "ET MALWARE AllaKore RAT CnC Checkin", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M1", "GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian andx overflow attempt", "ET EXPLOIT Possible Palo Alto SSL VPN sslmgr Format String Vulnerability (Inbound) (CVE-2019-1579)", "ET EXPLOIT Silver Peak Unity Orchestrator Exploitation Inbound (CVE-2020-12146)", "ET WEB_SPECIFIC_APPS Wordpress OptimizePress Arbitratry File Upload", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M4 (CVE-2020-14882)", "ET HUNTING Suspicious PHP Code in HTTP POST (Outbound)", "ET EXPLOIT TOTOLINK Router DNS Changer Exploit Attempt", "ET TELNET External Telnet Attempt To Cisco Device With No Telnet Password Set (Automatically Dissalowed Until Password Set)", "ET WEB_CLIENT Possible vBulletin object injection vulnerability Attempt", "ET EXPLOIT Possible Citrix Authentication Bypass Attempt Inbound (CVE-2020-8193)", "ET EXPLOIT Archeevo 5.0 - Local File Inclusion", "ET EXPLOIT UDP Technology Firmware (IP Cam) - certmngr.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (11)", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M5 (CVE-2020-14882)", "ET EXPLOIT HP Enterprise VAN SDN Controller Upload Backdoor 2", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M3", "ET EXPLOIT Possible Engineers Online Portal System Webshell Upload (CVE-2021-42669)", "GPL NETBIOS SMB-DS llsrconnect unicode little endian overflow attempt", "GPL FTP PASS overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M1", "ET EXPLOIT Cisco RV320/RV325 RCE (CVE-2019-1653)", "ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Outbound)", "ET EXPLOIT Inbound Hashicorp

	Consul RCE via Services API", "GPL NETBIOS SMB OpenKey little endian andx overflow attempt", "ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String ILMI", "ET EXPLOIT Atlassian Jira Unauth User Enumeration Attempt (CVE-2020-36289)", "ET EXPLOIT HackingTrio UA (Hello, World)", "ET EXPLOIT F5 BIG-IP iControl REST Unauthenticated RCE Inbound (CVE-2021-22986)", "ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M1", "ET EXPLOIT UDP Technology Firmware (IP Cam) - language.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "ET EXPLOIT VMware SD-WAN Orchestrator Authentication Bypass (CVE-2020-4001)", "GPL FTP STOU overflow attempt", "ET EXPLOIT SEOWON INTECH SLC-130/SLR-120S RCE Inbound M2 (CVE-2020-17456)", "ET SNMP Samsung Printer SNMP Hardcode RW Community String", "ET EXPLOIT UDP Technology Firmware (IP Cam) - simple_reclistjs.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M3", "ET EXPLOIT Microsoft Exchange SUID Disclosure via SSRF Inbound M1 (CVE-2021-31207)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M3", "ET EXPLOIT Possible Cacti Unauthenticated RCE Inbound M2 (CVE-2022-46169)", "ET EXPLOIT Paypal Pro < 1.1.65 SQLi (CVE-2020-14092)", "ET EXPLOIT Advantech iView RCE Setup via Config Overwrite Inbound (CVE-2021-22652)", "ET EXPLOIT Possible EXIM RCE Inbound (CVE-2019-15846) M2", "ET EXPLOIT OctoberCMS Auth Bypass Inbound M1 trigger_reset (CVE-2021-32648)", "ET WEB_SERVER Suspected China Chopper Variant Webshell Command (inbound)", "ET EXPLOIT CCBill Online Payment Systems RCE (Outbound)", "ET EXPLOIT WNR2000v4 HTTP POST RCE Attempt Via Timestamp Discovery", "ET EXPLOIT Smart Google Code Inserter < 3.5 SQLi (CVE-2018-3811)", "ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Outbound (CVE-2016-6255)", "ET WEB_SPECIFIC_APPS Atlassian JIRA Template Injection RCE (CVE-2019-11581)", "ET EXPLOIT Apache log4j RCE Attempt (udp dns) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Qualcomm QCMAP Stack-Based Buffer Overflow Attempt Inbound (CVE-2020-3657)", "ET EXPLOIT Extreme Networks ExtremeWireless Aerohive HiveOS and IQ Engine (LFI) (CVE-2020-16152) M2", "ET EXPLOIT Possible Spring Cloud Connector RCE Inbound (CVE-2022-22963)", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Fuzzing Inbound M2", "ET EXPLOIT Belkin N750 Buffer Overflow Attempt", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode little endian overflow attempt", "ET EXPLOIT eMerge E3 Command Injection Inbound (CVE-2019-7256)", "ET EXPLOIT Apache log4j RCE Attempt - Nested upper (udp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Equation Group ExtraBacon Cisco ASA AAAADMINAUTH Disable", "ET EXPLOIT Cisco Data Center Network Manager SQL Injection Inbound (CVE-2019-15984)", "ET EXPLOIT Possible Redis RCE Attempt - Dynamic Importing of liblua (CVE-2022-0543)", "ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1", "ET EXPLOIT Possible vRealize Operations Manager API SSRF Attempt (CVE-2021-21975)", "ET INFO Common JSP WebShell String Observed in HTTP Header M1", "ET EXPLOIT Possible WebShell JPEG Upload", "ET SCAN Tomcat admin-blank login credentials", "ET EXPLOIT Inbound VMware vCenter RCE Attempt M1 (CVE-2021-21972)", "ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate3 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M1", "ET EXPLOIT vBulletin 5.6.2 widget_tabbedContainer_tab_panel Remote Code Execution (Inbound)", "ET EXPLOIT Apache log4j RCE Attempt (udp iiop) (CVE-2021-44228)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance", "ET WEB_SPECIFIC_APPS Apache ActiveMQ File Upload RCE (CVE-2016-3088)", "ET EXPLOIT REDIS Attempted SSH Key Upload", "ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M3", "GPL NETBIOS SMB llsrconnect unicode little endian overflow attempt", "ET WEB_SERVER CVE-2014-6271 Attempt In HTTP Headers Line Continuation Evasion CRLF", "ET EXPLOIT Microsoft Exchange RCE Setup Inbound (CVE-2021-28482)", "ET EXPLOIT Possible Apache Text4shell RCE Attempt DNS Prefix (CVE-2022-42889) (Inbound)", "ET EXPLOIT Apache log4j RCE Attempt (tcp ldap)

	(Outbound) (CVE-2021-44228)", "ET WEB_SPECIFIC_APPS Kibana Prototype Pollution RCE Inbound (CVE-2019-7609)", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Fuzzing Inbound M1", "ET EXPLOIT D-Link - RCE Attempt Inbound (CVE-2021-45382)", "ET EXPLOIT Geutebruck Attempted Remote Command Injection Outbound", "ET EXPLOIT ManageEngine AdSelfService Plus - Possible Code Execution via openSSLTool (CVE-2021-40539)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3", "ET MALWARE Possible Linux.Mirai Login Attempt (54321)", "GPL NETBIOS SMB-DS llsrconnect unicode andx overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2", "GPL FTP MKD overflow attempt", "ET EXPLOIT Possible Zend Framework Exploit (CVE-2021-3007)", "ET EXPLOIT Possible rConfig 3.9.2 Remote Code Execution PoC M1 (CVE-2019-16662)", "ET WEB_SPECIFIC_APPS Possible Apache Unomi MVEL Eval RCE Inbound M1 (CVE-2020-13942)", "ET EXPLOIT Apache log4j RCE Attempt (http ldaps) (CVE-2021-44228)", "ET EXPLOIT Possible Apache ShardingSphere RCE Attempt (CVE-2020-1947) (PoC Based)", "ET WEB_SERVER Possible CVE-2014-3120 Elastic Search Remote Code Execution Attempt", "ET WEB_SERVER WEBSHELL Linux/Torte Uploaded", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (19)", "ET WEB_SERVER Possible WebLogic Admin Login With Default Creds", "ET EXPLOIT [NCC/FOX-IT] Possible F5 BIG-IP/BIG-IQ iControl REST RCE Attempt (CVE-2021-22986)", "ET EXPLOIT Inbound VMware vCenter RCE Attempt M2 (CVE-2021-21972)", "ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1600)", "ET EXPLOIT Seagate Business NAS Unauthenticated Remote Command Execution", "GPL NETBIOS DCERPC Remote Activation bind attempt", "GPL NETBIOS SMB-DS OpenKey andx overflow attempt", "ET WEB_SERVER Possible 3Com OfficeConnect Router Default User Account Remote Command Execution Attempt", "ET EXPLOIT SonicWall SMA 100 Series - Possible Heap-Based Overflow Activity (CVE-2021-20043)", "ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys successful exfiltration", "ET EXPLOIT Apache log4j RCE Attempt (http rmi) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Possible SaltStack Authentication Bypass CVE-2020-11651 M2", "ET TELNET busybox MEMES Hackers - Possible Brute Force Attack", "ET WEB_SERVER Possible CVE-2015-1427 Elastic Search Sandbox Escape Remote Code Execution Attempt", "GPL NETBIOS SMB DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt", "ET EXPLOIT Microsoft Edge Chakra - InlineArrayPush Type Confusion Inbound M1 (CVE-2018-8617)", "ET EXPLOIT [PT Security] Exim <4.90.1 Base64 Overflow RCE (CVE-2018-6789)", "ET WEB_SPECIFIC_APPS Possible WHMCS SQLi AES_ENCRYPT at start of value", "ET EXPLOIT Image Manager 5.2.4 - RCE Attempt", "GPL NETBIOS SMB-DS llsrconnect overflow attempt", "ET EXPLOIT Netgear ProSAFE Plus Possible Integer Overflow Attempt Inbound M2 (CVE-2020-35230)", "ET EXPLOIT VMware SD-WAN Orchestrator Path Traversal (CVE-2020-4000)", "ET EXPLOIT Qualcomm QCMAP NULL Pointer Dereference Attempt Inbound (CVE-2020-25858)", "ET EXPLOIT QNAP PhotoStation Authenticated Session Tampering Attempt", "ET MALWARE Possible Linux.Mirai Login Attempt (ikwb)", "ET EXPLOIT Amcrest Camera and NVR Buffer Overflow Attempt (CVE-2020-5735)", "ET EXPLOIT Apache log4j RCE Attempt (tcp rmi) (Outbound) (CVE-2021-44228)", "ET SCAN Dark Nexus IoT Variant User-Agent (Inbound)", "ET EXPLOIT Possible Oracle Database Text Component ctxsys.drvxtabc.create_tables Remote SQL Injection Attempt", "ET EXPLOIT Xiongmai/HiSilicon DVR - RTSP Buffer Overflow Attempt - CVE-2022-26259", "ET EXPLOIT EyesOfNetwork Autodiscover Command Injection (CVE-2020-8654)", "ET EXPLOIT DBltek GoIP GoIP-1 GSM Gateway - Local File Inclusion", "ET EXPLOIT 401TRG Liferay RCE (CVE-2020-7961)", "ET EXPLOIT Tenda OS Command Injection (CVE-2020-10987) (GET)", "ET EXPLOIT OptiLink ONT1GEW GPON RCE Outbound", "ET MALWARE Unattributed WebShell Access - File Upload", "ET EXPLOIT Possible Apache log4j RCE Attempt - HTTP URI Obfuscation (CVE-2021-44228) (Outbound)", "ET EXPLOIT [PwnedPiper] Exploitation Attempt - Small Malformed Translogic Packet (Multiple CVEs)", "ET EXPLOIT Possible CVE-2014-6271 exploit attempt via malicious DHCP ACK", "ET EXPLOIT vCenter Server RCE Chain Final Stage Inbound (CVE-2021-21985)", "ET EXPLOIT WatchGuard CVE-2022-26318 RCE Attempt

	M2", "ET EXPLOIT Possible FatPipe Unrestricted File Upload", "ET EXPLOIT Cisco IP Phones Web Server Vulnerability (CVE-2020-3161)", "ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M2", "ET EXPLOIT Cisco Data Center Network Manager Authentication Bypass Inbound (CVE-2019-15976)", "ET EXPLOIT CloudMe Sync Buffer Overflow", "ET EXPLOIT Cisco Security Manager Path Traversal - athena (CVE-2020-27130)", "GPL FTP REST overflow attempt", "ET EXPLOIT Possible WePresent WIPG1000 OS Command Injection", "ET EXPLOIT Edimax Technology EW-7438RPn-v3 Mini 1.27 - Remote Code Execution", "ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)", "GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian overflow attempt", "ET EXPLOIT Possible VMware Cloud Director RCE Attempt (CVE-2020-3956)", "ET EXPLOIT FortiOS SSL VPN - Information Disclosure (CVE-2018-13379)", "ET SCAN ELF/Mirai Variant User-Agent (Inbound)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper UDP Bypass) (CVE-2021-44228)", "GPL NETBIOS SMB CoGetInstanceFromFile little endian andx overflow attempt", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers", "ET MALWARE Possibly SLIGHTPULSE Related - Suspicious POST to Specific URI Path", "ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M1", "ET EXPLOIT Possible CVE-2014-6271 exploit attempt via malicious DNS", "ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys access attempt", "ET EXPLOIT Possible OpenSSL Punycode Email Address Buffer Overflow Attempt Outbound (CVE-2022-3602)", "ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M2 (CVE-2020-1350)", "ET EXPLOIT Unknown Vulnerability Exploit Attempt (Possible Mirai Activity)", "ET EXPLOIT Possible Microsoft Exchange RCE Inbound M1 (CVE-2021-34473)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M1", "ET EXPLOIT Apache log4j RCE Attempt (tcp dns) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Apache log4j RCE Attempt (tcp iiop) (CVE-2021-44228)", "ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toserver M4", "ET EXPLOIT Pulse Secure Post-Auth OS Command Injection (CVE-2019-11539)", "ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M1", "GPL POP3 AUTH overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M1", "ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M2", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M2", "ET EXPLOIT CyberArk Enterprise Password Vault XXE Injection Attempt", "GPL NETBIOS SMB-DS llsrconnect little endian overflow attempt", "ET MALWARE Possible Linux.Mirai Login Attempt (888888)", "ET EXPLOIT UPnP UUID Password Change Exploit Attempt Inbound - XR300 PoC Gadgets (CVE-2021-34991)", "GPL NETBIOS SMB OpenKey unicode little endian andx overflow attempt", "ET WEB_SPECIFIC_APPS Possible KLOG Server RCE Inbound (CVE-2020-35729)", "ET EXPLOIT Microsoft Exchange - Successful msExchEcpCanary Disclosure (CVE-2021-33766)", "ET EXPLOIT Possible F5 BIG-IP Infoleak and Out-of-Bounds Write Inbound (CVE-2021-22991)", "ET EXPLOIT Grafana 8.x Path Traversal (CVE-2021-43798)", "ET EXPLOIT FortiOS SSL VPN - Remote Code Execution (CVE-2018-13383)", "ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Inbound - Attempt to clear logs", "ET EXPLOIT Microsoft Exchange Remote Code Execution Attempt - OWASSRF (CVE-2022-41040, CVE-2022-41082)", "ET EXPLOIT Possible Citrix Information Disclosure Attempt Inbound (CVE-2020-8195)", "ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040) Server Response M1", "ET EXPLOIT Possible Mida eFramework RCE Attempt Inbound (CVE-2020-15922)", "ET EXPLOIT [401TRG] GhostCat LFI Attempt Inbound (CVE-2020-1938)", "ET EXPLOIT Possible Apache Text4shell RCE Attempt Script Prefix (CVE-2022-42889) (Outbound)", "ET EXPLOIT Possible WebShell GIF Upload", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW little endian andx overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M1", "ET EXPLOIT Linksys WRT54GL DNS Change GET Request", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode andx overflow attempt", "ET EXPLOIT Oracle WebLogic Unrestricted File Upload (CVE-2018-2894)", "GPL NETBIOS SMB-DS OpenKey unicode little endian overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1", "ET EXPLOIT

	HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3", "ET WEB_SPECIFIC_APPS [eSentire] Drupalgeddon2 <8.3.9 <8.4.6 <8.5.1 RCE Through Registration Form (CVE-2018-7600)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M3", "ET WEB_SPECIFIC_APPS LifterLMS Arbitrary File Write Attempt Inbound (CVE-2020-6008)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M1", "GPL NETBIOS SMB llsrconnect unicode overflow attempt", "ET EXPLOIT Possible SAP NetWeaver SQL Injection Attempt Inbound (CVE-2016-2386)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)", "ET HUNTING Suspicious Chmod Usage in URI (Inbound)", "ET MALWARE Possible Linux.Mirai Login Attempt (1111111)", "ET EXPLOIT Apache CouchDB JSON Remote Privesc Attempt (CVE-2017-12635)", "ET EXPLOIT Possible Malicious NAT-PMP Response Successful UDP Map to External Network", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M1", "ET EXPLOIT PAN-OS OS Command Injecton Attempt Inbound (CVE-2020-2038)", "ET WEB_SPECIFIC_APPS DNN DNNPersonalization Cookie RCE Attempt (CVE-2017-9822)", "ET MALWARE Suspected PULSECHECK Webshell Access Inbound", "ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M1", "ET EXPLOIT VMware VeloCloud Authorization Bypass (CVE-2019-5533)", "ET EXPLOIT TP-Link TL-WR840N EU v5 RCE Attempt (CVE-2021-41653)", "GPL EXPLOIT rsh froot", "ET EXPLOIT Cisco Data Center Network Manager Information Disclosure Inbound", "ET EXPLOIT VMware Spring Cloud Gateway Code Injection (CVE-2022-22947)", "ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2", "GPL FTP RNFR overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M2", "ET EXPLOIT ysoserial Payload in HTTP Header (JavassistWeld1) M1", "ET EXPLOIT Pulse Secure VPN RCE Chain Stage 3 Inbound - Execute Mal Config Trigger, PoC Based (CVE-2020-8260)", "ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M2", "GPL NETBIOS SMB trans2open buffer overflow attempt", "ET EXPLOIT Cisco RV320/RV325 Config Disclosure Attempt Inbound (CVE-2019-1653)", "GPL RPC CMSD TCP CMSD_CREATE buffer overflow attempt", "ET EXPLOIT Extensis Portfolio Unrestricted File Upload (CVE-2022-24252)", "ET EXPLOIT Possible ZyXELs ZynOS Configuration Download Attempt (Contains Passwords)", "GPL RPC CMSD UDP CMSD_CREATE buffer overflow attempt", "ET EXPLOIT AjaxPro RCE Attempt (CVE-2021-23758)", "ET EXPLOIT Netis E1+ 1.2.32533 - Unauthenticated WiFi Password Leak", "GPL NETBIOS SMB llsrconnect andx overflow attempt", "ET EXPLOIT Possible MeltDown PoC Download In Progress", "ET EXPLOIT SolarWinds Web Help Desk Hard Coded Credentials Request (CVE-2021-35232)", "ET EXPLOIT Linksys E-Series Device RCE Attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M3", "ET EXPLOIT Linksys Failed Upgrade BackDoor Access (Server Response)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)", "ET EXPLOIT Possible Authenticated Command Injection Inbound - Comtrend VR-3033 (CVE-2020-10173)", "ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1", "ET EXPLOIT UDP Technology Firmware (IP Cam) - simple_reclistjs.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 2", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M1", "ET EXPLOIT Eir D1000 Remote Command Injection Attempt Outbound", "ET EXPLOIT Authenticated QuickBox CE 2.5.5/Pro 2.1.8 RCE Attempt Inbound M2 (CVE-2020-13448)", "GPL NETBIOS SMB-DS llsrconnect little endian andx overflow attempt", "GPL POP3 LIST overflow attempt", "ET EXPLOIT Possible PYKEK Priv Esc in-use", "ET EXPLOIT Geutebruck Attempted Remote Command Injection Inbound", "ET EXPLOIT Centreon 20.04 Authenticated RCE (CVE-2020-12688)", "ET EXPLOIT ysoserial Payload in HTTP Header (JavassistWeld1) M3", "ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate3 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M2", "ET EXPLOIT Exim4 UAF Attempt (BDAT with non-printable chars)", "ET EXPLOIT Cisco HyperFlex HX RCE Inbound (CVE-2021-1498)", "ET EXPLOIT Suspicious SVCCTL CreateService Command via

	SMB - Observed Zerologon Post Compromise Activity", "ET WEB_CLIENT Possible Confluence SSTI Exploitation Attempt - Leads to RCE/LFI (CVE-2019-3396)", "ET EXPLOIT Trenda Router AC11 RCE Inbound (CVE-2021-31755)", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded WebUI Login Attempt M1", "ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Exploit Success", "ET EXPLOIT Successful Cisco RV320/RV325 Config Disclosure (CVE-2019-1653)", "ET EXPLOIT Azure Automation Authentication Bypass", "GPL NETBIOS SMB llsrconnect overflow attempt", "ET POLICY PPTP Requester is not authorized to establish a command channel", "ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys successful upload", "ET WEB_SERVER lolzilla WebSkimmer - Remote Code Execution Attempt M1", "ET EXPLOIT QNAP PhotoStation Privilege Escalation Attempt M2 (plaintext token)", "ET EXPLOIT PiHole Web Interface Regex Escape Leading to RCE Inbound M1 (CVE-2021-32706)", "ET EXPLOIT Possible Apache Shiro 1.2.4 Cookie RememberME Deserial RCE (CVE-2016-4437)", "ET EXPLOIT Guangzhou 1GE ONU OS Command Execution (CVE-2020-8958)", "GPL NETBIOS SMB-DS DCERPC Messenger Service buffer overflow attempt", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M1 (Outbound) (CVE-2021-44228)", "ET EXPLOIT Possible CVE-2017-8759 Soap File DL Over FTP", "ET EXPLOIT Fuel CMS 1.4.1 RCE (CVE-2018-16763)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (17)", "ET EXPLOIT Possible Microsoft RDP Client for Mac RCE", "ET EXPLOIT FCM-MB40 Attempted Remote Command Execution as Root", "ET EXPLOIT TP-LINK Known Malicious Router DNS Change GET Request", "ET EXPLOIT Attempted Mitel MiVoice Connect Data Validation RCE Inbound (CVE-2022-29499)", "ET MALWARE Possible Linux.Mirai DaHua Default Credentials Login", "ET EXPLOIT Mongo-Express RCE Inbound (CVE-2019-10758)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (4)", "ET EXPLOIT [401TRG] HPDM Backdoor Login", "ET EXPLOIT Dell KACE Attempted Remote Command Injection Inbound", "ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (pom.properties) (CVE-2021-26085)", "ET EXPLOIT Apache log4j RCE Attempt (udp iiop) (Outbound) (CVE-2021-44228)", "ET WEB_SPECIFIC_APPS Apache Struts ognl inbound OGNL injection remote code execution attempt", "ET EXPLOIT Linksys WAP54G debug.cgi Shell Access as Gemtek", "ET EXPLOIT Attempted Remote Command Injection Inbound (CVE-2018-7841)", "ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound", "ET WEB_CLIENT Metasploit Browser Autopwn Aug1 2016", "ET EXPLOIT Microsoft Exchange - Information Disclosure flowbit set (CVE-2021-33766)", "ET EXPLOIT Apache log4j RCE Attempt - Nested upper (tcp) (CVE-2021-44228)", "ET EXPLOIT Quanta LTE Router UDP Backdoor Activation Attempt", "ET EXPLOIT QNAP PhotoStation Pre-Auth Local File Disclosure Attempt", "ET EXPLOIT dotCMS Arbitrary File Upload Attempt (CVE-2022-26352) M2", "GPL RPC STATD TCP stat mon_name format string exploit attempt", "ET EXPLOIT Successful Cisco RV320/RV325 Debug Dump Disclosure (CVE-2019-1653)", "ET EXPLOIT File Sharing Wizard 1.5.0 - SEH Overflow Inbound (CVE-2019-16724)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M1", "ET EXPLOIT Possible Successful VMware Cloud Director RCE Attempt (CVE-2020-3956)", "GPL FTP RETR overflow attempt", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp nds) (CVE-2021-44228)", "ET EXPLOIT Possible Cisco REST API Container for Cisco IOS XE Software Authentication Bypass Attempt (CVE-2019-12643)", "ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 3", "GPL FTP STAT overflow attempt", "ET EXPLOIT Possible Edgewater Networks Edgemarc Blind Command Injection Attempt (CVE-2017-6079)", "ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Inbound", "ET EXPLOIT JCK Editor 6.4.4 SQLi Attempt (CVE-2018-17254)", "ET EXPLOIT Inbound VMware vCenter RCE Attempt with Untrusted SSH Key Upload (CVE-2021-21972)", "ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1601)", "ET EXPLOIT Belkin Wireless G Router DNS Change POST Request", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Client Body", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI", "ET EXPLOIT Oracle Coherence Deserialization RCE (CVE-2020-2555)", "ET EXPLOIT Supermicro BMC Password Disclosure 4", "ET EXPLOIT Citrix App Delivery Controller and Citrix Gateway M1 (CVE-2019-19781)", "ET TELNET busybox MIRAI hackers - Possible Brute Force Attack", "ET WEB_SPECIFIC_APPS

	Pandora FMS SQLi", "GPL NETBIOS SMB NDdeSetTrustedShareW unicode little endian overflow attempt", "ET EXPLOIT Monitorr 1.7.6m RCE Exploit Attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M2", "ET EXPLOIT Microsoft OMI RCE Exploit Attempt (CVE-2021-38647) M1", "ET EXPLOIT Apache log4j RCE Attempt (tcp dns) (CVE-2021-44228)", "ET EXPLOIT [CISA AA21-336A] Zoho ManageEngine ServiceDesk Possible Exploitation Activity (CVE-2021-44077)", "ET EXPLOIT Vulnerable Microsoft Exchange Server Response (CVE-2021-31207)", "ET EXPLOIT Wireless IP Camera (P2) WIFICAM Remote Code Execution", "ET WEB_SERVER Possible CVE-2014-6271 Attempt", "ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M2", "ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 2 Inbound - Upload Malicious Config (CVE-2020-8260)", "ET WEB_SPECIFIC_APPS Jetty WEB-INF Information Leak Successful Exploitation (CVE-2021-34429)", "ET EXPLOIT Klog Server Command Injection Inbound (CVE-2021-3317)", "ET WEB_SPECIFIC_APPS Apache SkyWalking GraphQL SQL Injection Inbound (CVE-2020-13921)", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie", "ET EXPLOIT Possible Pulse Secure VPN RCE Inbound (CVE-2020-8218)", "GPL POP3 STAT overflow attempt", "ET WEB_SERVER Possible SQL Injection (varchar)", "ET WEB_SPECIFIC_APPS Possible CVE-2013-2618 Attempt (PHP Weathermap Persistent XSS)", "ET EXPLOIT SonicWall SMA 100 Series - Unauthenticated File Upload Path Traversal (CVE-2021-20040)", "ET EXPLOIT Cisco Security Manager Path Traversal - cwhp (CVE-2020-27130)", "ET EXPLOIT Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)", "ET EXPLOIT VMWare View Planner RCE (CVE-2021-21978) Attempt M2", "ET WEB_SERVER SQLi - SELECT and sysobject", "ET EXPLOIT CCBill Online Payment Systems RCE (Inbound)", "ET MALWARE Possible Linux.Mirai Login Attempt (fucker)", "ET WEB_SPECIFIC_APPS Possible SharePoint RCE Attempt (CVE-2019-0604)", "ET SCAN SQLNinja Attempt To Recreate xp_cmdshell Using sp_configure", "ET WEB_SERVER DEWMODE Webshell Observed Outbound", "ET EXPLOIT TP-LINK Archer C5 v4 (CVE-2019-7405)", "ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (NT Create AndX .so) (CVE-2017-7494)", "ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (udp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT PiHole Web Interface Regex Escape Leading to RCE Inbound M2 (CVE-2021-32706)", "ET EXPLOIT FatPipe Unrestricted File Upload", "ET EXPLOIT Possible ManageEngine ADAudit Plus Directory Traversal Leading to Deserialization", "ET EXPLOIT DSLink 260E Router DNS Changer Exploit Attempt", "ET WEB_CLIENT Attempted WordPress GDPR Plugin Privilege Escalation M2 (Set as Administrator)", "ET EXPLOIT Possible Malicious NAT-PMP Response to External Network", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-30333) M2", "ET EXPLOIT Possible Microsoft Exchange RCE Inbound M3 (CVE-2021-34473)", "ET WEB_CLIENT Attempted WordPress GDPR Plugin Privilege Escalation M1 (Enable Registration)", "ET WEB_SERVER Possible Oracle SQL Injection utl_inaddr call in URI", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (8)", "ET WEB_SPECIFIC_APPS MediaWiki thumb.php RCE", "ET EXPLOIT Apache Spark RPC - Unauthenticated RegisterApplication Request - RCE Attempt (CVE-2020-9480)", "ET EXPLOIT Apache log4j RCE Attempt - Nested lower (udp) (CVE-2021-44228)", "ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x0003 (CVE-2020-35225)", "ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Inbound)", "ET EXPLOIT NetGain Enterprise Manager 7.2.562 Ping Command Injection", "ET EXPLOIT Possible Oracle Access Manager RCE Attempt (CVE-2021-35587)", "ET INFO Common JSP WebShell String Observed in HTTP Header M3", "ET EXPLOIT Sunhillo SureLine Unauthenticated OS Command Injection Inbound (CVE-2021-36380)", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M1", "ET SCAN SQLNinja Attempt To Create xp_cmdshell Session", "ET WEB_SERVER Webmin RCE CVE-2019-15107", "ET EXPLOIT VMware vCenter Unauthorized File Read Inbound", "ET WEB_SERVER ThinkPHP RCE Exploitation Attempt", "GPL NETBIOS SMB NDdeSetTrustedShareW unicode little endian andx overflow attempt", "ET WEB_SPECIFIC_APPS Modx Revolution RCE (CVE-2018-1000207)", "ET EXPLOIT Razer Sila Router - LFI Attempt Inbound (No CVE)", "GPL NETBIOS SMB OpenKey little endian overflow attempt", "ET EXPLOIT Dameware DMRC Buffer Overflow Attempt (CVE-2016-

	2345)", "ET WEB_SPECIFIC_APPS Possible Attempted Microsoft Exchange RCE (CVE-2020-0688)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M2", "ET EXPLOIT Dataprobe iBoot-PDU Pre-Auth Remote Code Execution Attempt via git-update.php (CVE-2022-3184) M2", "ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 3 Directory Set Inbound (CVE-2022-22965)", "GPL FTP APPE overflow attempt", "GPL NETBIOS SMB-DS OpenKey unicode overflow attempt", "ET EXPLOIT JBOSS Deserialization Attempt Inbound (CVE-2017-7504)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - certmngr.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "ET EXPLOIT ManageEngine AdSelfService Plus - Arbritrary File Upload Attempt (CVE-2021-40539)", "ET EXPLOIT TeamViewer .tvs iFrame Observed (CVE-2020-13699)", "GPL NETBIOS SMB llsrconnect unicode little endian andx overflow attempt", "ET WEB_SPECIFIC_APPS vBulletin RCE Inbound (CVE-2019-16759 Bypass)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M2", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded WebUI Login Attempt M2", "ET EXPLOIT QNAP PhotoStation Privilege Escalation Attempt M1 (encrypted token)", "ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x000a (CVE-2020-35225)", "ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M3", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (tcp) (Outbound) (CVE-2021-44228)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M1", "ET ATTACK_RESPONSE Linksys Router Returning Device Settings To External Source", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M3", "ET EXPLOIT TerraMaster TOS RCE via OS Command Injection Inbound (CVE-2020-28188)", "ET EXPLOIT Hikvision IP Camera RCE Attempt (CVE-2021-36260)", "ET EXPLOIT Attempted Netgear Buffer Overflow into RCE Inbound M2", "ET MALWARE Possible Linux.Mirai Login Attempt (juantech)", "ET EXPLOIT CVE-2015-0235 Exim Buffer Overflow Attempt (HELO)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - testcmd.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET EXPLOIT Exim New-Line Injection into Spool Header File Inbound - Information Disclosure Attempt (CVE-2020-28021)", "ET EXPLOIT VMWare View Planner RCE (CVE-2021-21978) Attempt M1", "ET EXPLOIT OpenMRS Deserialization Vulnerability CVE-2018-19276", "ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M3", "ET WEB_SPECIFIC_APPS Kibana Path Traversal Inbound (CVE-2018-17246)", "ET EXPLOIT Attempted HiSilicon DVR/NVR/IPCam RCE (Outbound)", "ET EXPLOIT Windows HTTP Protocol Stack UAF/RCE (CVE-2021-31166), http.sys DOS (CVE-2022-21907) Inbound", "ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M2", "ET EXPLOIT Cisco HyperFlex OS Command Injection M2 (CVE-2021-1497)", "ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)", "ET WEB_SPECIFIC_APPS Possible Oracle WebLogic RCE Inbound M6 (CVE-2020-14882)", "ET EXPLOIT Possible Exim 4.87-4.91 RCE Attempt Inbound (CVE-2019-10149)", "ET EXPLOIT TerraMaster TOS Unauthenticated Command Injection Inbound M2 (CVE-2022-24989)", "GPL EXPLOIT login buffer non-evasive overflow attempt", "ET WEB_SPECIFIC_APPS Possible MobileIron MDM RCE Inbound (CVE-2020-15505)", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC WebUI RCE ADD Attempt", "ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (pom.xml) (CVE-2021-26085)", "ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M2", "ET EXPLOIT Mi Router 3 Remote Code Execution CVE-2018-13023", "ET EXPLOIT InoERP 0.7.2 Unauthenticated Remote Code Execution (Outbound)", "ET EXPLOIT FortiOS SSL VPN - Pre-Auth Messages Payload Buffer Overflow (CVE-2018-13381)", "ET EXPLOIT Apache Obfuscated log4j RCE Attempt (tcp ldap) (CVE-2021-44228)", "ET EXPLOIT Microsoft OMI RCE Exploit Attempt (CVE-2021-38647) M2", "ET EXPLOIT Nagios XI OS Command Injection (CVE-2021-25296)", "ET EXPLOIT Possible SAP ICM MPI Desynchronization Scanning Activity (CVE-2022-22536) M1", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1", "ET EXPLOIT phpMyAdmin setup.php Local File Include", "ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (Unassigned CVE)", "ET EXPLOIT ysoserial Payload in HTTP Header

	(JavassistWeld1) M2", "ET MALWARE Possible Linux.Mirai Login Attempt (anko)", "ET EXPLOIT Kaseya VSA ManagedITSync SQL Injection (CVE-2017-18362)", "ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M1 (CVE-2020-1350)", "GPL NETBIOS SMB-DS Session Setup AndX request username overflow attempt", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M1 (Outbound) (CVE-2021-44228)", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M2", "ET EXPLOIT Motorola SBG900 Router DNS Change GET Request", "ET EXPLOIT OctoberCMS Auth Bypass Inbound M2 set_password (CVE-2021-32648)", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Stack Overflow in Base64 Authorization Mechanism M2", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (9)", "ET EXPLOIT IBM Data Risk Manager Authentication Bypass - Password Retrieval", "ET EXPLOIT Ultimate POS 4.4 Cross-Site Scripting (XSS) - Outbound", "ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M2", "ET EXPLOIT Possible EXIM RCE Inbound (CVE-2019-15846)", "ET EXPLOIT Netgear DGN Remote Code Execution", "ET EXPLOIT Linksys Auth Bypass share_editor.cgi", "ET EXPLOIT Linksys Auth Bypass switch_boot.cgi", "ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M2", "GPL POLICY PCAnywhere Attempted Administrator Login", "GPL NETBIOS DCERPC CoGetInstanceFromFile overflow attempt", "ET EXPLOIT Possible MPC Sharj 3.11.1 - Arbitrary File Download Attempt", "ET EXPLOIT Possible Apache log4j RCE Attempt (udp nds) (Outbound) (CVE-2021-44228)", "GPL NETBIOS DCERPC Messenger Service buffer overflow attempt", "ET EXPLOIT Cisco HyperFlex HX Data Platform Pre-Auth RCE Inbound (CVE-2021-1499)", "ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M2", "ET EXPLOIT Oracle Weblogic Server Deserialization RCE T3 (CVE-2015-4852)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M1", "ET EXPLOIT Cisco RV320/RV325 Command Injection Attempt Inbound (CVE-2019-1652)", "ET EXPLOIT Nagios XI <= 5.6.5 Privesc (CVE-2019-15949)", "ET EXPLOIT XXL-Job RCE", "ET EXPLOIT Attempted Remote Command Injection Outbound (CVE-2019-3929)", "ET EXPLOIT NodeJS System Information Library Command Injection Attempt (CVE-2021-21315)", "ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040) Server Response M2", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M2", "ET EXPLOIT Trend Micro IWSVA Unauthenticated Command Injection Inbound (CVE-2020-8466)", "ET EXPLOIT Juniper ScreenOS telnet Backdoor Default Password Attempt", "ET EXPLOIT IE Scripting Engine Memory Corruption Vulnerability M1 (CVE-2019-0752)", "ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (.so file write to share) (CVE-2017-7494)", "ET POLICY Dlink Soho Router Config Page Access Attempt", "ET EXPLOIT Microsoft Exchange - InboxRules.svc Access Observed Following Successful ProxyToken Attack", "ET EXPLOIT [401TRG] DeDeCMS RFI Attempt", "ET EXPLOIT FritzBox RCE POST Request", "ET EXPLOIT Jboss RCE (CVE-2017-12149)", "ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Inbound)", "ET EXPLOIT Apache log4j RCE Attempt (http rmi) (CVE-2021-44228)", "ET EXPLOIT Possible CVE-2018-0171 Exploit (PoC based)", "ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M2", "ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3", "ET EXPLOIT Vanguard v2.1 (Search) POST Inject Web Vulnerability", "ET WEB_SERVER lolzilla WebSkimmer - Remote Code Execution Attempt M2", "ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Inbound)", "GPL FTP MKD overflow", "GPL MISC rlogin root", "ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (tcp) (CVE-2021-44228)", "ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0vizxv)", "ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M1", "ET EXPLOIT WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion", "ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Outbound)", "ET WEB_SERVER lolzilla WebSkimmer - Remote Code Execution Attempt M3", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (13)", "ET MALWARE Possible Linux.Mirai Login Attempt (jvbzd)", "GPL FTP SITE CHOWN overflow attempt", "ET EXPLOIT Eir D1000 Remote Command Injection Attempt Inbound", "ET EXPLOIT Apache HTTP Server SSRF (CVE-2021-40438)", "ET EXPLOIT IPMI Cipher 0 Authentication mode set", "ET EXPLOIT Exim New-Line Injection into Spool Header File

	Inbound M2 (CVE-2020-28021)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (7)", "ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0admin)", "ET EXPLOIT Mitsubishi Electric smartRTU RCE Outbound (CVE-2019-14931)", "ET EXPLOIT rConfig < 3.9.7 SQLi (CVE-2020-10546)", "ET WEB_CLIENT Apple Quicktime RTSP Overflow (1)", "ET EXPLOIT Possible CVE-2014-6271 Attempt Against SIP Proxy", "ET EXPLOIT Fortinet FortiOS/FortiProxy SSL VPN Web Portal Path Traversal (CVE-2018-13379)", "ET WEB_SERVER SLIGHTPULSE WebShell Access Inbound M3", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (18)", "ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1", "ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M3", "ET EXPLOIT Possible Tenda OS Command Injection (CVE-2020-10987) (POST)", "ET WEB_SPECIFIC_APPS rConfig search.crud.php Command Injection (CVE-2019-16663)", "ET EXPLOIT ScadaBR RCE with JSP Shell Inbound (CVE-2021-26828)", "ET WEB_SPECIFIC_APPS SAP Possible CTC Auth/HTTP Verb Bypass Attempt", "ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010", "ET EXPLOIT Unknown Target Application Command Injection Inbound", "ET EXPLOIT Possible MovableTypePoC RCE Inbound (CVE-2021-20837)", "ET EXPLOIT AirLive RCI HTTP Request", "GPL FTP MDTM overflow attempt", "ET EXPLOIT Netgear passwordrecovered.cgi attempt", "ET EXPLOIT Apache log4j RCE Attempt (tcp iiop) (Outbound) (CVE-2021-44228)", "GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode overflow attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1", "ET EXPLOIT Microsoft Exchange Create User Configuration - xbit set 2 (CVE-2021-42321)", "ET EXPLOIT Apache log4j RCE Attempt (http dns) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Apache log4j RCE Attempt - Nested lower (tcp) (Outbound) (CVE-2021-44228)", "ET WEB_SPECIFIC_APPS Oracle Fusion Middleware BPEL Console Cross Site Scripting", "ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M1", "ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (tcp) (Outbound) (CVE-2021-44228)", "ET SCAN Possible WordPress xmlrpc.php BruteForce in Progress - Response", "GPL FTP SITE overflow attempt", "ET EXPLOIT Windows DNS Server RCE Attempt Inbound (CVE-2021-26897)", "ET EXPLOIT Exiftool RCE Inbound (CVE-2021-22204)", "ET WEB_SERVER Apache Struts Possible xwork Disable Method Execution", "GPL NETBIOS SMB-DS OpenKey little endian overflow attempt", "ET EXPLOIT vCenter Server RCE Chain Initial Stage Inbound (CVE-2021-21985)", "ET EXPLOIT VMware Spring Cloud Directory Traversal (CVE-2020-5405)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M1", "ET EXPLOIT HP Enterprise VAN SDN Controller Root Command Injection (Linux)", "ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate2 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M2", "GPL IMAP Overflow Attempt", "ET EXPLOIT VisualDoor Sonicwall SSL VPN Exploit Attempt", "ET EXPLOIT Apache log4j RCE Attempt - AWS Access Key Disclosure (CVE-2021-44228)", "ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Outbound)", "ET EXPLOIT DLink DNS 320 Remote Code Execution (CVE-2019-16057)", "GPL RPC STATD UDP stat mon_name format string exploit attempt", "ET HUNTING Suspicious Response (MS-Officecmd)", "ET EXPLOIT ManageEngine AdSelfService Plus - .jsp WebShell Upload Attempt (CVE-2021-40539)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (2)", "ET MALWARE Possible Linux.Mirai Login Attempt (realtek)", "ET EXPLOIT Exim Stack Exhaustion via BDAT Error Inbound (CVE-2020-28019)", "GPL NETBIOS SMB CoGetInstanceFromFile andx overflow attempt", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (20)", "ET EXPLOIT Suspected SAP EEM SOLMAN RCE (CVE-2020-6207)", "ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M3", "ET EXPLOIT Citrix Application Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt (CVE-2019-19781)", "GPL RPC STATD TCP monitor mon_name format string exploit attempt", "ET EXPLOIT Possible IBM Data Risk Manager Authentication Bypass - Password Retrieval", "ET EXPLOIT GoCD Authentication Bypass Successful Leak", "GPL NETBIOS SMB-DS llsrconnect unicode overflow attempt", "ET WEB_SPECIFIC_APPS Possible Wordpress Plugin TheCartPress Privilege Escalation Attempt Inbound", "ET WEB_SPECIFIC_APPS Possible Apache Unomi OGNL Eval RCE Inbound M2 (CVE-2020-13942)", "ET

	ATTACK_RESPONSE Possible CVE-2021-44228 Payload via LDAPv3 Response", "ET EXPLOIT Firefox 0-day used against TOR browser Nov 29 2016 M2", "ET EXPLOIT Nuuo NVR RCE Attempt (CVE-2018-15716)", "ET EXPLOIT Netgear DGN1000B Router DNS Change GET Request", "ET EXPLOIT Apache log4j RCE Attempt (udp ldap) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Ultimate POS 4.4 Cross-Site Scripting (XSS) - Inbound", "ET EXPLOIT Possible iOS Pegasus Safari Exploit (CVE-2016-4657)", "GPL NETBIOS SMB CoGetInstanceFromFile unicode andx overflow attempt", "ET EXPLOIT D-Link and TRENDnet ncc2 Service Vulnerability (fwupdate.cpp) 2015-1187", "ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M1", "ET EXPLOIT D-Link Router DNS Changer Exploit Attempt", "ET MALWARE Possible Linux.Mirai Login Attempt (hi3518)", "ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M2", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp corba) (CVE-2021-44228)", "ET EXPLOIT Redfish Exploitation Attempt (CVE-2022-40259)", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nis) (Outbound) (CVE-2021-44228)", "GPL FTP RMDIR overflow attempt", "ET EXPLOIT Possible Mirai Infection Attempt via OS Command Injection Inbound (CVE-2021-32305)", "ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M2", "ET MALWARE Possible Linux.Mirai Login Attempt (klv123)", "ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M2", "ET EXPLOIT Yachtcontrol Webservers RCE CVE-2019-17270 (Outbound)", "ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M5", "ET EXPLOIT QNAP MusicStation Pre-Auth RCE Inbound (CVE-2020-36197)", "ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M2", "ET EXPLOIT F5 BIG-IP rsync cmi access attempt", "GPL NETBIOS SMB OpenKey andx overflow attempt", "ET WEB_SERVER SLIGHTPULSE WebShell Access Inbound M2", "ET EXPLOIT WebSVN 2.6.0 OS Command Injection Inbound (CVE-2021-32305)", "ET EXPLOIT ARG-W4 ASDL Router DNS Changer Exploit Attempt", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M3", "ET EXPLOIT Default Apache CouchDB Erlang Cookie Observed (CVE-2022-24706)", "ET EXPLOIT Possible SpringCore RCE/Spring4Shell Inbound (CVE-2022-22965)", "ET INFO Possible NOP Sled Observed in Large DNS over TCP Packet M2", "ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1599)", "ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Exploit Attempt", "ET EXPLOIT Zoho ManagedEngine Desktop Central Authentication Bypass - File Upload Attempt (CVE-2021-44515)", "ET EXPLOIT TP-LINK TL-WR750N DNS Change GET Request", "ET EXPLOIT Possible Zimbra RCE Attempt Inbound (CVE-2022-27925)", "ET WEB_SERVER Generic Webshell Observed Outbound", "ET MALWARE Possible Linux.Mirai Login Attempt (klv1234)", "GPL NETBIOS SMB NDdeSetTrustedShareW little endian andx overflow attempt", "ET EXPLOIT Solr DataImport Handler RCE (CVE-2019-0193)", "ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M2 (CVE-2021-44228)", "ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M1", "ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M1", "ET EXPLOIT Belkin G F5D7230-4 Router DNS Change GET Request", "ET EXPLOIT Possible Qmail CVE-2014-6271 Mail From attempt", "ET EXPLOIT WinRAR WinAce Containing CVE-2018-20250 Inbound - Path Traversal leading to RCE", "ET EXPLOIT NodeBB Path Traversal (CVE-2021-43788)", "GPL RPC sadmind TCP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt M3", "ET EXPLOIT Cisco AnyConnect Path Traversal Priv Esc (CVE-2020-3153)", "ET EXPLOIT Possible OpenSMTPD RCE Inbound (CVE-2020-7247)", "ET EXPLOIT WatchGuard CVE-2022-26318 RCE Attempt M1", "ET EXPLOIT Bonitasoft Authorization Bypass and RCE Upload M1 (CVE-2022-25237)", "ET WEB_SPECIFIC_APPS Possible Apache Druid RCE Inbound (CVE-2021-25646)", "ET EXPLOIT Tenda ADSL2/2+ Router DNS Change GET Request", "ET ATTACK_RESPONSE Windows 64bit procdump Dump File Exfiltration", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian overflow attempt", "ET EXPLOIT Zerologon Phase 3/3 - NetrLogonSamLogonWithFlags Request with 0x00 Client Credentials (CVE-2020-1472)", "ET EXPLOIT Possible Microsoft Exchange RCE Inbound M2 (CVE-2021-34473)", "ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M1", "ET EXPLOIT EyesOfNetwork Cookie SQLi (CVE-2020-9465)", "ET EXPLOIT GoCD Authentication Bypass URI Path - add-on", "ET

	WEB_SERVER Suspected SUPERNOVA Webshell Command (Internal)", "ET EXPLOIT Bonitasoft Authorization Bypass and RCE Upload M2 (CVE-2022-25237)", "ET EXPLOIT REDIS Attemted SSH Authorized Key Writing Attempt", "ET EXPLOIT Possible Apache Text4shell RCE Attempt DNS Prefix (CVE-2022-42889) (Outbound)", "ET ATTACK_RESPONSE Possible CVE-2021-44228 Payload via LDAPv3 Response M2", "ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 2 Suffix Set Inbound (CVE-2022-22965)", "ET EXPLOIT CVE-2015-0235 Exim Buffer Overflow Attempt (EHLO)", "ET EXPLOIT Multiple CCTV-DVR Vendors RCE", "ET INFO Possible GoCD Authentication Bypass URI Path - add-on", "ET EXPLOIT vBulletin 5.6.2 widget_tabbedContainer_tab_panel Remote Code Execution (Outbound)", "ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access", "ET EXPLOIT Jira Server/Data Center 8.4.0 Remote File Read Attempt (CVE-2021-26086) M1", "GPL RPC STATD UDP monitor mon_name format string exploit attempt", "ET EXPLOIT Apache log4j RCE Attempt (udp rmi) (CVE-2021-44228)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - factory.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "GPL FTP RMD overflow attempt", "ET EXPLOIT Possible Vantage Velocity Field Unit RCE Inbound (CVE-2020-9020)", "ET WEB_SPECIFIC_APPS Possible CVE-2020-8518 (Horde Groupware RCE)", "ET EXPLOIT [401TRG] ZeroShell RCE Inbound (CVE-2019-12725)", "ET EXPLOIT Possible D-Link Command Injection Attempt Inbound (CVE-2020-13782)", "GPL NETBIOS SMB-DS OpenKey overflow attempt", "ET EXPLOIT Cisco HyperFlex HX RCE Outbound (CVE-2021-1498)", "ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2", "ET EXPLOIT Apache log4j RCE Attempt - Nested lower (udp) (Outbound) (CVE-2021-44228)", "ET WEB_SERVER Possible SQL Injection Attempt Danmec related (declare)", "ET EXPLOIT DNS Change Attempt (Unknown Device)", "ET WEB_SERVER lolzilla WebSkimmer - Remote Code Execution Attempt M4", "ET EXPLOIT Qianxin Netcom NGFW Command Injection", "ET EXPLOIT Apache log4j RCE Attempt (http ldap) (Outbound) (CVE-2021-44228)", "GPL POP3 x86 Linux overflow", "ET EXPLOIT Attempted Remote Command Injection Outbound (CVE-2018-7841)", "ET EXPLOIT DD-WRT UPNP Unauthenticated Buffer Overflow (CVE-2021-27137)", "ET EXPLOIT Exim receive_msg Integer Overflow Attempt Inbound M2 (CVE-2020-28020)", "ET WEB_SPECIFIC_APPS Atlassian Crowd Plugin Upload Attempt (CVE-2019-11580)", "ET EXPLOIT Attempted HiSilicon DVR/NVR/IPCam RCE (Inbound)", "ET EXPLOIT WP Download From Files Plugin <= 1.48 Arbitrary File Upload Attempt", "ET EXPLOIT Supermicro BMC Password Disclosure 1", "ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M3", "ET ATTACK_RESPONSE Possible CVE-2016-1287 Inbound Reverse CLI Shellcode", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M2", "ET EXPLOIT Possible Apache Text4shell RCE Attempt Script Prefix (CVE-2022-42889) (Inbound)", "ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass (CVE-2022-1388) M1", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt M1", "ET EXPLOIT IBM Data Risk Manager Remote Code Execution via NMAP Scan", "ET EXPLOIT D-Link DSL-2740R Remote DNS Change Attempt", "ET WEB_SERVER PHPMyAdmin BackDoor Access", "ET INFO Potential External VMware vRealize Automation Authentication Bypass Vulnerability", "ET EXPLOIT QNAP Shellshock script retrieval", "ET WEB_CLIENT Attempted RCE in Wordpress Social Warfare Plugin Inbound (CVE-2019-9978)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (27)", "ET EXPLOIT GraphQL Introspection Query Attempt", "ET EXPLOIT NetGear R6700v3 upnpd Buffer Overflow Inbound (CVE-2022-27643)", "ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-25075)", "ET EXPLOIT Apache Spark RPC - Unauthenticated RegisterApplication Request (CVE-2020-9480)", "ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Outbound)", "ET EXPLOIT Inbound VMware vCenter RCE Attempt M3 (CVE-2021-21972)", "ET EXPLOIT Possible Citrix ShareFile RCE Inbound (CVE-2021-22941)", "ET EXPLOIT Possible Apache Text4shell RCE Attempt JEXL Path (CVE-2022-42889) (Inbound)", "ET WEB_SPECIFIC_APPS Apache Struts inbound .getWriter OGNL injection remote code execution attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections5/MozillaRhino1/Vaadin)

	M1", "ET EXPLOIT IBM Data Risk Manager Authentication Bypass - Session ID Assignment (set)", "ET WEB_SERVER WEBSHELL pwn.jsp shell", "ET WEB_SERVER WGET Command Specifying Output in HTTP Headers", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp corba) (Outbound) (CVE-2021-44228)", "ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)", "ET EXPLOIT Qualcomm QCMAP Command Injection Attempt Inbound (CVE-2020-3657)", "ET EXPLOIT Complaint Management System 1.0 - Authentication Bypass Attempt", "ET MALWARE Unattributed WebShell Access - Command Execution", "ET EXPLOIT D-Link Devices Home Network Administration Protocol Command Execution", "ET SCAN Polaris Botnet User-Agent (Inbound)", "ET EXPLOIT Netgear ProSAFE Plus Possible Integer Overflow Attempt Inbound M1 (CVE-2020-35230)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M3", "GPL NETBIOS SMB llsrconnect little endian overflow attempt", "ET EXPLOIT Possible Microsoft Exchange RCE with Python PSRP Client UA Inbound (CVE-2021-34473)", "ET EXPLOIT COMTREND ADSL Router CT-5367 Remote DNS Change Attempt", "ET EXPLOIT Netgear ProSAFE Plus Unauthenticated RCE Inbound (CVE-2020-26919)", "ET EXPLOIT MikroTik RouterOS Chimay Red Remote Code Execution Probe", "ET EXPLOIT Nagios XI Post-Auth Path Traversal (CVE-2021-37343)", "ET EXPLOIT Possible Joomla RCE (CVE-2011-5148)", "ET EXPLOIT Possible Apache Text4shell RCE Attempt URL Prefix (CVE-2022-42889) (Outbound)", "ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 1 Inbound - Request Config Backup (CVE-2020-8260)", "ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (tcp) (CVE-2021-44228)", "ET EXPLOIT NUUO OS Command Injection M2", "ET EXPLOIT Possible CVE-2014-6271 malicious DNS response", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M1", "ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M1", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Client Body 2", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M2", "ET MALWARE Possible Linux.Mirai Login Attempt (666666)", "ET EXPLOIT Possible IBM Data Risk Manager Authentication Bypass - Session ID Assignment", "ET EXPLOIT Possible LG SuperSign EZ CMS 2.5 RCE (CVE-2018-17173)", "ET EXPLOIT Attempted Remote Command Injection Inbound (CVE-2019-3929)", "ET EXPLOIT SolarView Compact Command Injection Inbound (CVE-2022-29303)", "ET EXPLOIT Authenticated QuickBox CE 2.5.5/Pro 2.1.8 RCE Attempt Inbound M1 (CVE-2020-13448)", "ET EXPLOIT Sangoma Asterisk Originate AMI RCE (CVE-2019-18610) (PoC Based)", "ET EXPLOIT Citrix SD-WAN Unauthenticated RCE (CVE-2020-8271)", "GPL NETBIOS SMB-DS OpenKey unicode little endian andx overflow attempt", "ET EXPLOIT Cisco ASA and Firepower Path Traversal Vulnerability M2 (CVE-2020-3452)", "ET WEB_SERVER lwp-download Command Specifying Output in HTTP Headers", "ET EXPLOIT LibreOffice pydoc RCE Inbound (CVE-2018-16858)", "ET EXPLOIT Smart Google Code Inserter < 3.5 Auth Bypass (CVE-2018-3810)", "ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781)", "ET EXPLOIT TIBCO Data Virtualization <= 8.3 RCE Attempt (CVE-2016-2510)", "ET EXPLOIT Oracle WebLogic IIOP JNDI Injection (CVE-2020-14841)", "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)", "ET EXPLOIT UCM6202 1.0.18.13 - Remote Command Injection Attempt", "ET EXPLOIT Possible Microsoft Exchange Server Remote Code Execution Inbound (CVE-2021-42321)", "ET EXPLOIT Netgear Seventh Inferno Vulnerability (fake packet upload)", "ET EXPLOIT Netgear ProSAFE Plus Stored XSS Inbound (CVE-2020-35228)", "GPL FTP invalid MDTM command attempt", "ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 1 Pattern Set Inbound (CVE-2022-22965)", "GPL NETBIOS SMB NDdeSetTrustedShareW overflow attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M3", "GPL NETBIOS SMB CoGetInstanceFromFile unicode overflow attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian andx overflow attempt", "GPL NETBIOS DCERPC CoGetInstanceFromFile little endian overflow attempt", "ET EXPLOIT UDP Technology Firmware (IP Cam) - tmpapp.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - factory.cgi RCE via Command Injection

	Attempt Outbound (CVE-2021-33544)", "ET WEB_SPECIFIC_APPS [PT OPEN] Drupalgeddon2 <8.3.9 <8.4.6 <8.5.1 RCE Through Registration Form (CVE-2018-7600)", "ET EXPLOIT Citrix ShareFile Storage Zones Controller RCE Attempt (CVE-2021-22941)", "ET EXPLOIT Possible CloudMe Sync Stack-based Buffer Overflow Inbound (CVE-2018-6892)", "ET EXPLOIT Possible MobileIron RCE Attempt Inbound (CVE-2020-15505)", "ET EXPLOIT Microsoft Edge Chakra - InlineArrayPush Type Confusion Inbound M2 (CVE-2018-8617)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - Auth Bypass Attempt Inbound (CVE-2021-33543)", "ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M1", "ET EXPLOIT OptiLink ONT1GEW GPON RCE Inbound", "ET EXPLOIT Possible Pure-FTPd CVE-2014-6271 attempt", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M2", "ET EXPLOIT Microsoft Edge Chakra - NewScObjectNoCtor InitProtoType Confusion Inbound (CVE-2019-0567)", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nds) (CVE-2021-44228)", "ET EXPLOIT Cisco HyperFlex OS Command Injection M1 (CVE-2021-1497)", "ET EXPLOIT Attempted Netgear Buffer Overflow into RCE Inbound M1", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode overflow attempt", "GPL NETBIOS SMB CoGetInstanceFromFile overflow attempt", "GPL TFTP MISC TFTP32 Get Format string attempt", "ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Remote Code Execution Inbound (CVE-2019-0230)", "ET EXPLOIT EyesOfNetwork Generate API Key SQLi (CVE-2020-8656)", "ET EXPLOIT Prestashop Orderfiles Module Arbitrary File Upload", "ET EXPLOIT Possible OpenVPN CVE-2014-6271 attempt", "GPL FTP USER overflow attempt", "ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M2", "ET ATTACK_RESPONSE Windows 32bit procdump Dump File Exfiltration", "ET EXPLOIT ZKBioSecurity SQL Injection Attempt (CVE-2022-36635)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M3", "ET EXPLOIT TP-LINK Password Change GET Request (DNSChanger EK)", "GPL NETBIOS SMB llsrconnect little endian andx overflow attempt", "ET EXPLOIT Netis WF2419 2.2.36123 - Remote Code Execution CVE-2019-19356", "ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1", "ET MALWARE Possible Linux.Mirai Login Attempt (xmhdipc)", "ET EXPLOIT Possible Apache Airflow DAG Example RCE Attempt - Unpause (CVE-2020-11978)", "ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (16)", "ET EXPLOIT Multiple DLink Routers Remote Code Execution CVE-2019-16920", "ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (CVE-2021-42013) M2", "ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nis) (CVE-2021-44228)", "ET EXPLOIT Apache APISIX Admin API Authentication Bypass (CVE-2022-24112) M1", "ET EXPLOIT EnGenius EnShare IoT Gigabit Cloud Service RCE", "ET WEB_SPECIFIC_APPS WHMCS lt 5.2.8 SQL Injection", "ET EXPLOIT Linux/Attempted Hosts File Exfil", "ET EXPLOIT Apache APISIX Admin API Authentication Bypass (CVE-2022-24112) M2", "ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3", "ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M2", "ET EXPLOIT Netgear WNDR Router DNS Change POST Request", "ET EXPLOIT Aviatrix Controller Unrestricted File Upload with Path Traversal Inbound (CVE-2021-40870)", "ET WEB_SPECIFIC_APPS FancyBox Remote Code Inclusion POST Request", "ET EXPLOIT Apache Struts memberAccess and opensymphony inbound OGNL injection remote code execution attempt", "GPL NETBIOS SMB-DS llsrconnect andx overflow attempt", "ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Outbound)", "ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2", "ET EXPLOIT DotNetNuke 9.2-9.2.2 Cookie Deserialization Exploit (CVE-2018-15811)", "ET EXPLOIT Exim New-Line Injection into Spool Header File Inbound M1 (CVE-2020-28021)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - oem.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)", "GPL POP3 POP3 PASS overflow attempt", "ET EXPLOIT Apache Struts RCE Attempt (CVE-2020-17530)", "ET EXPLOIT UDP Technology Firmware (IP Cam) - oem.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)", "ET EXPLOIT VMware SD-WAN Orchestrator SQL Injection (CVE-2020-3984)"
DNS поверх HTTPS	"DNSoverHTTPS"

Попытки использования социальной инженерии	"ET PHISHING Likely Cloned .EDU Website Phishing Landing 2018-02-02", "ET PHISHING Possible Fedex Phishing Landing - Title over non SSL", "ET PHISHING Bank of America Phishing Landing 2018-01-18 M1", "ET PHISHING Weebly Phishing Landing Observed 2015-11-10", "ET PHISHING OneDrive Phishing Landing 2018-03-08", "ET PHISHING Cloned Telstra Page - Possible Phishing Landing", "ET PHISHING Verizon Wireless Phishing Landing 2018-01-30", "ET PHISHING LinkedIn Phishing Landing 2018-02-09 M2", "ET PHISHING Zimbra Phishing Landing on Appspot Hosting", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M9", "ET PHISHING Possible Phishing Landing via GetGoPhish Phishing Tool", "ET PHISHING Microsoft Live Phishing Landing", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M8", "ET PHISHING Generic Custom Logo Phishing Landing 2021-03-10", "ET PHISHING GET Request to Googleapis Hosting (set)", "ET PHISHING Upgrade Advantage Phishing Landing 2018-02-22", "ET PHISHING Wells Fargo Mobile Phishing Landing 2016-08-01", "ET PHISHING Chase/Bank of America Phishing Landing Uri Structure Nov 27 2012", "ET PHISHING Possible Chalbhai (Multibrand) Phishing Landing 2018-05-10", "ET PHISHING Phishing Landing via MyFreeSites.com M2 2016-03-31", "ET PHISHING Observed Phish Domain in DNS Lookup (snoc-projectae .com) 2022-12-05", "ET PHISHING Adobe Online Document Phishing Landing 2016-05-02", "ET MALWARE Observed Malsmoke Staging Domain in SNI", "ET PHISHING Possible Apple Store Phish Landing 2015-07-30", "ET PHISHING GET Request to Appspot Hosting (set)", "ET PHISHING Badoo Phishing Landing 2018-07-19", "ET PHISHING Observed Phish Domain in DNS Lookup (stalinschoolintlacademy .com) 2022-12-05", "ET PHISHING Observed Zimbra Phishing Landing Page 2021-08-09", "ET PHISHING Observed Phish Domain in DNS Lookup (westernmedicalspecialisthosp .com) 2022-12-05", "ET PHISHING Possible Adobe PDF Phishing Landing - Title over non SSL", "ET PHISHING Generic Multi-Email Phishing Landing 2018-08-30", "ET PHISHING OneDrive Phishing Landing on Appspot Hosting", "ET PHISHING Observed Phish Domain in DNS Lookup (hamraoilgroup .com) 2022-12-05", "ET PHISHING Multibank Captcha Phishing Landing", "ET PHISHING Possible Square Enix Phishing Domain 2016-08-15", "ET PHISHING [eSentire] Docusign Phishing Landing 2018-04-09", "ET PHISHING Possible Wells Fargo Phishing Landing - Title over non SSL", "ET PHISHING Successful TA398/Sidewinder APT Related Phish 2022-09-28", "ET PHISHING Observed Phish Domain in DNS Lookup (arabianmigration .com) 2022-12-05", "ET PHISHING Adobe Shared Document Phishing Landing Nov 19 2015", "ET PHISHING Outlook Web App Phishing Landing 2018-02-07", "ET PHISHING Observed Phish Domain in DNS Lookup (harvesttravelagency .com) 2022-12-05", "ET PHISHING Cloned Westpac Bank Page - Possible Phishing Landing", "ET PHISHING Cloned Scotiabank Page - Possible Phishing Landing", "ET WEB_CLIENT Microsoft Tech Support Phone Scam M4 Jul 07 2017", "ET PHISHING PDF Cloud Phishing Landing 2018-04-19", "ET PHISHING T-Mobile Phishing Landing", "ET WEB_CLIENT Tech Support Scam Landing M1 2019-04-15", "ET PHISHING Capital One Phishing Landing", "ET PHISHING Banque Populaire Phishing Landing 2018-02-05", "ET PHISHING Generic MRxJoker Phishing Landing 2018-09-27", "ET PHISHING Avast Phishing Landing 2016-06-02", "ET PHISHING Facebook Phishing Landing 2018-02-15", "ET PHISHING Possible Phishing Landing Obfuscation 2016-02-26", "ET PHISHING Email Storage Upgrade Phishing Landing 2016-08-15", "ET PHISHING PirateBay Phish - Possibly PirateMatryoshka Related", "ET PHISHING Common Form POST - SunTrust Phishing Landing 2020-06-11", "ET PHISHING Generic PhishKit Author Comment M2 2018-08-30", "ET PHISHING DHL Phish Landing Page 2015-10-17", "ET PHISHING Dropbox Phishing Landing 2018-02-14", "ET PHISHING Microsoft Encrypted Email Phishing Landing 2016-06-23", "ET PHISHING Observed Phish Domain in DNS Lookup (zbavitae .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (snocprojectae .com) 2022-12-05", "ET PHISHING Email Settings Error Phishing Landing Nov 16 2016", "ET PHISHING Windows Settings Phishing Landing Jul 22 2016", "ET PHISHING Observed Malicious SSL/TLS Certificate (PayPal Phish Landing)", "ET PHISHING Possible Apple Phishing Domain Mar 14 2016", "ET PHISHING Revalidation Phish Landing Nov 13 2015", "ET PHISHING Apple Phishing Landing 2018-04-09", "ET PHISHING [eSentire] OneDrive Phishing Landing 2018-06-15", "ET PHISHING Facebook Phishing Landing 2018-02-09", "ET PHISHING Santander Phishing Landing", "ET

	PHISHING Possible Phishing Landing via MoonFruit.com M1 2016-01-22", "ET WEB_CLIENT Tech Support Phone Scam Landing M2 2016-08-12", "ET PHISHING Multiple Javascript Unescapes - Common Obfuscation Observed in Phish Landing", "ET PHISHING GitLab Phishing Landing 2018-07-19", "ET PHISHING Possible Capitech Internet Banking Phishing Landing - Title over non SSL", "ET PHISHING Netsolhost SSL Proxying - Possible Phishing Nov 24 2015", "ET PHISHING Generic Google Firebase Hosted Phishing Landing", "ET PHISHING Possible Scotiabank Phishing Landing - Title over non SSL", "ET PHISHING Google/Adobe Shared Document Phishing Landing 2018-02-05", "ET PHISHING INTERAC Payment Multibank Phishing Landing Mar 14 2017", "ET PHISHING Possible Excel Online Phishing Landing - Title over non SSL", "ET PHISHING Linkedin Phishing Landing 2018-02-14", "ET PHISHING OneDrive Phishing Landing 2018-04-09", "ET PHISHING Mailbox Renewal Phish Landing 2015-08-14", "ET PHISHING Bank of America Phishing Landing 2018-04-19", "ET PHISHING Possible Phishing Landing - Tectite Web Form Abuse", "ET PHISHING Suspicious JS Refresh - Possible Phishing Redirect Feb 24 2017", "ET PHISHING Lucy Security Phishing Awareness Landing Page", "ET PHISHING Observed Phish Domain in DNS Lookup (snocuae .com) 2022-12-05", "ET PHISHING Generic Redirector Phishing Landing 2021-03-10", "ET PHISHING Bank of America Phishing Landing 2018-01-30", "ET PHISHING Possible Phishing Landing Captcha Check", "ET PHISHING UK GOV Identity Verification Phishing Landing", "ET PHISHING Adobe Shared Document Phishing Landing 2016-08-30", "ET PHISHING Mailbox Shutdown Phishing Landing 2017-12-11", "ET PHISHING Adobe PDF Online Phishing Landing", "ET PHISHING Common Form POST - Yahoo Phishing Landing 2020-06-11", "ET PHISHING American Express Phishing Landing", "ET PHISHING Adobe PDF Reader Phishing Landing 2018-03-27", "ET PHISHING DHL/EMS Documents Phishing Landing 2016-08-10", "ET PHISHING Chase Phishing Landing 2018-04-09", "ET PHISHING OneDrive Phishing Landing 2021-03-15", "ET PHISHING CDC Coronavirus Related Phishing Landing 2020-04-07", "ET PHISHING Possible MyMonero Phishing Landing - SSL/TLS Certificate Observed", "ET WEB_CLIENT Microsoft Tech Support Phone Scam M1 Jul 07 2017", "ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 4", "ET PHISHING Free Mobile Phishing Landing 2018-08-07", "ET PHISHING Turbotax Phishing Landing 2018-01-30", "ET PHISHING Paypal Phishing Landing 2018-02-05", "ET PHISHING Chalbhai Phishing Landing 2018-03-12", "ET PHISHING Mailbox Deactivation Phishing Landing 2016-12-15", "ET WEB_CLIENT Tech Support Scam - Windows Firewall M5 2021-08-17", "ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M3", "ET PHISHING Possible Facebook Help Center Phishing Landing - Title over non SSL", "ET PHISHING Anonisma Paypal Phishing Uri Structure 2015-12-29", "ET PHISHING Observed Phish Domain in DNS Lookup (sheikhmouradoil .com) 2022-12-05", "ET PHISHING Office 365 Phishing Landing 2018-01-29", "ET PHISHING Generic Tombol Microsoft Account Phishing Landing 2020-12-16", "ET WEB_CLIENT Fake AV Phone Scam Domain M2 Mar 3", "ET PHISHING NHS Gov UK COVID-19 Landing Page", "ET PHISHING Generic Multibrand NewInjection Phishing Landing Template", "ET PHISHING Dropbox Phishing Landing 2018-01-18", "ET HUNTING Suspicious HTTP Refresh to SMS Aug 16 2016", "ET PHISHING Smartermail Phishing Landing 2018-02-20", "ET PHISHING Dropbox Phishing Landing - Title over non SSL", "ET EXPLOIT_KIT ElTest SocENG Inject M2", "ET PHISHING Google Drive Phishing Landing 2016-08-25", "ET PHISHING Phishing Fake Mailbox Quota Increase Messages 2016-05-25", "ET PHISHING Facebook Phishing Landing 2018-04-09", "ET PHISHING Alibaba Phishing Landing 2018-08-07", "ET PHISHING Dropbox 000webhost Phishing Landing 2018-04-19", "ET WEB_CLIENT Tech Support Scam 2020-04-10", "ET WEB_CLIENT Microsoft Tech Support Scam M2 2016-09-15", "ET WEB_CLIENT Tech Support Scam Sep 08 2017", "ET PHISHING Covid19 Stimulus Payment Phish Inbound M1 (2021-10-21)", "ET PHISHING Adobe Shared Document Phish Landing 2015-11-14", "ET PHISHING Wells Fargo Phishing Landing 2018-02-22", "ET PHISHING Paypal Phishing Landing 2017-12-26", "ET PHISHING Dropbox Phishing Landing Feb 27 2017", "ET PHISHING Cloned South State Bank Page - Possible Phishing Landing", "ET PHISHING Shipping Document Phishing Landing 2016-06-23", "ET PHISHING Possible Compromised Wordpress - Generic Phishing Landing 2018-01-22", "ET PHISHING Apple iTunes Phishing Landing (DE) 2018-01-31", "ET

	PHISHING Bank of America Phishing Landing 2018-01-18 M2", "ET PHISHING Google Drive Phishing Landing 2018-02-07", "ET PHISHING Possible Phishing Landing - Common Multiple JS Unescape May 25 2017", "ET PHISHING Observed Phishing Domain in DNS Lookup (mcrsfts-passwdupdate .com)", "ET PHISHING [TW] Robin Banks HTTP HOST M1", "ET WEB_CLIENT Fake Virus Phone Scam Audio Oct 30", "ET PHISHING Microsoft Account Phishing Landing 2018-08-07", "ET PHISHING Possible Phishing Script Hosted on 000webhostapp", "ET PHISHING Impots Phishing Landing 2018-03-28", "ET PHISHING Possible Ebay Phishing Domain Jan 30 2017", "ET PHISHING Observed DNS Query to Phishing Domain (ficosha .com)", "ET PHISHING Microsoft Edge SmartScreen Page Spoof Attempt Dec 16 2016", "ET PHISHING Spotify Phishing Landing 2018-02-19", "ET PHISHING Observed Let's Encrypt Certificate containing Instagram", "ET PHISHING IRS Phishing Landing 2018-05-07", "ET PHISHING Observed Phish Domain in DNS Lookup (alfujairah-ae .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (rfq-taziz .com) 2022-12-05", "ET PHISHING Possible Base64 Obfuscated Phishing Landing 2015-11-30", "ET PHISHING Netflix Phishing Landing 2018-05-09", "ET PHISHING DrSpam Phishing Landing CSS 2016-06-08", "ET PHISHING Suspicious Yahoo Page - Possible Phishing Landing", "ET PHISHING Generic PhishKit Author Comment M8 2018-08-30", "ET PHISHING Possible Apple Phishing Landing - Title over non SSL", "ET PHISHING Suspicious HTML Decimal Obfuscated Title - Possible Phishing Landing Apr 19 2017", "ET PHISHING Adobe Cloud Phishing Landing 2016-06-02", "ET PHISHING Phishing Landing via MyFreeSites.com (set) 2016-03-31", "ET PHISHING Suspicious LastPass URI Structure - Possible Phishing", "ET PHISHING Credit Mutuel de Bretagne (FR) Phishing Landing 2018-02-26", "ET PHISHING Twitter Phishing Landing 2018-07-19", "ET PHISHING Cloned ATB Bank Online Page - Possible Phishing Landing", "ET PHISHING Cloned ADP Page - Possible Phishing Landing", "ET PHISHING AT&T Phishing Landing 2018-01-23", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M2", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M6", "ET PHISHING Mailbox Verification Phishing Landing 2018-01-31", "ET PHISHING Mailbox Verification Phishing Landing 2018-02-07", "ET PHISHING Observed Phish Domain in DNS Lookup (nipmse .com) 2022-12-05", "ET PHISHING Bank of America Phishing Landing 2018-05-01", "ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 M1", "ET PHISHING Obfuscated Phishing Landing 2015-11-05", "ET PHISHING PHOEN!X Phish Loading Page 2015-12-29", "ET PHISHING Dropbox Phishing Landing May 31 2017", "ET PHISHING Excel Online Phishing Landing Aug 09 2016", "ET PHISHING Generic Chalbhai Phishing Landing 2018-08-30", "ET HUNTING Suspicious Glitch Hosted GET Request - Possible Phishing Landing", "ET PHISHING Paypal Phishing Landing 2018-01-31", "ET PHISHING Generic AES Phishing Landing 2018-08-30", "ET PHISHING Common Form POST - CenturyLink Phishing Landing 2020-06-11", "ET PHISHING Possible Capital One Phishing Landing - Title over non SSL", "ET PHISHING Office 365 Phishing Landing 2018-02-22", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M9", "ET PHISHING Netflix Phishing Landing 2017-07-20", "ET PHISHING Microsoft Account Phishing Landing 2021-03-10", "ET PHISHING Possible Docusign Phishing Landing - Title over non SSL", "ET PHISHING Observed Phish Domain in DNS Lookup (kilimondoilgas-dubai .com) 2022-12-05", "ET HUNTING Suspicious Glitch Hosted TLS SNI Request - Possible Phishing Landing", "ET PHISHING Mailbox Update Phishing Landing 2018-02-26", "ET PHISHING Wells Fargo Phishing Landing 2018-02-01", "ET PHISHING Cloned Impots Gouv FR Page - Possible Phishing Landing", "ET PHISHING Paypal Phishing Landing 2018-01-29", "ET PHISHING Obfuscated Chase Phishing Landing 2016-03-23", "ET PHISHING Cloned Website Phishing Landing - Saved Website Comment Observed", "ET PHISHING Generic PhishKit Author Comment M4 2018-08-30", "ET PHISHING Yahoo Account Verification Phishing Landing 2018-02-05", "ET PHISHING Metro Document Phishing Landing 2015-11-17", "ET PHISHING Possible iCloud Phishing Landing - Title over non SSL", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M1", "ET PHISHING Generic Popupwnd Phishing Landing 2018-04-19", "ET PHISHING Possible Ziraat Bank (TK) Phishing Landing - Title over non SSL", "ET PHISHING Apple Phishing Redirect 2019-01-02", "ET PHISHING Observed Phish Domain in DNS Lookup (contracts-adnoc .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (eaglestravels-ae .com) 2022-12-05",

	"ET PHISHING USAA Phishing Landing 2016-02-26", "ET PHISHING Obfuscated Phishing Landing 2016-12-19", "ET WEB_CLIENT Fake AV Phone Scam Landing July 20 2015 M4", "ET PHISHING Phishing Landing via Tripod.com Mar 31 M3", "ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 EXE Download", "ET PHISHING Observed Phish Domain in DNS Lookup (contractors-adnoc .com) 2022-12-05", "ET PHISHING Cloned Societe Generale FR Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (flywaytravelandtourism .com) 2022-12-05", "ET PHISHING Apple Phishing Landing M2 Feb 13 2017", "ET PHISHING Common Form POST - Microsoft Account Phishing Landing 2020-06-11", "ET PHISHING Cloned ABSA Bank Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (qatarenergys .com) 2022-12-05", "ET PHISHING Possible Google Drive Phishing Domain Aug 25 2016", "ET PHISHING Adobe Phishing Landing M1 2016-08-16", "ET PHISHING Common Unhidebody Function Observed in Phishing Landing", "ET PHISHING Common Form POST - Instagram Phishing Landing 2020-06-11", "ET PHISHING Possible Raiffeisen Bank Phishing Landing - Title over non SSL", "ET PHISHING Google Drive Phishing Landing 2015-11-17", "ET PHISHING Observed Phish Domain in DNS Lookup (proposal-enoc .com) 2022-12-05", "ET PHISHING Dropbox Phishing Landing 2018-08-30", "ET PHISHING Webmail Validator Phishing Landing 2016-09-02", "ET PHISHING Ebay Phishing Landing 2018-02-07", "ET PHISHING Possible MyEtherWallet Phishing Landing - SSL/TLS Certificate Observed", "ET PHISHING DHL/Adobe/Excel Phishing Landing 2016-01-07", "ET PHISHING Google Drive Phishing Landing Jul 10 2015", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M6", "ET PHISHING Generic 302 Redirect to Phishing Landing", "ET PHISHING Mailbox Update Phishing Landing M2 2016-05-16", "ET PHISHING OWA Phishing Landing 2016-04-04 M2", "ET PHISHING Phishing Landing via Tripod.com M2 2016-03-31", "ET PHISHING Generic Multi-Email Popupwnd Phishing Landing 2018-01-25", "ET PHISHING Chase Phishing Landing 2018-03-28", "ET PHISHING Mailbox Upgrade Phishing Landing 2016-06-27", "ET PHISHING Successful Generic Credential Phish 2022-08-23", "ET PHISHING Anonisma Phishing CSS 2015-12-29", "ET PHISHING Observed Phish Domain in DNS Lookup (stabluk .com) 2022-12-05", "ET PHISHING Hellion Postmaster Phishing Landing 2018-08-30", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M11", "ET PHISHING Microsoft Account Redirect to Phishing Landing", "ET PHISHING Generic Financial Phish Landing 2017-12-21", "ET PHISHING Possible Dropbox Phishing Landing - Title over non SSL", "ET PHISHING Excel Online Phish Landing 2015-12-08", "ET PHISHING Observed Phish Domain in DNS Lookup (dubaiferryae .com) 2022-12-05", "ET PHISHING Successful National Australia Bank 2016-09-28", "ET WEB_CLIENT Tech Support Scam - Windows Firewall M1 2021-08-17", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M1", "ET PHISHING Email Verification/Upgrade Phishing Landing 2018-01-22", "ET PHISHING Paypal Phishing Landing 2018-08-07", "ET PHISHING ABSA Online Phishing Landing 2018-01-23", "ET PHISHING Successful Microsoft Credential Phish 2022-05-26", "ET PHISHING Observed Phish Domain in DNS Lookup (contact-adnocae .com) 2022-12-05", "ET WEB_CLIENT Microsoft Tech Support Phone Scam M3 Jul 07 2017", "ET PHISHING Successful Generic Credential Phish", "ET PHISHING Mailbox Update Phishing Landing M1 2016-05-16", "ET PHISHING Google Drive Phishing Landing Sept 3", "ET PHISHING Observed Possible Phishing Landing Page 2021-06-24", "ET PHISHING Generic Roundcube Multi-Brand Phishing Landing 2018-01-31", "ET PHISHING Common Form POST - Facebook Phishing Landing 2020-06-11", "ET PHISHING Credito Emiliano Credential Phish Landing Page 2022-05-26", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M10", "ET PHISHING Email System Manager Phishing Landing 2016-04-12", "ET PHISHING Targeted Office 365 Phishing Landing 2016-08-23", "ET PHISHING Webmail Update Phishing Landing 2016-01-15", "ET PHISHING Chase Phish Landing 2020-10-13", "ET PHISHING Generic Multibrand Ajax XHR CredPost Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (ae-snoctenders .com) 2022-12-05", "ET PHISHING Email Termination Phishing Landing 2016-06-22", "ET MALWARE Fake Windows Scam ScreenLocker", "ET PHISHING cPanel Phishing Landing 2015-12-01", "ET PHISHING Chase Phishing Landing 2018-02-15", "ET PHISHING Possible Phishing Redirect Feb 24 2017", "ET PHISHING Cloned Telekom / Tmobile Page

	- Possible Phishing Landing", "ET PHISHING Google Drive Phishing Landing 2015-11-20", "ET PHISHING Possible Sparkasse Phishing Domain 2021-04-05", "ET PHISHING Generic Financial Phone Support Scam/Phishing Landing M2", "ET WEB_CLIENT Tech Support Scam - Generic Components", "ET PHISHING Observed Phish Domain in DNS Lookup (oceanicflyimmigration .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (uae-snoctenders .com) 2022-12-05", "ET PHISHING Google Docs Phishing Landing 2018-08-30", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M5", "ET WEB_CLIENT Microsoft Tech Support Scam Landing M1 Oct 13 2017", "ET PHISHING Observed Phish Domain in DNS Lookup (gulfins-ae .com) 2022-12-05", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M6", "ET PHISHING Account Credential Phish Landing Page 2022-10-10", "ET PHISHING Microsoft Document Phishing Landing 2018-08-30", "ET PHISHING Outlook Webmail Phishing Landing 2015-11-21", "ET PHISHING Successful Credential Phish M3 2022-09-23", "ET PHISHING Possible Adobe ID Phishing Landing - Title over non SSL", "ET WEB_CLIENT Fake Virus Phone Scam Landing Mar 09 2017", "ET PHISHING Observed Phish Domain in DNS Lookup (specgulfae .com) 2022-12-05", "ET PHISHING Outlook WebApp Phish Landing 2015-11-05", "ET PHISHING Common Form POST - M&T Bank Phishing Landing 2020-06-11", "ET PHISHING Cloned CIBC Bank Page - Possible Phishing Landing M2", "ET PHISHING Observed Phish Domain in DNS Lookup (ae-snocproject .com) 2022-12-05", "ET WEB_CLIENT Tech Support Phone Scam Landing Jun 29 M3", "ET PHISHING Possible Phishing Landing Obfuscation 2016-03-17", "ET PHISHING Possible Facebook Phishing Landing - Title over non SSL", "ET PHISHING Sparkasse Phishing Domain Nov 03 2017", "ET PHISHING Google Drive Phishing Landing M2 July 24 2015", "ET WEB_CLIENT Microsoft Tech Support Scam 2020-03-24", "ET PHISHING Suspicious Wordpress Redirect - Possible Phishing Landing Jan 7 2016", "ET PHISHING Ourtime Phishing Landing 2018-03-12", "ET PHISHING Possible AOL Mail Phishing Landing - Title over non SSL", "ET PHISHING Mailbox Revalidation Phishing Landing 2018-02-09", "ET PHISHING Generic Phishing Landing M2 2018-01-29", "ET PHISHING Stripe Phishing Landing 2018-08-30", "ET PHISHING [TW] EvilProxy AiTM Network Reporting", "ET PHISHING Apple Phishing Landing Nov 10 2017", "ET PHISHING Yahoo Account Phish Landing 2015-10-23", "ET PHISHING Adobe Phishing Landing 2016-03-10", "ET PHISHING Possible Phishing Landing via Moonfruit M1 2016-10-03", "ET PHISHING Shared Document Phishing Landing Nov 16 2016", "ET PHISHING Horde Webmail Phishing Landing 2015-08-21", "ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain M1 Feb 29", "ET PHISHING Possible Phishing Data Submitted to yolasite.com M2", "ET PHISHING Office Related Appspot Hosted Shared Document Phishing Landing", "ET PHISHING Microsoft Phishing Landing 2018-08-07", "ET PHISHING Observed Possible Phishing 2021-06-29", "ET PHISHING Possible Generic Phishing Landing Jul 12 2013", "ET PHISHING Dropbox Shared Document Phishing Landing Feb 21 2017", "ET PHISHING Paypal Phishing Landing Jun 28 2017", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M1", "ET PHISHING Raiffeisen Phishing Domain Nov 03 2017", "ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 30 M2", "ET PHISHING Generic PhishKit Author Comment M6 2018-08-30", "ET PHISHING IRS Phishing Landing 2016-01-15", "ET PHISHING Facebook Phishing Landing 2018-01-23", "ET PHISHING Common Form POST - Webmail Mini Phishing Landing 2020-06-11", "ET PHISHING AT&T Phishing Landing 2018-08-30", "ET PHISHING Observed Phishing Domain in DNS Lookup (microsoftonlinesupport .cf)", "ET PHISHING Suspicious Redirect - Possible Phishing May 25 2016", "ET PHISHING [TW] Robin Banks Redirect M1", "ET PHISHING Suspicious Dropbox Page - Possible Phishing Landing", "ET PHISHING PhishMe.com Phishing Landing Exercise", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M5", "ET PHISHING Common Form POST - VK Phishing Landing 2020-06-11", "ET PHISHING Generic Cryptocurrency Credential Phish Related Domain in DNS Lookup (thedoodles .site)", "ET PHISHING Paypal Phishing Landing 2018-05-02", "ET PHISHING Office 365 Phishing Landing 2018-02-06", "ET PHISHING Cloned NAB Page - Possible Phishing Landing", "ET PHISHING Lucy Security Phishing Server Reply", "ET PHISHING Observed Phish Domain in DNS Lookup (adio-gov .com) 2022-12-05", "ET PHISHING TeamIPwned/Hellion Phishing Landing 2016-08-30", "ET PHISHING BankAustria

	Phishing Domain Nov 03 2017", "ET PHISHING Suspicious File Download Post-Phishing 2016-05-25", "ET PHISHING Possible Phishing Landing Page 2021-05-24", "ET PHISHING Redirect to Adobe Shared Document Phishing M3 2016-04-18", "ET PHISHING Observed Phish Domain in DNS Lookup (enocbids .com) 2022-12-05", "ET PHISHING Possible Chase Phishing Domain Mar 14 2016", "ET PHISHING French Government COVID-19 Landing Page", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M1", "ET PHISHING Cloned Godaddy Page - Possible Phishing Landing", "ET PHISHING Possible USAA Phishing Landing 2016-07-05", "ET WEB_CLIENT Tech Support Phone Scam Landing (msg.mp3) 2016-08-12", "ET PHISHING Observed Phish Domain in DNS Lookup (ahaliahospitalae .com) 2022-12-05", "ET WEB_CLIENT Tech Support Scam - Windows Firewall M4 2021-08-17", "ET PHISHING Email Account Exceeded Quota Phishing Landing 2016-07-11", "ET WEB_CLIENT Tech Support Phone Scam Landing 2018-01-10", "ET PHISHING Suspicious Compound Refresh - Possible Phishing Redirect 2016-06-09", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M3", "ET PHISHING Observed Phish Domain in DNS Lookup (abdul-sattar-abdul-tr .com) 2022-12-05", "ET PHISHING Possible Google Docs Phishing Landing - Title over non SSL", "ET WEB_CLIENT Microsoft Tech Support Scam M1 2016-09-15", "ET PHISHING Suspicious Wordpress Redirect - Possible Phishing Landing (set) Jan 7", "ET WEB_CLIENT Tech Support Phone Scam Landing M1 2016-08-12", "ET PHISHING Possible Phishing Verified by Visa title over non SSL Feb 17 2017", "ET PHISHING AES Crypto Observed in Javascript - Possible Phishing Landing", "ET PHISHING Microsoft Live Email Account Phishing Landing Mar 16 2017", "ET PHISHING Generic PhishKit Author Comment M9 2018-08-30", "ET PHISHING Google Drive Phishing Landing 2015-07-28", "ET PHISHING Observed Phish Domain in DNS Lookup (uae-snocproject .com) 2022-12-05", "ET PHISHING Generic Encoded Phishing Landing 2021-03-10", "ET PHISHING Possible Phishing Landing via Moonfruit M2 2016-10-03", "ET WEB_CLIENT Tech Support Phone Scam Landing M2 Jul 29 2016", "ET PHISHING Microsoft Account Phishing Landing M1 2018-04-19", "ET PHISHING Observed Phish Domain in DNS Lookup (safetravel-services .com) 2022-12-05", "ET PHISHING Netflix Phishing Landing 2016-08-17", "ET PHISHING Generic Email Validation Phishing Landing 2018-02-13", "ET PHISHING Generic PhishKit Author Comment M3 2018-08-30", "ET PHISHING Adobe Shared Document Phishing Landing on Appspot Hosting", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M2", "ET PHISHING Observed Phish Domain in DNS Lookup (horsespeedtravel .com) 2022-12-05", "ET PHISHING Generic PhishKit Author Comment M10 2018-08-30", "ET PHISHING Microsoft Live Login Phishing Landing 2018-02-01", "ET PHISHING Cloned Cox Page - Possible Phishing Landing M1", "ET PHISHING Cloned Linkedin Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (enacopetroleum .com) 2022-12-05", "ET PHISHING Canada Revenue Agency COVID-19 Assistance Eligibility Phishing Landing 2020-04-01", "ET PHISHING Common Paypal Phishing URI Feb 24 2017", "ET PHISHING Google Maps Phishing Landing 2016-02-17", "ET PHISHING Capital One Phishing Landing 2018-02-13 M2", "ET PHISHING Bank of America Phishing Landing", "ET WEB_CLIENT Tech Support Scam - Windows Firewall M3 2021-08-17", "ET PHISHING Paypal Phishing Landing (DE) 2016-10-04", "ET PHISHING OneDrive Phishing Landing 2018-02-12", "ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jan 20 2017", "ET PHISHING AES Crypto Observed in Javascript - Possible Phishing Landing M1 Dec 28 2015", "ET WEB_CLIENT Microsoft Tech Support Phone Scam M2 Jul 07 2017", "ET PHISHING [TW] EvilProxy AiTM Set-Cookie", "ET PHISHING Common Form POST - Netease Webmail Phishing Landing 2020-06-11", "ET PHISHING DrSpam Phishing Landing 2016-06-08", "ET PHISHING Canada Revenue Agency Phishing Landing 2016-01-25", "ET PHISHING Javascript XOR Encoding - Observed in Apple Phishing 2016-12-09", "ET PHISHING Shared Document Base64 Phishing Landing 2016-01-20", "ET WEB_CLIENT Tech Support Phone Scam Landing 2016-07-21 M1", "ET PHISHING Possible Websc Phishing Page 2016-02-05", "ET PHISHING Observed Malicious SSL Cert (Office365 Phish Landing Page 2020-01-09)", "ET PHISHING Paypal Phishing Landing 2018-04-09", "ET PHISHING Possible Phishing Data Submitted to yolasite.com", "ET PHISHING Banque et Assurances Phishing Landing", "ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M3", "ET PHISHING Observed

	Phish Domain in DNS Lookup (bid-adnoc .com) 2022-12-05", "ET PHISHING Fedex Phishing Landing on Appspot Hosting", "ET PHISHING Possible NatWest Bank Phishing Landing - Title over non SSL", "ET PHISHING Common Form POST - Multibrand Phishing Landing 2020-06-11", "ET PHISHING DHL Phishing Landing 2018-04-09", "ET PHISHING Orange Phishing Landing 2018-02-05 (FR)", "ET PHISHING Capital One Phishing Landing 2018-02-13 M1", "ET PHISHING Anonisma AES Crypto Observed in Javascript - Possible Phishing Landing 2015-12-29", "ET WEB_CLIENT Tech Support Scam - Windows Firewall M2 2021-08-17", "ET PHISHING Apple Phishing Landing 2016-03-01 M3", "ET WEB_CLIENT Tech Support Phone Scam Landing (warning.mp3) Jan 24 2017", "ET PHISHING Google Drive Phishing Landing M1 July 24 2015", "ET PHISHING Dropbox Phishing Landing 2018-02-15", "ET PHISHING Outlook Web App Phishing Landing 2018-04-26", "ET PHISHING Apple Phishing Landing M1 Sep 14 2017", "ET PHISHING Observed Phish Domain in DNS Lookup (alfayhaatravels .com) 2022-12-05", "ET PHISHING Microsoft Questionnaire Phishing Landing 2018-01-19", "ET PHISHING Dropbox/OneDrive Phishing Landing 2018-02-07", "ET PHISHING Paypal Phishing Landing 2018-07-30", "ET PHISHING Common /mpp/ Phishing URI Structure 2016-02-08", "ET PHISHING Phishing Landing via Weebly.com (set) 2016-02-02", "ET PHISHING Google Drive Phishing Landing Jul 24 2015", "ET PHISHING Chase Mobile Phishing Landing M2", "ET PHISHING Possible Credentials Sent to Suspicious TLD via HTTP GET", "ET PHISHING DHL Phish Landing Sept 14 2015", "ET PHISHING Square Phishing Landing 2018-02-15", "ET PHISHING Excel/Adobe Online Phishing Landing Nov 25 2015", "ET PHISHING Possible Desjardins Phishing Landing - Title over non SSL", "ET PHISHING Observed Phish Domain in DNS Lookup (salacomimmigration .com) 2022-12-05", "ET WEB_CLIENT Fake AV Phone Scam Landing June 11 2015 M1", "ET PHISHING Adobe Shared Document Phishing Landing Common CSS 2016-08-10", "ET PHISHING Wells Fargo Phishing Landing 2016-01-07", "ET PHISHING Lucy Security Time Tracking POST", "ET PHISHING Adobe Shared Document Phishing Landing M2 2016-08-31", "ET PHISHING US Bank Phishing Landing", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M7", "ET PHISHING LCL Banque Phishing Landing 2018-04-19", "ET PHISHING Webmail Phishing Landing 2016-06-22", "ET PHISHING JS Obfuscation - Possible Phishing 2016-03-01", "ET PHISHING DHL Phishing Landing 2016-01-07", "ET PHISHING Generic Multi-Email Phishing Landing 2018-01-25", "ET PHISHING Apple Phishing Landing 2018-01-29 M1", "ET PHISHING Retrieve Pending Emails Phishing Landing 2018-03-12", "ET PHISHING Comcast/Xfinity Phishing Landing 2018-04-19", "ET PHISHING ASB Bank Phishing Landing 2018-02-09 M2", "ET PHISHING Cloned Chase Page - Possible Phishing Landing", "ET PHISHING iCloud Phishing Landing 2016-09-02", "ET PHISHING Adobe Online Document Phishing Landing M1 Mar 25 2017", "ET PHISHING Observed Phish Domain in DNS Lookup (abienceinvestments-fze .com) 2022-12-05", "ET PHISHING Webmail Account Upgrade Phishing Landing 2016-07-20", "ET PHISHING Phishing Landing via Webeden.co.uk M1 2016-01-22", "ET PHISHING Possible MyEtherWallet Phishing Landing - Title over non SSL", "ET PHISHING Observed Phish Domain in DNS Lookup (llhhospitals .com) 2022-12-05", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M3", "ET PHISHING Observed Phish Domain in DNS Lookup (camschooluae .com) 2022-12-05", "ET PHISHING Generic Smail Phishing Landing 2018-01-29", "ET PHISHING Common Form POST - Whatsapp/Facebook Phishing Landing 2020-06-11", "ET PHISHING Apple Phishing Landing M3 Sep 14 2017", "ET PHISHING Amazon Phish Landing Jun 22 2017", "ET PHISHING [eSentire] Wells Fargo Phishing Landing 2018-06-20", "ET PHISHING Generic Xbalti Phishing Landing 2018-11-26", "ET PHISHING Observed UK Gov Support Landing 2021-06-01", "ET PHISHING Observed Phish Domain in DNS Lookup (atenaeps .com) 2022-12-05", "ET WEB_CLIENT SocEng Fake Font Download Template Nov 14 2017", "ET PHISHING Dropbox Business Phishing Landing 2018-02-07", "ET PHISHING Phishing Landing via Weebly.com 2016-06-22", "ET PHISHING Centurylink Phishing Landing 2018-04-19", "ET INFO Trend Micro Phishing Simulation Service", "ET PHISHING Observed Phish Domain in DNS Lookup (bid-enoc .com) 2022-12-05", "ET PHISHING Cloned Dropbox Page - Possible Phishing Landing", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M3", "ET PHISHING [TW] EvilProxy AiTM Cookie Value", "ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 M2",

	"ET PHISHING Miniproxy Cloned Page - Possible Phishing Landing", "ET PHISHING Generic XBALTI Phishing Landing", "ET PHISHING Google Drive Phish Landing 2016-09-01", "ET PHISHING Microsoft Ajax Phishing Landing 2018-08-07", "ET PHISHING IRS COVID-19 Landing Page", "ET PHISHING Possible Phishing Redirect Dec 13 2016", "ET PHISHING Outlook 365 Encrypted Email Phishing Landing M1 2016-08-31", "ET PHISHING Possible Apple Phishing Domain 2016-06-14", "ET PHISHING Common Form POST - Paypal Phishing Landing 2020-06-11", "ET PHISHING Generic Credential Phishing Landing Aug 11 2015", "ET WEB_CLIENT Tech Support Phone Scam Landing M1 Oct 16 2016", "ET PHISHING Google Drive Phishing Landing Nov 6 2015 M1", "ET PHISHING Possible Generic Microsoft Hosted Phishing Landing M2", "ET WEB_CLIENT Tech Support Scam Landing Jul 19 2017", "ET PHISHING Cloned Simplii Page - Possible Phishing Landing", "ET PHISHING Generic Bank Captcha Phishing Landing", "ET PHISHING Possible Linkedin Phishing Domain Dec 09 2016", "ET PHISHING [TW] Robin Banks Redirect M2", "ET PHISHING Possible Paypal Phishing Domain Mar 14 2016", "ET PHISHING Observed Phish Domain in DNS Lookup (investinadio .com) 2022-12-05", "ET PHISHING Alibaba Phishing Landing 2016-08-31", "ET PHISHING Observed Phish Domain in DNS Lookup (proposal-ae-enoc .com) 2022-12-05", "ET PHISHING Generic PhishKit Author Comment M5 2018-08-30", "ET PHISHING DHL Phishing Landing 2016-07-11", "ET WEB_CLIENT Tech Support Scam Landing 2018-07-18", "ET PHISHING USAA Phishing Landing 2018-02-20", "ET PHISHING Yahoo Phishing Landing 2018-02-20", "ET PHISHING Stripe Phishing Landing Dec 09 2016", "ET PHISHING Outlook Web App Phishing Landing on Appspot Hosting", "ET PHISHING Observed Phish Domain in DNS Lookup (iconiqueimmigration .com) 2022-12-05", "ET PHISHING Possible Webmail Phishing Landing Utilizing Clearbit", "ET PHISHING Observed Phish Domain in DNS Lookup (flylinkimmigration .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (registration-ae-enoc .com) 2022-12-05", "ET PHISHING Office 365 Phishing Landing 2018-01-18", "ET PHISHING Common Form POST - Possible Generic Phishing Landing 2020-06-11", "ET PHISHING Suspected Appspot Hosted Phishing Domain", "ET PHISHING Possible Google Drive Phishing Landing 2015-07-13", "ET PHISHING Generic Phishing Landing 2018-01-12", "ET PHISHING Cloned American Express Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (alzarafatravellsae .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (consultant-enoc .com) 2022-12-05", "ET WEB_CLIENT Multibrowser Resource Exhaustion observed in Tech Support Scam", "ET PHISHING Generic Mailbox Phishing Landing 2018-08-30", "ET PHISHING Yahoo Password Strength Phishing Landing 2016-08-24", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M7", "ET PHISHING Adobe Shared Document Phishing Landing 2016-08-19", "ET PHISHING Chalbhai Phishing Landing Feb 18 2016", "ET PHISHING Possible Amazon Phishing Domain 2016-06-21", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M2", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M2", "ET PHISHING Chase Account Phish Landing Oct 22", "ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)", "ET PHISHING Paypal Phishing Landing 2018-01-25", "ET PHISHING Interac (CA) Account Credential Phish Landing Page 2022-09-30", "ET PHISHING PayPal Phishing Landing Nov 24 2014", "ET MALWARE Javascript Click and Removal of Download Element", "ET PHISHING IRS Phishing Landing 2018-03-28", "ET PHISHING Covid19 Stimulus Payment Phish Inbound M4 (2021-10-21)", "ET PHISHING Generic Phishing Landing M1 2017-02-13", "ET PHISHING Observed Phish Domain in DNS Lookup (consultants-ae-enoc .com) 2022-12-05", "ET PHISHING Lucy Security Phishing Landing Page M2", "ET PHISHING Chase Phish Landing 2020-11-26", "ET PHISHING Observed OneDrive Phishing Landing Page 2021-08-09", "ET PHISHING Possible Phishing Landing via MoonFruit.com (set)", "ET WEB_CLIENT Microsoft Tech Support Phone Scam Landing 2018-09-12", "ET PHISHING Chalbhai Phishing Landing 2020-06-22", "ET PHISHING Linkedin Phishing Landing 2018-08-30", "ET PHISHING Observed Phish Domain in DNS Lookup (emarataljabrisolicitors .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (rakpetrolae .com) 2022-12-05", "ET PHISHING Cloned Website Phishing Landing - Mirrored Website Comment Observed", "ET PHISHING Paypal Phishing Redirect M1 Feb 24 2017", "ET

	PHISHING Observed Phish Domain in DNS Lookup (bidders-enoc .com) 2022-12-05", "ET PHISHING Possible Phishing Landing via Moonfruit M2 2016-01-26", "ET PHISHING Apple Phishing Landing Jan 30 2014", "ET PHISHING Observed Phish Domain in DNS Lookup (adbntogo .com) 2022-12-05", "ET PHISHING [TW] EvilProxy AiTM Username Checkin", "ET WEB_CLIENT Apple Tech Support Phone Scam Jul 07 2017", "ET PHISHING Anonisma Phishing Landing 2015-12-01", "ET PHISHING Post.ch Cloned Phishing Landing 2018-04-09", "ET PHISHING USPS Phishing Landing 2016-02-10", "ET PHISHING Observed Phish Domain in DNS Lookup (fenczyflyemiratetravels .com) 2022-12-05", "ET PHISHING Apple Account Phishing Landing 2015-11-18", "ET PHISHING Facebook Mobile Phishing Landing 2018-02-26", "ET PHISHING Impots.gouv.fr Phishing Landing 2018-01-30", "ET PHISHING Chalbhai Phishing Landing Oct 23 2017", "ET PHISHING Covid19 Stimulus Payment Phish Inbound M3 (2021-10-21)", "ET PHISHING Observed Phish Domain in DNS Lookup (administrator-enoc .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (snocprojectuae .com) 2022-12-05", "ET PHISHING Smartsheet Phishing Landing 2018-01-29", "ET PHISHING Instagram Fake Copyright Infringement Hosted on 000webhostapp", "ET PHISHING Generic PhishKit Author Comment M1 2018-08-30", "ET PHISHING Amazon Phishing Landing (DE) 2018-02-26", "ET PHISHING Observed Phish Domain in DNS Lookup (vendor-enocbid .com) 2022-12-05", "ET PHISHING Google Drive Phishing Landing 2018-04-14", "ET PHISHING Cloned Instagram Page - Possible Phishing Landing M3", "ET PHISHING Successful Generic Credential Phish (.ngrok .io)", "ET PHISHING HM Revenue Phishing Landing", "ET PHISHING Christian Mingle Phishing Landing 2018-08-07", "ET WEB_CLIENT Fake AV Phone Scam Domain M3 Mar 3", "ET PHISHING France Ministry of Action and Public Accounts Phish Landing", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M4", "ET PHISHING Synchronize Email Account Phishing Landing 2016-07-15", "ET PHISHING Comcast/Xfinity Phishing Landing 2018-03-30", "ET PHISHING Wells Fargo Phishing Landing 2018-02-13", "ET PHISHING Observed Phish Domain in DNS Lookup (tenders-aisschools .com) 2022-12-05", "ET WEB_CLIENT Fake Update/Installer ForceDL Template Nov 03 2017", "ET PHISHING Instagram Phishing Landing 2020-10-13", "ET PHISHING Cloned La Banque Postale FR Page - Possible Phishing Landing", "ET PHISHING Cloned Match Dating Page - Possible Phishing Landing", "ET PHISHING Paypal Phishing Landing 2018-01-18 M2", "ET PHISHING Base64 Data URI Javascript Refresh - Possible Phishing Landing", "ET PHISHING Phishing Landing via Weebly.com M3 2016-02-02", "ET PHISHING Netflix Phishing Landing 2018-05-02", "ET PHISHING Cloned Comcast / Xfinity Page - Possible Phishing Landing", "ET PHISHING Mailbox Phishing Landing 2018-01-29", "ET PHISHING Caixa Phishing Landing", "ET PHISHING Suntrust Captcha Phishing Landing", "ET PHISHING Generic Custom Logo Phishing Landing", "ET PHISHING Navy Federal Credit Union Phishing Landing 2016-01-30", "ET PHISHING Paypal Phishing Landing Feb 24 2017", "ET WEB_CLIENT Tech Support Phone Scam Landing M5 Jun 3", "ET PHISHING Office 365 Phishing Landing 2018-01-25", "ET PHISHING Mailgun Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (emsclikoil .com) 2022-12-05", "ET PHISHING Possible HMRC Phishing Domain 2016-06-08", "ET PHISHING Common Form POST - Linkedin Phishing Landing 2020-06-11", "ET PHISHING Google Drive Phishing Landing Nov 6 2015 M2", "ET PHISHING Microsoft Office Phishing Landing 2016-12-18", "ET PHISHING Possible YapiKredi Bank (TR) Phishing Landing - Title over non SSL", "ET PHISHING ASB Bank Phishing Landing 2018-02-09 M1", "ET PHISHING Sparkasse Phishing Landing 2018-02-15", "ET PHISHING Paypal Phishing Landing", "ET PHISHING Common Form POST - Chase Phishing Landing 2020-06-11", "ET PHISHING Generic Email Login Phishing Landing 2016-06-02", "ET PHISHING Outlook Phishing Landing 2020-10-23", "ET PHISHING Cloned Microsoft Office Apps Page - Possible Phishing Landing", "ET PHISHING Paypal Phishing Landing 2018-01-18 M1", "ET WEB_CLIENT Fake AV Phone Scam Landing July 20 2015 M2", "ET PHISHING Anonisma Phishing CSS 2015-12-01", "ET PHISHING Potential Data URI Phishing Oct 02 2015", "ET PHISHING [eSentire] DHL Phish Landing July 24 2018", "ET PHISHING Microsoft Account Phishing Landing", "ET PHISHING [eSentire] Adobe Phishing Landing 2018-07-04", "ET PHISHING PHOEN!X Apple Phish Landing Page 2015-12-29", "ET PHISHING Bank of America

	Phishing Landing Aug 19 2015", "ET PHISHING Common Form POST - Cox Phishing Landing 2020-06-11", "ET PHISHING Mailbox Renewal Phish Landing Nov 13", "ET PHISHING Possible Cartasi Phishing Domain Nov 08 2016", "ET PHISHING Microsoft Onedrive Phishing Landing 2018-01-29", "ET PHISHING Cloned Instagram Page - Possible Phishing Landing M2", "ET PHISHING DHL Phishing Landing 2016-08-31", "ET PHISHING Cloned IRS Page - Possible Phishing Landing", "ET PHISHING DHL Phish Landing 2015-11-14", "ET PHISHING Phishing Landing via Webeden.co.uk (set) 2016-01-22", "ET PHISHING Suspicious Byethost Phishing Redirect 2016-10-04", "ET PHISHING Fake World Health Organization COVID-19 Portal 2020-03-20", "ET PHISHING Suspicious HTML Hex Obfuscated Title - Possible Phishing Landing Jun 28 2017", "ET PHISHING Suspicious TikTok Domain Request - Possible Phishing or Scam", "ET PHISHING Office 365 Phishing Landing", "ET PHISHING Generic Hidden Text - Possible Phishing Landing", "ET PHISHING Successful Generic Phish Observed", "ET PHISHING Possible Phishing Blockchain title over non SSL Jul 10 2017", "ET PHISHING Phishing Landing via Weebly.com M4 2016-02-02", "ET PHISHING Successful Credential Phish M1 2022-09-23", "ET PHISHING Chrome Extension Phishing HTTP Request", "ET PHISHING Possible Tsukuba Banker Edwards Packed proxy.pac", "ET PHISHING Observed Phish Domain in DNS Lookup (diligencefinconsultants .com) 2022-12-05", "ET HUNTING Suspicious Netlify Hosted GET Request - Possible Phishing Landing", "ET PHISHING Phishing Landing via Tripod.com M1 2016-03-31", "ET PHISHING LCL Banque et Assurance (FR) Phishing Landing 2018-01-23", "ET MALWARE Javascript Displays malicious download page", "ET PHISHING Spox Phishkit HTTP POST Observed", "ET PHISHING Mailbox Upgrade Phishing Landing 2018-02-05", "ET PHISHING WeTransfer Phishing Landing 2018-08-30", "ET PHISHING Observed Phish Domain in DNS Lookup (nowmcopetroleum .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (gulfcoastoilngas-ae .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (hpschooluae .com) 2022-12-05", "ET PHISHING [TW] Robin Banks HTTP GET Struct", "ET PHISHING Observed Phish Domain in DNS Lookup (emspgenerahospae .com) 2022-12-05", "ET PHISHING Possible Instagram Phishing Domain", "ET PHISHING Observed Phish Domain in DNS Lookup (dibfinancialservice-uae .com) 2022-12-05", "ET PHISHING Phishing Landing via Weebly.com M2 2016-02-02", "ET PHISHING Observed Phish Domain in DNS Lookup (contract-snoc .com) 2022-12-05", "ET PHISHING Wells Fargo Phishing Landing 2018-02-12", "ET PHISHING Possible Protonmail Phishing Domain in DNS Query", "ET PHISHING Base64 HTTP URL Refresh - Common Phish Landing Obfuscation 2016-01-01", "ET PHISHING Facebook Phishing Landing 2016-09-02", "ET PHISHING LinkedIn Phishing Landing 2018-02-09 M1", "ET PHISHING Possible OWA Mail Phishing Landing - Title over non SSL", "ET PHISHING Observed Phish Domain in DNS Lookup (snoc-projectuae .com) 2022-12-05", "ET PHISHING MyADP Phishing Landing 2018-04-19", "ET PHISHING Wells Fargo Phishing Landing 2018-02-09", "ET PHISHING Apple AES Phishing Landing 2018-08-30", "ET HUNTING Suspicious Netlify Hosted TLS SNI Request - Possible Phishing Landing", "ET PHISHING Paypal Phishing Landing 2018-05-09", "ET PHISHING Possible barclays .co. uk Phishing Domain 2016-06-22", "ET PHISHING OneDrive Phishing Landing 2020-04-10", "ET PHISHING Blocked Email Account Phishing Landing 2016-08-23", "ET PHISHING OneDrive Phishing Landing 2018-05-01", "ET PHISHING Possible TSB Bank Phishing Landing 2018-05-07", "ET PHISHING Adobe Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (tenders-adio .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (snocproject-ae .com) 2022-12-05", "ET PHISHING TSB Bank / Lloyds Bank Phishing Landing 2018-02-01", "ET PHISHING Possible BMO Bank of Montreal Phishing Landing - Title over non SSL", "ET PHISHING Observed Phish Domain in DNS Lookup (registrations-adnoc .com) 2022-12-05", "ET PHISHING Spox Phishkit Landing Page Inbound", "ET PHISHING Facebook Upgrade Payment Phishing Landing 2018-02-05", "ET PHISHING Linkedin Phishing Landing on Appspot Hosting", "ET PHISHING Generic PhishKit Author Comment M7 2018-08-30", "ET PHISHING Docusign Phishing Landing Hosted via Weebly", "ET PHISHING Possible Bank of America Phishing Domain Aug 15 2016", "ET PHISHING Observed Phish Domain in DNS Lookup (zirvaenergy .com) 2022-12-05", "ET PHISHING Possible Fedex Phishing Landing 2015-07-28", "ET PHISHING

	Observed Phish Domain in DNS Lookup (gulfmarineoilservices .com) 2022-12-05", "ET WEB_CLIENT Fake AV Phone Scam Landing Feb 12", "ET PHISHING iTunes Connect Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (dahilalcapitalinvest .com) 2022-12-05", "ET PHISHING Hellion Postmaster Phishing Landing 2018-01-31", "ET PHISHING LinkedIn Phishing Landing 2018-02-13", "ET PHISHING Possible Discover Phishing Domain Feb 02 2017", "ET PHISHING L33bo Phishing Landing 2016-03-29", "ET PHISHING Spotify Phishing Landing 2020-04-14", "ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M4", "ET PHISHING Observed OWA Phishing Landing Page 2021-08-20", "ET PHISHING Generic Phishing Kit Landing", "ET PHISHING Account Update Phishing Landing 2016-09-06", "ET PHISHING Docusign Phishing Landing Mar 08 2017", "ET PHISHING Facebook Phishing Landing 2018-02-12", "ET PHISHING Observed Phishing Domain in DNS Lookup (infollnes-r-us .co .uk)", "ET PHISHING Mail Verification Phishing Landing 2018-04-18", "ET PHISHING Chase Phishing Landing 2018-02-07", "ET PHISHING Apple Suspended Account Phishing Landing Aug 09 2016", "ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M2", "ET PHISHING Observed Phish Domain in DNS Lookup (biding-enoc .com) 2022-12-05", "ET WEB_CLIENT Tech Support Scam Landing M2 2019-04-15", "ET PHISHING Observed Phish Domain in DNS Lookup (toursolutions4u .com) 2022-12-05", "ET PHISHING Possible Halkbank (TK) Phishing Landing - Title over non SSL", "ET PHISHING Generic Paypal Phish Kit Landing", "ET PHISHING LinkedIn Phishing Landing 2017-07-20", "ET PHISHING Observed Possible Phishing Landing Page 2021-06-22", "ET PHISHING Wells Fargo Phishing Landing 2018-04-09", "ET PHISHING Possible Google Drive/Dropbox Phishing Landing Jul 10 2015", "ET PHISHING Office 365 Credential Harvesting Domain (rightofcourse .com) in TLS SNI", "ET PHISHING Office 365 Credential Harvesting Domain (rightofcourse .com) in DNS Lookup", "ET PHISHING Possible CIBC Phishing Landing - Title over non SSL", "ET WEB_CLIENT Fake AV Phone Scam Landing Apr 4", "ET PHISHING Possible USAA Phishing Domain Mar 14 2016", "ET PHISHING Adobe Online Document Phishing Landing M1 2016-04-25", "ET PHISHING Adobe Online Document Phishing Landing M2 2016-04-25", "ET PHISHING Observed Phish Domain in DNS Lookup (globalhospae .com) 2022-12-05", "ET WEB_CLIENT Tech Support Phone Scam Landing (err.mp3) 2016-08-12", "ET PHISHING Facebook Phishing Landing 2018-02-13 M2", "ET WEB_CLIENT Tech Support Scam Landing 2020-08-19", "ET PHISHING Suspicious Credential POST to FormBuddy.com - Possible Phishing Aug 10 2016", "ET PHISHING Microsoft Account Phishing Landing on Appspot Hosting", "ET PHISHING Cloned Itscom Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (mohregov-ae .com) 2022-12-05", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M5", "ET WEB_CLIENT Tech Support Phone Scam Landing Feb 09 2017", "ET PHISHING Cloned EWE Telecom Page - Possible Phishing Landing", "ET PHISHING Covid19 Stimulus Payment Phish Inbound M2 (2021-10-21)", "ET PHISHING Observed Phish Domain in DNS Lookup (siemenoilandgas .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (quickcitytravel .com) 2022-12-05", "ET WEB_CLIENT Generic Fake Support Phone Scam Mar 9 M3", "ET PHISHING Cloned RBC Royal Bank Page - Possible Phishing Landing", "ET PHISHING Apple Phishing Landing M2 Sep 14 2017", "ET PHISHING Microsoft Account Phishing Landing M2 2018-04-19", "ET PHISHING Observed Phish Domain in DNS Lookup (bid-taqa .com) 2022-12-05", "ET PHISHING Am3Refh Obfuscated Phishing Landing 2016-02-23", "ET PHISHING Observed Phish Domain in DNS Lookup (alhmodzinoilfildservices .com) 2022-12-05", "ET PHISHING Team IPwned Phishing Landing 2016-08-24", "ET WEB_CLIENT Fake Virus Phone Scam Landing Mar 9 M2", "ET PHISHING Possible Generic Antibots Phishing Landing 2018-02-05", "ET INFO Suspected Phishing Simulation Service Domain in DNS Lookup (employees-portal .com)", "ET INFO Suspected Phishing Simulation Service Activity", "ET HUNTING Suspicious Netlify Hosted DNS Request - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (builds-emaar .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (biddings-enoc .com) 2022-12-05", "ET PHISHING Facebook Phishing Landing", "ET PHISHING Possible Phishing Redirect Feb 09 2016", "ET PHISHING Microsoft Account Login Hosted on Firebasestorage", "ET WEB_CLIENT Tech Support Phone Scam Landing M2 Oct 16

	2016", "ET PHISHING Possible Phishing Landing - Data URI Inline Javascript 2016-02-09", "ET PHISHING Observed Phish Domain in DNS Lookup (contractor-enoc .com) 2022-12-05", "ET WEB_CLIENT Generic Fake Support Phone Scam Mar 8", "ET PHISHING Bank of America Phishing Landing 2018-08-30", "ET PHISHING Blocked Incoming Emails Phishing Landing 2018-01-23", "ET PHISHING Possible Free Mobile Phishing Landing - Title over non SSL", "ET PHISHING Instagram Phishing Landing 2020-04-10", "ET PHISHING Possible Generic Phishing Landing Jul 28 2015", "ET PHISHING Cloned Spotify Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (rambolloil .com) 2022-12-05", "ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jun 29 2016", "ET PHISHING Cloned Discover Page - Possible Phishing Landing", "ET WEB_CLIENT Tech Support Phone Scam Landing Dec 30 M1", "ET PHISHING Apple Phishing Landing 2015-07-27", "ET PHISHING Generic Financial Phone Support Scam/Phishing Landing M1", "ET MALWARE Domen SocEng Redirect - Landing Page Observed", "ET PHISHING Possible Phishing Landing via MoonFruit.com M2 2016-01-22", "ET PHISHING Generic Personalized Google Firebase Hosted Phishing Landing", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M4", "ET PHISHING Facebook Phishing Landing 2018-02-13 M1", "ET PHISHING Cloned Google Tools Page - Possible Phishing Landing", "ET PHISHING Chase Phishing Landing 2018-01-18", "ET WEB_CLIENT Fake AV Phone Scam Landing June 16 2015 M4", "ET PHISHING DNS Query to Generic 107 Phishing Domain", "ET PHISHING s0m3 Phishing Landing 2018-04-09", "ET PHISHING Successful Credential Phish M2 2022-09-23", "ET PHISHING Paypal Phishing Landing Jan 09 2017", "ET PHISHING Phishing Fake Document Loading Error 2015-10-01", "ET PHISHING Observed Phish Domain in DNS Lookup (registration-adnoc .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (proposals-ae-enoc .com) 2022-12-05", "ET PHISHING Observed Phish Domain in DNS Lookup (tenders-adnoc .com) 2022-12-05", "ET PHISHING Possible Paypal Phishing Domain (IT) Oct 10 2017", "ET PHISHING [TW] Robin Banks HTTP HOST M2", "ET PHISHING Email Server Mobile Security Settings Phishing Landing 2018-01-22", "ET PHISHING Possible Chase Phishing Landing - Title over non SSL", "ET PHISHING Craigslist Phishing Landing 2018-02-26", "ET PHISHING Possible Office 365 Phishing Landing 2016-08-24", "ET PHISHING Observed Phish Domain in DNS Lookup (aiischools .com) 2022-12-05", "ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M3", "ET PHISHING Possible Yahoo Phishing Landing - Title over non SSL", "ET PHISHING Suspicious Browser Plugin Detect - Observed in Phish Landings", "ET PHISHING Microsoft Live External Link Phishing Landing M2 Feb 14 2017", "ET PHISHING Universal Webmail Phishing Landing 2016-08-19", "ET PHISHING Possible iTunes Phishing Landing - Title over non SSL", "ET PHISHING Apple Phishing Landing 2016-03-01 M2", "ET PHISHING Possible Phishing Landing via MoonFruit.com M3 2016-01-22", "ET PHISHING Phishing Landing via Webeden.net 2016-10-13", "ET PHISHING Cloned Yahoo Page - Possible Phishing Landing", "ET PHISHING Observed Phish Domain in DNS Lookup (easternbaytravels .com) 2022-12-05", "ET PHISHING Lucy Security Phishing Landing Page M1", "ET PHISHING Observed Phish Domain in DNS Lookup (registrations-enoc .com) 2022-12-05", "ET WEB_CLIENT Tech Support Phone Scam Landing 2017-07-26", "ET PHISHING Amazon Phishing Landing 2020-10-13", "ET PHISHING Fedex Javascript Phishing Landing 2016-09-08", "ET PHISHING Observed Phish Domain in DNS Lookup (abbrossgeneralhospital .com) 2022-12-05", "ET WEB_CLIENT Fake AV Phone Scam Domain M1 Mar 3", "ET PHISHING Observed Phish Domain in DNS Lookup (tender-adnoc .com) 2022-12-05", "ET PHISHING Adobe PDF Phishing Landing 2018-08-30", "ET PHISHING Cloned Fidelity Page - Possible Phishing Landing", "ET PHISHING Apple ID Phishing Landing 2015-08-19", "ET PHISHING Tech Support/Refund Scam Landing Inbound 2022/04/25", "ET HUNTING Suspicious Glitch Hosted DNS Request - Possible Phishing Landing", "ET PHISHING Generic Phishing Landing Hosted via Weebly", "ET PHISHING Observed Phish Domain in DNS Lookup (duramtravelagency .com) 2022-12-05", "ET PHISHING Phishing Landing via Weebly.com M1 2016-02-02", "ET PHISHING Cloned Ziggo NL Page - Possible Phishing Landing", "ET PHISHING Possible Instagram Phishing or Scam Landing Page", "ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M8", "ET PHISHING Facebook Phishing Landing 2018-02-14", "ET PHISHING

	Possible Alibaba Phishing Landing - Title over non SSL", "ET PHISHING Anonisma Paypal Phishing Loading Page 2015-12-29", "ET PHISHING Observed Phishing Domain in DNS Lookup (circle-ci .com)", "ET PHISHING Possible Paypal Phishing Landing - Title over non SSL", "ET PHISHING Phishing Landing via Tripod.com (set) 2016-03-31", "ET PHISHING Webmail Account Upgrade Phishing Landing 2016-07-15", "ET PHISHING Observed Phish Domain in DNS Lookup (consultant-ae-enoc .com) 2022-12-05", "ET PHISHING Cloned Instagram Page - Possible Phishing Landing M1", "ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M5", "ET PHISHING Generic Goth Phishing Landing", "ET PHISHING Possible DHL Phishing Landing - Title over non SSL", "ET PHISHING Paypal Phishing Landing 2018-01-03", "ET PHISHING Generic NewInjection Phishing Landing 2021-03-10", "ET PHISHING Possible Phishing Landing - Data URI Inline Javascript Mar 07 2016", "ET WEB_CLIENT Fake Video Player Update Scam Oct 30", "ET PHISHING Google Drive Phishing Landing 2015-11-06", "ET PHISHING Generic T.Goe Phishing Landing", "ET PHISHING Cloned CIBC Bank Page - Possible Phishing Landing M1", "ET PHISHING Fake Webmail Account Phishing Landing 2015-09-10", "ET WEB_CLIENT Tech Support Scam 2019-11-14", "ET PHISHING Adobe Phishing Landing 2018-08-07", "ET PHISHING Outlook Webapp Phishing Landing on Appspot Hosting", "ET PHISHING Assurance Maladie Phishing Landing", "ET PHISHING Upgrade Email Account Phishing Landing 2018-03-12", "ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M1", "ET PHISHING Wire Transfer Phishing Landing 2015-11-19", "ET PHISHING Suspicious Google Docs Page - Possible Phishing Landing", "ET PHISHING Cloud Drive Phish Landing 2015-08-12", "ET PHISHING Possible Phishing Landing - Zeus365 Encoding", "ET PHISHING Github Phishing Landing 2018-07-19"
Попытки выполнить системный вызов	"GPL SHELLCODE sparc setuid 0"
GeoIP Страны Юго-Восточной Азии	"GeoIP Индонезия", "GeoIP Тайланд", "GeoIP Лаос", "GeoIP Бруней Даруссалам", "GeoIP Филиппины", "GeoIP Сингапур", "GeoIP Вьетнам", "GeoIP Малайзия", "GeoIP Восточный Тимор", "GeoIP Мьянма", "GeoIP Камбоджа"
GeoIP Страны Восточной Европы	"GeoIP Литва", "GeoIP Словакия", "GeoIP Польша", "GeoIP Эстония", "GeoIP Латвия", "GeoIP Украина", "GeoIP Молдова", "GeoIP Румыния", "GeoIP Болгария", "GeoIP Чехия", "GeoIP Венгрия"
Блокирование некорректных попыток получения привилегий пользователя	"GPL NETBIOS SMB-DS repeated logon failure", "ET SCAN Potential FTP Brute-Force attempt response", "GPL NETBIOS SMB repeated logon failure", "GPL RPC rexec username too long response", "GPL RPC rlogin login failure", "GPL SQL sa login failed", "GPL SQL sa brute force failed login attempt", "GPL POLICY PCAnywhere Failed Login", "GPL SQL sa brute force failed login unicode attempt", "GPL MISC Invalid PCAnywhere Login"
Использование DNS трафика для управления вредоносным ПО	"ET MALWARE BlackMatter CnC Domain in DNS Lookup (paymenthacks .com)", "ET MALWARE Observed Malicious SSL Cert (CobInt CnC)", "ET MOBILE_MALWARE Arid Viper (fasebcak .co in DNS Lookup)", "ET MOBILE_MALWARE Arid Viper (fasebaok .co in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (MageCart Staging Domain)", "ET MALWARE Observed Malicious SSL Cert (MassLogger)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-chat .xyz)", "ET MALWARE DPRK APT Related Domain in DNS Lookup (cryptais .com)", "ET MALWARE Observed Malicious SSL Cert (StrongPity Domain)", "ET MALWARE Observed Lazarus Maldoc CnC Domain (shopweblive .com in TLS SNI)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (scannermcscanface-edgescan .com)", "ET MALWARE Mustang Panda APT PlugX Related Domain in DNS Lookup (hilifimyanmar .com)", "ET MALWARE Observed Gamaredon APT Related Domain (dwn-files .shop in TLS SNI)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (marwapetersson .info)", "ET MALWARE Observed Malicious SSL Cert (Turla/APT34 CnC Domain)", "ET MALWARE Magniber Ransomware CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Observed APT-C-23 Related Domain (linda-gaytan .website in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ksew .kpt-gov .org)", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (f15fwd322 .regularhours .net)", "ET MALWARE PoetRAT CnC Domain in DNS Lookup", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (number1g .top in TLS SNI)",

	"ET MALWARE Cobalt Strike Related Domain in DNS Lookup (ledikexive .com)", "ET MALWARE Chaos Botnet CnC Domain (a .nqb001 .com) in DNS Lookup", "ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)", "ET MOBILE_MALWARE Arid Viper (stand-by-97c5c .firebaseio .com in DNS Lookup)", "ET MALWARE Observed DarkSide Ransomware Domain (catsdegree .com in TLS SNI)", "ET MALWARE Gamaredon CnC Observed in DNS Query", "ET MALWARE Observed Malicious SSL/TLS Certificate (Knotweed/SubZero)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-chat .xyz)", "ET MALWARE Phorpiex CnC Domain in DNS Query", "ET MALWARE Qakbot/Cobalt Strike Domain (tevokaxol .com) in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-cdn .xyz)", "ET MALWARE Donot APT Related Domain in DNS Lookup (biteupdates .live)", "ET MALWARE Observed OSX/GMERA.A CnC Domain (appstockfolio .com in TLS SNI)", "ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .website)", "ET MALWARE Win32\Cryptbot CnC Domain (suqzpe02 .top) in DNS Lookup", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (flowersarrows .com)", "ET MALWARE Win32\Cryptbot CnC Domain (okwnyw02 .top) in DNS Lookup", "ET MALWARE CN Based APT Related Domain in DNS Lookup (sign .sanaqsign .org)", "ET MALWARE TeamTNT Gattling Gun CnC Domain in DNS Lookup", "ET MALWARE Observed Ursnif Domain in TLS SNI", "ET MALWARE Observed BazarLoader Domain (doldig .xyz in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (jennifer-marler .pw in DNS Lookup)", "ET MALWARE DPRK APT Related Domain in DNS Lookup (tokenais .com)", "ET MALWARE Win32\Cryptbot CnC Domain (suqycd05 .top) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (APT29)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-schnellvpn .com)", "ET MOBILE_MALWARE Android.Trojan.Rana.A (fullplayersoftware .com in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)", "ET MALWARE Observed DangerousPassword APT Related Domain (cop .osonlines .co in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)", "ET MALWARE Chaos Botnet CnC Domain (ai .nqb001 .com) in DNS Lookup", "ET MALWARE Patchwork Staging Domain in DNS Query", "ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (msstore .io)", "ET MALWARE TransparentTribe CnC Domain in DNS Lookup", "ET MALWARE Magecart CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (SilentLibrarian)", "ET MALWARE ChromeLoader CnC Domain (imenttogethe .xyz) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (wendy-johnston .pw in DNS Lookup)", "ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .info)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-endpoint .xyz)", "ET MALWARE Observed CobaltStrike/TEARDROP CnC Domain Domain in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-chat .com)", "ET MALWARE Observed DonotGroup CnC in DNS Query", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (unicornhub .top)", "ET MALWARE FerociousKitten CnC Domain in DNS Lookup (microsoft .microcaft .xyz)", "ET MALWARE Observed DNS Query to Ursnif CnC Domain (horulenuke .us)", "ET MALWARE TA444 Domain in DNS Lookup (gdocshare .one)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (notixow .com)", "ET MALWARE Observed StrongPity CnC Domain in TLS SNI", "ET MALWARE Observed Glupteba CnC Domain (zaoshang .ooo in TLS SNI)", "ET MALWARE Qakbot/Cobalt Strike Domain (vopaxafi .com) in DNS Lookup", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (mail .igov-service .net)", "ET MALWARE Observed Malicious SSL Cert (IcedID CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (ellechina .online)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Zeus CnC)", "ET MALWARE Observed Malicious SSL Cert (More_eggs CnC)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (gimmegimmejimmy .top in TLS SNI)", "ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Malicious Browser Ext CnC)", "ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .site)", "ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .xyz)", "ET MALWARE Chaos Botnet CnC Domain (abc .cfed .cc) in DNS Lookup", "ET MALWARE Chaos Botnet CnC Domain (bb .hash3688 .com) in DNS

	Lookup", "ET MALWARE Win32\Cryptbot CnC Domain (towhfs22 .top) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (fasebcck .com in DNS Lookup)", "ET MALWARE Observed DNS Query to Ursnif CnC Domain (vorulenuke. us)", "ET MALWARE Observed Glupteba CnC Domain (checkpos .net in TLS SNI)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (notfiled .com)", "ET MALWARE Donot APT Related Domain in DNS Lookup (submitonline .club)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)", "ET MALWARE RedDelta Poison Ivy Domain in DNS Lookup", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (whatsthescore .top in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Ursnif Injects)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (scorerabbate .site)", "ET MALWARE Confucious APT CnC Domain (microsoftonedriver .com) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (FIN7/GRIFFON CnC)", "ET MALWARE Observed Malicious SSL Cert (Possible Godlua CnC)", "ET MALWARE TA453 Related CnC Domain in DNS Lookup (0storageatools0 .xyz)", "ET MALWARE Observed Malicious SSL Cert (FIN8 ShellTea CnC)", "ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (theguardian .webredirect .org)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (footballstar .top in TLS SNI)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 8", "ET MALWARE Inception Group CnC Observed in DNS Query (ms-check-new-update .com)", "ET MOBILE_MALWARE Arid Viper (es-last-telegram .firebaseio .com in DNS Lookup)", "ET MALWARE APT28/Sofacy Zebrocy CnC DNS Lookup (support-cloud .life)", "ET MALWARE Microcin Backdoor Related Domain in DNS Lookup (holdmem .dbhubspi .com)", "ET MALWARE WinGo/YT Stealer CnC Domain in DNS Lookup", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (qh2020 .org)", "ET MALWARE Observed APT41 Malicious SSL Cert (ColunmTK Campaign)", "ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (ebook .port25 .biz)", "ET MALWARE Shuckworm CnC Domain (leonardis .ru) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (FIN8 CnC)", "ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (newtrendmicro .com)", "ET MALWARE TA444 Related Domain in DNS Lookup (cloud .prosec .ink)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (log .exposedbotnets .ru)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (lump .semara .ru)", "ET MALWARE Malicious SSL Certificate detected (Patchwork CnC)", "ET MALWARE Observed Upatre CnC Domain in TLS SNI", "ET MALWARE Maldoc CnC Domain in DNS Lookup", "ET MALWARE SHARPEXT CnC Domain in DNS Lookup (gonamod .com)", "ET MALWARE TA444 Related Domain in DNS Lookup (meeting .work .gd)", "ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (trustdomains .net)", "ET MALWARE RShell CnC Domain (linux .updatelive-oline .com) in DNS Lookup", "ET MALWARE Shuckworm CnC Domain (a0698649 .xsph .ru) in DNS Lookup", "ET MALWARE Observed DNS Query to TA444 Domain (mufg .tokyo)", "ET MALWARE ErbiumStealer CnC Domain (mamamiya137 .ru) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (followmeasap13 .top)", "ET MALWARE EvilNum APT Related Domain in DNS Lookup (bookaustriavisit .com)", "ET MALWARE Observed BazarLoader Domain (cntrhum .xyz in TLS SNI)", "ET MALWARE Observed BLINDINGCAN Domain (www .automercado .co .cr in TLS SNI)", "ET MALWARE Win32\Cryptbot CnC Domain (suqyqu10 .top) in DNS Lookup", "ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (thelegendofberia .top)", "ET MALWARE Targeted Activity - CnC Domain in SNI", "ET MALWARE Observed Win32.Raccoon Stealer Domain (cheapfacechange .top in TLS SNI)", "ET MALWARE Observed DNS Query to Buer - DomainInfo Domain", "ET MALWARE Unk/LNKR CnC Domain Observed in DNS Query", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (tapewormorchestra .top in TLS SNI)", "ET MALWARE Transparent Tribe APT Related Domain in DNS Lookup", "ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (dmnadmin .com)", "ET MALWARE Observed Malicious SSL Cert (Unattributed CnC)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 1/2 Staging Domain)", "ET MALWARE DPRK APT Related Domain in DNS Lookup (dafom .dev)", "ET MALWARE

	Observed Malicious SSL Cert (OceanLotus APT CnC)", "ET MALWARE APT41 CnC Domain (www .vietsovspeedtest .com) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC)", "ET MALWARE DNS Query to MINEBRIDGE CnC Domain (fatoftheland .top)", "ET MALWARE Chaos Botnet CnC Domain (kivspace .xyz) in DNS Lookup", "ET MALWARE Observed Jupyter Stealer CnC Domain (blackl1vesmatter .org in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Turla CnC)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (birdmilk .top in TLS SNI)", "ET MALWARE Observed Cobalt Strike CnC Domain (onlineworkercz .com in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (tim-jordan .info in DNS Lookup)", "ET MALWARE IceXLoader CnC Domain (www .filifilm .com .br) in DNS Lookup", "ET MALWARE Thallium CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Maldoc/Zloader CnC)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bahriafoundation .live)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-chat .com)", "ET MALWARE Octopus Energy Themed Trojan CnC Domain (docusign-octopus-energy .com) in DNS Lookup", "ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (mykessef .com)", "ET MALWARE APT10 Related Domain in DNS Lookup (08mma .com)", "ET MALWARE SoulSearcher Malware Domain in DNS Lookup (community .weblives .net)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (heroofthe .top)", "ET MOBILE_MALWARE Arid Viper (fasebcoki .com in DNS Lookup)", "ET MALWARE Donot APT Related Domain in DNS Lookup (soundvista .club)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (ser .dermlogged .xyz)", "ET MALWARE Observed Malicious SSL Cert (TaurusStealer CnC)", "ET MALWARE Observed Malicious SSL Cert (Donot Group/APT-C-35 CnC)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (office360-expert .online)", "ET MALWARE Gh0st Variant CnC Domain in DNS Lookup (rninhsss .com)", "ET PHISHING Observed DNS Query to Phishing Domain (apiujpnkbrhsdn57oi0ns0qmbaj0wcdzjhblj6frlh1tr .eur .lc)", "ET MALWARE NOBELIUM (TA421) CEELOADER CnC Domain in DNS Lookup", "ET MALWARE NIGHTSCOUT Malware CnC Domain in DNS Lookup (update .boshiamys .com)", "ET MALWARE Unknown CN Related APT Domain in DNS Lookup (upportteam .lingrevelat .com)", "ET MALWARE Observed Malicious Domain Targeting Minority Groups (tcahf .org in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21 3)", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (nicholasuhl .website)", "ET MOBILE_MALWARE Arid Viper (kentporter .site in DNS Lookup)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (notburpcollaborator .net)", "ET MALWARE Observed Malicious Powershell Payload Delivery Domain (onerecovery .click) in TLS SNI", "ET MALWARE Win32\Cryptbot CnC Domain (suqzyt03 .top) in DNS Lookup", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (smoothcbots .xyz in TLS SNI)", "ET MALWARE TA444 Related Domain in DNS Lookup (cloudprotect .us .org)", "ET MALWARE DCRat Related CnC Domain in DNS Lookup", "ET MALWARE SteamStealer Malicious SSL Certificate Detected", "ET MALWARE Windows/OriginLogger CnC Domain (originpro .me) in DNS Lookup", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (avira .ltd) in DNS Lookup", "ET MALWARE Bitter APT Related Domain in DNS Lookup (signalpremium .com)", "ET POLICY dnslog .cn Observed in DNS Query", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (telecomly .info)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (globalseasurfer .xyz)", "ET MALWARE ROMCOM RAT CnC Domain (you-supported .com) in DNS Lookup", "ET MALWARE Stonefly APT Related Domain in DNS Lookup (tecnojournals .com)", "ET MALWARE Maldoc Domain in DNS Lookup (travelcrimea .info)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (skype .se .net) in DNS Lookup", "ET MALWARE Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup", "ET MALWARE W32/CoinMinerESJ!tr CnC Domain (ox .mygoodluck .best) in DNS Lookup", "ET MALWARE Mozart Loader CnC Checkin (getid)", "ET MALWARE Observed Malicious SSL Cert (MonetizUs/LNKR)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (pleaseletmesleep .fun)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Sinkhole)", "ET

	MALWARE Observed Unk.PowerShell Loader CnC Domain in TLS SNI", "ET MALWARE APT-C-27 CnC Domain Observed in DNS Query", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 10", "ET MALWARE Observed Malicious SSL Cert (Gozi CnC)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (ny .silvergatehr .com)", "ET MALWARE Observed Malicious SSL Cert (Upatre CnC)", "ET MALWARE Observed Glupteba CnC Domain (mastiakele .cyou in TLS SNI)", "ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (aj .0x0x0x0x0 .best) in DNS Lookup", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (gov .mil .ua .aspx .io)", "ET MALWARE Suspicious Domain (judgebryantweekes .com) in TLS SNI", "ET MALWARE Observed DarkSide Ransomware Domain (temisleyes .com in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (margarita-smith .host in DNS Lookup)", "ET MALWARE PolyglotDuke Domain Observed", "ET MALWARE Parallax RAT CnC Domain Observed in DNS Query", "ET MALWARE Observed Malicious SSL Cert (Blackrota)", "ET MALWARE Observed Malicious SSL Cert (DonotGroup FireStarter CnC)", "ET MALWARE Gallium APT Related Domain in DNS Lookup (hinitial .com)", "ET MALWARE ELF/FontOnLake Related CnC Domain in DNS Lookup (hm2 .yrnykx .com)", "ET MALWARE Malicious SSL Cert (Magecart)", "ET MALWARE Observed Malicious SSL Cert (Darkme CnC)", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (sharemanage .elwoodasset .xyz)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)", "ET MALWARE APT41 CnC Domain (c .ymvh8w5 .xyz) in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-cdn .xyz)", "ET MALWARE Observed Glupteba CnC Domain (cdneurops .pics in TLS SNI)", "ET MALWARE Observed DNS Query to TA444 Domain (careersbankofamerica .us)", "ET MALWARE Observed Glupteba CnC Domain (limeprime .com in TLS SNI)", "ET MALWARE Donot APT Related Domain in DNS Lookup (dataupdates .live)", "ET MALWARE Observed Puzzlemaker Remote Shell Domain (media-seoengine .com in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MageCart CnC)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (phoenix-panel .firebaseio .com in DNS Lookup)", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (deangelomcnay .news)", "ET MALWARE DNS Query to MINEBRIDGE CnC Domain (compilator333 .top)", "ET MALWARE Observed Glupteba CnC Domain (zaoshanghao .su in TLS SNI)", "ET MALWARE IcedID CnC Domain in SSL/TLS SNI", "ET MALWARE Observed SSV Agent CnC Domain (edgecloudc .com in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (tmetres .com in TLS SNI)", "ET MALWARE Group 21 CnC Domain Observed in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-endpoint .com)", "ET MOBILE_MALWARE Arid Viper (fasebaook .com in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (Meterpreter Paranoid Mode CnC)", "ET MALWARE Observed Malicious SSL Cert (BitRAT CnC)", "ET MALWARE Arid Gopher Related Domain in DNS Lookup (grace-fraser .site)", "ET MALWARE PHPStudy CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (CryptoMimic Staging CnC)", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (quantumbots .xyz in TLS SNI)", "ET MALWARE TraderTraitor CnC Domain (www .esilet .com) in DNS Lookup", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (fuvataren .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-schnellvpn .com)", "ET MALWARE Observed TrojanSpy.SH.HADGLIDER.A Exfil Domain in DNS Query", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 10", "ET MALWARE Win32/DuckLogs Malware Related Domain in DNS Lookup (ducklogs .com)", "ET MALWARE DTLoader Domain (ahgwqrq .xyz in TLS SNI)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)", "ET MALWARE TA444 Related Domain in DNS Lookup (onlinecloud .cloud)", "ET MALWARE Observed DOUBLEBACK CnC Domain (bestcake .ca in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (cdneurops .health in TLS SNI)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (overingtonray .info)", "ET MALWARE OWOWA Stealer CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (APT32 JEShell CnC)", "ET MALWARE Bitter APT Related Domain in DNS Lookup (emshedulersvc .com)", "ET

	MALWARE NetSupport RAT Domain (tradinghuy .duckdns .org) in DNS Lookup", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (font .backuplogs .xyz)", "ET MALWARE Quasar CnC Domain in DNS Lookup (societyf500 .ddns .net)", "ET MALWARE Golang/Webbfustator Related Domain in DNS Lookup (xmlschemeformat .com)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (gurumades .ru)", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (nhansudaihoi13 .org)", "ET MALWARE Observed DNS Query to Known Gelsemium CnC", "ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (api-cdnw5 .net)", "ET MOBILE_MALWARE Observed Malicious SSL Cert (DonotGroup Android CnC)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (rce .ee)", "ET MALWARE Observed Malicious SSL Cert (CoreDn/BLINDINGCAN Activity)", "ET MALWARE Malicious SSL certificate detected (OSX/Keydnap CnC)", "ET MALWARE TA444 Related Domain in DNS Lookup (googlesheet .info)", "ET MALWARE Observed Elysium Stealer Domain (phonefix .bar in TLS SNI)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (genericalphabet .top in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Zepakab CnC)", "ET MALWARE Observed CobaltStrike CnC Domain (stg .pesrado .com in TLS SNI)", "ET ADWARE_PUP Observed Honeygain Domain (api .honeygain .com in TLS SNI)", "ET MALWARE Redline Stealer Related Domain in DNS Lookup (windows-upgraded .com)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (doctorstrange .buzz)", "ET MALWARE RShell CnC Domain (time .ntp-server .asia) in DNS Lookup", "ET MALWARE Observed DonotGroup Related Domain (furnish .spacequery .live in TLS SNI)", "ET MALWARE Observed JS/Skimmer (likely Magecart) Domain in TLS SNI (imprintcenter .com)", "ET MALWARE Mekotio Banking Trojan CnC Domain (zautoservice .eu) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Gozi ISFB)", "ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup", "ET MALWARE Shuckworm CnC Domain (destroy .asierdo .ru) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (nameyourcatlikeshedeserved .top)", "ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (sephardimension .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 4", "ET MALWARE Suspected APT28 Related Domain in DNS Lookup (wordkeyvpload .net)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-cdn .xyz)", "ET MALWARE OSX/MapperState CnC Domain in DNS Lookup", "ET MALWARE Observed DNS Query to Redkeeper Ransomware Domain", "ET MOBILE_MALWARE Android.Trojan.Rana.A (whoisdomainpc .com in DNS Lookup)", "ET MALWARE ELF/Rekoobe CnC Observed in DNS Query", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (aconitum .xyz)", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (zakaria-chotzen .info)", "ET MALWARE APT/Sidewinder CnC Domain in DNS Lookup (afcat .xyz)", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (signverydn .sharebusiness .xyz)", "ET MALWARE Observed Malicious SSL Cert (WastedLoader CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (syriahr .eu)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (return2monkey .fun)", "ET MALWARE Observed Cobalt Strike CnC Domain (windowsupdatesc .com in TLS SNI)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (ceye .io)", "ET MALWARE Earth Berberoka Domain in DNS Lookup", "ET MALWARE PowerShell/PowHeartBeat CnC Domain (central .suhypercloud .org) in DNS Lookup", "ET MALWARE Observed Malware Delivery Domain (analyticsnet .top in TLS SNI)", "ET MOBILE_MALWARE APT-C-23 Related CnC Domain in DNS Lookup (javan-demsky .website)", "ET MOBILE_MALWARE Arid Viper (dash-chat-c02b3 .appspot .com in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (OilRig QUADAGENT CnC)", "ET MALWARE APT/FamousSparrow CnC Domain in DNS Lookup (credits.offices-analytics .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 12", "ET MALWARE PHP Skimmer CnC Domain in DNS Lookup (secure-authorize .net)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-blog .xyz)", "ET MALWARE DNS Query to MINEBRIDGE CnC Domain (creatorz123 .top)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01", "ET MALWARE Bitter APT CnC Domain (updnangelgroup .com) in DNS Lookup", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (dshellelink .gcloud-share .com)", "ET MALWARE Mozart Loader Command Request (getupdates)",

	"ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (shehootastayonwhatshelirned .top)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mynameisgarfield .top)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (update-real .com) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (hannah-parsons .info in DNS Lookup)", "ET MALWARE Malicious SSL Certificate detected (PyXie)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (dofixifa .co)", "ET MALWARE Observed IcedID CnC Domain in TLS SNI", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (marcobrando .xyz in TLS SNI)", "ET MALWARE Observed DCRat CnC Domain in TLS SNI", "ET MALWARE TA444 Related Domain in DNS Lookup (angelbridge .capital)", "ET MALWARE Observed Malicious SSL Cert (FIN7/JSSLoader CnC)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-blog .com)", "ET MOBILE_MALWARE Android Brunhilda Dropper (flowdivison .club in DNS Lookup)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (roskazna .net)", "ET MALWARE MoonBounce Backdoor Related Domain in DNS Lookup (kinopoisksu .com)", "ET MALWARE Konni Group CnC Domain in DNS Lookup", "ET MALWARE Windows/OriginLogger CnC Domain (originproducts .pw) in DNS Lookup", "ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)", "ET MOBILE_MALWARE Android/IRATA CnC Domain (rimotgozaran .tk) in DNS Lookup", "ET MALWARE PhantomNet/Smanager Related Domain in DNS Lookup", "ET MALWARE Malicious SSL Certificate detected (Cobalt Strike CnC)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (log4j. leakix .net)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21 2)", "ET MALWARE Observed Malicious SSL Cert (FIN8 Staging CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (news .networkslaoupdate .com)", "ET MALWARE Observed DNS Query to ElectronBot Domain (11k .online)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (xlssmooth .xyz)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 11", "ET MALWARE Observed Malicious SSL Cert (Cobalt Strike)", "ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (allmedicalpro .com)", "ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)", "ET MALWARE TA402/Molerats Related Domain in DNS Lookup", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (mktrending .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-cdn .com)", "ET MALWARE Kimsuky CnC Domain Observed in DNS Query", "ET MALWARE IXWARE Stealer Domain in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-endpoint .com)", "ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (ethdns .mywire .org)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (gopstoporchestra .top in TLS SNI)", "ET MALWARE Kimsuky APT CnC Domain in DNS Lookup", "ET MALWARE BlackCat Ransomware Related Domain in TLS SNI (updatedaemon .com)", "ET MOBILE_MALWARE Android/LoanBee Data Stealer Data Exfiltration Domain (api .loanbee .tech) in DNS Lookup", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (hierodula .online)", "ET MALWARE Gamaredon CnC Domain (celticso .ru) in DNS Lookup", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (pgp .eu .com) in DNS Lookup", "ET MALWARE Observed Magecart Domain (webscriptly .com in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (getyourgift .life in TLS SNI)", "ET MALWARE Inception/CloudAtlas CnC Domain in DNS Lookup (ms-officeupdate .com)", "ET MALWARE EvilNum APT Related Domain in DNS Lookup (estimefm .org)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (allinfostudio .com)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (gismolow .com)", "ET MALWARE Observed Malicious Domain Targeting Minority Groups Domain (unohcr .org in TLS SNI)", "ET MALWARE SoulSearcher Malware Domain in DNS Lookup (app .tomelife .com)", "ET MALWARE Win32/Matanbuchus Loader Related Domain in DNS Lookup (collectiontelemetrysystem .com)", "ET MALWARE Bitter APT Related Domain in DNS Lookup (huandocimama .com)", "ET EXPLOIT_KIT Observed BottleEK Domain in DNS Lookup 2021-04-15", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (onthewire1 .top)", "ET MALWARE Observed Cobalt Strike Related Domain (mail .igov-service .net in TLS SNI)", "ET MALWARE Mozart Loader Command Request (gettasks)",

	"ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (page .googledocpage .com)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (world .healthamericacu .com)", "ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (krakenfolio .com)", "ET MALWARE APT/Bitter Related CnC Domain in DNS Lookup", "ET MALWARE DPRK APT Related Domain in DNS Lookup (beastmodser .club)", "ET MALWARE AppleJeus - Dorusio CnC Domain in DNS Lookup (dorusio .com)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 11 CnC)", "ET MALWARE Observed Blackrota Domain (blackrato .ga in TLS SNI)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30", "ET MALWARE Confucious APT Related Domain in DNS Lookup (bonimoni .xyz)", "ET MALWARE Observed Malicious SSL Cert (Win32/Unk Downloader CnC)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (attentionmagnet .top in TLS SNI)", "ET MOBILE_MALWARE Observed Trojan-Spy.AndroidOS.Origami.b / Donot Domain in TLS SNI", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (log4j .binaryedge .io)", "ET MALWARE Observed Malicious SSL Cert (Panda Banker C2)", "ET MALWARE Observed Malicious SSL Cert (Zeromax Stealer CnC)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-service .com)", "ET MALWARE Observed MSIL/n2019cov (COVID-19) Ransomware CnC Domain in TLS SNI", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-chat .com)", "ET MALWARE Observed Win32/Eternity Stealer Domain (eternitypr .net in TLS SNI)", "ET MALWARE Sidecopy APT Backdoor Related Domain in DNS Lookup (kokotech .xyz)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07", "ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (juliansturgill .info)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-schnellvpn .xyz)", "ET MALWARE ShadowPad Backdoor Related Domain in DNS Lookup (grandfoodtony .com)", "ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (mediqhealthcare .com)", "ET MALWARE Observed Malicious SSL Cert (DonotGroup/Patchwork CnC)", "ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)", "ET MALWARE BlackTech ELF/TSCookie CnC Observed in DNS Query", "ET MALWARE Instagram Like Bot (like4u) CnC Domain in DNS Lookup", "ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query", "ET MALWARE Observed DarkSide Ransomware CnC Domain in TLS SNI", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (pejapezey .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-cdn .com)", "ET MALWARE Observed Malicious SSL Cert (POWERRATANKBA CnC)", "ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (airbseeker .com)", "ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)", "ET MALWARE Observed BazarLoader Domain (vighik .xyz in TLS SNI)", "ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (cdn-chrome .com)", "ET MALWARE Observed Malicious SSL Cert for IRS Credential Phish Domain (supportmicrohere .com)", "ET MOBILE_MALWARE Android/Zanubis CnC Domain (fullcircleteam .com) in DNS Lookup", "ET MALWARE ErbiumStealer Domain (erbium .ml) in TLS SNI", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-cdn .com)", "ET MALWARE Observed Malicious SSL Cert (JS WebSkimmer Exfil Site)", "ET MALWARE Observed GoBotKR Domain in TLS SNI", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (seattlecarwash .fun)", "ET MALWARE Observed Malicious SSL Cert (Win32/Gadwats Banker CnC Domain)", "ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (adobefile .ru)", "ET MOBILE_MALWARE Arid Viper (fasebaak .com in DNS Lookup)", "ET MALWARE Unknown APT Related Domain in DNS Lookup", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (earlahenry .com)", "ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (transplugin .io)", "ET MALWARE TA444 Related Domain in DNS Lookup (mufg .college)", "ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (microsoft-support .net)", "ET MALWARE Observed Elysium Stealer Domain in TLS SNI (manholi .xyz)", "ET MALWARE Woody RAT CnC Domain (kurmakata .duckdns .org) in DNS Lookup", "ET MALWARE APT41 KEYPLUG Related

	Domain in DNS Lookup", "ET MALWARE Spark Backdoor CnC Domain Query", "ET MALWARE Observed GhostWriter APT Related Cobalt Strike Domain (ao3 .hmgo .pw in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (mastiakele .ae .org in TLS SNI)", "ET MOBILE_MALWARE SSL/TLS Certificate Observed (Betcity CnC)", "ET MALWARE Observed Malicious SSL Cert (AsyncRAT Server)", "ET MALWARE Observed Cobalt Strike Stager Domain in DNS Query", "ET MALWARE DNS Query to MINEBRIDGE CnC Domain (123faster .top)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (companyllc .top)", "ET MALWARE Observed BlackCat Ransomware Related SSL Cert (updatedaemon .com)", "ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (habbybearshop .top)", "ET MALWARE Donot APT Related Domain in DNS Lookup (seasonsbackup .xyz)", "ET MALWARE Python PyPi Typo Squatting Package Payload Delivery Domain (anarchydev .com) in DNS Request", "ET MALWARE NIGHTSCOUT Malware CnC Domain in DNS Lookup (q. cloudistcdn .com)", "ET MALWARE Chaos Botnet CnC Domain (botnet .ddoswow .site) in DNS Lookup", "ET MALWARE Observed StrongPity Domain (singlefunctionapp .com in TLS SNI)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup (files-dwn .shop)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (lifemaindecision .top)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-schnellvpn .xyz)", "ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (cdnmobile .io)", "ET MOBILE_MALWARE Arid Viper (play-store-51182 .firebaseio .com in DNS Lookup)", "ET MALWARE Observed Cobalt Strike CnC Domain (gojihu .com in TLS SNI)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (yourblogcenter .com)", "ET MALWARE Possible APT28 Phishing Domain in DNS Query", "ET MALWARE Observed Malicious SSL Cert (Various CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (wikipedia-book .vote)", "ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (transferwiser .io)", "ET MALWARE Donot APT Related Domain in DNS Lookup (tplinkupdates .space)", "ET MALWARE Patchwork APT Related Domain in DNS Lookup (dayspringdesk .xyz)", "ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (blacknurse .lib)", "ET MALWARE Observed BLINDINGCAN Domain (www .sanlorenzoyacht .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup", "ET MALWARE Observed Cobalt Strike Domain (zuyonijobo .com) in TLS SNI", "ET MALWARE Win32/Beapy CnC Domain in DNS Lookup", "ET MALWARE SocGholish Related Domain in DNS Lookup (irsgetwell .net)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (hiduwu .com)", "ET MALWARE BlackMatter CnC Domain in DNS Lookup (mojobiden .com)", "ET MALWARE Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI)", "ET MALWARE Chaos Botnet CnC Domain (ars1 .wemix .cc) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Possible APT33 CnC)", "ET MALWARE Observed Malicious SSL Cert (AgentTesla CnC)", "ET MALWARE Observed BazarLoader Domain (numklo .xyz in TLS SNI)", "ET MALWARE MageCart CnC Domain Observed in DNS Query", "ET MALWARE Malicious Doc CnC Domain (e-demarches .kodeo .ch) in DNS Lookup", "ET MALWARE BLINDEAGLE CnC Domain (systemwin .linkpc .net) in DNS Lookup", "ET MALWARE Observed MSIL/Heracles Variant CnC Domain (stainless .fun in TLS SNI)", "ET MALWARE Observed AridViper CnC Domain in TLS SNI", "ET MALWARE Observed Malicious SSL/TLS Certificate (Jasper CnC)", "ET MALWARE Observed Win32.Raccoon Stealer Domain (hellowoodie .top in TLS SNI)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-cdn .xyz)", "ET MALWARE Observed ErbiumStealer Domain (ozaron .beget .tech) in TLS SNI", "ET MALWARE Observed Reimageplus Ransomware Domain in TLS SNI", "ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI", "ET MALWARE Moses Staff APT Related Domain in DNS Lookup (techzenspace .com)", "ET MALWARE Observed Malicious SSL Cert (BitRAT)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (portraits .studio-94-photography .com)", "ET MALWARE EvilNum APT Related Domain in DNS Lookup (msdllopt .com)", "ET MALWARE IceXLoader CnC Domain (stealthelite .one) in DNS Lookup", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (cloud-avira .com) in DNS Lookup", "ET MOBILE_MALWARE Android.BankBot.11270 (DNS Lookup)", "ET MALWARE Suspected Middle East Threat Group Domain in DNS Lookup (liveupdatedriver .com)", "ET MALWARE Observed

	Malicious SSL Cert (MageCart Exfil Domain)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (kinksdoc .ru)", "ET MALWARE TA444 Related Domain in DNS Lookup (smbc-vc .com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paknavy .comsats .xyz)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.t (DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (Fake Gmail Self Signed - Possible Cobalt Stirke)", "ET MALWARE Observed SSV Agent CnC Domain (hostupoeui .com in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (mastiakele .icu in TLS SNI)", "ET MALWARE Generic AsyncRAT Style SSL Cert", "ET MALWARE Observed Magecart/Skimmer - _try_action CnC Domain (cdn-frontend .com in TLS SNI)", "ET MALWARE Kutaki Stealer CnC Domain (terebinnahicc .club) in DNS Lookup", "ET MALWARE Observed Cobalt Strike CnC Domain in TLS SNI (cs .lg22l .com)", "ET MALWARE Observed Malicious SSL Cert (PhantomNet/Smanager CnC)", "ET MALWARE Observed Lunar Builder Domain (lunarbuilder .000webhostapp .com in TLS SNI)", "ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (idtpl .org)", "ET MALWARE DonotGroup Related Domain in DNS Lookup (orangeholister .buzz)", "ET MALWARE Observed Malicious SSL Cert (Python RAT (Aurora Campaign))", "ET MALWARE Observed Get2 CnC Domain in TLS SNI", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-endpoint .xyz)", "ET MALWARE Unknown Chinese Threat Actor CnC Domain in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-chat .xyz)", "ET MALWARE APT10 Related Domain in DNS Lookup (microsofts .cc)", "ET MALWARE China Based APT Related Domain in DNS Lookup (portal .super-encrypt .com)", "ET MALWARE Observed DNS Query to Blackrota Domain", "ET MALWARE Win32/Eternity Stealer CnC Domain in DNS Lookup (eternitypr .net)", "ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (blog .br0vvnn .io)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (gallant-william .icu)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (pwn .af)", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (montanatony .xyz in TLS SNI)", "ET MALWARE Chaos Botnet CnC Domain (bitantcoins .pro) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (JS/Ostap CnC)", "ET MOBILE_MALWARE Arid Viper (julie-parker .top in DNS Lookup)", "ET MALWARE Observed OSX/Silver Sparrow Download Domain in TLS SNI", "ET MALWARE Observed Glupteba CnC Domain (greenphoenix .xyz in TLS SNI)", "ET MOBILE_MALWARE Android Gymdrop Dropper (onlinefitnessanalysis .com in DNS Lookup)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mansizeprofile .top)", "ET MALWARE Observed StrongPity Domain (lurkingnet .com in TLS SNI)", "ET MALWARE AppleJeus - CoinGoTrade CnC Domain in DNS Lookup (coingotrade .com)", "ET MALWARE Observed Malicious SSL Cert (SideWinder APT CnC)", "ET MALWARE CloudAtlas APT Related CnC Domain in DNS Lookup (checklicensekey .com)", "ET MALWARE Smanager CnC Domain in DNS Lookup", "ET MALWARE Qakbot/Cobalt Strike Domain (jesofidiwi .com) in DNS Lookup", "ET MOBILE_MALWARE Coper Banking Trojan Related Domain in DNS Lookup", "ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (tempest .lib)", "ET MALWARE Win32/Flooder.Agent.NAS CnC Domain in DNS Lookup", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (ansonwhitmore .live)", "ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI", "ET MALWARE Donot APT Related Domain in DNS Lookup (oceansurvey .club)", "ET MALWARE Observed DNS Query to Stitch C2 Domain", "ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (besaintegration .com)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (canarytokens .com)", "ET MALWARE Likely Malicious SSL Cert With Script Tags", "ET MALWARE Observed DNS Query to ElectronBot Domain (Electron-Bot .s3 .eu-central-1 .amazonaws .com)", "ET MALWARE Observed Targeted Attack Malicious SSL Cert (opsonew3org .sg)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Bancos/DarkTequila CnC)", "ET MALWARE Observed Cobalt Strike CnC Domain (defenderupdateav .com in TLS SNI)", "ET MALWARE Observed PoetRAT Domain (dellgenius .hoptop .org in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain in TLS SNI", "ET MALWARE Observed DNS Query to Known Indexsinas CnC Domain", "ET MALWARE Lazarus APT Related Domain in DNS

	Lookup (docusign .agency)", "ET MALWARE Mercury APT Related Domain in DNS Lookup (sygateway .com)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup (vasimgo .shop)", "ET MALWARE Observed DNS Query to XWORM RAT Domain (pujakumari .duckdns .org)", "ET MALWARE Maldoc Domain in DNS Lookup (aljazeera .cc)", "ET MALWARE Win32\Cryptbot CnC Domain (okwydg05 .top) in DNS Lookup", "ET MALWARE APT/Donot Group CnC Domain in DNS Lookup (request .soundedge .live)", "ET MALWARE Observed Cobalt Strike CnC Domain (sazoya .com in TLS SNI)", "ET POLICY Observed Packity Proxy Domain in TLS SNI", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (srvrfontsdrive .xyz)", "ET MALWARE FIN7 JSSLoader Related Domain in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-blog .xyz)", "ET MALWARE TA444 Domain in DNS Lookup (hoststudio .org)", "ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (zuppohealth .com)", "ET MALWARE Malicious Rust Crate Related Domain in DNS Lookup (api .kakn .li)", "ET MALWARE Maldoc Related Domain in DNS Lookup", "ET MALWARE AppleJeus - Union Crypto CnC Domain in DNS Lookup (unioncrypto .vip)", "ET MALWARE Lazarus APT Maldoc Related Domain in DNS Lookup (markettrendingcenter .com)", "ET MALWARE Observed Malicious SSL Cert (MalDoc 2020-03-09)", "ET MALWARE Nobelium APT Related Domain in DNS Lookup (ernesttheskoolie .com)", "ET MALWARE Bitter APT Related Domain in DNS Lookup (youtubepremiumapp .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-cdn .com)", "ET MALWARE Observed Malicious SSL Cert (ShadowHammer CnC)", "ET MALWARE Donot APT Related Domain in DNS Lookup (printerjobs .xyz)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (ougreen .com)", "ET MALWARE SolarMarker Backdoor Related Domain in DNS Lookup (noelfpar .com)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (tomond .ru)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (sdilok .com)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 3 Staging Domain)", "ET MALWARE IcedID CnC Domain in SNI", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (thundernews .org)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (appledocs .ru)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (* .asset .tradingvein .xyz)", "ET MALWARE Observed Cobalt Strike CnC Domain (Gojihu .com in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (ELF/Rekoobe CnC)", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (product .onlinedoc .dev)", "ET MALWARE Ghostwriter/UNC1151 Related Domain in DNS Lookup", "ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (mcafee-upgrade .com)", "ET MALWARE Win32\Cryptbot CnC Domain (suqosk04 .top) in DNS Lookup", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (gogleadser .xyz in TLS SNI)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-schnellvpn .com)", "ET MALWARE Observed DNS Query to MoserPass Download Domain (passwordstate-18ed2 .kxcdn .com)", "ET MALWARE Observed Ttint CnC Domain in DNS Query", "ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (product2020 .mrbasic .com)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC) 2019-11-18", "ET MALWARE Gh0st Variant CnC Domain in DNS Lookup (dexercisep .com)", "ET MALWARE Observed Magecart CnC Domain in TLS SNI", "ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (mert .my03 .com)", "ET MALWARE JEUSD CnC Domain Observed in DNS Query", "ET MALWARE Chaos Botnet CnC Domain (tomca1 .com) in DNS Lookup", "ET MALWARE Observed Maldoc Domain (travelcrimea .info in TLS SNI)", "ET MALWARE CloudAtlas APT Related Domain in DNS Lookup", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (stilloak .net)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (offerings .love4lifewellness .com)", "ET MALWARE POWERTON CnC Domain in DNS Lookup", "ET MALWARE Win32/Backdoor Related Domain in DNS Lookup (swordoke .com)", "ET MALWARE Observed Lazarus APT Related Domain (designautocad .org in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21)", "ET MALWARE APT10 Related Domain in DNS Lookup (7cnbo .com)", "ET MALWARE Woody RAT CnC Domain (oakrussia .ru) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mariofart8 .top)", "ET MOBILE_MALWARE Arid Viper (stacks-zadar .website in DNS Lookup)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI

	(teastycandycoffe .top)", "ET MALWARE TA471/UNC2589 Related Domain in DNS Lookup (skreatortemp .site)", "ET MALWARE MageCart Skimmer Domain in DNS Lookup (bootstrap2 .xyz)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)", "ET MALWARE Suspected Middle East Threat Group Domain in DNS Lookup (dnsnamefinder .com)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (rpirpiwhyyouleaveyourhorse .top)", "ET MALWARE Observed Malicious SSL Cert (Win32/SandCat CnC)", "ET MALWARE Mozart Loader Command Request (reporttask)", "ET MALWARE TA444 Related Domain in DNS Lookup (docs-view .cloud)", "ET MALWARE Observed Jupyter Stealer CnC Domain (vincentolife .com in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2019-11-15)", "ET MALWARE LYCEUM CnC Domain in DNS Lookup", "ET MALWARE Observed sLoad Related Domain (angedionisu .eu in TLS SNI)", "ET MALWARE OceanLotus APT Related Domain in DNS Lookup (confusion-cerulean-samba .glitch .me)", "ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (globalkeystroke .com)", "ET MALWARE Observed JSSLoader Variant Domain (legislationient .com in TLS SNI)", "ET MOBILE_MALWARE Observed Android ERMAC Banker (PL) Domain (bolt-food .site in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (RampantKitten CnC)", "ET MALWARE Observed DNS Query to Vicious Panda CnC Domain", "ET MALWARE PlugX DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (chMiner/RAT)", "ET MALWARE Observed Malicious SSL Cert (Zloader CnC)", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (omegabots .xyz in TLS SNI)", "ET PHISHING Observed DNS Query to Phishing Domain (hombreymaquina .com)", "ET MALWARE AppleJeus - Kupay Wallet CnC Domain in DNS Lookup (kupaywallet .com)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (telegram-update .com) in DNS Lookup", "ET MALWARE TA455 CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (stand-by-97c5c .appspot .com in DNS Lookup)", "ET MALWARE Observed FinSpy Domain (browserupdate .download in TLS SNI)", "ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (qb .1c1c1c1c .best) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (log-yoheo .info in DNS Lookup)", "ET MOBILE_MALWARE Backdoor.AndroidOS.Ahmyth.f (DNS Lookup)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (hitfromthebong .top)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)", "ET MALWARE Win32/PurpleFox Related Domain in DNS Lookup", "ET MALWARE Observed Cobalt Strike Related Domain (world .healthamericacu .com in TLS SNI)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (letsmakesome .fun)", "ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (Likely Shylock/URLzone/Gootkit/Zeus Panda C2)", "ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .aexhausts .com)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (youcanfindmeonthe .top)", "ET MALWARE Win32/Spark Backdoor Related Domain in DNS Lookup (bundanesia .com)", "ET MALWARE Observed Malicious SSL Cert (ACBackdoor CnC)", "ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (crashparadox .net)", "ET MALWARE Observed Malicious SSL Cert (StrongPity CnC)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (onlinestockwatch .net)", "ET MALWARE Observed Glupteba CnC Domain (revouninstaller .homes in TLS SNI)", "ET MALWARE Maldoc Related Domain in DNS Lookup (ms-office .services)", "ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain", "ET MALWARE Magecart CnC Domain Observed in DNS Query", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (www .googlesheetpage .org)", "ET MALWARE Observed CobaltStrike CnC Domain (charity-wallet .com in TLS SNI)", "ET MALWARE Observed Cobalt Strike CnC Domain (security-desk .com in TLS SNI)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-schnellvpn .xyz)", "ET MALWARE Observed Malicious SSL Cert (APT MustangPanda CnC)", "ET MALWARE PowerGhost Staging CnC in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-schnellvpn .com)", "ET MALWARE TA444 Related Domain in DNS Lookup (fclouddown .co)", "ET MALWARE ChromeLoader CnC Domain (istakechau .autos) in DNS Lookup", "ET MALWARE

	Observed Cobalt Strike CnC Domain (dimentos .com in TLS SNI)", "ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .me)", "ET MALWARE BLINDEAGLE CnC Domain (upxsystems .com) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (marty-colvard .top in DNS Lookup)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (kryptoslogic-cve-2021-44228 .com)", "ET MALWARE Observed Malicious SSL/TLS Certificate (IcedID CnC)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (norayowell .info)", "ET MALWARE Observed DNS Query to Reverse Shell Payload Domain (opentunnel .quest)", "ET MALWARE Observed Targeted Attack Malicious SSL Cert (investbooking .de)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (clipboardgames .xyz)", "ET MALWARE Observed Glupteba CnC Domain (cdneurop .cloud in TLS SNI)", "ET MALWARE Observed Ursnif CnC Domain (Vloderuniok .website in TLS SNI)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (mindbreaker .top in TLS SNI)", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (billionaireshore .top)", "ET MALWARE OilRig SideTwist CnC Domain in DNS Lookup (sarmsoftware .com)", "ET MALWARE ErbiumStealer CnC Domain (ozaron .beget .tech) in DNS Lookup", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (superdocs .ru)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (uk2privat .com) in DNS Lookup", "ET MALWARE SocGholish CnC Domain in DNS Lookup (moments .abledity .com)", "ET MALWARE Chaos Botnet CnC Domain (quanquandd .top) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mydrinksare .top)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-07-29)", "ET MALWARE Observed GoLang Dropper Domain (en7dftkjiipor .x .pipedream .net in TLS SNI)", "ET MALWARE TraderTraitor CnC Domain (aideck .net) in DNS Lookup", "ET MALWARE TA444/Lazarus Related Domain in DNS Lookup (microshare .cloud)", "ET MALWARE StrongPity APT Related Domain in DNS Lookup (sessionprotocol .com)", "ET MALWARE 8220 Gang Related Domain in DNS Lookup (oracleservice .top)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (worldpro .buzz)", "ET MALWARE LazyScripter Related Domain in DNS Lookup (hpsj .firewall-gateway .net)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (fitnesscheck .xyz)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (lomhasnopryiyome .top in TLS SNI)", "ET MALWARE DonotGroup Staging Domain Observed in DNS Query", "ET MALWARE APT-C-48 Related CnC Domain in DNS Lookup (nitb .pk-gov .org)", "ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup", "ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (securemanag .com)", "ET MALWARE Shuckworm/Gamaredon CnC Domain (motoristo .ru) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (MosaicRegressor WinHTTP Downloader)", "ET MALWARE CN Based APT Related Domain in DNS Lookup (open .zerdeopen .top)", "ET MALWARE Observed Malicious SSL Cert (Strongpity CnC)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (windowsupadates .com) in DNS Lookup", "ET MALWARE Win32/MysterySnail RAT CnC Domain in DNS Lookup", "ET MALWARE Observed Win32/Eternity Stealer Domain (eterprx .net in TLS SNI)", "ET MALWARE Observed CloudAtlas APT Related Domain (checklicensekey .com in TLS SNI)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-chat .xyz)", "ET MOBILE_MALWARE Arid Viper (chad-jessie .info in DNS Lookup)", "ET MALWARE TA444 Related Domain in DNS Lookup (microshare .cloud)", "ET MALWARE EvilNum APT Related Domain in DNS Lookup (pcamanalytics .com)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (cloud-documents .com)", "ET MALWARE AllcomeClipper CnC Domain (dba692117be7b6d3480fe5220fdd58b38bf .xyz) in DNS Lookup", "ET MOBILE_MALWARE Android.Trojan.Rana.A (softwareplayertop .com in DNS Lookup)", "ET MALWARE PlugX Related Domain in DNS Lookup (wps .daj8 .me)", "ET MALWARE Observed Malicious SSL Cert (ServHelper RAT CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (koltary .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-blog .com)", "ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (hotspot .accesscam .org)", "ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup", "ET MALWARE Bitter APT Related Domain in DNS Lookup

	(signal-premium-app .org)", "ET MALWARE Observed Malicious SSL Cert (Cobalt Group/More_Eggs CnC)", "ET MALWARE PlugX Related Domain in DNS Lookup (ntpserver .xyz)", "ET MALWARE Observed DangerousPassword APT Related Domain (datacentre .center in TLS SNI)", "ET MALWARE Magecart Related Domain in DNS Lookup (cdn-mediahub .com)", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (share .devprocloud .com)", "ET MALWARE Woody RAT CnC Domain (fns77 .ru) in DNS Lookup", "ET MALWARE Chaos Botnet CnC Domain (skyeda .vip) in DNS Lookup", "ET MALWARE CN Based APT Related Domain in DNS Lookup (news .wooordhunts .com)", "ET MALWARE 8220 Gang Related Domain in DNS Lookup (onlypirate .top)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (number2g .top in TLS SNI)", "ET MALWARE Win32\Cryptbot CnC Domain (towspd42 .top) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (gogowormdealer .top)", "ET MALWARE Observed SSL/TLS Cert (Splashtop Remote Support)", "ET MALWARE Observed Malicious Mustang Panda APT Related SSL Cert (File Transfer Service)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit MITM)", "ET MALWARE Observed DarkSide Ransomware Domain (rumahsia .com in TLS SNI)", "ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (sendbits .m2stor4ge .xyz)", "ET MALWARE Donot APT Related Domain in DNS Lookup (lovingallupdates .life)", "ET MALWARE APT-C-48 Related CnC Domain in DNS Lookup (ntc-pk .sytes .net)", "ET MALWARE Observed Malicious SSL Cert (Mirrortheif group)", "ET MALWARE Observed Malicious SSL/TLS Certificate (MageCart Payload CnC)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-chat .xyz)", "ET MALWARE Chaos Botnet CnC Domain (xiaomai233 .f3322 .net) in DNS Lookup", "ET MALWARE Observed Elysium Stealer Domain in TLS SNI (get-europe-group .bar)", "ET MALWARE Win32/Eternity Stealer CnC Domain in DNS Lookup (eterprx .net)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-blog .xyz)", "ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (magento-plugin .com)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (portal .gfinanzen .net)", "ET MALWARE Observed Cobalt Strike CnC Domain in DNS Lookup (nirsoft .me)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (hojimizeg .com)", "ET MALWARE Maldoc CnC Domain in DNS Lookup (r .significantbyte .com)", "ET MALWARE Lazarus CnC Domain Observed in DNS Query", "ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (a .pwn-t .tk)", "ET MALWARE Observed SSV Agent CnC Domain (flushcdn .com in TLS SNI)", "ET MALWARE Observed Win32/Wacapew.A!ml Domain in TLS SNI (zytrox .tk)", "ET MALWARE Kimsuky APT Related Domain in DNS Lookup (gooeglle .mypressonline .com)", "ET MALWARE TraderTraitor CnC Domain (cryptais .com) in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-endpoint .com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (mailh .alit .live)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (thecloudnet .org)", "ET MALWARE Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27", "ET MALWARE Observed Malware Delivery Landing Page Domain (bigeront .top in TLS SNI)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (ekb .tanzedrom .ru)", "ET MALWARE Observed Malicious SSL Cert (POWERSTATS Proxy CnC)", "ET MALWARE APT10 Related Domain in DNS Lookup (3mmlq .com)", "ET MALWARE Windows/OriginLogger CnC Domain (originproducts .xyz) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (DeadlyKiss APT)", "ET MALWARE Observed JS/Skimmer (likely Magecart) CnC Domain in DNS Lookup", "ET MALWARE Woody RAT CnC Domain (microsoft-telemetry .ru) in DNS Lookup", "ET MALWARE sLoad Related CnC Domain in DNS Lookup (angedionisu .eu)", "ET MALWARE Observed DCRat CnC Domain (dud-shotline .000webhostapp .com in TLS SNI)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (blattodea .ru)", "ET MALWARE TA444 Domain in DNS Lookup (updatezone .org)", "ET MALWARE Observed Cobalt Strike CnC Domain (www .msfthelpdesk .com in TLS SNI)", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tinmoivietnam .com)", "ET MOBILE_MALWARE Arid Viper (anna-sanchez .online in DNS Lookup)", "ET MALWARE Observed Zingo/GinzoStealer CnC Domain (nominally .ru in TLS SNI)", "ET MALWARE Observed DNS Query to XWORM RAT Domain (esteticamarbai .es)", "ET MALWARE

	Observed Malicious SSL Cert (CopperStealer CnC)", "ET MOBILE_MALWARE Arid Viper (moggfelicio .info in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (OSX/Nukesped CnC)", "ET MALWARE Loli Stealer CnC Domain in DNS Lookup (webstealer .ru)", "ET MALWARE Donot APT Related Domain in DNS Lookup (packetbite .live)", "ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (secure-daddy .com)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (nyqualitypizza .top)", "ET MALWARE Win32/Sephora Related Domain in DNS Lookup (sephus .me)", "ET MOBILE_MALWARE Arid Viper (log-yoahao .co in DNS Lookup)", "ET MALWARE Golang/Webbfustator Related Domain in DNS Lookup (updatesagent .com)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (discover .jsfconnections .com)", "ET MALWARE Observed Malicious SSL Cert (Bancos Variant CnC)", "ET MOBILE_MALWARE NSO Pegasus iOS CnC Domain in DNS Lookup (opposedarrangement .net)", "ET MALWARE Observed Malicious SSL Cert (Gelsemium CnC)", "ET MALWARE BIOPASS RAT Related Domain in DNS Lookup (0x3s .com)", "ET MALWARE Gallium APT Related Domain in DNS Lookup (micfkbeljacob .com)", "ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (ui .0x0x0x0x0 .xyz) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert IRS Credential Phish Domain (jbdelmarket .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-chat .com)", "ET MALWARE Confucious APT Related Domain in DNS Lookup (info-updates .ddns .net)", "ET MALWARE 8220 Gang Related Domain in DNS Lookup (letmaker .top)", "ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware C2)", "ET MALWARE Windows/OriginLogger CnC Domain (originlogger .com) in DNS Lookup", "ET MOBILE_MALWARE Android/RatMilad CnC Domain (api .numrent .shop) in DNS Lookup", "ET MALWARE Observed Win32/DecryptStealer Exfil Domain (geroipanel .site in TLS SNI)", "ET MALWARE Suspected APT28 Related Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (MSIL/Agent.TRM CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup", "ET MALWARE Kutaki Stealer CnC Domain (treysbeatend .com) in DNS Lookup", "ET MALWARE Observed BazarLoader Domain (moig .xyz in TLS SNI)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (irenewansley .icu)", "ET MALWARE Observed Cobalt Strike CnC Domain (yuxicu .com in TLS SNI)", "ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query", "ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (mihannevis .com)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (digiboxes .us)", "ET MALWARE Observed TA444/Lazarus Domain (one .microshare .cloud) in TLS SNI", "ET MALWARE CN Based APT Related Domain in DNS Lookup (supportteam .lingrevelat .com)", "ET MOBILE_MALWARE Arid Viper (stevensmalley .pro in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (jssLoader CnC)", "ET MALWARE Malicious SSL certificate detected (FindPOS)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (checkauj .com)", "ET MALWARE Observed Malicious SSL Cert (MICROPSIA CnC Domain)", "ET MALWARE Observed TA444 Domain (gdocshare .one in TLS SNI)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (doc .filesaves .cloud)", "ET MALWARE Observed Malicious SSL Cert (AsyncRAT)", "ET MALWARE Observed Malicious SSL Cert (Sidewinder APT CnC)", "ET MALWARE Observed Malicious SSL/TLS Certificate (APT-C-55/BabyShark Staging Domain)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (stockme .top in TLS SNI)", "ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (adtracker .link)", "ET PHISHING Observed DNS Query to Phishing Domain (igconsulting. pe)", "ET MOBILE_MALWARE Android/SharkBot Related Domain in DNS Lookup", "ET MALWARE ALFA Shell APT33 DNS Lookup (solevisible .com)", "ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup (eleed .online)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 7", "ET MALWARE APT 41 CnC Domain Observed in DNS Query", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-05-27)", "ET MALWARE Observed Malicious SSL Cert (APT34 CnC)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (videomart .top)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-chat .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 6", "ET MALWARE RShell CnC Domain (center .veryssl .org) in DNS Lookup", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup

	(facebookdeck .com)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (extic .icu)", "ET MALWARE Observed Malicious SSL Cert (TinyNuke Variant CnC) 2020-02-09", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (bloggersglobbers .top)", "ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)", "ET MALWARE Win32\Cryptbot CnC Domain (suqpvu08 .top) in DNS Lookup", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (youaresoslow .top)", "ET MALWARE Observed Adwind RAT CnC DNS Query", "ET MALWARE SocGholish CnC Domain in DNS Lookup (* .fate .truelance .com)", "ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (api-cdn .net)", "ET MALWARE Possible APT38 CnC Domain Observed in DNS Query", "ET MALWARE Donot APT Related Domain in DNS Lookup (resolverequest .live)", "ET MALWARE Observed Buer Loader Domain (officewestunionbank .com in TLS SNI)", "ET MALWARE Nobelium APT Related Domain in DNS Lookup (theskoolieblog .com)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (clank .hazari .ru)", "ET MALWARE TA455 Related CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL/TLS Certificate (MagnitudeEK Associated)", "ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (woodmate .it)", "ET MALWARE Observed StrongPity Domain (autoconfirmations .com in TLS SNI)", "ET MALWARE Mozart Loader Command Request (reportupdates)", "ET MALWARE TA453 Related CnC Domain in DNS Lookup (0brandaeyes0 .xyz)", "ET MALWARE TA402/Molerats Related Malware Domain in DNS Lookup", "ET MALWARE TA444 Related Domain in DNS Lookup (inst .shconstmarket .com)", "ET MALWARE Observed DangerousPassword APT Related Domain (shopapppro .com in TLS SNI)", "ET MALWARE Buhtrap SourSnack Domain in DNS Lookup (widget .forum-pokemon .com)", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (cooperron .me)", "ET MOBILE_MALWARE Arid Viper (fasbcaok .com in DNS Lookup)", "ET MALWARE PowerGhost Checkin CnC in DNS Query", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (greatersky .top)", "ET MALWARE Chaos Botnet CnC Domain (js .wanpay1 .cn) in DNS Lookup", "ET ADWARE_PUP Observed PUA SSL/TLS Certificate (HoneyGain)", "ET MALWARE Observed VikroStealer CnC Domain in TLS SNI", "ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (codevexillium .org)", "ET MALWARE AppleJeus - Ants2Whale CnC Domain in DNS Lookup (qnalytica .com)", "ET MALWARE Observed Win32/Backdoor Related Domain (swordoke .com in TLS SNI)", "ET MALWARE Observed Malicious SSL/TLS Certificate (CobaltStrike C2)", "ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)", "ET MALWARE Observed BazarLoader Domain (sh78bug .xyz in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MageCart Exfil)", "ET MALWARE Observed Malicious SSL Cert (Ursnif Inject Domain)", "ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup (eleed .cloud)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-endpoint .xyz)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (dixavokij .com)", "ET MALWARE China Based APT Related Domain in DNS Lookup (p1 .offline-microsoft .com)", "ET MALWARE Observed CobInt CnC Domain in TLS SNI", "ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup", "ET MALWARE NOBELIUM (TA421) CnC Domain in DNS Lookup", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (brainassault .top)", "ET MALWARE WebMonitor/RevCode RAT CnC Domain in DNS Lookup", "ET MALWARE FerociousKitten CnC Domain in DNS Lookup (microsoft .com-view .space)", "ET MALWARE Observed AZORult CnC Domain (miscrosoftworrd .000webhostapp .com in TLS SNI)", "ET MALWARE Observed SSV Agent CnC Domain (rsnet-devel .com in TLS SNI)", "ET MALWARE Observed DangerousPassword Related Domain (www .thecloudnet .org in TLS SNI)", "ET MALWARE Chinese Based APT Related Domain in DNS Lookup (ramblercloud .com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (navy-mil-bd .jmicc .xyz)", "ET MALWARE Kimsuky APT BabyShark/SHARPEXT Related Domain in DNS Lookup (worldinfocontact .club)", "ET MALWARE Shuckworm/Gamaredon CnC Domain (heato .ru) in DNS Lookup", "ET MALWARE DonotGroup Related Domain in DNS Lookup (wordfile .live)", "ET MALWARE Win32/Bisonal Backdoor CnC Domain in DNS Lookup", "ET MALWARE Observed Glupteba CnC Domain (cdneurops .buzz in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-

	44228 Security Scanner Domain (log4shell .huntress .com)", "ET MALWARE Laplas Clipper CnC Domain (clipper .guru) in DNS Lookup", "ET MALWARE Malicious SSL certificate detected (Possible Sinkhole)", "ET MALWARE Observed Jupyter Stealer CnC Domain (gogohid .com in TLS SNI)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (newageiscoming .top in TLS SNI)", "ET MALWARE Observed DNS Query for APT40 Possible DADSTACHE CnC Domain", "ET MALWARE Win32/Ramsay CnC Domain in DNS Query", "ET MALWARE Observed Malicious SSL Cert (SmokeLoader CnC)", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (bananakick .net)", "ET MALWARE Observed JSSLoader Domain (essentialsmassageanddayspa .com) in TLS SNI", "ET MALWARE Observed SSV Agent CnC Domain (be-government .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paf-gov .org)", "ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (dragon .lib)", "ET MALWARE Magecart Skimmer Domain in DNS Lookup (cdn-jsnode-call .com)", "ET MALWARE Observed Malicious SSL Cert (BazaLoader CnC)", "ET MALWARE Observed Malicious SSL Cert (CONFUCIOUS_B CnC)", "ET MALWARE Win32/Matanbuchus Loader Related Domain in DNS Lookup (telemetrysystemcollection .com)", "ET MALWARE Observed Malicious SSL Cert (Acme Co)", "ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (xs .0x0x0x0x0 .club) in DNS Lookup", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (jaxebiridi .com)", "ET MALWARE Observed APT/SideWinder CnC Domain in TLS SNI", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (esr .suppservices .xyz)", "ET MALWARE Observed Magecart Skimmer Domain (cloudflare-cdnjs .com in TLS SNI)", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (corporatelover .top)", "ET MALWARE Win32/Lumma Stealer CnC Domain (evetesttech .net) in DNS Lookup", "ET MALWARE TraderTraitor CnC Domain (creaideck .com) in DNS Lookup", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (annafraudy .top in TLS SNI)", "ET MALWARE Maldoc Related Domain in DNS Lookup (ms-offices .com)", "ET MALWARE Observed Arid Viper APT Related Domain (zakaria-chotzen .info in TLS SNI)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (simsimsalabim .top)", "ET MALWARE Arid Gopher Related Domain in DNS Lookup (pam-beesly .site)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08", "ET MALWARE Observed Cobalt Strike CnC Domain (securityupdateav .com in TLS SNI)", "ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (securetourspd .com)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (belochkaneprihoditodna .top in TLS SNI)", "ET MALWARE FIN7 Related CnC Domain in DNS Lookup (tnskvggujjqfcskwk .com)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (rus .feedpolicy .xyz)", "ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup", "ET MALWARE Kimsuky CnC Domain (jojoa .mypressonline .com) Observed in DNS Query", "ET MALWARE Maldoc Related Domain in DNS Lookup (template-openxml .com)", "ET MALWARE Observed FIN7 CnC Domain (injuryless .com in TLS SNI)", "ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (gofinancesolutions .com)", "ET MALWARE CASHY200 CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (GRIFFON CnC)", "ET MALWARE Chaos Botnet CnC Domain (tf .xiaozhuddos .co) in DNS Lookup", "ET MALWARE Observed Card Skimmer CnC Domain in TLS SNI", "ET INFO Ransomware Decryptor Domain in DNS Query (decoder .re)", "ET MALWARE Observed SSV Agent CnC Domain (gitcloudcache .com in TLS SNI)", "ET MALWARE Observed BLUELIGHT Payload Domain (storage .jquery .services in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Quasar CnC)", "ET MALWARE Observed Malicious SSL Cert (Lazarus APT MalDoc DL 2020-05-05)", "ET MALWARE EvilNominatus Ransomware Related Domain in DNS Lookup", "ET INFO Ransomware Decryptor Domain in DNS Query (decryptor .top)", "ET MALWARE Observed BazarLoader Domain (gut45bg .xyz in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL) 2019-10-24", "ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)", "ET MALWARE Lemon_Duck CnC Domain in DNS Lookup", "ET EXPLOIT_KIT PurpleFox EK Domain in DNS Lookup", "ET MALWARE Suspected POLONIUM CnC Domain (consulting-ukraine .tk) in DNS Lookup", "ET MALWARE PhantomNet/Smanager CnC Domain in DNS Lookup (office365.blogdns .com)", "ET MALWARE Donot APT Related Domain in DNS Lookup (printerupdates

	.online)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (bald-panel .firebaseio .com in DNS Lookup)", "ET MALWARE Observed DCRat Related Domain (crystalfiles .ru in TLS SNI)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (mikkelbourke .pro)", "ET MALWARE Win32\Cryptbot CnC Domain (suqyjb01 .top) in DNS Lookup", "ET MALWARE Observed Evil Keitaro TDS Redirection Domain (fiberswatch .com in TLS SNI)", "ET MALWARE CosmicStrand Rootkit Related Domain in DNS Lookup (update .bokts .com)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (tobaccosafe .xyz)", "ET MALWARE APT10 Related Domain in DNS Lookup (microsofts .top)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2019-09-17 1)", "ET MALWARE CN Based APT Related Domain in DNS Lookup (instructor .giize .com)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (shopapptech .com)", "ET MALWARE Observed JS/Magecart Domain in TLS SNI (manag .icu)", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tocaoonline .com)", "ET MALWARE Observed Magecart Skimmer Domain (static-zdassets .com in TLS SNI)", "ET MALWARE Observed Silver Implant Domain (raspoly .biz in TLS SNI)", "ET MALWARE Observed JSSLoader Domain (deprivationant .com in TLS SNI)", "ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (cdn-cgi .net)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (advanced-ip-scanners .com)", "ET MALWARE Win32\Cryptbot CnC Domain (okwyeg04 .top) in DNS Lookup", "ET MOBILE_MALWARE Android.BankBot.11270 (TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Get2 CnC)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (cosmodron .com)", "ET MALWARE Observed Glupteba CnC Domain (mastiakele .xyz in TLS SNI)", "ET MALWARE Observed Glupteba CnC Domain (zaoshang .moscow in TLS SNI)", "ET MALWARE TraderTraitor CnC Domain (alticgo .com) in DNS Lookup", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (gsheet .gdocsdown .com)", "ET MALWARE BlackCat Ransomware Related Domain in DNS Lookup (updatedaemon .com)", "ET MALWARE Observed Chinese APT Related Domain (ramblercloud .com in TLS SNI)", "ET MALWARE Win32/Lumma Stealer CnC Domain (765mm .xyz) in DNS Lookup", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (dev .sslsharecloud .net)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (perfectscenario .top)", "ET MALWARE Observed Ursnif CnC Domain (Gloderuniok .website in TLS SNI)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (who .worksolution .buzz)", "ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (callbinary .xyz in TLS SNI)", "ET MALWARE SparklingGoblin/Winnti Group SideWalk Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (MageCart)", "ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .weekendorg .com)", "ET MALWARE PhantomNet/Smanager CnC Domain in DNS Lookup (vgca.homeunix .org)", "ET MOBILE_MALWARE Arid Viper (hidden-chat-e58d7 .appspot .com in DNS Lookup)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-endpoint .xyz)", "ET MALWARE Donot APT Related Domain in DNS Lookup (printersolutions .live)", "ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (myrric-uses .singlejets .com)", "ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (highcolumn .webredirect .org)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (oob .li)", "ET WEB_CLIENT Exchange Webshell CnC Domain in DNS Lookup", "ET MALWARE Observed Cobalt Stike CnC Domain (nirsoft .me in TLS SNI)", "ET MALWARE TA453 Related Domain in DNS Lookup (universityofmhealth .biz)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (beetelson .xyz)", "ET MALWARE BlackMatter CnC Domain in DNS Lookup (nowautomation .com)", "ET MALWARE PinkBot CnC Domain in DNS Lookup (cnc .pinklander .com)", "ET MALWARE Win32\Cryptbot CnC Domain (kyrsti44 .top) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)", "ET MALWARE NIGHTSCOUT Poison Ivy Variant CnC Domain in DNS Lookup (cdn. cloudistcdn .com)", "ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)", "ET MOBILE_MALWARE APT-C-23 Related CnC Domain in DNS Lookup (linda-gaytan .website)", "ET MALWARE Mustang Panda APT PlugX Related Domain in DNS Lookup (myanmarnewsonline .org)", "ET MALWARE Microcin Backdoor Related Domain in DNS Lookup (m .necemarket .com)",

	"ET MALWARE Win32\Cryptbot CnC Domain (kyrjwt45 .top) in DNS Lookup", "ET MALWARE Hisoka CnC Domain Observed in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-cdn .com)", "ET MALWARE Observed Malicious SSL Cert (OSX/AppleJeus Variant CnC)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (runfs .icu)", "ET MALWARE DonotGroup APT Related Domain in DNS Lookup (kotlinn .xyz)", "ET MALWARE Observed BazarLoader Domain (dghns .xyz in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (Magecart/Skimmer CnC)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI", "ET MALWARE Bitter APT CnC Domain (mobisharestock .com) in DNS Lookup", "ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (img565vv6 .holdmydoor .com)", "ET MALWARE Observed Malicious SSL Cert (PHPs Labyrinth Stage1 CnC)", "ET MALWARE Observed TaurusStealer CnC Domain in TLS SNI", "ET MALWARE Malicious Cobalt Strike SSL Cert (asurecloud .tech)", "ET MOBILE_MALWARE Android/IRATA CnC Domain (rimot-anitain .tk) in DNS Lookup", "ET MALWARE Ghostwriter/UNC1151 Related Domain in DNS Lookup (tvasahi .online)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-cdn .xyz)", "ET MALWARE Observed Malicious SSL Cert (AnubisStealer CnC)", "ET MOBILE_MALWARE Android ERMAC Banker (PL) Related Domain in DNS Lookup (bolt-food .site)", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (lm-career .com)", "ET MALWARE Inception/CloudAtlas CnC Domain in DNS Lookup (newmsoffice .com)", "ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (centr-security .com)", "ET MALWARE TraderTraitor CnC Domain (tokenais .com) in DNS Lookup", "ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (centralgoogle .com)", "ET MALWARE Observed Malicious SSL Cert (Lazarus APT MalDoc 2020-11-30)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (realityarchitector .top)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (zuyonijobo .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 3", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (pedaily .online)", "ET MALWARE Observed CobaltStrike/TEARDROP CnC Domain Domain in TLS SNI (mobilnweb .com)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (mejito .ru)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (vasepinay .com)", "ET MALWARE Observed MSIL/Lightning Stealer Domain (panelss .xyz in TLS SNI)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (asureupdate .pro)", "ET MALWARE Observed Malicious SSL Cert (NHS UK Covid Passport Phish)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (scanworld .net)", "ET MOBILE_MALWARE Bahamut Group Fake VPN CnC Domain (ft8hua063okwfdcu21pw .de) in DNS Lookup", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (aloyadakmashin .com)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup (admin-dpsu .org)", "ET MALWARE DonotGroup Related Domain in DNS Lookup (furnish .spacequery .live)", "ET MALWARE SilentLibrarian Domain in DNS Lookup (login .cardiff .acuk .me)", "ET MALWARE Win32/PlugX Related Domain in DNS Lookup", "ET MALWARE Observed PoetRAT Domain (slimip .accesscam .org in TLS SNI)", "ET MALWARE VileRAT Related Domain in DNS Lookup (hubflash .co)", "ET MALWARE Gamaredon CnC Domain (kuckuduk .ru) in DNS Lookup", "ET MALWARE Chaos Botnet CnC Domain (linuxddos .net) in DNS Lookup", "ET MALWARE NOBELIUM Cobalt Strike CnC Domain in DNS Lookup", "ET MALWARE Observed DarkSide Ransomware Domain (baroquetees .com in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (ReactGet Group)", "ET MALWARE Observed Malicious DNS Query (BazarLoader/Team9 Backdoor CnC Domain)", "ET MALWARE TA445/Ghostwrite APT Related Domain in DNS Lookup (xbeta .online)", "ET MALWARE DNS Query to MINEBRIDGE CnC Domain (conversia91 .top)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (server-avira .com) in DNS Lookup", "ET MALWARE Observed CobaltStrike CnC Domain (defendersecyrity .com in TLS SNI)", "ET MALWARE PurpleFox Backdoor Related Domain in DNS Lookup (qq .c1c .ren)", "ET MALWARE SideCopy Related Domain in DNS Lookup (securedesk .one)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 1/2 CnC)", "ET MALWARE Observed Glupteba CnC Domain (cdntokiog .studio in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (DCRat)", "ET MALWARE Observed DonotGroup

	Related Domain (orangeholister .buzz in TLS SNI)", "ET MALWARE Observed Cobalt Strike CnC Domain (Yuxicu .com in TLS SNI)", "ET MALWARE Observed IcedID CnC Domain (nothingtodo .co in TLS SNI)", "ET MALWARE Win32/Lumma Stealer CnC Domain (safe-car .ru) in DNS Lookup", "ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .carelessnessing .com)", "ET MALWARE Observed CobaltStrike Loader Domain (cybersecyrity .com in TLS SNI)", "ET MALWARE Observed Maldoc CnC Domain (cloud-documents .com in TLS SNI)", "ET MALWARE Arid Viper APT Related Domain in DNS Lookup (dorothymambrose .live)", "ET MALWARE TA444 Related Domain in DNS Lookup (documentworkspace .io)", "ET MOBILE_MALWARE Android Brunhilda Dropper (readyqrscanner .club in DNS Lookup)", "ET MALWARE AppleJeus - JMT Trading CnC Domain in DNS Lookup (jmttrading .org)", "ET MALWARE Kimsuky CnC Domain (okihs .mypressonline .com) Observed in DNS Query", "ET MALWARE Suspicious Domain (lawyeryouwant .com) in TLS SNI", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (blogsolutions .top in TLS SNI)", "ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (babaroga .lib)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (jobs .registermegod .online)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (4qzm .com)", "ET MALWARE PlugX Related Domain in DNS Lookup (wpsup .daj8 .me)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (www .datacentre .center)", "ET MALWARE Win32\Cryptbot CnC Domain (pefjfw62 .top) in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-endpoint .xyz)", "ET MALWARE SocGholish CnC Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Sidewinder CnC)", "ET MALWARE Observed CobaltStrike CnC Domain (gmbfrom .com in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (goerge-amper .website in DNS Lookup)", "ET MALWARE EvilNum APT Related Domain in DNS Lookup (imageztun .com)", "ET INFO localtunnel Tunneling Domain in DNS Lookup (loca .lt)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ptcl-gov .com)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (linda-callaghan .icu)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (www .get .adobe .com .aspx .io)", "ET MALWARE Observed Malicious SSL Cert (MirrorThief CnC)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-blog .xyz)", "ET MALWARE Observed DNS Query to DonotGroup Domain (stokpro .buzz)", "ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tocaoonline .org)", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (stanculinaryblog .top in TLS SNI)", "ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (belcherjacky .info)", "ET MALWARE ErbiumStealer CnC Domain (a0715952 .xsph .ru) in DNS Lookup", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Agent.aam CnC Domain in DNS Lookup", "ET MALWARE Observed DNS Query to TA444 Domain (azure-protect .online)", "ET MALWARE TA452 Related Domain in DNS Lookup", "ET MALWARE TeamTNT Related Domain in DNS Lookup (chimaera .cc)", "ET MOBILE_MALWARE Trojan-Ransom.AndroidOS.Agent.bi CnC Domain in DNS Lookup", "ET MALWARE DPRK APT Related Domain in DNS Lookup (alticgo .com)", "ET MALWARE Observed Malicious SSL Cert (SedUploader)", "ET MOBILE_MALWARE Android/Drinik CnC Domain (gia .3utilities .com) in DNS Lookup", "ET MOBILE_MALWARE Arid Viper (fasebcak .com in DNS Lookup)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)", "ET MOBILE_MALWARE Arid Viper (vickeryduncan .site in DNS Lookup)", "ET MALWARE lu0bot CnC Domain in DNS Lookup", "ET MALWARE Observed DangerousPassword APT Related Domain (shopapptech .com in TLS SNI)", "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)", "ET MALWARE Observed Malicious SSL Cert (CoreBot C2)", "ET MALWARE ErbiumStealer CnC Domain (www .f0679086 .xsph .ru) in DNS Lookup", "ET MALWARE SSL/TLS Certificate Observed (Link Implant Default)", "ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (rp .oiwcvbnc2e .stream) in DNS Lookup", "ET MOBILE_MALWARE Android Brunhilda Dropper (multifuctionscanner .club in DNS Lookup)", "ET MALWARE Win32\Cryptbot CnC Domain (suqoyw07 .top) in DNS Lookup", "ET MALWARE Arid Gopher Related Domain in DNS Lookup (mozelllittel

	.com)", "ET MALWARE Observed SSV Agent CnC Domain (drmtake .tk in TLS SNI)", "ET MALWARE APT36/TransparentTribe CnC Domain (richa-sharma .ddns .net) in DNS Lookup", "ET MALWARE Observed BazarLoader Domain (bigjamg .xyz in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (fasibauik .co in DNS Lookup)", "ET MALWARE Gamaredon CnC Domain Observed in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-blog .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Origami.b / Donot DNS Lookup", "ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Guerrilla.h CnC Domain in DNS Lookup", "ET MALWARE Win32/Warzone RAT Variant CnC Domain in DNS Lookup (dost .igov-service .net)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (advanced-ip-scaner .com)", "ET MALWARE Observed Glupteba CnC Domain (cdneurops .shop in TLS SNI)", "ET MOBILE_MALWARE Arid Viper (richardbeman .info in DNS Lookup)", "ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (git-api .com)", "ET MALWARE Observed Elysium Stealer Domain in TLS SNI (download-serv-234116 .xyz)", "ET MALWARE TraderTraitor CnC Domain (dafom .dev) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Silver Implant)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (thereisnoscheme .top)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 5", "ET MALWARE Observed Malicious SSL Cert (ElegyRAT)", "ET MALWARE RustyBuer CnC Domain in SNI", "ET MALWARE Observed FIN12 Related Domain (hdhuge .com in TLS SNI)", "ET MALWARE Observed CobaltStrike CnC Domain (krinsop .com in TLS SNI)", "ET MALWARE Maldoc Domain (word2022 .c1 .biz) in DNS Lookup", "ET MALWARE Qakbot/Cobalt Strike Domain (dimingol .com) in DNS Lookup", "ET MALWARE AppleJeus - Ants2Whale CnC Domain in DNS Lookup (ants2whale .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-endpoint .com)", "ET MALWARE TA444 Related Domain in DNS Lookup (prosec .ink)", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (gentlebouncer .top)", "ET MALWARE Suspected CloudAtlas Related Domain in DNS Lookup (protocol-list .com)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (msresearchcenter .top in TLS SNI)", "ET MALWARE Confucious APT Related Domain in DNS Lookup (viterwin .club)", "ET MALWARE Observed Glupteba CnC Domain (zaoshang .ru in TLS SNI)", "ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)", "ET MALWARE Observed Malicious SSL Cert (DonotGroup Stage 2 CnC)", "ET MALWARE Observed Malicious SSL Cert (LazarusGroup CnC)", "ET MALWARE Observed Malicious SSL Cert (OZH Rat)", "ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (service .exfil .site)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup (bitsbfree .com)", "ET MALWARE Win32\Cryptbot CnC Domain (towcqx32 .top) in DNS Lookup", "ET MALWARE Suspected POLONIUM CnC Domain (ukrsupport .info) in DNS Lookup", "ET MALWARE Shuckworm/Gamaredon CnC Domain (pasamart .ru) in DNS Lookup", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (designautocad .org)", "ET MALWARE APT41 CnC Domain (www .affice366 .com) in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-endpoint .com)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (kc-3 .ru)", "ET MALWARE JSSLoader CnC Domain (essentialsmassageanddayspa .com) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (Cobalt Strike Malleable C2 Domain)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup (faristo .site)", "ET MOBILE_MALWARE Possible Trojan-Banker.AndroidOS.Sharkbot Activity (DNS Lookup)", "ET MALWARE DonotGroup CnC Domain in DNS Query", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-schnellvpn .xyz)", "ET MOBILE_MALWARE Arid Viper (hidden-chat-e58d7 .firebaseio .com in DNS Lookup)", "ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (vikingsofnorth .top)", "ET MALWARE Stonefly APT Related Domain in DNS Lookup (semiconductboard .com)", "ET MALWARE Chaos Botnet CnC Domain (x .xlg360 .xyz) in DNS Lookup", "ET MALWARE FIN7 Related CnC Domain in DNS Lookup (bypassociation .com)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (autopartslarry .top)", "ET MALWARE SHARPEXT CnC Domain in DNS Lookup (siekis .com)", "ET MALWARE Observed DNS Query to Malicious Powershell Payload domain (onerecovery .click)", "ET MALWARE Suspected APT28 Related Domain in DNS Lookup

	(jimbeam .live)", "ET MALWARE Matanbuchus CnC Domain in DNS Lookup (eonsabode .at)", "ET MALWARE PlugX Related Domain in DNS Lookup (cxks8 .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-blog .com)", "ET MALWARE Observed Malicious SSL Cert (Moist Stealer CnC)", "ET MALWARE SManager Backdoor Domain in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (W32/TrojanDownloader.Agent.FBF Variant CnC)", "ET MOBILE_MALWARE Arid Viper (joe-rumley .pw in DNS Lookup)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (realonlinetrend .top in TLS SNI)", "ET MALWARE SocGholish Related Domain in DNS Lookup (irsbusinessaudit .net)", "ET MALWARE IcedID CnC Domain in DNS Lookup", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-blog .com)", "ET MOBILE_MALWARE Arid Viper (fasebaok .com in DNS Lookup)", "ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (youareperfect2day .top in TLS SNI)", "ET MALWARE Win32/CopperStealer CnC Domain (ec083aa56dc0449a .com) in DNS Lookup", "ET MALWARE Loki Locker Ransomware CnC Domain in DNS Lookup", "ET MALWARE Rovnix CnC Domain in DNS Query", "ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-blog .xyz)", "ET MALWARE Metador CnC Domain (networkselfhelp .com) in DNS Lookup", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (hawkshaw-cae48 .firebaseio .com in DNS Lookup)", "ET MALWARE Observed Glupteba CnC Domain (zaoshanghaoz .net in TLS SNI)", "ET MALWARE DPRK APT Related Domain in DNS Lookup (esilet .com)", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-schnellvpn .com)", "ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (finalcountdown .top)", "ET MOBILE_MALWARE Arid Viper (kevin-good .top in DNS Lookup)", "ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (update-pgp .com) in DNS Lookup", "ET MALWARE DonotGroup Staging Domain in DNS Query", "ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain", "ET MALWARE Donot APT Related Domain in DNS Lookup (biteupdates .site)", "ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-06-18)", "ET MALWARE MoonBounce Backdoor Related Domain in DNS Lookup (glbaitech .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (spitfirepanel .firebaseio .com in DNS Lookup)", "ET MALWARE Gamaredon CnC Domain in DNS Lookup (lovers .semara .ru)", "ET MALWARE Observed ZLoader Related Domain (lkjhgfgsdshja .com in TLS SNI)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 9", "ET MALWARE TA444 Related Domain in DNS Lookup (auto-protection .cloud)", "ET MALWARE BLINDEAGLE CnC Domain (laminascol .linkpc .net) in DNS Lookup", "ET MALWARE Chaos Botnet CnC Domain (are .nishabig .pro) in DNS Lookup", "ET MALWARE GhostWriter APT Related Cobalt Strike Domain in DNS Lookup (hmgo .pw)", "ET MALWARE Observed Ttint Update CnC Domain in DNS Query", "ET MALWARE Observed Elysium Stealer Variant CnC Domain (all-brain-company .xyz in TLS SNI)", "ET MALWARE MagicRAT CnC Domain (gendoraduragonkgp126 .com) in DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (APT32 CnC)", "ET MALWARE Observed Targeted Attack Malicious SSL Cert (angeldonationblog .com)", "ET MALWARE Observed Malicious SSL Cert (Gootkit CnC)", "ET MALWARE Win32\Cryptbot CnC Domain (okwerh01 .top) in DNS Lookup", "ET MALWARE TA453 Related CnC Domain in DNS Lookup (0standavalue0 .xyz)", "ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (shopapppro .com)", "ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (melindas .ru)", "ET MALWARE AppleJeus - Kupay Wallet CnC Domain in DNS Lookup (levelframeblog .com)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (bqtconsulting .com)", "ET MALWARE PowerShell/PowHeartBeat CnC Domain (airplane .travel-commercials .agency) in DNS Lookup", "ET MALWARE Observed Reverse Shell Payload Delivery Domain (opentunnel .quest) in TLS SNI", "ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-schnellvpn .xyz)", "ET MALWARE Evilnum APT Related Domain in DNS Lookup (image .jamespage .net)", "ET MOBILE_MALWARE Android.Trojan.Rana.A (wherisdomaintv .com in DNS Lookup)", "ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)", "ET MALWARE SoulSearcher Malware Domain in DNS Lookup (gmy .cimadlicks .net)", "ET MALWARE Observed OSX/WizardUpdate Domain in TLS SNI

	(.dlvplayer .com)", "ET MOBILE_MALWARE Arid Viper (lordblackwood .club in DNS Lookup)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (internal .blessedfoodshalalmeat .com)", "ET MALWARE Observed Win32/DuckLogs Malware Domain (ducklogs .com in TLS SNI)", "ET MALWARE Observed Malicious SSL Cert (MageCart Group 5 Staging Domain)", "ET MALWARE Observed Malicious SSL Cert (Panda Banker Injects)", "ET MALWARE DonotGroup CnC Domain Observed in DNS Query", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (jersydok .com)", "ET MOBILE_MALWARE Arid Viper (play-store-51182 .appspot .com in DNS Lookup)", "ET MALWARE ActionLoader CnC Domain in DNS Lookup (azure-tech .pro)"
SSL-сертификаты используемые вредоносным ПО и ботнетами	"SSL Fingerprint Blacklist: Malicious SSL certificate detected (Qadars C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Cobalt C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Malware distribution)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Geodo MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Qadars MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (ZLoader C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Worm.Dorkbot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Teslacrypt C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Android Marcher C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Dridex)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (PandaZeuS C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Android Exobot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (ZeuS C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Downloder-Bot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (URLzone C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Rovnix C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (TorrentLocker C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (VMZeuS C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Hancitor C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (AKBuilder C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (ZeuS MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (TrickBot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Zloader C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (VMZeuS MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Ransomware C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Flokibot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (PandaBanker C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Quakbot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Chthonic MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (CryptoLocker C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Gozi MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Upatre C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Vawtrak MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Vawtrak C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Tilon MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Spambot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Nexuslogger C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Corebot C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (PandaZeuS MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Send-Safe C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (DiamondFox C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Bebloh C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Kronos MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Tinba MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Smoke Loader C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Chthonic C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (CryptoWall C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (URLzone)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Redyms C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (KINS C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Malware C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate

	detected (Gozi C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Neutrino C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Gootkit C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (H1N1 C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Sofacy C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (RockLoader C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Downloader.Pony C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Adwind C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Marcher C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Tuhkit C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Silon MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (KINS MITM)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (FindPOS C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (ProxyChanger C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Retefe C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Shylock C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (JBifrost C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (TorrrentLocker C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Dridex C&C)", "SSL Fingerprint Blacklist: Malicious SSL certificate detected (Shifu C&C)"
Ошибки в сетевых протоколах	"ET INFO SOCKSv4 HTTP Proxy Inbound Request (Windows Source)", "GPL NETBIOS SMB IPC$ unicode share access", "GPL NETBIOS SMB-DS winreg little endian bind attempt", "GPL NETBIOS SMB ADMIN$ unicode share access", "ET INFO SOCKSv5 DNS Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS RemoteActivation little endian andx attempt", "ET INFO SOCKSv4 HTTP Proxy Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS NT Trans NT CREATE unicode oversized Security Descriptor attempt", "GPL NETBIOS SMB IrotIsRunning andx attempt", "GPL NETBIOS SMB-DS ADMIN$ unicode andx share access", "ET INFO WinHttp AutoProxy Request wpad.dat Possible BadTunnel", "GPL NETBIOS SMB-DS IrotIsRunning unicode little endian attempt", "GPL SQL MYSQL root login attempt", "GPL NETBIOS SMB nddeapi andx bind attempt", "ET INFO SOCKSv5 Port 1863 Inbound Request (Linux Source)", "GPL NETBIOS SMB irot bind attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode attempt", "GPL NETBIOS SMB-DS nddeapi unicode create tree attempt", "GPL NETBIOS SMB-DS IrotIsRunning unicode attempt", "GPL NETBIOS SMB ISystemActivator little endian bind attempt", "GPL NETBIOS SMB winreg little endian andx bind attempt", "GPL NETBIOS SMB llsrpc unicode bind attempt", "GPL NETBIOS DCERPC LSASS direct bind attempt", "GPL NETBIOS SMB-DS irot unicode little endian andx bind attempt", "GPL NETBIOS SMB-DS winreg andx create tree attempt", "GPL NETBIOS SMB-DS Session Setup NTMLSSP asn1 overflow attempt", "GPL NETBIOS SMB-DS ISystemActivator bind attempt", "GPL NETBIOS DCERPC LSASS bind attempt", "ET SCAN MYSQL 4.0 brute force root login attempt", "GPL NETBIOS SMB-DS D$ unicode share access", "GPL NETBIOS SMB-DS ADMIN$ share access", "GPL NETBIOS DCERPC IActivation little endian bind attempt", "GPL NETBIOS SMB-DS llsrpc unicode andx create tree attempt", "GPL NETBIOS SMB NT Trans NT CREATE unicode invalid SACL ace size dos attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Response)", "GPL NETBIOS SMB NT Trans NT CREATE invalid SACL ace size dos attempt", "ET INFO SOCKSv4 Port 443 Inbound Request (Windows Source)", "GPL NETBIOS SMB ADMIN$ share access", "GPL SQL connect_data remote version detection attempt", "GPL NETBIOS SMB-DS IrotIsRunning unicode little endian andx attempt", "GPL NETBIOS SMB-DS RemoteActivation unicode little endian andx attempt", "GPL NETBIOS SMB-DS NT Trans NT CREATE unicode invalid SACL ace size dos attempt", "ET INFO PTUNNEL INBOUND", "GPL NETBIOS SMB-DS ISystemActivator unicode little endian bind attempt", "GPL NETBIOS SMB RemoteActivation andx attempt", "GPL NETBIOS SMB ISystemActivator unicode little endian andx bind attempt", "GPL NETBIOS SMB Session Setup NTMLSSP unicode andx asn1 overflow attempt", "GPL NETBIOS SMB-DS RemoteActivation little endian attempt", "ET POLICY MS Terminal Server Root login", "GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt", "ET MALWARE MS Remote Desktop edc User Login Request", "GPL NETBIOS SMB CoGetInstanceFromFile little endian andx attempt", "GPL NETBIOS SMB DCERPC LSASS bind attempt", "GPL NETBIOS

	SMB-DS NT Trans NT CREATE DACL overflow attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag false change port flag false)", "GPL NETBIOS SMB nddeapi unicode bind attempt", "GPL NETBIOS SMB IActivation little endian bind attempt", "GPL NETBIOS SMB irot unicode bind attempt", "GPL NETBIOS SMB-DS InitiateSystemShutdown little endian andx attempt", "GPL NETBIOS SMB winreg andx bind attempt", "ET INFO SOCKSv4 Port 1863 Inbound Request (Linux Source)", "GPL NETBIOS SMB NT Trans NT CREATE SACL overflow attempt", "ET SCAN MYSQL MySQL Remote FAST Account Password Cracking", "GPL NETBIOS SMB irot unicode little endian bind attempt", "GPL NETBIOS SMB-DS C$ share access", "ET INFO SOCKSv4 Port 1863 Inbound Request (Windows Source)", "GPL NETBIOS SMB nddeapi unicode andx create tree attempt", "GPL NETBIOS SMB NT Trans NT CREATE andx oversized Security Descriptor attempt", "GPL NETBIOS SMB llsrpc bind attempt", "GPL NETBIOS SMB IActivation unicode little endian andx bind attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian attempt", "GPL NETBIOS SMB msqueue little endian andx bind attempt", "GPL NETBIOS SMB IrotIsRunning unicode little endian attempt", "GPL NETBIOS DCERPC msqueue bind attempt", "ET POLICY MS Remote Desktop POS User Login Request", "GPL NETBIOS SMB-DS irot little endian bind attempt", "GPL NETBIOS SMB ISystemActivator andx bind attempt", "GPL NETBIOS SMB-DS IActivation little endian bind attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian andx attempt", "GPL NETBIOS SMB-DS IrotIsRunning unicode andx attempt", "GPL NETBIOS SMB-DS llsrpc andx bind attempt", "ET INFO SOCKSv4 Port 25 Inbound Request (Windows Source)", "GPL NETBIOS SMB nddeapi create tree attempt", "GPL NETBIOS SMB-DS llsrpc unicode little endian andx bind attempt", "GPL NETBIOS SMB-DS winreg andx bind attempt", "ET WEB_CLIENT Microsoft OLE Compound File With Flash", "GPL NETBIOS SMB-DS InitiateSystemShutdown little endian attempt", "GPL NETBIOS SMB msqueue bind attempt", "GPL NETBIOS SMB irot unicode andx bind attempt", "GPL NETBIOS DCERPC IActivation bind attempt", "ET INFO SOCKSv5 Port 443 Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS NT Trans NT CREATE unicode SACL overflow attempt", "GPL NETBIOS SMB IActivation andx bind attempt", "GPL NETBIOS SMB winreg unicode create tree attempt", "ET INFO SOCKSv4 Port 5050 Inbound Request (Linux Source)", "GPL NETBIOS SMB RemoteActivation little endian andx attempt", "GPL NETBIOS SMB IrotIsRunning little endian attempt", "GPL NETBIOS SMB-DS irot little endian andx bind attempt", "GPL NETBIOS SMB-DS nddeapi bind attempt", "GPL NETBIOS SMB IPC$ share access", "GPL NETBIOS SMB nddeapi bind attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile attempt", "GPL NETBIOS SMB-DS llsrpc unicode little endian bind attempt", "GPL NETBIOS SMB msqueue andx bind attempt", "GPL NETBIOS SMB-DS RemoteActivation andx attempt", "GPL NETBIOS SMB irot little endian bind attempt", "GPL FTP LIST directory traversal attempt", "GPL NETBIOS SMB winreg little endian bind attempt", "ET INFO SOCKSv5 Port 5190 Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS ISystemActivator unicode andx bind attempt", "ET MALWARE MS Remote Desktop micros User Login Request", "GPL NETBIOS SMB-DS IPC$ share access", "GPL NETBIOS SMB IrotIsRunning attempt", "GPL NETBIOS SMB llsrpc unicode little endian bind attempt", "GPL NETBIOS SMB NT Trans NT CREATE andx DACL overflow attempt", "GPL NETBIOS SMB-DS msqueue unicode little endian andx bind attempt", "GPL NETBIOS SMB llsrpc little endian bind attempt", "GPL NETBIOS SMB CoGetInstanceFromFile attempt", "GPL NETBIOS SMB-DS IrotIsRunning little endian attempt", "GPL NETBIOS DCERPC msqueue little endian bind attempt", "GPL NETBIOS SMB InitiateSystemShutdown andx attempt", "GPL NETBIOS SMB-DS nddeapi unicode bind attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag true change port flag true)", "GPL NETBIOS SMB-DS winreg little endian andx bind attempt", "GPL NETBIOS SMB-DS DCERPC ISystemActivator bind attempt", "GPL NETBIOS SMB-DS NT Trans NT CREATE SACL overflow attempt", "GPL NETBIOS SMB NT Trans NT CREATE andx SACL overflow attempt", "GPL NETBIOS SMB-DS irot unicode little endian bind attempt", "GPL NETBIOS SMB-DS llsrpc little endian andx bind attempt", "GPL NETBIOS SMB-DS msqueue andx bind attempt", "GPL NETBIOS SMB-DS winreg unicode little endian andx

	bind attempt", "GPL NETBIOS SMB-DS winreg bind attempt", "GPL NETBIOS SMB msqueue little endian bind attempt", "GPL NETBIOS SMB-DS ISystemActivator unicode bind attempt", "GPL NETBIOS SMB-DS msqueue little endian andx bind attempt", "ET POLICY Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 1 with default BMC usernames (Admin|root|Administrator|USERID)", "GPL NETBIOS SMB-DS D$ unicode andx share access", "GPL NETBIOS SMB-DS InitiateSystemShutdown unicode attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian attempt", "GPL NETBIOS SMB-DS D$ share access", "GPL NETBIOS SMB C$ unicode share access", "GPL NETBIOS SMB RemoteActivation little endian attempt", "GPL NETBIOS SMB InitiateSystemShutdown attempt", "ET INFO PTUNNEL OUTBOUND", "GPL NETBIOS SMB-DS msqueue unicode little endian bind attempt", "GPL NETBIOS SMB ISystemActivator unicode bind attempt", "GPL NETBIOS SMB-DS IPC$ unicode andx share access", "GPL NETBIOS SMB ISystemActivator unicode andx bind attempt", "GPL NETBIOS SMB D$ unicode share access", "GPL NETBIOS SMB-DS winreg unicode little endian bind attempt", "GPL NETBIOS SMB CoGetInstanceFromFile unicode andx attempt", "ET INFO NBNS Name Query Response Possible WPAD Spoof BadTunnel", "GPL NETBIOS DCERPC irot little endian bind attempt", "ET INFO SOCKSv4 Port 443 Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS InitiateSystemShutdown unicode little endian andx attempt", "GPL NETBIOS SMB-DS nddeapi andx create tree attempt", "GPL NETBIOS SMB-DS llsrpc bind attempt", "GPL NETBIOS SMB-DS IActivation unicode little endian andx bind attempt", "ET INFO SOCKSv5 Port 443 Inbound Request (Windows Source)", "GPL NETBIOS SMB InitiateSystemShutdown little endian andx attempt", "GPL NETBIOS SMB-DS C$ unicode andx share access", "ET INFO SOCKSv5 Port 5190 Inbound Request (Windows Source)", "GPL NETBIOS SMB-DS RemoteActivation unicode little endian attempt", "ET INFO SOCKSv5 DNS Inbound Request (Windows Source)", "GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian andx attempt", "GPL NETBIOS SMB-DS nddeapi unicode andx create tree attempt", "GPL NETBIOS SMB-DS nddeapi andx bind attempt", "GPL NETBIOS SMB IrotIsRunning unicode little endian andx attempt", "ET ATTACK_RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 2 status code Unauthorized Name", "GPL NETBIOS SMB winreg unicode andx bind attempt", "GPL NETBIOS SMB-DS llsrpc unicode andx bind attempt", "GPL NETBIOS SMB IrotIsRunning unicode attempt", "GPL NETBIOS SMB-DS winreg unicode andx create tree attempt", "GPL NETBIOS DCERPC irot bind attempt", "GPL NETBIOS SMB-DS NT Trans NT CREATE invalid SACL ace size dos attempt", "ET INFO SOCKSv4 Port 5050 Inbound Request (Windows Source)", "GPL NETBIOS SMB-DS InitiateSystemShutdown unicode little endian attempt", "GPL NETBIOS SMB-DS msqueue unicode bind attempt", "GPL NETBIOS SMB IActivation unicode andx bind attempt", "ET POLICY MS Remote Desktop Service User Login Request", "GPL NETBIOS SMB winreg bind attempt", "GPL NETBIOS SMB-DS IActivation andx bind attempt", "GPL NETBIOS SMB winreg andx create tree attempt", "GPL NETBIOS SMB-DS DCERPC ISystemActivator unicode bind attempt", "GPL NETBIOS SMB ISystemActivator bind attempt", "GPL NETBIOS SMB-DS winreg unicode bind attempt", "GPL NETBIOS SMB-DS IActivation unicode little endian bind attempt", "GPL NETBIOS SMB msqueue unicode little endian andx bind attempt", "GPL NETBIOS SMB-DS llsrpc unicode bind attempt", "GPL NETBIOS SMB llsrpc little endian andx bind attempt", "ET WEB_CLIENT Microsoft OLE Compound File Magic Bytes Flowbit Set", "ET ATTACK_RESPONSE MySQL User Account Enumeration", "GPL NETBIOS SMB msqueue unicode little endian bind attempt", "GPL NETBIOS SMB CoGetInstanceFromFile andx attempt", "GPL NETBIOS SMB-DS ADMIN$ andx share access", "GPL NETBIOS SMB Session Setup NTMLSSP andx asn1 overflow attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag true change port flag false)", "ET SCAN MYSQL 4.1 brute force root login attempt", "GPL NETBIOS SMB CoGetInstanceFromFile little endian attempt", "GPL NETBIOS SMB-DS IActivation unicode bind attempt", "GPL NETBIOS SMB-DS NT Trans NT CREATE oversized Security Descriptor attempt", "GPL NETBIOS SMB-DS ISystemActivator unicode little endian andx bind attempt", "GPL NETBIOS SMB winreg create tree attempt", "GPL NETBIOS

	SMB-DS nddeapi unicode andx bind attempt", "GPL NETBIOS SMB-DS C$ unicode share access", "GPL NETBIOS SMB nddeapi unicode create tree attempt", "ET POLICY MS Remote Desktop Administrator Login Request", "GPL FTP large PWD command", "ET INFO SOCKSv5 HTTP Proxy Inbound Request (Windows Source)", "GPL NETBIOS SMB-DS ADMIN$ unicode share access", "GPL NETBIOS SMB RemoteActivation unicode little endian attempt", "GPL NETBIOS SMB ISystemActivator little endian andx bind attempt", "GPL NETBIOS SMB-DS RemoteActivation attempt", "GPL NETBIOS SMB InitiateSystemShutdown little endian attempt", "GPL NETBIOS SMB NT Trans NT CREATE unicode DACL overflow attempt", "ET INFO SOCKSv5 Port 25 Inbound Request (Windows Source)", "GPL NETBIOS SMB IActivation unicode bind attempt", "ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag false change port flag true)", "GPL NETBIOS SMB InitiateSystemShutdown unicode attempt", "GPL NETBIOS SMB-DS DCERPC LSASS bind attempt", "ET INFO SOCKSv4 Port 5190 Inbound Request (Windows Source)", "ET INFO SOCKSv4 Port 5190 Inbound Request (Linux Source)", "GPL NETBIOS SMB RemoteActivation attempt", "GPL NETBIOS SMB msqueue unicode bind attempt", "GPL NETBIOS SMB msqueue unicode andx bind attempt", "GPL NETBIOS SMB-DS IActivation unicode andx bind attempt", "GPL NETBIOS SMB-DS IPC$ andx share access", "GPL NETBIOS SMB llsrpc unicode andx bind attempt", "GPL NETBIOS SMB-DS ISystemActivator little endian andx bind attempt", "GPL NETBIOS SMB-DS IPC$ unicode share access", "GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode andx attempt", "GPL NETBIOS SMB RemoteActivation unicode attempt", "GPL NETBIOS SMB IActivation unicode little endian bind attempt", "GPL NETBIOS SMB DCERPC LSASS direct bind attempt", "GPL NETBIOS SMB winreg unicode bind attempt", "GPL NETBIOS SMB-DS CoGetInstanceFromFile andx attempt", "GPL NETBIOS SMB winreg unicode little endian bind attempt", "GPL NETBIOS SMB winreg unicode andx create tree attempt", "GPL NETBIOS SMB ISystemActivator unicode little endian bind attempt", "GPL NETBIOS SMB llsrpc andx bind attempt", "GPL NETBIOS SMB C$ share access", "GPL NETBIOS SMB-DS IrotIsRunning little endian andx attempt", "ET INFO SOCKSv5 Port 5050 Inbound Request (Windows Source)", "GPL NETBIOS SMB InitiateSystemShutdown unicode andx attempt", "GPL NETBIOS SMB irot little endian andx bind attempt", "GPL NETBIOS SMB nddeapi andx create tree attempt", "GPL NETBIOS SMB IActivation little endian andx bind attempt", "GPL NETBIOS SMB-DS NT Trans NT CREATE unicode DACL overflow attempt", "GPL NETBIOS SMB NT Trans NT CREATE unicode andx SACL overflow attempt", "GPL NETBIOS SMB-DS IrotIsRunning andx attempt", "GPL SQL MYSQL show databases attempt", "ET INFO SOCKSv5 Port 5050 Inbound Request (Linux Source)", "GPL NETBIOS SMB CoGetInstanceFromFile unicode attempt", "GPL NETBIOS SMB-DS InitiateSystemShutdown attempt", "GPL NETBIOS SMB irot andx bind attempt", "GPL NETBIOS SMB irot unicode little endian andx bind attempt", "GPL NETBIOS SMB-DS ISystemActivator little endian bind attempt", "GPL NETBIOS SMB llsrpc create tree attempt", "GPL NETBIOS SMB IActivation bind attempt", "GPL NETBIOS SMB-DS IActivation bind attempt", "GPL NETBIOS SMB RemoteActivation unicode andx attempt", "ET INFO SOCKSv5 HTTP Proxy Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS IrotIsRunning attempt", "GPL NETBIOS SMB winreg unicode little endian andx bind attempt", "ET INFO Web Proxy Auto Discovery Protocol WPAD DHCP 252 option Possible BadTunnel", "GPL NETBIOS SMB-DS irot unicode andx bind attempt", "GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian attempt", "GPL NETBIOS DCERPC IrotIsRunning attempt", "GPL NETBIOS SMB-DS ISystemActivator andx bind attempt", "GPL NETBIOS SMB nddeapi unicode andx bind attempt", "GPL NETBIOS SMB-DS DCERPC LSASS direct bind attempt", "GPL NETBIOS SMB-DS RemoteActivation unicode attempt", "GPL NETBIOS SMB-DS winreg create tree attempt", "GPL NETBIOS SMB NT Trans NT CREATE DACL overflow attempt", "GPL NETBIOS SMB-DS msqueue bind attempt", "GPL NETBIOS SMB-DS llsrpc little endian bind attempt", "GPL NETBIOS SMB-DS InitiateSystemShutdown andx attempt", "GPL NETBIOS SMB-DS nddeapi create tree attempt", "GPL NETBIOS SMB InitiateSystemShutdown unicode little endian attempt", "GPL NETBIOS SMB-DS msqueue little endian bind attempt", "GPL NETBIOS SMB IrotIsRunning unicode andx

	attempt", "GPL NETBIOS SMB-DS msqueue unicode andx bind attempt", "GPL NETBIOS SMB-DS winreg unicode andx bind attempt", "GPL NETBIOS SMB InitiateSystemShutdown unicode little endian andx attempt", "GPL FTP CWD Root directory transversal attempt", "GPL NETBIOS SMB-DS RemoteActivation unicode andx attempt", "GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian andx attempt", "GPL NETBIOS SMB D$ share access", "GPL NETBIOS SMB-DS DCERPC LSASS unicode bind attempt", "ET INFO SOCKSv5 Port 1863 Inbound Request (Windows Source)", "GPL FTP invalid MODE", "GPL NETBIOS SMB RemoteActivation unicode little endian andx attempt", "GPL NETBIOS SMB llsrpc unicode little endian andx bind attempt", "GPL NETBIOS SMB NT Trans NT CREATE unicode oversized Security Descriptor attempt", "ET INFO SOCKSv5 Port 25 Inbound Request (Linux Source)", "GPL NETBIOS SMB-DS irot unicode bind attempt", "GPL NETBIOS DCERPC IrotIsRunning little endian attempt", "GPL NETBIOS SMB-DS irot bind attempt", "GPL NETBIOS SMB-DS IActivation little endian andx bind attempt", "GPL NETBIOS SMB-DS InitiateSystemShutdown unicode andx attempt", "GPL NETBIOS SMB-DS winreg unicode create tree attempt", "GPL NETBIOS SMB-DS irot andx bind attempt", "GPL NETBIOS SMB NT Trans NT CREATE unicode SACL overflow attempt", "GPL NETBIOS SMB IrotIsRunning little endian andx attempt", "GPL NETBIOS SMB NT Trans NT CREATE oversized Security Descriptor attempt"
Анонимайзеры	"Stealthy", "Anonymizer from United Kingdom", "Anonymizer detected", "Browsec", "ZenMate API", "RusVPN detected", "Proxy detected", "ZenMate proxy", "proxy from vk-unblock", "Anonymizer from United States", "Firefox VPN Add-on", "Yandex Turbo", "Anonymox HTTP", "friGate", "Opera VPN", "Anonymizer from Netherlands", "ZenMate DNS", "Anonymizer from Canada", "Opera Turbo", "Anonymox", "dostup-rutracker", "HotspotShield detected", "Anonymizer from Poland"
Нежелательное программное обеспечение	"ET ADWARE_PUP User-Agent (MyIE/1.0)", "ET ADWARE_PUP Fake Adobe Update Request", "ET ADWARE_PUP Win-touch.com Spyware User-Agent (WTInstaller)", "ET USER_AGENTS Suspicious User-Agent (Updater)", "ET ADWARE_PUP Best-targeted-traffic.com Spyware Install", "ET ADWARE_PUP Mysearch.com/Morpheus Bar Spyware User-Agent (Morpheus)", "ET ADWARE_PUP Realtimegaming.com Online Casino Spyware Gaming Checkin", "ET ADWARE_PUP Megaupload Spyware User-Agent (Megaupload)", "ET ADWARE_PUP Observed Win32/Foniad Domain (enclosely .info in TLS SNI)", "ET ADWARE_PUP Win32/Spy.Agent.QCL Variant Activity (POST) M2", "ET ADWARE_PUP Suspicious User Agent Custom_56562_HttpClient/VER_STR_COMMA", "ET USER_AGENTS Suspicious User-Agent (ClickAdsByIE)", "ET ADWARE_PUP Common Adware Library ISX User Agent Detected", "ET ADWARE_PUP SuperAntiSpyware Install Checkin", "ET ADWARE_PUP Conduit Trovi Adware/PUA", "ET ADWARE_PUP Successful QuizScope Installation", "ET ADWARE_PUP LNKR landing page (possible compromised site) M4", "ET ADWARE_PUP Crossrider Spyware Checkin", "ET ADWARE_PUP Win32/InstallCore Initial Install Activity 1", "ET ADWARE_PUP Adware.InstallCore.B Checkin", "ET ADWARE_PUP User-Agent (FileDownloader)", "ET ADWARE_PUP Context Plus User-Agent (PTS)", "ET ADWARE_PUP Win32/Adware.InstallCommerce.A CnC Checkin", "ET ADWARE_PUP Look2me Spyware Activity (1)", "ET ADWARE_PUP Fun Web Products Spyware User-Agent (FunWebProducts)", "ET ADWARE_PUP Crackswin Downloader Activity", "ET ADWARE_PUP User-Agent (0xa10xa1HttpClient)", "ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (B Register)", "ET ADWARE_PUP W32/BettrExperience.Adware POST Checkin", "ET ADWARE_PUP VilnyNet VPN Install Started", "ET ADWARE_PUP Win32/LoadMoney Adware Activity", "ET ADWARE_PUP Morpheus Spyware Install User-Agent (SmartInstaller)", "ET ADWARE_PUP AdWare.MSIL.Solimba.b POST", "ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin M6", "ET ADWARE_PUP Shopathomeselect .com Spyware User-Agent (WebDownloader)", "ET ADWARE_PUP Observed Win32/Foniad Domain (suggedin .info in TLS SNI)", "ET ADWARE_PUP Sogou Toolbar Checkin", "ET ADWARE_PUP Theinstalls.com Initial Checkin", "ET ADWARE_PUP LNKR landing page (possible compromised site) M5", "ET ADWARE_PUP Best-targeted-traffic.com Spyware Checkin", "ET ADWARE_PUP OSX/Adware.Pirrit Web Injects", "ET ADWARE_PUP Loadmoney.A Checkin 4", "ET ADWARE_PUP FLV/Youtube Downloader Install Activity",

	"ET ADWARE_PUP MuLauncher Telemetry Gathering Attempt", "ET ADWARE_PUP CoinSurf Proxy CnC Response", "ET ADWARE_PUP debelizombi.com (Rizo) related Spyware User-Agent (mc_v1.2.6)", "ET ADWARE_PUP Shop at Home Select Spyware User-Agent (Bundle)", "ET ADWARE_PUP SilverSpeedup Generic PUA Software UA", "ET ADWARE_PUP SoftwareTracking Site - Download Report", "ET ADWARE_PUP W32/RocketfuelNextUp.Adware CnC Beacon", "ET ADWARE_PUP iframebiz - loadadv***.exe", "ET ADWARE_PUP ezday.co .kr Related Spyware User-Agent (Ezshop)", "ET ADWARE_PUP ZenoSearch Spyware User-Agent", "ET ADWARE_PUP W32/OpenTrio User-Agent (Open3)", "ET ADWARE_PUP qq.com related Spyware User-Agent (QQGame)", "ET ADWARE_PUP Adware-Win32/EoRezo Reporting", "ET ADWARE_PUP Loadmoney Checkin 1", "ET ADWARE_PUP Win-touch.com Spyware User-Agent (WinTouch)", "ET ADWARE_PUP 180solutions Spyware Keywords Download", "ET ADWARE_PUP AdWare.MSIL.Solimba.b GET", "ET ADWARE_PUP W32/Linkular.Adware Icons.dat Second Stage Download", "ET ADWARE_PUP Antivirgear.com Fake Anti-Spyware User-Agent (AntiVirGear)", "ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTP_FILEDOWN)", "ET ADWARE_PUP Win32/DomaIQ Checkin", "ET ADWARE_PUP DealPly Adware CnC Beacon 4", "ET ADWARE_PUP Drpcclean.com Related Spyware User-Agent (DrPCClean Transmit)", "ET ADWARE_PUP Gamehouse.com User-Agent (GAMEHOUSE.NET.URL)", "ET ADWARE_PUP host-domain-lookup.com spyware related Start Report", "ET ADWARE_PUP Observed DNS Query to OSX/Bundalore Domain", "ET ADWARE_PUP User-Agent (Firefox) - Possible Trojan Downloader", "ET ADWARE_PUP AskSearch Toolbar Spyware User-Agent (AskBar)", "ET ADWARE_PUP Fake AV User-Agent (N1)", "ET ADWARE_PUP Win32/ReImageRepair.T CnC Cookie Pattern", "ET ADWARE_PUP [PTsecurity] Adware.SearchGo (start_page)", "ET ADWARE_PUP W32/LoudMo.Adware Checkin", "ET ADWARE_PUP Cpushpop.com Spyware User-Agent (CPUSH_UPDATER)", "ET ADWARE_PUP ZCOM Adware/Spyware User-Agent (ZCOM Software)", "ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 2", "ET ADWARE_PUP Deskwizz.com Spyware Install INI Download", "ET ADWARE_PUP PCAcceleratePro PUA/Adware User-Agent", "ET ADWARE_PUP Observed Malicious SSL Cert (OSX/Calender 2 Mining)", "ET ADWARE_PUP W32/Stan Malvertising.Dropper CnC Beacon", "ET ADWARE_PUP Spylocked Fake Anti-Spyware User-Agent (SpyLocked)", "ET ADWARE_PUP Win32/YTDDownloader.F Variant CnC Activity", "ET ADWARE_PUP W32/Wajam.Adware Successful Install", "ET ADWARE_PUP User-Agent (http-get-demo) Possible Reverse Web Shell", "ET ADWARE_PUP Dropspam.com Spyware Reporting", "ET ADWARE_PUP Win32/Tibs Checkin", "ET ADWARE_PUP Loadmoney Checkin 4", "ET ADWARE_PUP Zugo.com SearchToolbar User-Agent (SearchToolbar)", "ET ADWARE_PUP Adware/FakeAV.Kraddare Checkin UA", "ET ADWARE_PUP yupsearch.com Spyware Install - protector.exe", "ET ADWARE_PUP CoinSurf Proxy CnC Response (Network Configuration)", "ET ADWARE_PUP Windows Explorer Tab Add-on Post Install Checkin", "ET ADWARE_PUP LNKR landing page (possible compromised site) M1", "ET ADWARE_PUP Platinumreward.co.kr Spyware User-Agent (WT_GET_COMM)", "ET ADWARE_PUP SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)", "ET ADWARE_PUP W32/SearchSuite Install CnC Beacon", "ET ADWARE_PUP Spyware User-Agent (count)", "ET ADWARE_PUP Win32/Agent.PMS Variant CnC Activity", "ET ADWARE_PUP ISearchTech.com XXXPornToolbar Activity (IST)", "ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 1", "ET ADWARE_PUP Loadmoney User Agent", "ET ADWARE_PUP Ezula Install .exe", "ET ADWARE_PUP Win32/SuperDiag PUP CnC Activity", "ET ADWARE_PUP User-Agent (Internet Explorer 6.0) - Possible Trojan Downloader", "ET ADWARE_PUP PUA Related User-Agent (WINTERNET)", "ET ADWARE_PUP Win32/Atshz.A Checkin", "ET ADWARE_PUP Win32/Systweak Checkin M2", "ET ADWARE_PUP Fake Wget User-Agent (wget 3.0) - Likely Hostile", "ET USER_AGENTS Suspicious User-Agent (lineguide)", "ET ADWARE_PUP Miva Spyware User-Agent (Travel Update)", "ET ADWARE_PUP Loadmoney.A Checkin 8", "ET ADWARE_PUP DealPly Adware CnC Beacon 2", "ET ADWARE_PUP GMUnpackerInstaller.A Checkin", "ET ADWARE_PUP Malicious Chrome Extension", "ET ADWARE_PUP Spyware User-Agent (sureseeker)", "ET ADWARE_PUP

	STOPzilla Download Accelerator Activity", "ET ADWARE_PUP Loadmoney.A Checkin 1", "ET ADWARE_PUP W32/Amonetize.Downloader Executable Download Request", "ET ADWARE_PUP Alexa Search Toolbar User-Agent 2 (Alexa Toolbar)", "ET ADWARE_PUP Errorsafe.com Fake antispyware User-Agent (ErrorSafe)", "ET ADWARE_PUP Smileware Connection Spyware Related User-Agent (Smileware Connection)", "ET ADWARE_PUP Win32/Adware.BrowSecX.AB Install Log Sent", "ET ADWARE_PUP W32/iBryte.Adware Installer Download", "ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (BoBrowser)", "ET ADWARE_PUP Tool.InstallToolbar.24 Reporting", "ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTPFILEDOWN)", "ET ADWARE_PUP Win32/Adware.Agent.NSU CnC Activity M2", "ET ADWARE_PUP BInet Information Install Report", "ET ADWARE_PUP Observed DNS Query to PUP Domain (superdiag .xyz)", "ET ADWARE_PUP W32/Toolbar.WIDGI User-Agent (WidgiToolbar-)", "ET ADWARE_PUP ToolbarPartner Spyware Agent Download (1)", "ET ADWARE_PUP My Search Spyware Config Download", "ET ADWARE_PUP Adware.Win32/SProtector.A Client Checkin", "ET ADWARE_PUP Win32/DownloadAssistant.A PUP CnC", "ET ADWARE_PUP clickspring.com Spyware Install User-Agent (CS Fingerprint Module)", "ET ADWARE_PUP All Numerical .cn Domain Likely Malware Related", "ET ADWARE_PUP Antibody Software Installed (PUA)", "ET ADWARE_PUP LNKR landing page (possible compromised site) M3", "ET ADWARE_PUP MySearch Products Spyware User-Agent (MySearch)", "ET ADWARE_PUP Downer.B Variant Checkin", "ET ADWARE_PUP SweetIM Install in Progress", "ET ADWARE_PUP Luxsoft Win32/ICLoader User-Agent", "ET ADWARE_PUP User-Agent (webcount)", "ET ADWARE_PUP AdWare.Win32.Yotoon.hs Checkin", "ET ADWARE_PUP Ads2Srv Bundle Installer Offer Request", "ET USER_AGENTS Suspicious User-Agent (downloader)", "ET ADWARE_PUP BundledInstaller PUA/PUP Downloader", "ET ADWARE_PUP DealPly Adware CnC Beacon 3", "ET ADWARE_PUP Misspelled Mozilla User-Agent (Mozila)", "ET ADWARE_PUP Win32/LoadMoney Adware Activity M2", "ET ADWARE_PUP Outerinfo.com Spyware Advertising Campaign Download", "ET ADWARE_PUP Malicious Adware Chrome Extension Detected (1)", "ET ADWARE_PUP AppControls.com User-Agent", "ET ADWARE_PUP Win32/Spy.Agent.QCL Variant Activity (POST)", "ET ADWARE_PUP LoadMoney Checkin 5", "ET ADWARE_PUP Loadmoney.A Checkin 7", "ET ADWARE_PUP W32/InstallMonetizer.Adware Beacon 1", "ET ADWARE_PUP Trojan.FakeAV.SystemDefender Checkin", "ET ADWARE_PUP Searchmiracle.com Spyware Install (protector.exe)", "ET ADWARE_PUP iDownloadAgent Spyware User-Agent (iDownloadAgent)", "ET ADWARE_PUP Zango Seekmo Bar Spyware User-Agent (Seekmo Toolbar)", "ET ADWARE_PUP Win32/2345.H Variant Activity (POST)", "ET ADWARE_PUP YourSiteBar User-Agent (istsvc)", "ET ADWARE_PUP Generic Adware Install Report", "ET ADWARE_PUP Suspicious User Agent EXE2", "ET ADWARE_PUP Statblaster.com Spyware User-Agent (fetcher)", "ET ADWARE_PUP Gator/Clarian Agent", "ET ADWARE_PUP W32/iBryte.Adware Affiliate Campaign Executable Download", "ET ADWARE_PUP Casalemedia Spyware Reporting URL Visited 2", "ET ADWARE_PUP W32/InstallRex.Adware Report CnC Beacon", "ET ADWARE_PUP Observed Win32/Foniad Domain (aclassigned .info in TLS SNI)", "ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (updatesodui)", "ET ADWARE_PUP InstallCore PUA/Adware Activity M2", "ET ADWARE_PUP Win32/DownloadAssistant.Q Variant Checkin", "ET ADWARE_PUP Adaware.BarACE Checkin and Update", "ET ADWARE_PUP Predator Anti Ban CnC Activity", "ET ADWARE_PUP Artro Downloader User-Agent Detected", "ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 3", "ET ADWARE_PUP Win32/RemoteUtilities Checkin via SMTP", "ET ADWARE_PUP UBar Trojan/Adware Checkin 3", "ET ADWARE_PUP Win32/DealPly CnC Checkin", "ET ADWARE_PUP Hotbar Tools Spyware User-Agent (hbtools)", "ET ADWARE_PUP DriverPack Update Checkin", "ET ADWARE_PUP PUP/DriverRestore Sending System Information to Affiliate", "ET ADWARE_PUP Internet Optimizer Activity User-Agent (IOKernel)", "ET USER_AGENTS Suspicious User-Agent (Huai_Huai)", "ET ADWARE_PUP Observed DownloadAssistant User-Agent", "ET ADWARE_PUP Win32/Adware.Agent.NSF CnC Checkin M1", "ET ADWARE_PUP Zenosearch Malware Checkin HTTP POST (2)", "ET ADWARE_PUP [PTsecurity] DeathBot.Java (Minecraft

	Spambot)", "ET ADWARE_PUP Win32/Xetapp Installer Checkin", "ET ADWARE_PUP Grandstreet Interactive Spyware User-Agent (IEP)", "ET ADWARE_PUP Loadmoney Checkin 2", "ET ADWARE_PUP W32/BettrExperience.Adware Initial Checkin", "ET ADWARE_PUP SUPERAntiSpyware Install Checkin", "ET ADWARE_PUP [PTsecurity] Adware.FileFinder Activity", "ET ADWARE_PUP PUP Win32/Conduit.SearchProtect.O CnC Beacon", "ET ADWARE_PUP Win32/DealPly Checkin", "ET ADWARE_PUP W32/BettrExperience.Adware Update Checkin", "ET ADWARE_PUP Win32/BrowseFox.H Checkin 2", "ET ADWARE_PUP Unknown Malware patchlist.xml Request", "ET ADWARE_PUP Win32/Onescan FraudWare User-Agent", "ET ADWARE_PUP Win32/Hadsruda!bit Adware/PUA Installation Activity", "ET ADWARE_PUP User-Agent (AgavaDwnl) - Possibly Xema", "ET ADWARE_PUP WinSoftware.com Spyware User-Agent (WinSoftware)", "ET ADWARE_PUP W32/WinWrapper.Adware Initial Install Beacon", "ET USER_AGENTS Suspicious User-Agent (Mozilla/4.0 (compatible ICS))", "ET ADWARE_PUP Adware.MultiInstaller checkin 2", "ET ADWARE_PUP Malicious Adware Chrome Extension Detected (2)", "ET ADWARE_PUP W32/MediaGet Checkin", "ET ADWARE_PUP Regnow.com Access", "ET ADWARE_PUP 180solutions (Zango) Spyware Local Stats Post", "ET ADWARE_PUP Win32/ReImageRepair.T CnC Checkin", "ET ADWARE_PUP Potentially Unwanted Application AirInstaller CnC Beacon", "ET ADWARE_PUP Zenotecnico Adware 2", "ET ADWARE_PUP Observed Win32/Foniad Domain (insupposity .info in TLS SNI)", "ET ADWARE_PUP PUP Win32/AdWare.Sendori User-Agent", "ET ADWARE_PUP CoinSurf Proxy Client Login", "ET ADWARE_PUP Lavasoft PUA/Adware Client Install", "ET ADWARE_PUP LNKR Request for LNKR js file M1", "ET USER_AGENTS Suspicious User-Agent (My Session)", "ET ADWARE_PUP Gator Agent Traffic", "ET ADWARE_PUP Adware.Ezula Checkin", "ET ADWARE_PUP Win32/Adware.VrBrothers.AI Variant CnC Activity", "ET ADWARE_PUP Webhancer Data Upload", "ET ADWARE_PUP Observed Win32/Foniad Domain (suggedin .info in DNS Lookup)", "ET ADWARE_PUP LNKR landing page (possible compromised site) M2", "ET ADWARE_PUP User-Agent (HTTP)", "ET ADWARE_PUP Carder Card Checking Tool try2check.me SSL Certificate on Off Port", "ET ADWARE_PUP suspicious User-Agent (vb wininet)", "ET ADWARE_PUP Miva User-Agent (TPSystem)", "ET ADWARE_PUP Errclean.com Related Spyware User-Agent (Locus NetInstaller)", "ET ADWARE_PUP Win32/Speedbit Variant Checkin", "ET ADWARE_PUP User-Agent (XieHongWei-HttpDown/2.0)", "ET ADWARE_PUP PUP Win32/ELEX Checkin", "ET ADWARE_PUP AntiSpywareMaster.com Fake AV User-Agent (AsmUpdater)", "ET MOBILE_MALWARE XX-Net VPN Client CnC Checkin", "ET ADWARE_PUP Debelizombi.com Spyware User-Agent (blahrx)", "ET ADWARE_PUP DriverPack Domain in DNS Query", "ET ADWARE_PUP Win32/Adware.Winggo.AB Checkin", "ET ADWARE_PUP User-Agent (Mozilla) - Possible Spyware Related", "ET ADWARE_PUP User-Agent (Microsoft Internet Explorer 6.0) Possible Reverse Web Shell", "ET ADWARE_PUP Win32/DealPly Reporting Details to CnC", "ET ADWARE_PUP Win32 Handy Cafe Checkin", "ET ADWARE_PUP W32/SmartPops Adware Outbound Off-Port MSSQL Communication", "ET ADWARE_PUP Trojan.Win32.InternetAntivirus User-Agent (General Antivirus)", "ET ADWARE_PUP ASKTOOLBAR.DLL Reporting", "ET ADWARE_PUP W32/PullUpdate.Adware CnC Beacon", "ET ADWARE_PUP Fake Adobe Update Download", "ET ADWARE_PUP User-Agent (microsoft) - Possible Trojan Downloader", "ET ADWARE_PUP dialno Dialer User-Agent (dialno)", "ET ADWARE_PUP Casino on Net Reporting Data", "ET ADWARE_PUP Adware.MultiInstaller", "ET ADWARE_PUP SurfSidekick Activity", "ET ADWARE_PUP Bestoffersnetwork.com Related Spyware User-Agent (TBONAS)", "ET ADWARE_PUP AskSearch Spyware User-Agent (AskSearchAssistant)", "ET ADWARE_PUP Spyware User-Agent (XXX)", "ET ADWARE_PUP Antispywaremaster.com/Privacyprotector.com Fake AV Checkin", "ET ADWARE_PUP Gamehouse.com Related Spyware User-Agent (Sprout Game)", "ET ADWARE_PUP Doctorvaccine.co.kr Related Spyware User-Agent (DoctorVaccine)", "ET ADWARE_PUP CommonName.com Spyware/Adware User-Agent (CommonName Agent)", "ET ADWARE_PUP W32/Linkular.Adware Successful Install Beacon", "ET USER_AGENTS Suspicious User-Agent (006)", "ET ADWARE_PUP vaccine-program.co.kr Related Spyware User-Agent (vaccine)", "ET ADWARE_PUP iwin.com Games/Spyware

	User-Agent (iWin GameInfo Installer Helper)", "ET ADWARE_PUP Win32/Atshz.A Checkin M2", "ET ADWARE_PUP Win32/GameHack.DJC CnC Activity", "ET ADWARE_PUP Fun Web Products Spyware User-Agent (MyWay)", "ET ADWARE_PUP Win32/Mando Activity (GET)", "ET ADWARE_PUP DownloadAssistant Activity", "ET ADWARE_PUP ErrorNuker FakeAV User-Agent (ERRN2004 (Windows XP))", "ET ADWARE_PUP OSX/Bundalore Loader Activity", "ET ADWARE_PUP MAC/Conduit Component Download", "ET ADWARE_PUP Lookup of Malware Domain twothousands.cm Likely Infection", "ET ADWARE_PUP HTTP Connection to go2000.cn - Common Malware Checkin Server", "ET ADWARE_PUP Win32/2144FlashPlayer.E Checkin", "ET ADWARE_PUP W32/Dialer.Adultchat Checkin", "ET ADWARE_PUP User-Agent (Win95)", "ET ADWARE_PUP OSX ADWARE/AD Injector", "ET ADWARE_PUP searchenginebar.com Spyware User-Agent (RX Bar)", "ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 4", "ET ADWARE_PUP Ask.com Toolbar/Spyware User-Agent (AskPBar)", "ET ADWARE_PUP Miuref/Boaxxe Checkin", "ET ADWARE_PUP Observed Win32/Foniad Domain (acinster .info in TLS SNI)", "ET ADWARE_PUP Sidebar Related Spyware User-Agent (Sidebar Client)", "ET ADWARE_PUP MySideSearch Browser Optimizer", "ET ADWARE_PUP Vombanetwork Spyware User-Agent (VombaProductsInstaller)", "ET ADWARE_PUP klm123.com Spyware User Agent", "ET ADWARE_PUP 180solutions Spyware (tracked event 2 reporting)", "ET ADWARE_PUP Clickspring.net Spyware Reporting Successful Install", "ET ADWARE_PUP LNKR CnC Activity M3", "ET ADWARE_PUP TryMedia Spyware User-Agent (TryMedia_DM_2.0.0)", "ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (aaaabbb)", "ET ADWARE_PUP User-Agent (Mozilla/4.0 (compatible))", "ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (VersionDwl)", "ET ADWARE_PUP AdVantage Malware URL Infection Report", "ET ADWARE_PUP OSX/Fake Flash Player Download Oct 20", "ET ADWARE_PUP ProxyGearPro Proxy Tool PUA", "ET ADWARE_PUP Win32/Hao123.C Variant CnC Activity", "ET ADWARE_PUP Win32/InstallCore.GF CnC Activity", "ET ADWARE_PUP User-Agent (ms)", "ET ADWARE_PUP Win32/YTDDownloader.F Activity", "ET ADWARE_PUP Searchmeup Spyware Install (mstask)", "ET ADWARE_PUP Win32.Magania", "ET ADWARE_PUP SurfSidekick Download", "ET ADWARE_PUP MSIL.Amiricil.gen HTTP Checkin", "ET ADWARE_PUP MyGlobalSearch Spyware bar update", "ET ADWARE_PUP Win32/Adware.Kraddare.FJ Checkin", "ET ADWARE_PUP MSIL/Adload.AT Beacon", "ET ADWARE_PUP Enhance My Search Spyware User-Agent (HelperH)", "ET ADWARE_PUP Win32/CloudScout Checkin", "ET ADWARE_PUP Possible FakeAV Binary Download", "ET ADWARE_PUP Observed OSX/PremierOpinionD Collection Domain in TLS SNI", "ET ADWARE_PUP Clickspring.net Spyware Reporting", "ET ADWARE_PUP DealPly Adware CnC Beacon", "ET ADWARE_PUP OptimizerPro Checkin", "ET ADWARE_PUP Ezula Related User-Agent (mez)", "ET ADWARE_PUP Win32/DownWare.V Checkin", "ET ADWARE_PUP Easy Search Bar Spyware User-Agent (ESB)", "ET ADWARE_PUP Better Internet Spyware User-Agent (poller)", "ET ADWARE_PUP PUP Optimizer Pro Adware GET or POST to C2", "ET ADWARE_PUP PUP TheSZ AutoUpdate CnC Beacon", "ET ADWARE_PUP User-Agent (Internet)", "ET ADWARE_PUP Win32/Adware.Agent.NPP CnC Activity", "ET ADWARE_PUP Win32/Zonebac Traffic Redirect", "ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (startupfraction)", "ET ADWARE_PUP malwarewipeupdate.com Spyware User-Agent (MalwareWipe)", "ET ADWARE_PUP User-Agent (Example)", "ET ADWARE_PUP Freeze.com Spyware Download", "ET ADWARE_PUP W32/DownloadAdmin.Adware User-Agent", "ET ADWARE_PUP Win32/Adware.YoutubeDownloaderGuru.A Variant CnC Activity", "ET USER_AGENTS Suspicious User-Agent (FaceCooker)", "ET ADWARE_PUP [PTsecurity] Adware/Rukometa(LoadMoney) Fake PNG File", "ET ADWARE_PUP Win32/InstallDisck SMTP Checkin", "ET ADWARE_PUP Vaccineprogram.co.kr Related Spyware User Agent (pcsafe)", "ET ADWARE_PUP Win32/TrojanClicker Variant Activity (GET)", "ET ADWARE_PUP Win32.Bublik.B/Birele/Variant.Kazy.66443 Checkin", "ET USER_AGENTS Suspicious User-Agent (update)", "ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M2", "ET ADWARE_PUP SoftwareTracking Site - Install Report", "ET ADWARE_PUP Visicom Spyware User-Agent (Visicom)", "ET ADWARE_PUP Searchmeup

	Spyware Install (systime)", "ET ADWARE_PUP PUP Win32.SoftPulse Retrieving data", "ET ADWARE_PUP Freeze.com Spyware/Adware (Install)", "ET ADWARE_PUP FormatFactory Install Checkin", "ET ADWARE_PUP User Agent (TEST) - Likely Webhancer Related Spyware", "ET ADWARE_PUP Sidetab or Related Trojan Checkin", "ET ADWARE_PUP Hex Encoded IP HTTP Request - Likely Malware", "ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (search.feedvertizus)", "ET ADWARE_PUP UCMore Spyware User-Agent (EI)", "ET ADWARE_PUP User-Agent (Mozilla/4.0 (SP3 WINLD))", "ET ADWARE_PUP User-Agent (CustomSpy)", "ET ADWARE_PUP Win32/Adware.WDJiange.A CnC Checkin M1", "ET ADWARE_PUP User-Agent (TALWinInetHTTPClient)", "ET ADWARE_PUP Loadmoney.A Checkin 6", "ET ADWARE_PUP Freeze.com Spyware User-Agent (YourScreen123)", "ET ADWARE_PUP IE Toolbar User-Agent (IEToolbar)", "ET ADWARE_PUP Media Pass ActiveX Install", "ET ADWARE_PUP yupsearch.com Spyware Install - sideb.exe", "ET ADWARE_PUP Win32.Perinet CnC Checkin", "ET ADWARE_PUP Suspicious User-Agent (MediaLabsSiteInstaller)", "ET ADWARE_PUP PUP Win32.SoftPulse Checkin", "ET ADWARE_PUP MALWARE W32/WinWrapper.Adware POST CnC Beacon", "ET ADWARE_PUP Zenotecnico Spyware Install Report", "ET ADWARE_PUP Adrevmedia Related Media Manager Spyware Checkin", "ET ADWARE_PUP System-defender.com Fake AV Install Checkin", "ET ADWARE_PUP Potentially Unwanted Application AirInstaller", "ET ADWARE_PUP W32/OnlineGames Checkin", "ET USER_AGENTS Suspicious User Agent (Autoupdate)", "ET ADWARE_PUP Loadmoney Checkin 3", "ET ADWARE_PUP Adload.Generic Spyware User-Agent (ProxyDown)", "ET ADWARE_PUP WinSoftware.com Spyware User-Agent (NetInstaller)", "ET ADWARE_PUP Searchmeup Spyware Install (prog)", "ET ADWARE_PUP Bluebox Data Exfiltration", "ET ADWARE_PUP MyGlobalSearch Spyware bar update 2", "ET ADWARE_PUP [PTsecurity] WebToolbar.Win32.Searchbar.k HTTP JSON Artifact", "ET ADWARE_PUP Surfaccuracy.com Spyware Install User-Agent (SF Installer)", "ET ADWARE_PUP Winxpperformance.com Related Spyware User-Agent (Microsoft Internet Browser)", "ET ADWARE_PUP Zredirector.com Related Spyware User-Agent (BndDriveLoader)", "ET ADWARE_PUP W32/Linkular.Adware Successful Install Beacon (2)", "ET ADWARE_PUP Win32/DealPly Configuration File Inbound", "ET ADWARE_PUP Websearch.com Spyware", "ET ADWARE_PUP Optimum Installer User-Agent IE6 on Windows XP", "ET ADWARE_PUP LNKR Possible Response for LNKR js file", "ET ADWARE_PUP Win32/Adware.Vonteera.M Variant CnC Activity", "ET ADWARE_PUP W32/GameVance Adware User Agent", "ET ADWARE_PUP Win-touch.com Spyware User-Agent (WTRecover)", "ET ADWARE_PUP Adload.Generic Spyware User-Agent (91castInstallKernel)", "ET ADWARE_PUP Win32/TrojanDownloader.Agent.BXA CnC Activity", "ET ADWARE_PUP OSX/Adware.Pirrit CnC Checkin", "ET ADWARE_PUP User-Agent (HTTP_Query)", "ET ADWARE_PUP Downloader Checkin - Downloads Rogue Adware", "ET ADWARE_PUP Gator/Claria Data Submission", "ET ADWARE_PUP Mirage.ru Related Spyware User-Agent (szNotifyIdent)", "ET ADWARE_PUP Win32/Agent.NDV Receiving Task Config File", "ET ADWARE_PUP AdWare.Win32.Sushi.au Checkin", "ET ADWARE_PUP UBar Trojan/Adware Checkin 1", "ET ADWARE_PUP Observed Win32/Foniad Domain (efishedo .info in TLS SNI)", "ET ADWARE_PUP Win32/Sogou.H Variant Request", "ET ADWARE_PUP Win32/GameHack.ADW CnC Activity", "ET ADWARE_PUP User-Agent (browserbob.com)", "ET ADWARE_PUP SearchProtect PUA User-Agent Observed", "ET ADWARE_PUP InstallCore PUA/Adware Activity M4", "ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (LogEvents)", "ET ADWARE_PUP Suspicious User-Agent (GeneralDownloadApplication)", "ET ADWARE_PUP W3i Related Adware/Spyware", "ET ADWARE_PUP W32/SoftonicDownloader.Adware User Agent", "ET ADWARE_PUP Context Plus Spyware User-Agent (Apropos)", "ET ADWARE_PUP Searchmiracle.com Spyware Install (silent_install)", "ET ADWARE_PUP Zango Cash Spyware User-Agent (ZC XML-RPC C++ Client)", "ET ADWARE_PUP Win32/Adware.Neoreklami.MI Activity M1", "ET ADWARE_PUP InstallCore PUA/Adware Activity M3", "ET ADWARE_PUP W32/PlaySushi User-Agent", "ET ADWARE_PUP Win32/SmartTab PUP Install Activity 2", "ET ADWARE_PUP OSX

	ADWARE/Mackeeper Checkin", "ET ADWARE_PUP Toolbar User-Agent (BrandThunderHelper)", "ET ADWARE_PUP MediaTickets Download", "ET ADWARE_PUP ABX Toolbar ActiveX Install", "ET ADWARE_PUP Qcbar/Adultlinks Spyware User-Agent (IBSBand)", "ET ADWARE_PUP [eSentire] Win32/Adware.Adposhel.lgvk CnC Checkin", "ET ADWARE_PUP User-Agent (Live Enterprise Suite)", "ET ADWARE_PUP Observed Malicious SSL Cert (showmypc.com)", "ET ADWARE_PUP W32/GameVance Adware Checkin", "ET ADWARE_PUP LNKR CnC Activity M1", "ET ADWARE_PUP ZeroTier P2P VPN Activity M1", "ET ADWARE_PUP Loadmoney.A Checkin 2", "ET ADWARE_PUP Win32/Adware.Qjwmonkey.H Variant CnC Activity M2", "ET ADWARE_PUP Win32/Swjoy.A Telemetry Checkin", "ET ADWARE_PUP W32/InstallRex.Adware Initial CnC Beacon", "ET ADWARE_PUP User-Agent Mozilla/3.0", "ET ADWARE_PUP Dollarrevenue.com Spyware Code Download", "ET ADWARE_PUP Observed Win32/Foniad Domain (maraukog .info in TLS SNI)", "ET ADWARE_PUP Adware.Kraddare Checkin", "ET ADWARE_PUP W32/SpeedRunner User-Agent SRRemove", "ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTPGETDATA)", "ET ADWARE_PUP Matcash Trojan Related Spyware Code Download", "ET ADWARE_PUP User-Agent (Download Agent) Possibly Related to TrinityAcquisitions.com", "ET ADWARE_PUP Win32/Eyoorun.D Variant Checkin", "ET ADWARE_PUP W32/PicColor Adware CnC Beacon", "ET ADWARE_PUP Topgame-online.com Ruch Casino Install User-Agent (RichCasino)", "ET ADWARE_PUP PrivaZer Checkin", "ET ADWARE_PUP Context Plus Spyware Install", "ET ADWARE_PUP Spyware User-Agent (install_s)", "ET USER_AGENTS Suspicious User-Agent (NSIS_DOWNLOAD)", "ET ADWARE_PUP RogueAntiSpyware.AntiVirusPro Checkin", "ET ADWARE_PUP Snoopstick.net Related Spyware User-Agent (SnoopStick Updater)", "ET ADWARE_PUP Suspicious User-Agent (go-diva)", "ET ADWARE_PUP User-Agent (Explorer)", "ET ADWARE_PUP Drivecleaner.com Spyware User-Agent (DriveCleaner Updater)", "ET ADWARE_PUP DriverTurbo Domain (driverfinderpro .com) in DNS Lookup", "ET ADWARE_PUP PUP.GigaClicks Checkin", "ET ADWARE_PUP pdfspeedup Initial CnC Checkin", "ET ADWARE_PUP RubyFortune Spyware Capabilities User-Agent (Microgaming Install Program) - GET", "ET ADWARE_PUP Freeze.com Spyware/Adware (Install Registration)", "ET ADWARE_PUP UBar Trojan/Adware Checkin 2", "ET ADWARE_PUP User-Agent (MSIE7 na)", "ET ADWARE_PUP ThunderUnion Install Checkin", "ET ADWARE_PUP Suspicious User Agent Smart-RTP", "ET ADWARE_PUP Win32.AdWare.iBryte.C Install", "ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (opurie)", "ET ADWARE_PUP Mycomclean.com Spyware User-Agent (HTTP_GET_COMM)", "ET ADWARE_PUP User-Agent (Fast Browser Search)", "ET ADWARE_PUP User-Agent (???)", "ET ADWARE_PUP SecureDriverUpdater Checkin", "ET ADWARE_PUP Outerinfo.com Spyware Activity", "ET ADWARE_PUP Hotbar Spyware User-Agent (Hotbar)", "ET ADWARE_PUP Carder Card Checking Tool try2check.me SSL Certificate", "ET ADWARE_PUP E2give Related Downloading Code", "ET ADWARE_PUP ISearchTech.com XXXPornToolbar Activity (2)", "ET ADWARE_PUP overtls.com adware request", "ET ADWARE_PUP Spyware Related User-Agent (UtilMind HTTPGet)", "ET ADWARE_PUP User-Agent (User-Agent Mozilla/4.0 (compatible))", "ET ADWARE_PUP Yourscreen.com Spyware User-Agent (FreezeInet)", "ET ADWARE_PUP Observed DNS Query to PUP Domain (omnatuor .com)", "ET ADWARE_PUP Shop at Home Select Spyware User-Agent (SAH)", "ET ADWARE_PUP Win32/RemoteUtilities Checkin via SMTP M2", "ET ADWARE_PUP SurfAccuracy.com Spyware Updating", "ET ADWARE_PUP Win32/Toolbar.Conduit.AG Checkin", "ET ADWARE_PUP LNKR CnC Activity M2", "ET ADWARE_PUP EELoader Malware Packages User-Agent (EELoader)", "ET ADWARE_PUP PUP W32/DownloadGuide.D", "ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 5", "ET ADWARE_PUP Win32/GameHack.COG Variant CnC Activity", "ET ADWARE_PUP Win32/TrojanDownloader.Adload.NSD Variant Checkin", "ET ADWARE_PUP Target Saver Spyware User-Agent (TSA)", "ET ADWARE_PUP User-Agent (Save)", "ET ADWARE_PUP Win32/OutBrowse.G Variant Checkin", "ET ADWARE_PUP UCMore Spyware User-Agent (UCmore)", "ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 3", "ET ADWARE_PUP Win32/Toolbar.CrossRider.A Checkin", "ET ADWARE_PUP Adware pricepeep

	Adware.Shopper.297", "ET ADWARE_PUP Trinityacquisitions.com and Maximumexperience.com Spyware Activity", "ET USER_AGENTS Suspicious User Agent (FTP)", "ET ADWARE_PUP Sality Virus User Agent Detected (KUKU)", "ET ADWARE_PUP W32/MediaGet.Adware Installer Download", "ET ADWARE_PUP Dropspam.com Spyware Install User-Agent (DSInstall)", "ET ADWARE_PUP User-Agent (AdVantage)", "ET ADWARE_PUP Suspicious User-Agent (gettingAnswer)", "ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M3", "ET ADWARE_PUP Internet Optimizer User-Agent (ROGUE)", "ET ADWARE_PUP my247eshop .com User-Agent", "ET ADWARE_PUP User-Agent (Download Master) - Possible Malware Downloader", "ET ADWARE_PUP User-Agent (double dashes)", "ET ADWARE_PUP Adware.PUQD Checkin", "ET ADWARE_PUP Xpire.info Spyware Install Reporting", "ET ADWARE_PUP Adware.Gen5 Reporting", "ET ADWARE_PUP Downloader.NSIS.OutBrowse.b Checkin", "ET ADWARE_PUP chnsystem.com Spyware User-Agent (Update1.0)", "ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M3", "ET ADWARE_PUP LNKR Request for LNKR js file M2", "ET ADWARE_PUP W32/AdLoad.Downloader Download", "ET ADWARE_PUP W32/OpenCandy Adware Checkin", "ET ADWARE_PUP Toplist.cz Related Spyware Checkin", "ET ADWARE_PUP Likely Hostile User-Agent (Forthgoer)", "ET ADWARE_PUP SoundCloud Downloader Install Beacon", "ET ADWARE_PUP Observed DNS Query to DriverPack Domain (.drp .su)", "ET ADWARE_PUP MALWARE W32/WinWrapper.Adware User-Agent", "ET ADWARE_PUP Win32/SoftPulse.H Checkin", "ET ADWARE_PUP PUP Win32/DownloadAssistant.A Checkin", "ET ADWARE_PUP User-Agent (DIALER)", "ET ADWARE_PUP Win32/Qihoo360.J Variant Install Report", "ET ADWARE_PUP 2020search/PowerSearch Toolbar Adware/Spyware - GET", "ET ADWARE_PUP Security-updater.com Spyware Posting Data", "ET ADWARE_PUP CoinSurf Proxy CnC Response (Refesh Token)", "ET ADWARE_PUP Webhancer Data Post", "ET ADWARE_PUP Searchmiracle.com Spyware Installer silent.exe Download", "ET ADWARE_PUP GreatArcadeHits CnC Activity", "ET ADWARE_PUP CoolWebSearch Spyware User-Agent (iefeatsl)", "ET ADWARE_PUP User-Agent (Gbot)", "ET ADWARE_PUP WiseCleaner Installed (PUA)", "ET ADWARE_PUP Win32/Adware.Qjwmonkey.H Variant CnC Activity", "ET ADWARE_PUP Observed DNS Query to Malvertising Related Domain", "ET ADWARE_PUP CoinSurf Proxy Client Registration", "ET ADWARE_PUP Mirar Bar Spyware User-Agent (Mbar)", "ET ADWARE_PUP NewWeb User-Agent (Lobo Lunar)", "ET ADWARE_PUP Elitemediagroup.net Spyware Config Download", "ET ADWARE_PUP Adware.Gamevance.AV Checkin", "ET ADWARE_PUP Win32/Adware.Neoreklami.MI Activity M2", "ET ADWARE_PUP BInet Information Upload", "ET ADWARE_PUP Context Plus Spyware User-Agent (Envolo)", "ET ADWARE_PUP Win32/DownWare.G Installer Request", "ET ADWARE_PUP Win32.LoadMoney User Agent 2", "ET ADWARE_PUP Simbar Spyware User-Agent Detected", "ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M1", "ET ADWARE_PUP Win32/Adware.iBryte.BO CnC Activity", "ET ADWARE_PUP EZULA Spyware User Agent", "ET ADWARE_PUP InstallCore PUA/Adware Activity M1", "ET ADWARE_PUP User-Agent (ie) - Possible Trojan Downloader", "ET ADWARE_PUP Searchmeup Spyware Receiving Commands", "ET ADWARE_PUP PUA Boxore User-Agent", "ET ADWARE_PUP Suspicious User Agent Mozi11a", "ET ADWARE_PUP Win32/SWInformer.B Checkin", "ET ADWARE_PUP User-Agent (User Agent) - Likely Hostile", "ET ADWARE_PUP Lowercase mozilla/2.0 User-Agent Likely Malware", "ET ADWARE_PUP Loadmoney.A Checkin 5", "ET ADWARE_PUP W32/MultiPlug.Adware Adfraud Traffic", "ET ADWARE_PUP User-Agent (SogouExplorerMiniSetup)", "ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 4", "ET ADWARE_PUP DriverFinder User-Agent Observed in HTTP Traffic", "ET ADWARE_PUP MultiPlug.J Checkin", "ET ADWARE_PUP W32/Softpulse PUP Install Failed Beacon", "ET ADWARE_PUP NavExcel Spyware User-Agent (NavHelper)", "ET ADWARE_PUP DriverTurbo Domain (driverturbo .com) in DNS Lookup", "ET ADWARE_PUP Java.Deathbot Requesting Proxies", "ET ADWARE_PUP Pigeon.AYX/AVKill Related User-Agent (CTTBasic)", "ET ADWARE_PUP 180 Solutions (Zango Installer) User Agent", "ET ADWARE_PUP DownLoadAdmin Activity", "ET ADWARE_PUP Casino Related Spyware User-Agent Detected (Viper 4.0)", "ET

	ADWARE_PUP Rogue.WinPCDefender Checkin", "ET ADWARE_PUP BetterInstaller", "ET ADWARE_PUP MyWebSearch Spyware User-Agent (MyWebSearch)", "ET ADWARE_PUP Lantern Checkin", "ET ADWARE_PUP W32/Eorezo.Adware CnC Beacon", "ET ADWARE_PUP PUP Optimizer Pro Adware Download", "ET ADWARE_PUP Kuwo Music Installer Log", "ET ADWARE_PUP W32/GameplayLabs.Adware Installer Checkin", "ET ADWARE_PUP Win32/ReImageRepair.T CnC Activity", "ET ADWARE_PUP User-Agent (M0zilla)", "ET ADWARE_PUP Outerinfo.com Spyware Checkin", "ET ADWARE_PUP Tibsystems Spyware Download", "ET ADWARE_PUP APN/Ask Toolbar PUA/PUP User-Agent", "ET ADWARE_PUP LNKR Request for validate-site.js", "ET ADWARE_PUP pdfspeedup Keep-Alive", "ET ADWARE_PUP TopTools PUP Install Activity", "ET ADWARE_PUP MultiPlug.A checkin", "ET ADWARE_PUP dns-look-up.com Spyware User-Agent (KRSystem)", "ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M1", "ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M2", "ET ADWARE_PUP MediaDrug CnC Activity", "ET ADWARE_PUP Spyware User-Agent (Sidesearch)", "ET ADWARE_PUP CWS Trafcool.biz Related Installer", "ET ADWARE_PUP UCMore Spyware Reporting", "ET ADWARE_PUP CoolWebSearch Spyware (Feat)", "ET ADWARE_PUP Suspicious User-Agent (Nimo Software HTTP Retriever 1.0)", "ET ADWARE_PUP Trafficadvance.net Spyware User-Agent (Internet 1.0)", "ET ADWARE_PUP Known Malicious User-Agent (x) Win32/Tracur.A or OneStep Adware Related", "ET ADWARE_PUP Win32.EZula Adware Reporting Successful Install", "ET ADWARE_PUP Win32/DownloadAssistant.G Variant Error Report", "ET ADWARE_PUP Loadmoney.A Checkin 3", "ET ADWARE_PUP PUP Win32/DownloadGuide.A" |
Подключения к потенциально уязвимым web-приложениям	"ET WEB_SERVER MSSQL Server OLEDB asp error", "ET MALWARE Jembot PHP Webshell (system command)", "ET WEB_SERVER Weevely PHP backdoor detected (exec() function used)", "ET WEB_SERVER Weevely PHP backdoor detected (system() function used)", "ET WEB_SERVER log4jAdmin access from non-local network (can modify logging levels)", "ET ATTACK_RESPONSE r57 phpshell footer detected", "ET WEB_SERVER Weevely PHP backdoor detected (python_eval() function used)", "ET WEB_SERVER JBoss jmx-console Probe", "ET INFO PHP Xdebug Extension Query Parameter (XDEBUG_SESSION_START)", "GPL WEB_SERVER globals.pl access", "GPL WEB_SERVER printenv access", "ET WEB_SERVER WebShell - Unknown - .php?x=img&img=", "ET SCAN Nikto Scan Remote File Include Retrieval", "ET WEB_SERVER WebShell - Unknown - self-kill", "ET SCAN Core-Project Scanning Bot UA Detected", "ET WEB_SERVER Unusually Fast HTTP Requests With Referer Url Matching DoS Tool", "ET WEB_CLIENT Samsung Galaxy Knox Android Browser RCE smdm attempt", "GPL WEB_SERVER authors.pwd access", "ET MALWARE Jembot PHP Webshell (file upload)", "ET WEB_SERVER Weevely PHP backdoor detected (popen() function used)", "ET WEB_SERVER Weevely PHP backdoor detected (shell_exec() function used)", "ET WEB_SERVER Weevely PHP backdoor detected (passthru() function used) M3", "ET PHISHING Generic Phishing Panel Accessed on External Server", "ET SCAN w3af Scan Remote File Include Retrieval", "ET SCAN Web Scanner - Fuzz Faster U Fool (Inbound)", "ET INFO Spring Boot Actuator Health Check Request", "GPL WEB_SERVER service.cnf access", "GPL MISC HP Web JetAdmin setinfo access", "ET WEB_SERVER WeBaCoo Web Backdoor Detected", "ET SCAN bsqlbf Brute Force SQL Injection", "GPL WEB_SERVER author.exe access", "ET WEB_SERVER FaTaLisTiCz_Fx Webshell Detected", "ET SCAN COMMIX Command injection scan attempt", "ET ATTACK_RESPONSE x2300 phpshell detected", "GPL EXPLOIT site/iisamples access", "ET WEB_SERVER Weevely PHP backdoor detected (passthru() function used) M1", "GPL WEB_SERVER Oracle Java Process Manager access", "GPL MISC HP Web JetAdmin file write attempt", "ET INFO Liferay JSON Web Services Invoker", "ET WEB_SERVER DataCha0s Web Scanner/Robot", "GPL EXPLOIT /iisadmpwd/aexp2.htr access", "ET INFO Apache Solr System Information Request", "GPL WEB_SERVER mod_gzip_status access", "GPL WEB_SERVER services.cnf access", "ET WEB_SERVER Weevely PHP backdoor detected (perl->system() function used)", "ET WEB_SPECIFIC_APPS Miva Merchant Cross Site Scripting Attack", "ET EXPLOIT [ConnectWise CRU] Java ECDSA (Psychic) Signed JWT Bypass (CVE-2022-21449)", "GPL EXPLOIT administrators.pwd access", "ET HUNTING Suspicious HTML Script Tag in 401 Unauthorized Response

	(External Source)", "ET WEB_SERVER log4jAdmin access from non-local network Page Body (can modify logging levels)", "ET WEB_SERVER Weevely PHP backdoor detected (passthru() function used) M2", "ET WEB_SERVER Weevely PHP backdoor detected (pcntl_exec() function used)", "GPL EXPLOIT fpcount access", "GPL WEB_SERVER service.pwd", "ET PHISHING Generic Phishing Panel Accessed on Internal Server", "ET WEB_CLIENT Observed JavaScript Event Listener with Clipboard Data", "GPL WEB_SERVER global.asa access", "ET WEB_SERVER JBoss jmx-console Access Control Bypass Attempt", "GPL WEB_SERVER DELETE attempt", "GPL WEB_SERVER writeto.cnf access", "ET WEB_SERVER Weevely PHP backdoor detected (proc_open() function used)", "GPL WEB_SERVER apache ?M=D directory list attempt", "GPL MISC HP Web JetAdmin remote file upload attempt", "ET WEB_SERVER WebShell - PHP eMailer"
Обнаружение подозрительной сетевой активности	"ET INFO Commonly Abused File Sharing Site Domain Observed (anonfiles .com in DNS Lookup)", "ET HUNTING HTTP POST Request XOR Key f6", "ET INFO JAVA - ClassID", "ET HUNTING HTTP POST Request XOR Key 3d", "ET HUNTING HTTP POST Request XOR Key a3", "ET INFO Applied Privacy DNS over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key ca", "ET HUNTING HTTP GET Request XOR Key 69", "ET HUNTING HTTP POST Request XOR Key e5", "ET MALWARE DNS Query for Suspicious cvredirect.no-ip.net Domain - CoinLocker Domain", "ET WEB_CLIENT Proxy - OWASP Zed Attack Proxy Certificate Seen", "ET HUNTING HTTP POST Request XOR Key f0", "ET INFO Observed Image Hosting Domain (imgyukle .com in TLS SNI)", "ET INFO SyncroMSP Remote Remote Management Software Install Registration", "ET INFO Delivr .to Phishing/Security Simulation Service Domain in DNS Lookup (delivrto .me)", "ET HUNTING HTTP GET Request XOR Key c8", "ET HUNTING HTTP POST Request XOR Key 2f", "ET HUNTING HTTP POST Request XOR Key 1c", "ET HUNTING HTTP GET Request XOR Key 95", "ET HUNTING Possible EXE Download From Suspicious TLD (.science) - set", "ET INFO URL Shortener Service Domain in DNS Lookup (cutt .ly)", "ET POLICY Pastebin-style service (note .youdao .com) in TLS SNI", "ET HUNTING HTTP GET Request XOR Key f5", "ET INFO Python SimpleHTTP ServerBanner", "ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M3", "ET INFO Blokada DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 5d", "ET INFO Observed ZeroSSL Certificate for Suspicious TLD (.xyz)", "ET INFO URL Shortener Service Domain in DNS Lookup (2 .ua)", "ET INFO Baidu MiniDownloader System Fingerprint Exfiltration", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M2", "ET HUNTING HTTP GET Request XOR Key 76", "ET INFO Image Hosting Domain in DNS Lookup (imgyukle .com)", "ET GAMES UnknownApps Game Cheat Service Checkin (auth .unknownp .one)", "ET HUNTING HTTP POST to .php on Appspot Hosting - Possible Phishing", "ET HUNTING HTTP GET Request XOR Key 0f", "ET HUNTING Terse Request to note .youdao .com - Possible Download", "ET HUNTING HTTP GET Request XOR Key e3", "ET INFO Minimal HTTP GET Request to rebrand .ly", "ET INFO Observed URL Shortening Service Domain (e .vg in TLS SNI)", "ET HUNTING Possible EXE Download From Suspicious TLD (.gdn) - set", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_3_middle_out", "ET INFO DNS Query for Suspicious .cf Domain", "ET INFO Flowbit set for POST to Quicken Updater", "ET HUNTING HTTP GET Request XOR Key 88", "ET HUNTING HTTP POST Request XOR Key b7", "ET USER_AGENTS Shadowcoin Cryptocurrency UA Observed", "ET HUNTING Possible Fake Edu Host with __test Cookie", "ET HUNTING HTTP POST Request XOR Key e2", "ET HUNTING ZIP file exfiltration over raw TCP", "ET FTP Outbound Java Anonymous FTP Login", "ET HUNTING HTTP POST Request XOR Key 93", "ET HUNTING HTTP GET Request XOR Key 56", "ET HUNTING HTTP GET Request XOR Key d0", "ET HUNTING HTTP GET Request XOR Key e2", "ET INFO Switch DNS Over HTTPS Certificate Inbound", "ET HUNTING PE EXE Download over raw TCP", "ET HUNTING HTTP GET Request XOR Key 03", "ET HUNTING HTTP GET Request XOR Key 63", "ET HUNTING HTTP POST Request XOR Key 19", "ET HUNTING HTTP GET Request XOR Key 1d", "ET POLICY File Being Uploaded to SendSpace File Hosting Site", "ET HUNTING HTTP GET Request XOR Key 2b", "ET CHAT IRC USER Likely bot with 0 0 colon checkin", "ET HUNTING HTTP POST Request XOR Key f2", "ET HUNTING HTTP POST Request XOR Key 53", "ET HUNTING HTTP GET Request XOR Key dd", "ET HUNTING HTTP POST Request

	XOR Key 7b", "ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack", "ET INFO Ordns DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 4c", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.3322.net", "ET HUNTING HTTP POST Request XOR Key 94", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_3_reverse", "ET INFO AhaDNS DNS Over HTTPS Certificate Inbound", "ET INFO Null31 DNS Over HTTPS Certificate Inbound", "ET POLICY Outbound Multiple Non-SMTP Server Emails", "ET INFO Ryan Palmer DNS Over HTTPS Certificate Inbound", "ET POLICY PCHunter CnC activity", "ET HUNTING HTTP POST Request XOR Key d8", "ET HUNTING HTTP GET Request XOR Key eb", "ET HUNTING HTTP POST Request XOR Key 3b", "ET INFO dnsHome DNS Over HTTPS Certificate Inbound", "ET CHAT IRC USER command", "ET EXPLOIT NTDump Session Established Reg-Entry port 139", "ET HUNTING HTTP POST Request XOR Key f4", "ET HUNTING HTTP POST Request XOR Key ce", "ET HUNTING HTTP GET Request XOR Key 26", "ET INFO DYNAMIC_DNS Query to didns .ru Domain", "ET HUNTING HTTP POST Request XOR Key 9d", "ET HUNTING HTTP POST Request XOR Key 6a", "ET HUNTING HTTP GET Request XOR Key ee", "ET HUNTING HTTP GET Request XOR Key 1f", "ET HUNTING HTTP GET Request XOR Key 51", "ET HUNTING HTTP POST Request XOR Key ba", "ET HUNTING HTTP GET Request XOR Key af", "ET HUNTING HTTP GET Request XOR Key 45", "ET HUNTING HTTP GET Request XOR Key 55", "ET HUNTING HTTP GET Request XOR Key 10", "ET HUNTING HTTP GET Request XOR Key 0c", "ET INFO Possible MSXMLHTTP Request (msi) unset (no exe)", "ET INFO Observed Proxy Domain (proxynet .io in TLS SNI)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (officences .com)", "ET INFO Observed DNS Query to Pastebin-style Service (pasteio .com)", "ET HUNTING HTTP POST Request XOR Key 01", "ET INFO Suspicious Domain (*.cf) in TLS SNI", "ET HUNTING HTTP POST Request XOR Key 45", "ET INFO Observed DNS Query to Remote Utilities Domain", "ET HUNTING HTTP POST Request XOR Key 10", "ET INFO Observed DNS Query to Pastebin-style Service (justpaste .it)", "ET INFO Observed ZeroSSL SSL/TLS Certificate", "ET POLICY Outbound HTTP Connection From Cisco IOS Device", "ET EXPLOIT Serialized Java Object Calling Common Collection Function", "ET HUNTING HTTP POST Request XOR Key db", "ET HUNTING HTTP POST Request XOR Key 31", "ET HUNTING HTTP POST Request XOR Key c8", "ET HUNTING HTTP GET Request XOR Key ff", "ET HUNTING HTTP POST Request XOR Key 34", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (officenced .com)", "ET INFO URL Shortener Service Domain in DNS Lookup (wa .sv)", "ET HUNTING HTTP POST Request XOR Key 3f", "ET USER_AGENTS BLEXBot User-Agent", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharepointin .com)", "ET INFO TRR DNS over HTTPS detected", "ET HUNTING HTTP GET Request XOR Key bc", "ET HUNTING HTTP GET Request XOR Key 01", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (officence .com)", "ET HUNTING HTTP GET Request XOR Key 9a", "ET POLICY Signed TLS Certificate with md5WithRSAEncryption", "ET INFO Namecheap URL Forward", "ET HUNTING HTTP POST Request XOR Key aa", "ET HUNTING HTTP POST Request XOR Key 4c", "ET HUNTING HTTP GET Request XOR Key 14", "ET INFO Request for EXE via GO HTTP Client", "ET INFO Suspicious Domain (*.ga) in TLS SNI", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.8866.org", "ET HUNTING HTTP POST Request XOR Key 5d", "ET HUNTING Suspicious BITS EXE DL From Dotted Quad", "ET INFO DNSlow DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key f4", "ET INFO Observed Instagram Story Viewer Domain (dumpor .com in TLS SNI)", "ET INFO NextDNS DNS Over HTTPS Certificate Inbound", "ET INFO Download of Embedded OpenType (EOT) File flowbit set", "ET INFO Commonly Abused File Sharing Site Domain Observed (sendspace .com in DNS Lookup)", "GPL ICMP_INFO PING Pinger Windows", "ET HUNTING HTTP GET Request XOR Key 1c", "ET INFO Observed DNS Query to Filesharing Service (mega .co .nz)", "ET HUNTING HTTP POST Request XOR Key 05", "ET HUNTING HTTP GET Request XOR Key a6", "ET USER_AGENTS Suspicious HttpSocket User-Agent Observed", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (officentry .com)", "ET HUNTING HTTP POST Request XOR Key c4", "ET HUNTING HTTP POST Request XOR Key 42", "ET HUNTING Bit.do Shortened Link Request to EXE", "ET INFO Possible MSXMLHTTP Request (exe) unset (no exe)", "ET POLICY External

	Unencrypted Connection To Aanval Console", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.2288.org", "ET INFO URL Shortener Service Domain in DNS Lookup (snip .ly)", "ET HUNTING HTTP POST Form Submitted to Weebly Free Hosting", "ET HUNTING HTTP POST Request XOR Key fd", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.3322.org", "ET INFO Abused File Sharing Site Domain Observed (qaz .su) in TLS SNI", "ET EXPLOIT libPNG - Possible integer overflow in allocation in png_handle_sPLT", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (officentry .com)", "ET HUNTING HTTP POST Request XOR Key af", "ET HUNTING HTTP GET Request XOR Key d5", "ET HUNTING HTTP POST Request XOR Key 47", "ET INFO Suspicious File Extension Inbound (.phonk)", "ET HUNTING HTTP GET Request XOR Key 85", "ET HUNTING HTTP POST Request XOR Key 08", "ET HUNTING Possible EXE Download From Suspicious TLD (.biz) - set", "ET INFO ET INFO Observed URL Shortening Service Domain (s59 .site) in TLS SNI", "ET INFO URL Shortener Service Domain in DNS Lookup (id .sv)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (prizewings .com)", "ET INFO Plan9-dns DNS Over HTTPS Certificate Inbound", "ET INFO Outdated Browser Landing Page M2", "ET HUNTING HTTP POST Request XOR Key f1", "ET HUNTING Suspicious HTTP POST to Free Web Host Atwebpages", "ET HUNTING HTTP POST Request XOR Key f9", "ET HUNTING Suspicious Possible CollectGarbage in base64 1", "ET HUNTING HTTP GET Request XOR Key 36", "ET HUNTING HTTP POST Request XOR Key be", "ET INFO Certificate with Unknown Content M1", "ET HUNTING HTTP POST Request XOR Key c0", "ET INFO Generic 302 Redirect to Google", "ET INFO Free Hosting Domain (*.freehostia .com in DNS Lookup)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (officence .com)", "ET HUNTING HTTP GET Request XOR Key 64", "ET INFO MyDNS .network DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 86", "ET HUNTING HTTP GET Request XOR Key 47", "ET HUNTING Possible EXE Download From Suspicious TLD (.icu) - set", "ET HUNTING HTTP GET Request XOR Key b8", "ET HUNTING HTTP GET Request XOR Key aa", "ET HUNTING HTTP POST Request XOR Key 71", "ET HUNTING HTTP POST Request XOR Key 82", "ET USER_AGENTS SideStep User-Agent", "ET SCAN Behavioral Unusual Port 1434 traffic Potential Scan or Infection", "ET WEB_CLIENT Encoded javascriptdocument.write - usually hostile", "ET HUNTING HTTP POST Request XOR Key ac", "ET INFO Packetriot Tunneling Domain in DNS Lookup (reversetunnel .net)", "ET HUNTING HTTP GET Request XOR Key 0e", "GPL ICMP_INFO PING BeOS4.x", "ET INFO Commonly Abused File Sharing Site Domain Observed (fex .net in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 32", "ET POLICY Mattermost API Usage", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M5", "ET INFO EXE - Served Attached HTTP", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol lower Bypass (udp) (CVE-2021-44228)", "ET HUNTING Cloned Page Hosted on Microsoft Hosting", "ET HUNTING HTTP POST Request XOR Key 2c", "ET INFO JAVA - document.createElement applet", "ET INFO Malware Destroyer Checkin", "ET HUNTING HTTP GET Request XOR Key 50", "ET INFO Restena DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key c3", "ET USER_AGENTS Discord Bot User-Agent Observed (DiscordBot)", "ET HUNTING HTTP GET Request XOR Key f0", "ET HUNTING HTTP GET Request XOR Key d6", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (prizewel .com)", "ET HUNTING HTTP POST Request XOR Key c7", "ET HUNTING HTTP POST Request XOR Key 50", "ET HUNTING HTTP POST Request XOR Key 56", "ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M2", "ET HUNTING HTTP GET Request XOR Key 2a", "ET INFO Python BaseHTTP ServerBanner", "ET HUNTING Suspicious Windows Executable CreateRemoteThread", "ET HUNTING HTTP POST Request XOR Key 87", "ET INFO URL Shortening Service Domain in DNS Lookup (maxiurl .com)", "ET HUNTING HTTP POST Request XOR Key 76", "ET USER_AGENTS BeeMovie Related Activity", "ET HUNTING HTTP POST Request XOR Key df", "ET HUNTING HTTP GET Request XOR Key ea", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncDeletePrinterDriver", "ET HUNTING HTTP POST Request XOR Key dc", "GPL ICMP_INFO PING BayRS Router", "ET HUNTING Possible EXE Download From Suspicious TLD (.click) - set", "ET INFO QR Code Generator Domain in DNS Lookup (qr-code-generator .com)", "ET INFO Abused File

	Hosting Domain in DNS Lookup (transferxl .com)", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.8866.org", "ET INFO Generic 000webhostapp.com POST 2018-09-27 (set)", "ET HUNTING HTTP GET Request XOR Key 40", "ET HUNTING HTTP POST Request XOR Key b8", "ET HUNTING HTTP POST Request XOR Key 81", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharestion .com)", "ET HUNTING HTTP POST Request XOR Key 84", "ET HUNTING [TW] Internet Computer HTTP Referer Observed", "ET INFO ZoneAlarm Download Flowbit Set", "ET INFO Observed DNS Over HTTPS Domain (dns .alidns .com in TLS SNI)", "ET INFO Observed File Sharing Service (www .uplooder .net) in DNS Lookup", "ET HUNTING HTTP GET Request XOR Key c7", "ET HUNTING HTTP POST Request XOR Key 1b", "ET INFO Observed URL Shortener Domain (lk .tc in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 4b", "ET INFO URL Shortener Service Domain in DNS Lookup (fb .sv)", "ET INFO URL Shortener Service Domain in DNS Lookup (ya .sv)", "ET INFO User-Agent (wininet)", "ET INFO Powershell Base64 Decode Command Inbound", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (instantrevert .net)", "ET INFO Observed DNS Query to BaitAndPhish Domain", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (officested .com)", "ET HUNTING HTTP POST Request XOR Key 85", "ET HUNTING HTTP POST Request XOR Key 1d", "ET INFO Commonly Abused File Sharing Site Domain Observed (sendspace .com in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 79", "ET HUNTING HTTP POST Request XOR Key 32", "ET HUNTING HTTP POST Request XOR Key 37", "ET HUNTING HTTP POST Request XOR Key 7c", "ET HUNTING HTTP GET Request XOR Key 24", "ET HUNTING HTTP POST Request XOR Key 8d", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (com-onlinebanking .com)", "ET HUNTING HTTP GET Request XOR Key 84", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M4", "ET HUNTING HTTP POST Request XOR Key c2", "ET HUNTING HTTP GET Request XOR Key 2c", "ET HUNTING HTTP GET Request XOR Key ac", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharepointle .com)", "ET POLICY Pastebin-style service note .youdao .com in DNS query", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M1", "ET HUNTING HTTP GET Request XOR Key 6d", "ET INFO EXE - OSX Disk Image Download", "ET INFO Observed Image Hosting Domain (resimupload .org in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 59", "ET INFO EXE - Served Inline HTTP", "ET HUNTING HTTP GET Request XOR Key 72", "ET INFO Artikel10 DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 9e", "ET HUNTING HTTP POST Request XOR Key 22", "ET HUNTING HTTP GET Request XOR Key 83", "ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key fb", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (magnetonics .com)", "ET HUNTING HTTP GET Request XOR Key 8c", "ET INFO Windows OS Submitting USB Metadata to Microsoft", "ET MALWARE Medfos Connectivity Check", "ET INFO HTTP Sniffer Domain in TLS SNI (httpdebugger .com)", "ET INFO DYNAMIC_DNS Query to *.duckdns. Domain", "ET HUNTING HTTP POST Request XOR Key 2a", "ET HUNTING [TW] Internet Computer HTTP Request Observed", "ET HUNTING HTTP POST Request XOR Key 13", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper UDP Bypass) (Outbound) (CVE-2021-44228)", "ET EXPLOIT NTDump.exe Service Started port 139", "ET HUNTING HTTP POST Request XOR Key 23", "ET HUNTING HTTP GET Request XOR Key 19", "ET SCAN Rapid POP3S Connections - Possible Brute Force Attack", "ET WEB_CLIENT Download of .MOV Content flowbit set", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (phishwall .net)", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_2_bottom_half", "ET INFO Generic HTTP EXE Upload Outbound", "ET HUNTING HTTP POST Request XOR Key b1", "ET HUNTING HTTP POST Request XOR Key 8f", "ET HUNTING HTTP GET Request XOR Key f2", "ET HUNTING Microsoft Malware Protection User-Agent Observed to Non-Microsoft Domain", "ET INFO URL Shortener Service Domain in DNS Lookup (do .sv)", "ET HUNTING HTTP GET Request XOR Key 38", "ET HUNTING HTTP GET Request XOR Key 62", "ET INFO Adguard DNS Over HTTPS Certificate Inbound", "ET INFO Suspicious Domain (*.ml) in TLS SNI", "ET INFO Bit.do

	Shortened Link Request (set)", "ET HUNTING HTTP POST Request XOR Key 77", "ET HUNTING HTTP POST Request XOR Key ee", "ET HUNTING HTTP POST Request XOR Key 96", "ET HUNTING HTTP GET Request XOR Key 81", "ET HUNTING HTTP GET Request XOR Key a4", "ET HUNTING HTTP GET Request XOR Key 0b", "ET HUNTING HTTP POST Request XOR Key d5", "ET INFO Brahma World DNS Over HTTPS Certificate Inbound", "ET INFO Ibksturm DNS Over HTTPS Certificate Inbound", "ET INFO Possible MSXMLHTTP Request (no .exe)", "ET HUNTING Suspicious Windows Executable WriteProcessMemory", "ET HUNTING HTTP POST Request XOR Key da", "ET HUNTING HTTP GET Request XOR Key 17", "ET HUNTING HTTP GET Request XOR Key b2", "ET HUNTING HTTP GET Request XOR Key 30", "ET INFO Java Downloading Class flowbit no alert", "ET PHISHING SSL/TLS Certificate Observed (Lucy Phishing Awareness Default Certificate)", "ET HUNTING Suspicious EXE requested with Java UA", "ET HUNTING HTTP GET Request XOR Key 90", "ET POLICY TeamViewer Keep-alive outbound", "ET HUNTING HTTP POST Request XOR Key 58", "ET USER_AGENTS Observed Malicious CASPER/Mirai UA", "ET INFO SAFIB Assistant Remote Administration Tool CnC Checkin", "ET INFO Instagram Story Viewer Domain in DNS Lookup (greatfon .com)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (CVE-2021-44228)", "ET HUNTING HTTP GET Request XOR Key 35", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol TCP (Outbound) (CVE-2021-44228)", "ET INFO URL Shortener Service Domain in DNS Lookup (sa .sv)", "ET INFO 3XX redirect to data URL", "ET INFO DNSForge DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 8a", "ET CHAT IRC PONG response", "ET INFO EXE SCardForgetReaderGroupA (Used in Malware Anti-Debugging)", "ET INFO Splashtop Domain in DNS Lookup (splashtop .com)", "ET HUNTING HTTP POST Request XOR Key 4e", "ET ATTACK_RESPONSE Obfuscated JS - URL Encoded Unescape Function Call Inbound", "ET HUNTING Possible EXE Download From Suspicious TLD (.top) - set", "ET HUNTING Possible EXE Download From Suspicious TLD (.webcam) - set", "ET HUNTING HTTP GET Request XOR Key 25", "ET HUNTING HTTP GET Request XOR Key f9", "ET INFO Cisco Smart Install Protocol Observed", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol UDP (CVE-2021-44228)", "ET HUNTING HTTP GET Request XOR Key c6", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncCorePrinterDriverInstalled", "ET HUNTING HTTP POST Request XOR Key 12", "ET HUNTING HTTP POST Request XOR Key b0", "ET HUNTING HTTP GET Request XOR Key 41", "GPL ICMP_INFO PING WhatsupGold Windows", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (com-token-auth .com)", "ET HUNTING HTTP POST Request XOR Key 11", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (prizemons .com)", "ET INFO URL Shortener Service Domain in DNS Lookup (is .gd)", "ET HUNTING HTTP POST Request XOR Key d6", "ET HUNTING HTTP GET Request XOR Key 9f", "ET HUNTING HTTP GET Request XOR Key 68", "ET INFO Certificate with Unknown Content M2", "ET HUNTING HTTP POST Request XOR Key e6", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharestion .com)", "ET HUNTING HTTP POST Request XOR Key d3", "ET HUNTING HTTP GET Request XOR Key c2", "ET HUNTING HTTP GET Request XOR Key a7", "ET HUNTING HTTP POST Request XOR Key 5f", "ET HUNTING HTTP GET Request XOR Key 27", "ET HUNTING HTTP GET Request XOR Key 58", "ET POLICY Telnet to HP JetDirect Printer With No Password Set", "ET HUNTING HTTP POST Request XOR Key 49", "ET HUNTING HTTP POST Request XOR Key 48", "ET HUNTING HTTP POST Request XOR Key 66", "ET HUNTING Suspected Malicious Telegram Communication (POST)", "ET INFO Safe Surfer DNS Over HTTPS Certificate Inbound", "ET INFO Free File Hosting Domain in DNS Lookup (fileditch .com)", "ET HUNTING HTTP GET Request XOR Key 6f", "ET HUNTING HTTP POST Request XOR Key 29", "ET HUNTING HTTP POST Request XOR Key 5b", "ET INFO PK/Compressed doc/JAR header", "ET INFO Gophish X-Server", "ET INFO DNS For Family DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 57", "ET HUNTING HTTP GET Request XOR Key 02", "ET INFO Observed URL Shortener Service Domain (cutt .ly in TLS SNI)", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (malwarebouncer .com)", "ET WEB_CLIENT Proxy - BurpSuite PortSwigger Proxy Certificate Seen", "ET HUNTING HTTP GET Request XOR Key e7", "ET

	INFO DigitalSize DNS Over HTTPS Certificate Inbound", "ET INFO Packed Executable Download", "ET INFO URL Shortener Service Domain in DNS Lookup (tg .sv)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (Outbound) (CVE-2021-44228)", "ET INFO Observed Abused File Hosting Domain (transferxl-download .com in TLS SNI)", "ET HUNTING [TW] Likely Hex Executable String", "ET HUNTING HTTP GET Request XOR Key 7b", "ET HUNTING HTTP GET Request XOR Key 97", "ET MALWARE Observed DNS Query to Temporary File Hosting Domain (temp .sh)", "ET HUNTING Possible EXE Download From Suspicious TLD (.accountant) - set", "ET HUNTING HTTP POST Request XOR Key b9", "ET HUNTING HTTP POST Request XOR Key ea", "ET HUNTING HTTP GET Request XOR Key a9", "ET HUNTING HTTP GET Request XOR Key da", "ET INFO URL Shortener Service Domain in DNS Lookup (yt .sv)", "ET INFO OpenSea API Query NFT Discovery Details (GET)", "ET POLICY [TW] IPFS Protocol HTTP Headers Observed", "ET INFO Image Hosting Domain in DNS Lookup (resimupload .org)", "ET HUNTING Possible EXE Download From Suspicious TLD (.work) - set", "ET HUNTING Possible Generic Stealer Sending System Information", "ET HUNTING HTTP POST Request XOR Key 9b", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.8800.org", "ET HUNTING HTTP GET Request XOR Key e6", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (windocyte .com)", "ET HUNTING HTTP POST Request XOR Key 7d", "ET HUNTING Suspicious Request to Image with User-Agent Ending in .exe", "ET INFO Instagram Story Viewer Domain in DNS Lookup (smihub .com)", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharesbyte .com)", "ET HUNTING HTTP POST Request XOR Key a2", "ET INFO URL Shortener Domain in DNS Lookup (lk .tc)", "ET INFO URL Shortener Service Domain in DNS Lookup (tra-ta-ta.it .com)", "ET HUNTING HTTP POST Request XOR Key 67", "ET HUNTING HTTP GET Request XOR Key 94", "ET INFO Observed Custom Logo Domain (seeklogo .com in TLS SNI)", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncInstallPrinterDriverFromPackage", "ET HUNTING HTTP POST Request XOR Key a9", "ET USER_AGENTS Microsoft Office Existence Discovery User-Agent", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.7766.org", "ET INFO BitNinja IO Security Check", "GPL SCAN PING CyberKit 2.2 Windows", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (net-login .com)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharession .com)", "ET HUNTING HTTP POST Request XOR Key 64", "ET HUNTING HTTP GET Request XOR Key 5e", "ET HUNTING HTTP GET Request XOR Key 21", "ET INFO [401TRG] RPCNetlogon UUID (CVE-2020-1472) (Set)", "ET INFO Edgy DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key d2", "ET HUNTING Observed Telegram API Domain (api .telegram .org in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 59", "ET HUNTING HTTP GET Request XOR Key 42", "ET HUNTING HTTP POST Request XOR Key c5", "ET HUNTING HTTP GET Request XOR Key e1", "ET INFO URL Shortener Service Domain DNS Lookup (zii .to)", "ET HUNTING HTTP GET Request XOR Key 1b", "ET INFO External IP Lookup HTTP Request (ip .dnsexit .com)", "ET HUNTING HTTP GET Request XOR Key 8f", "ET CHAT IRC authorization message", "ET INFO EXE - OSX Executable Download - PowerPC Arch", "ET SCAN Rapid POP3 Connections - Possible Brute Force Attack", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (mcsharepoint .com)", "ET HUNTING HTTP GET Request XOR Key b7", "ET HUNTING HTTP POST Request XOR Key f3", "ET HUNTING HTTP POST Request XOR Key b2", "ET INFO URL Shortener Service Domain in DNS Lookup (u .to)", "ET INFO Paesa DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 88", "ET HUNTING HTTP GET Request XOR Key c5", "ET INFO Hitian .me DNS Over HTTPS Certificate Inbound", "ET INFO GameHouse License Check", "ET HUNTING HTTP POST Request XOR Key 4f", "ET HUNTING HTTP GET Request XOR Key d8", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.3322.net", "ET GAMES Solaris2 Checkin", "ET HUNTING HTTP POST Request XOR Key 24", "ET HUNTING HTTP POST Request XOR Key 72", "ET HUNTING HTTP GET Request XOR Key 77", "ET HUNTING HTTP GET Request XOR Key 65", "ET INFO Splashtop Domain in DNS Lookup (splashtop .eu)", "ET HUNTING HTTP POST Request XOR Key 99", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_2_top_half", "ET HUNTING HTTP POST Request XOR Key 3e", "ET POLICY [MS-RPRN] Windows

	Printer Spooler Activity - AddPrinterDriverEx with Suspicious Filepath", "ET CHAT IRC NICK command", "ET HUNTING HTTP GET Request XOR Key db", "ET HUNTING HTTP GET Request XOR Key 4f", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncGetCorePrinterDrivers", "ET INFO DYNAMIC_DNS HTTP Request to a *.dyndns.* domain", "ET HUNTING Redirect to Joom AG Hosted Document - Potential Phishing", "ET HUNTING HTTP GET Request XOR Key ab", "ET PHISHING IRS Credential Phish Domain in DNS Lookup (jbdelmarket .com)", "ET HUNTING HTTP POST Request XOR Key 4d", "ET WEB_SERVER OptionsBleed (CVE-2017-9798)", "ET INFO DYNAMIC_DNS Query to Abused Domain *.mooo.com", "ET INFO DYNAMIC_DNS Query to dynnamn .ru Domain", "ET INFO WeDNS DNS Over HTTPS Certificate Inbound", "ET INFO External File Sharing Service in DNS Lookup (sharefile .com)", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (prizegives .com)", "ET HUNTING HTTP GET Request XOR Key 67", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (templatern .com)", "ET HUNTING HTTP GET Request XOR Key a5", "ET HUNTING HTTP POST Request XOR Key d1", "ET HUNTING HTTP GET Request XOR Key 91", "ET INFO Cisco Umbrella (OpenDNS) DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 4b", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.9966.org", "ET VOIP H.323 in Q.931 Call Setup - Inbound", "ET INFO Outdated Browser Landing Page M3", "ET HUNTING PNG image exfiltration over raw TCP", "ET CHAT IRC PING command", "ET HUNTING Possible EXE Download From Suspicious TLD (.men) - set", "ET INFO PDF - Acrobat Enumeration - var PDFObject", "ET HUNTING HTTP GET Request XOR Key 8d", "ET HUNTING HTTP GET Request XOR Key 99", "ET INFO Observed DNS Query to (proxies .black) Web Proxy/Anonymizer Domain/Sub-Domain", "ET INFO Observed Free Hosting Domain (mypressonline .com) in DNS Lookup", "ET HUNTING HTTP POST Request XOR Key 90", "ET HUNTING HTTP POST Request XOR Key 98", "ET HUNTING HTTP GET Request XOR Key 37", "ET HUNTING HTTP GET Request XOR Key 18", "ET HUNTING HTTP GET Request XOR Key 71", "ET HUNTING HTTP POST Request XOR Key 74", "ET INFO Commonly Abused File Sharing Site Domain Observed (anonfiles .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key d9", "ET INFO Possible WinHttpRequest (no .exe)", "ET HUNTING HTTP GET Request XOR Key 87", "ET INFO Generic HTTP EXE Upload Inbound", "ET INFO UncensoredDNS DNS Over HTTPS Certificate Inbound", "ET INFO Commonly Abused File Sharing Site Domain Observed (send .exploit .in in DNS Lookup)", "ET INFO DropBox User Content Download Access over SSL M2", "ET HUNTING Possible Fake Edu Host On InfinityFree Service", "ET INFO MSSQL sp_addextendedproc Command Observed", "ET INFO Observed Instagram Story Viewer Domain (smihub .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 4a", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.9966.org", "ET HUNTING RAR file exfiltration over raw TCP", "GPL ICMP_INFO PING Flowpoint2200 or Network Management Software", "ET INFO URL Shortener Service Domain in DNS Lookup (rebrand .ly)", "ET HUNTING HTTP POST Request XOR Key 21", "ET INFO Observed Cloudflare Universal (Shared) Certificate, Retired", "GPL ICMP_INFO PING Network Toolbox 3 Windows", "ET HUNTING HTTP GET Request XOR Key 78", "ET HUNTING HTTP POST Request XOR Key 1f", "GPL SCAN PING Delphi-Piette Windows", "ET HUNTING HTTP GET Request XOR Key ad", "ET INFO Observed Let's Encrypt Certificate from Retired Intermediate", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (doctricant .com)", "ET HUNTING Improperly Spaced Accept Header in User-Agent", "ET USER_AGENTS ABBCCoin Activity Observed", "ET HUNTING HTTP GET Request XOR Key be", "ET HUNTING HTTP GET Request XOR Key 6a", "ET HUNTING [TW] Internet Computer HTTP Location Redirect Observed", "ET MALWARE Generic DNS Query for Suspicious CryptoWall (crpt) Domains", "ET INFO DNS Query to a Free Hosting Domain Domain (*.ct8 pl)", "ET WEB_CLIENT Microsoft Office RTF Stack Buffer Overflow", "ET HUNTING HTTP GET Request XOR Key 39", "ET HUNTING SUSPICIOUS Single JS file inside of ZIP Download (Observed as lure in malspam campaigns)", "ET HUNTING HTTP GET Request XOR Key bd", "ET HUNTING HTTP POST Request XOR Key 7a", "ET HUNTING HTTP POST Request XOR Key ec", "ET HUNTING Possible EXE Download From Suspicious TLD (.download) - set", "ET HUNTING HTTP GET Request XOR Key 05", "ET INFO Observed URL Shortening Service Domain (s

	.id in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 6c", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncGetPrinterDriverDirectory", "ET POLICY Cisco IOS Self Signed Certificate Served to External Host", "ET INFO ControlId DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key b6", "ET HUNTING HTTP POST Request XOR Key b4", "ET HUNTING HTTP POST Request XOR Key a4", "ET HUNTING HTTP GET Request XOR Key cc", "ET INFO Splashtop Domain (splashtop .com) in TLS SNI", "ET HUNTING HTTP POST Request XOR Key c9", "ET HUNTING HTTP GET Request XOR Key 7d", "ET INFO GET Request Exfiltrating Username and Hostname", "ET INFO Observed Telegram Domain (t .me in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key a8", "ET INFO URL Shortener Service Domain in DNS Lookup (bd .sv)", "ET HUNTING HTTP GET Request XOR Key 08", "ET HUNTING HTTP GET Request XOR Key 4d", "ET INFO IQDNS DNS Over HTTPS Certificate Inbound", "ET HUNTING Possible Malicious Document Request to NOIP DynDNS Domain", "ET HUNTING URL Observed in PDF Downloaded via Dropbox", "ET POLICY External FTP Connection TO Local HP JetDirect Printer", "GPL EXPLOIT rsyncd module list access", "ET HUNTING HTTP GET Request XOR Key a3", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower UDP Bypass) (Outbound) (CVE-2021-44228)", "ET HUNTING Suspicious Possible CollectGarbage in base64 2", "ET HUNTING SUSPICIOUS Local file read using read protocol", "ET HUNTING HTTP POST Request XOR Key 26", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (doctricant .com)", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.2288.org", "ET INFO URL Shortener Service Domain in DNS Lookup (ai .sv)", "ET HUNTING [TW] Internet Computer Domain Observed", "ET HUNTING Go-http-client POSTing IP Address and Username", "ET INFO Microsoft Compact Office Document Format File Download", "ET SCAN Behavioral Unusual Port 139 traffic Potential Scan or Infection", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (CVE-2021-44228)", "ET HUNTING HTTP POST Request XOR Key bf", "ET HUNTING HTTP GET Request XOR Key 5a", "ET EXPLOIT Serialized Spring Java Object Generated by ysoserial", "ET INFO Alekberg DNS Over HTTPS Certificate Inbound", "ET INFO URL Shortener Service Domain in DNS Lookup (vk .sv)", "ET HUNTING HTTP POST Request XOR Key 9c", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (Outbound) (CVE-2021-44228)", "ET HUNTING HTTP GET Request XOR Key fd", "ET POLICY EXE File Downloaded from Discord", "GPL ATTACK_RESPONSE isakmp login failed", "ET HUNTING HTTP POST Request XOR Key 9a", "ET INFO SSH-2.0-Go version string Observed in Network Traffic - Outbound", "ET HUNTING HTTP POST Request XOR Key c6", "ET FTP Outbound Java Downloading jar over FTP", "ET INFO LibreDNS DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key cf", "ET HUNTING HTTP GET Request XOR Key 12", "ET HUNTING HTTP GET Request XOR Key 9c", "ET HUNTING HTTP POST Request XOR Key 5a", "ET HUNTING HTTP POST Request XOR Key 54", "ET HUNTING HTTP POST Request XOR Key de", "ET HUNTING HTTP GET Request XOR Key 60", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (shareholds .com)", "ET SCAN Rapid IMAP Connections - Possible Brute Force Attack", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.7766.org", "ET INFO Observed DNS Query to xsph .ru Domain", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncUploadPrinterDriverPackage", "ET HUNTING HTTP POST Request XOR Key fe", "ET HUNTING HTTP GET Request XOR Key ed", "ET INFO SAFIB Assistant Remote Administration Tool Keepalive", "ET HUNTING HTTP GET Request XOR Key b3", "ET HUNTING HTTP GET Request XOR Key 7a", "ET HUNTING Possible Generic Stealer Sending a Screenshot", "ET INFO URL Shortening Service Domain in DNS Lookup (e .vg)", "ET SCAN NNG MS02-039 Exploit False Positive Generator - May Conceal A Genuine Attack", "ET POLICY PCHunter Download Observed", "ET HUNTING HTTP POST Request XOR Key 92", "ET HUNTING HTTP GET Request XOR Key 22", "ET HUNTING HTTP POST Request XOR Key 55", "ET HUNTING HTTP GET Request XOR Key 6e", "ET HUNTING HTTP GET Request XOR Key d4", "ET HUNTING HTTP POST Request XOR Key 02", "ET WEB_CLIENT Download of PDF With Uncompressed Flash Content flowbit set", "ET INFO Infotek DNS Over HTTPS Certificate Inbound", "ET HUNTING EXE Downloaded from Github", "ET HUNTING HTTP POST

	Request XOR Key 6d", "ET INFO Limo Telu DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 3c", "ET HUNTING Possible Malicious Document Request to ChangeIP Dynamic DNS Domain", "ET POLICY ABBCCoin Checkin", "ET HUNTING HTTP GET Request XOR Key cd", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_2_middle_out", "ET POLICY Metasploit Framework Checking For Update", "ET HUNTING HTTP GET Request XOR Key 3f", "ET MALWARE Known Sinkhole Response Kryptos Logic", "ET HUNTING HTTP POST Request XOR Key 52", "ET PHISHING Successful Wombat Phishing Test", "ET HUNTING HTTP GET Request XOR Key ca", "ET INFO Free Web Hosting Domain (c1 .biz) in DNS Lookup", "ET INFO DYNAMIC_DNS Query to *.dyndns. Domain", "ET HUNTING HTTP POST Request XOR Key 04", "ET POLICY Java Client HTTP Request", "ET HUNTING HTTP POST Request XOR Key 28", "ET POLICY Inbound Frequent Emails - Possible Spambot Inbound", "ET HUNTING HTTP GET Request XOR Key 5c", "ET HUNTING HTTP POST Request XOR Key e4", "ET HUNTING HTTP POST Request XOR Key b3", "ET INFO URL Shortener Service Domain in DNS Lookup (tt .sv)", "ET HUNTING Possible EXE Download From Suspicious TLD", "ET HUNTING HTTP GET Request XOR Key 3e", "ET INFO Observed URL Shortening Service Domain (maxiurl .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key fc", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (mcsharepoint .com)", "ET INFO stopify .co Domain in DNS Lookup", "ET HUNTING HTTP POST Request XOR Key c1", "ET HUNTING Outbound POST Request with Zipped Directory Traversal Filename", "ET HUNTING [TW] Page Contains Redirect to Likely Urlpages Web Hosting Technique", "ET HUNTING HTTP POST Request XOR Key ae", "ET INFO Symantec Download Flowbit Set", "ET INFO Possible Outdated Browser Landing Page M1", "ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol TCP (CVE-2021-44228)", "ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent", "ET HUNTING HTTP GET Request XOR Key 07", "ET INFO ffmuc DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 83", "ET HUNTING HTTP GET Request XOR Key 80", "ET USER_AGENTS Microsoft Windows Vista UA - Commonly Abused", "ET HUNTING HTTP GET Request XOR Key c1", "ET HUNTING HTTP POST Request XOR Key 18", "GPL ICMP_INFO PING Seer Windows", "ET INFO URL Shortener Service Domain in DNS Lookup (me .sv)", "ET HUNTING HTTP GET Request XOR Key 5f", "ET CHAT IRC USER Off-port Likely bot with 0 0 colon checkin", "ET EXPLOIT NTDump.exe Service Started port 445", "ET HUNTING HTTP POST Request XOR Key 73", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_2_forward", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (mesharepoint .com)", "ET INFO URL Shortener Service Domain DNS Lookup (zshorten .com)", "ET INFO CZ.NIC DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 2d", "ET INFO localhost .run TLS Certification Observed", "ET INFO LavaDNS DNS Over HTTPS Certificate Inbound", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (bloemlight .com)", "ET INFO URL Shortening Service Domain in DNS Lookup (shrtcnl .com)", "ET HUNTING HTTP GET Request XOR Key d1", "ET HUNTING HTTP GET Request XOR Key 13", "GPL ICMP_INFO PING speedera", "ET HUNTING HTTP POST Request XOR Key 1e", "ET HUNTING HTTP POST Request XOR Key ef", "ET HUNTING HTTP GET Request XOR Key e8", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharesbyte .com)", "ET INFO MegaNerd DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 82", "ET HUNTING HTTP GET Request XOR Key 8e", "ET HUNTING Possible EXE Download From Suspicious TLD (.gq) - set", "ET HUNTING HTTP POST Request XOR Key e9", "ET HUNTING HTTP GET Request XOR Key e0", "ET HUNTING HTTP GET Request XOR Key 54", "ET HUNTING HTTP GET Request XOR Key 4a", "ET INFO Splashtop Domain (splashtop .eu) in TLS SNI", "ET INFO HTTP Request for ISO File Direct to IP", "ET HUNTING HTTP POST Request XOR Key 78", "ET HUNTING HTTP GET Request XOR Key 15", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharepointen .com)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (prizemons .com)", "ET HUNTING HTTP GET Request XOR Key 43", "ET HUNTING Suspicious NULL DNS Request", "ET HUNTING HTTP GET Request XOR Key e5", "ET HUNTING HTTP POST Request XOR Key 6f", "ET INFO Image

	Hosting Domain in DNS Lookup (hizliresim .com)", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncGetPrinterDriver", "ET INFO infinityfree .net Domain in DNS Lookup", "ET HUNTING HTTP GET Request XOR Key a2", "ET INFO Cloudflare DNS Over HTTPS Certificate Inbound", "ET WEB_SERVER WebShell - PostMan", "ET INFO Observed URL Shortening Service Domain (shrtcnl .com in TLS SNI)", "ET INFO DYNAMIC_DNS Query to 3322.net Domain *.6600.org", "ET CHAT IRC JOIN command", "ET HUNTING HTTP GET Request XOR Key df", "ET INFO URL Shortener Service Domain in DNS Lookup (rt .sv)", "ET ATTACK_RESPONSE PowerShell Geo Check Before Execution", "ET HUNTING HTTP POST Form Submitted to 123formbuilder Free Hosting", "GPL ICMP_INFO PING *NIX", "ET INFO Observed URL Shortener Service Domain (www .kisa .link in TLS SNI)", "ET INFO Custom Logo Domain in DNS Lookup (seeklogo .com)", "ET ATTACK_RESPONSE Obfuscated JS - Possible URL Encoded JS Inbound", "ET INFO Internet Initiative Japan DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key eb", "ET HUNTING Microsoft cmd.exe Banner Output - Decimal Encoded", "ET HUNTING HTTP GET Request XOR Key 61", "ET HUNTING HTTP GET Request XOR Key 48", "ET HUNTING HTTP GET Request XOR Key b9", "ET HUNTING HTTP POST Request XOR Key 57", "ET HUNTING HTTP POST Request XOR Key a7", "ET HUNTING HTTP GET Request XOR Key dc", "ET HUNTING HTTP POST Request XOR Key 65", "ET HUNTING HTTP POST Request XOR Key e1", "ET INFO Proxy Domain in DNS Lookup (proxynet .io)", "ET HUNTING HTTP GET Request XOR Key 9d", "ET HUNTING HTTP POST Request XOR Key 46", "ET INFO Observed SyncroMSP Remote Management Software Domain in DNS Lookup (kabutoservices .com)", "ET HUNTING HTTP GET Request XOR Key cf", "ET CHAT IRC PRIVMSG command", "ET HUNTING Suspicious Possible CollectGarbage in base64 3", "ET HUNTING HTTP GET Request XOR Key f3", "ET INFO Online Code Editor Domain in DNS Lookup (trinket .io)", "ET HUNTING HTTP GET Request XOR Key 31", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (windocyte .com)", "ET PHISHING IRS Credential Phish Domain in DNS Lookup (supportmicrohere .com)", "ET USER_AGENTS Go HTTP Client User-Agent", "ET HUNTING HTTP POST Request XOR Key 95", "ET HUNTING HTTP GET Request XOR Key d9", "ET INFO DNSPod DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 28", "ET HUNTING HTTP POST Request XOR Key 16", "ET HUNTING HTTP POST Request XOR Key 25", "ET HUNTING HTTP POST Request XOR Key 33", "ET INFO LLNMR query response to wpad", "ET HUNTING HTTP GET Request XOR Key 3a", "ET INFO Observed Dynamic DNS Service Domain in TLS SNI (duia .ro)", "ET HUNTING HTTP GET Request XOR Key 06", "ET HUNTING Possible EXE Download From Suspicious TLD (.yokohama) - set", "ET GAMES UnknownApps Game Cheat Service Checkin (auth .hwidspoof .me)", "ET HUNTING HTTP POST Request XOR Key 09", "ET HUNTING HTTP POST Request XOR Key bb", "ET HUNTING HTTP GET Request XOR Key b6", "ET POLICY SSL/TLS Certificate Observed (Upaste)", "ET INFO IRC Nick change on non-standard port", "ET HUNTING HTTP GET Request XOR Key ce", "ET INFO File Sharing Service Domain (docdroid .net) in TLS SNI", "ET HUNTING HTTP POST Request XOR Key 97", "ET MALWARE DNS Query for Suspicious cvredirect.ddns.net Domain - CoinLocker Domain", "ET HUNTING HTTP GET Request XOR Key 73", "ET HUNTING HTTP GET Request XOR Key 74", "ET INFO URL Shortener Service Domain in DNS Lookup (kisa .link)", "ET INFO Killbot JS Configuration - Possible Phishing", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (mesharepoint .com)", "ET HUNTING HTTP POST Request XOR Key ff", "ET HUNTING HTTP POST Request XOR Key 80", "ET INFO Observed SSL Cert (logodownload .org)", "ET INFO EXE CheckRemoteDebuggerPresent (Used in Malware Anti-Debugging)", "ET HUNTING HTTP POST Request XOR Key 75", "ET HUNTING HTTP GET Request XOR Key 23", "ET INFO Observed Delivr .to Phishing/Security Simulation Service Domain (delivrto .me in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 0f", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (kb4 .io)", "ET INFO myobfuscate.com Encoded Script Calling home", "ET INFO Observed File Sharing Service Domain (www .uplooder .net) in TLS SNI", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_3_invalid", "ET INFO Commonly Abused Github-like Site (codeberg .org in DNS Lookup)", "ET HUNTING HTTP GET Request XOR Key 8a", "ET HUNTING HTTP POST Request XOR Key 7e", "ET

	HUNTING HTTP GET Request XOR Key cb", "ET INFO URL Shortener Service Domain in DNS Lookup (in .sv)", "ET INFO Observed URL Shortener Service Domain (zshorten .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key d2", "ET HUNTING HTTP POST Request XOR Key 79", "ET HUNTING HTTP POST Request XOR Key 0b", "ET INFO Bortzmeyer DNS Over HTTPS Certificate Inbound", "ET INFO URL Shortener Service Domain in DNS Lookup (wc .sv)", "ET HUNTING HTTP POST Request XOR Key 5e", "ET INFO Charter DNS Over HTTPS Certificate Inbound", "ET HUNTING Telegram API Domain in DNS Lookup", "ET INFO Adobe PKG Download Flowbit Set", "ET HUNTING HTTP GET Request XOR Key 93", "ET HUNTING HTTP POST Request XOR Key 41", "ET HUNTING HTTP POST Request XOR Key 44", "ET INFO SSH-2.0-Go version string Observed in Network Traffic - Inbound", "ET HUNTING SUSPICIOUS PPT Download with Embedded OLE Object", "ET HUNTING HTTP POST Request XOR Key 36", "ET HUNTING Chrome/0 in User-Agent", "ET INFO Observed DNS Query to HTTP Sniffer Domain (httpdebugger .com)", "ET INFO TheRifleMan DNS Over HTTPS Certificate Inbound", "ET HUNTING RAR file download over raw TCP", "ET HUNTING HTTP POST Request XOR Key 07", "ET HUNTING HTTP GET Request XOR Key 53", "ET POLICY Microsoft TEREDO IPv6 tunneling", "ET HUNTING HTTP POST Request XOR Key 15", "ET HUNTING HTTP POST Request XOR Key cc", "ET INFO URL Shortener Service Domain in DNS Lookup (tw .sv)", "ET INFO Image Hosting Domain in DNS Lookup (resimag .com)", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharession .com)", "ET EXPLOIT Serialized Groovy Java Object Generated by ysoserial", "ET HUNTING HTTP POST Request XOR Key ab", "GPL SCAN PING Sniffer Pro/NetXRay network scan", "ET HUNTING HTTP GET Request XOR Key b5", "ET WEB_SERVER Possible SSRF Attempt Inbound Using Common Dork M7", "ET HUNTING HTTP GET Request XOR Key 44", "ET POLICY RDP connection confirm", "ET INFO Public Array DNS Over HTTPS Certificate Inbound", "ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol UDP (Outbound) (CVE-2021-44228)", "ET HUNTING HTTP POST Request XOR Key f5", "ET HUNTING HTTP GET Request XOR Key 9b", "ET INFO Packetriot Tunneling Domain in DNS Lookup (betabuild .dev)", "ET INFO EXE - OSX Executable Download - Intel Arch", "ET HUNTING HTTP GET Request XOR Key ba", "ET INFO URL Shortener Service Domain in DNS Lookup (youlinkto .com)", "ET INFO External Host Querying Erlang Port Mapper Daemon", "ET HUNTING HTTP GET Request XOR Key fe", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.6600.org", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (attemplate .com)", "ET INFO DNS Query for Suspicious .ga Domain", "ET POLICY External Unencrypted Connection to BASE Console", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncDeletePrinterDriverPackage", "ET INFO Abused File Sharing Site Domain Observed (qaz .im) in DNS Lookup", "ET INFO Java Downloading Archive flowbit no alert", "ET INFO webhook .site in TLS SNI", "ET HUNTING HTTP GET Request XOR Key 1a", "ET EXPLOIT Serialized Java Object Generated by ysoserial", "ET HUNTING HTTP POST Request XOR Key 43", "ET HUNTING HTTP GET Request XOR Key 33", "ET INFO Zip File", "ET HUNTING HTTP POST Request XOR Key e3", "ET HUNTING HTTP GET Request XOR Key de", "ET MALWARE DNS Query for Suspicious tolotor.com Domain - Possible CryptoWall Activity", "ET HUNTING HTTP GET Request XOR Key fb", "ET POLICY Proxy Server Lookup (nntime)", "ET HUNTING Possible EXE Download From Suspicious TLD (.win) - set", "ET HUNTING HTTP GET Request XOR Key 66", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_3_forward", "ET HUNTING [TW] Uri Contains Likely Urlpages Web Hosting Technique", "ET INFO DYNAMIC_DNS Query to 4nmn .com Domain", "ET INFO Njalla DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key 2e", "ET HUNTING HTTP GET Request XOR Key 2e", "ET INFO User-Agent (python-requests) Inbound to Webserver", "ET POLICY TeamViewer Keep-alive inbound", "ET HUNTING HTTP GET Request XOR Key bb", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_1_middle_out", "ET HUNTING HTTP POST Request XOR Key 14", "ET HUNTING HTTP GET Request XOR Key fc", "ET HUNTING HTTP POST Request XOR Key 0c", "ET INFO Commonly Abused File Sharing Site Domain Observed (fex .net in DNS Lookup)", "ET INFO DNSlify DNS Over HTTPS Certificate Inbound", "ET EXPLOIT NTDump Session Established Reg-Entry port 445", "ET INFO Observed

	Microsoft Attack Simulation Training SSL Cert (prizegives .com)", "ET USER_AGENTS Willowcoin Cryptocurrency UA Observed", "ET INFO jp.tiar DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key c9", "ET HUNTING HTTP GET Request XOR Key 49", "ET HUNTING HTTP POST Request XOR Key 3a", "ET HUNTING HTTP POST Request XOR Key 69", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharepointin .com)", "ET HUNTING HTTP GET Request XOR Key 29", "ET HUNTING EXE Base64 Encoded potential malware", "ET HUNTING HTTP POST Request XOR Key 17", "ET HUNTING HTTP GET Request XOR Key 2f", "ET INFO Observed Pastebin-style Service Domain (pasteio .com in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 96", "ET INFO Possible ThousandEyes User-Agent Inbound", "ET HUNTING HTTP POST Request XOR Key d7", "ET INFO Commonly Abused File Sharing Site Domain Observed (send .exploit .in in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key 20", "ET HUNTING HTTP GET Request XOR Key c3", "ET INFO Mullvad DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key a5", "GPL POLICY PCAnywhere server response", "ET INFO Andrews & Arnold DNS Over HTTPS Certificate Inbound", "ET INFO FutaDNS DNS Over HTTPS Certificate Inbound", "ET INFO CIRA Canadian Shield DNS Over HTTPS Certificate Inbound", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (templatent .com)", "ET INFO Observed URL Shortener Service Domain Domain (zii .to in TLS SNI)", "ET HUNTING HTTP GET Request XOR Key ec", "ET INFO DnsCrypt DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 09", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (sharepointle .com)", "ET HUNTING HTTP GET Request XOR Key a0", "ET INFO Faelix DNS Over HTTPS Certificate Inbound", "ET SCAN ICMP @hello request Likely Precursor to Scan", "ET HUNTING HTTP GET Request XOR Key c0", "ET HUNTING HTTP POST Request XOR Key e7", "GPL ICMP_INFO PING BSDtype", "ET INFO URL Shortener Service Domain in DNS Lookup (cli .co)", "ET INFO Abused File Sharing Site Domain Observed (qaz .su) in DNS Lookup", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (officested .com)", "ET HUNTING Telegram API Certificate Observed", "ET INFO URL Shortener Service Domain in DNS Lookup (dl .sv)", "ET HUNTING HTTP GET Request XOR Key 0a", "ET INFO Packetriot Tunneling Domain in DNS Lookup (pktriot .net)", "ET HUNTING HTTP GET Request XOR Key 52", "ET INFO Observed External IP Lookup Domain (geoiplookup .io in TLS SNI)", "ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection", "ET HUNTING HTTP POST Request XOR Key ed", "ET HUNTING HTTP GET Request XOR Key 7f", "ET HUNTING HTTP GET Request XOR Key 34", "ET INFO URL Shortener Service Domain in DNS Lookup (4 .fo)", "ET INFO Observed Pastebin-style Service Domain (justpaste .it) in TLS SNI", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (officenced .com)", "ET HUNTING HTTP GET Request XOR Key 1e", "ET INFO DYNAMIC_DNS Query to 3322.org Domain", "ET HUNTING HTTP GET Request XOR Key 11", "ET POLICY [TW] IPFS File Request Observed", "ET HUNTING HTTP POST Request XOR Key 35", "ET HUNTING Possible EXE Download From Suspicious TLD (.stream) - set", "ET INFO SyncroMSP Remote Remote Management Software Install Checkin", "ET HUNTING HTTP POST Request XOR Key 8e", "ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)", "ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M3", "ET HUNTING HTTP GET Request XOR Key a8", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (templateau .com)", "ET HUNTING Possible Malicious Document Request to Afraid.org Top 100 Dynamic DNS Domain", "ET HUNTING Generic Phishkit Javascript Response with Phishy Text", "ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M1", "ET HUNTING HTTP POST Request XOR Key cd", "ET HUNTING HTTP POST Request XOR Key b5", "ET INFO DNS Query for Suspicious .ml Domain", "ET HUNTING HTTP GET Request XOR Key c4", "ET INFO DYNAMIC_DNS HTTP Request to a no-ip Domain", "ET HUNTING HTTP POST Request XOR Key 89", "ET HUNTING HTTP GET Request XOR Key 0d", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (prizewings .com)", "ET HUNTING HTTP GET Request XOR Key 89", "ET HUNTING HTTP POST Request XOR Key 62", "ET SCAN Behavioral Unusually fast

	Terminal Server Traffic Potential Scan or Infection (Outbound)", "ET INFO MSSQL SELECT SPID Query Observed", "ET INFO Abused File Sharing Site Domain Observed (qaz .im) in TLS SNI", "ET HUNTING HTTP GET Request XOR Key bf", "ET HUNTING HTTP POST Request XOR Key 2b", "ET HUNTING HTTP GET Request XOR Key 92", "ET INFO URL Shortener Service Domain in DNS Lookup (qq .sv)", "ET HUNTING HTTP GET Request XOR Key b1", "ET HUNTING HTTP GET Request XOR Key f7", "ET INFO DYNAMIC_DNS HTTP Request to a 3322.net Domain *.8800.org", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (templatent .com)", "ET HUNTING HTTP POST Request XOR Key 20", "ET GAMES Dragon Raja Activity", "ET HUNTING HTTP POST Request XOR Key 0a", "ET INFO Observed SSL Cert (hizliresim .com)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (templatern .com)", "ET HUNTING HTTP POST Request XOR Key a1", "ET INFO Lars Lehmn DNS Over HTTPS Certificate Inbound", "ET INFO Bebasid DNS Over HTTPS Certificate Inbound", "ET INFO Temporary File Hosting Domain in TLS SNI (temp .sh)", "ET HUNTING Possible EXE Download From Suspicious TLD (.link) - set", "ET HUNTING HTTP POST Request XOR Key 51", "ET INFO Observed Abused File Hosting Domain (transferxl .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 0d", "ET HUNTING HTTP POST Request XOR Key e0", "ET HUNTING HTTP POST Request XOR Key 0e", "ET HUNTING HTTP GET Request XOR Key 3c", "ET INFO e-utp DNS Over HTTPS Certificate Inbound", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncAddPrinterDriver", "ET INFO Possible MSXMLHTTP Request to Dotted Quad", "ET HUNTING HTTP POST Request XOR Key 03", "ET INFO URL Shortener Service Domain in DNS Lookup (tiny .one)", "ET INFO Possible ThousandEyes User-Agent Outbound", "ET HUNTING HTTP GET Request XOR Key 3b", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (templateau .com)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (shareholds .com)", "ET HUNTING HTTP POST Request XOR Key f7", "ET INFO Possible Sandvine PacketLogic Injection", "ET HUNTING HTTP POST Request XOR Key a6", "ET HUNTING HTTP GET Request XOR Key f1", "ET HUNTING Possible Malicious Document Request to Hostinger Domains", "ET HUNTING HTTP GET Request XOR Key ef", "ET WEB_CLIENT Proxy - Fiddler Proxy Certificate Seen", "ET HUNTING HTTP POST Request XOR Key 1a", "ET HUNTING HTTP POST Request XOR Key 06", "ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M6", "ET HUNTING HTTP POST Request XOR Key bc", "ET HUNTING HTTP POST Request XOR Key 9f", "ET INFO URL Shortener Service Domain in DNS Lookup (go .sv)", "ET INFO Observed Image Hosting Domain (resimag .com in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 7f", "ET HUNTING HTTP GET Request XOR Key 6b", "ET HUNTING HTTP POST Request XOR Key d4", "ET HUNTING HTTP POST Request XOR Key 6c", "ET INFO Packetriot Tunneling Domain in DNS Lookup (mediastreamer .app)", "ET HUNTING HTTP POST Request XOR Key 60", "ET INFO HTTP Request to Free Hosting Domain (*.ct8 .pl)", "ET INFO URL Shortener Service Domain in DNS Lookup (bitly .ws)", "ET HUNTING HTTP POST Request XOR Key 27", "ET INFO Keweon Center DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 8b", "ET INFO EXE - OSX Executable Download - Multi Arch w/PowerPC", "ET INFO Observed DNS Query to Dynamic DNS Service Domain (duia .ro)", "ET HUNTING ZIP file download over raw TCP", "ET INFO URL Shortener Service Domain in DNS Lookup (lc .sv)", "ET INFO PureDNS DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP POST Request XOR Key cb", "ET HUNTING HTTP POST Request XOR Key bd", "ET HUNTING HTTP POST Request XOR Key 70", "ET HUNTING HTTP POST Request XOR Key d0", "ET HUNTING HTTP POST Request XOR Key 39", "ET HUNTING HTTP GET Request XOR Key 9e", "ET HUNTING HTTP POST Request XOR Key f8", "ET HUNTING HTTP GET Request XOR Key 75", "ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection", "ET HUNTING HTTP POST Request XOR Key dd", "ET HUNTING HTTP GET Request XOR Key 86", "ET INFO Qihoo 360 DNS Over HTTPS Certificate Inbound", "ET INFO Observed File Sharing Service (docdroid .net) in DNS Lookup", "ET HUNTING HTTP GET Request XOR Key ae", "ET POLICY PDF File Containing arguments.callee in Cleartext - Likely Hostile", "ET HUNTING HTTP GET Request XOR Key 3d", "ET HUNTING HTTP POST Request XOR Key 6e", "ET HUNTING HTTP POST to XYZ TLD Containing Pass - Possible Phishing", "ET INFO

	Delphi JEDI Visual Component Library User-Agent (JEDI-VCL)", "ET HUNTING HTTP POST Request XOR Key 91", "ET INFO URL Shortener Service Domain in DNS Lookup (link .sv)", "ET INFO QR Code Generator Domain in DNS Lookup (qrco .de)", "ET HUNTING HTTP GET Request XOR Key 46", "GPL ICMP_INFO PING Ping-O-MeterWindows", "ET POLICY External Unencrypted Connection to Ossec WUI", "ET INFO Rezhajul DNS Over HTTPS Certificate Inbound", "ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)", "ET HUNTING HTTP POST Request XOR Key 8b", "ET INFO Commonly Abused File Sharing Site Domain Observed (privatlab .net in DNS Lookup)", "ET HUNTING HTTP GET Request XOR Key f8", "ET HUNTING HTTP GET Request XOR Key d3", "ET HUNTING HTTP POST Request XOR Key ad", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (ancillarycheese .com)", "ET INFO EXE - OSX Executable Download - Multi Arch w/Intel", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (prizewel .com)", "GPL ICMP_INFO PING IP NetMonitor Macintosh", "ET HUNTING HTTP POST Request XOR Key 68", "ET POLICY TLS possible TOR SSL traffic", "ET INFO Microsoft Attack Simulation Training Domain in DNS Lookup (officences .com)", "ET SCAN Behavioral Unusual Port 137 traffic Potential Scan or Infection", "ET HUNTING HTTP GET Request XOR Key e9", "ET HUNTING HTTP GET Request XOR Key 7e", "ET INFO La Contre-Voie DNS Over HTTPS Certificate Inbound", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (attemplate .com)", "ET INFO Commonly Abused File Sharing Site Domain Observed (privatlab .net in TLS SNI)", "ET INFO Usable Privacy DNS Over HTTPS Certificate Inbound", "ET USER_AGENTS Microsoft Edge on Windows 10 SET", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (msftemail .com)", "ET INFO Observed Microsoft Attack Simulation Training SSL Cert (sharepointen .com)", "ET HUNTING HTTP GET Request XOR Key 7c", "ET HUNTING HTTP POST Request XOR Key 8c", "ET HUNTING HTTP POST Request XOR Key 61", "ET INFO Instagram Story Viewer Domain in DNS Lookup (dumpor .com)", "ET HUNTING Possible Phishing Page - Page Saved with SingleFile Extension", "ET HUNTING HTTP POST Request XOR Key a0", "ET HUNTING HTTP POST Request XOR Key 2d", "ET INFO Suspicious User-Agent (CustomStringHere)", "ET INFO URL Shortener Service Domain in DNS Lookup (to .sv)", "ET HUNTING HTTP GET Request XOR Key 04", "ET HUNTING HTTP GET Request XOR e4", "ET HUNTING HTTP POST Request XOR Key 6b", "ET HUNTING HTTP GET Request XOR Key a1", "ET HUNTING HTTP GET Request XOR Key f6", "ET HUNTING HTTP GET Request XOR Key 16", "ET HUNTING HTTP GET Request XOR Key 5b", "ET HUNTING HTTP POST Request XOR Key 40", "GPL ICMP_INFO PING Cisco Type.x", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncDeletePrinterDriverEx", "ET SCAN ICMP PING IPTools", "ET HUNTING HTTP GET Request XOR Key b0", "GPL ICMP_INFO PING Microsoft Windows", "ET HUNTING HTTP GET Request XOR Key 98", "ET POLICY File Downloaded via ge.tt Filesharing Service", "ET WEB_CLIENT PROPFIND Flowbit Set", "ET INFO Observed Ordns DNS over HTTPS Domain (Ordns .he .net in TLS SNI)", "ET INFO Possible MSXMLHTTP Request (msp) unset (no exe)", "ET INFO PDF - Acrobat Enumeration - pdfobject.js", "ET POLICY [MS-PAR] Windows Printer Spooler Activity - RpcAsyncGetPrinterDriverPackagePath", "ET INFO URL Shortener Service Domain in DNS Lookup (fl .sv)", "ET INFO DropBox User Content Domain (dl .dropboxusercontent .com in TLS SNI)", "ET INFO Suspicious HTTP POST to 404.php", "ET INFO Open Internet DNS Over HTTPS Certificate Inbound", "ET INFO Custom Logo Domain Domain in DNS Lookup (logodownload .org)", "ET HUNTING HTTP GET Request XOR Key b4", "ET INFO Observed Instagram Story Viewer Domain (greatfon .com in TLS SNI)", "ET INFO Malware Destroyer FTP Login", "ET INFO MySQL Database Query Version OS compile", "ET HUNTING HTTP GET Request XOR Key d7", "ET HUNTING HTTP POST Request XOR Key 38", "ET HUNTING HTTP POST Request XOR Key 63", "ET HUNTING Possible EXE Download From Suspicious TLD (.tokyo) - set", "ET HUNTING HTTP POST Request XOR Key 5c", "ET POLICY Observed DNS Query to KnowBe4 Simulated Phish Domain (compromisedblog .com)", "ET HUNTING HTTP POST Request XOR Key fa", "ET INFO Possible JARM Fingerprinting Client Hello via tls1_2_reverse", "ET HUNTING HTTP POST Request XOR Key 30", "ET POLICY File Uploaded to ge.tt Filesharing Service", "ET INFO localhost .run Domain in DNS Lookup DNS Lookup (.lhr .life)", "ET HUNTING Possible

	Malicious Document Request to .tk domain", "ET SCAN ICMP Delphi Likely Precursor to Scan", "ET WEB_CLIENT Download of PDF With Compressed Flash Content", "ET HUNTING HTTP GET Request XOR Key 70", "ET HUNTING HTTP GET Request XOR Key fa", "ET HUNTING HTTP POST Request XOR Key e8", "ET INFO Aaflalo .me DNS Over HTTPS Certificate Inbound", "ET HUNTING HTTP GET Request XOR Key 4e"
Целевое использование вредоносного ПО	"ET MOBILE_MALWARE Android APT-C-23 (accaunts-googlc .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (kristy-milligan .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (hareyupnow .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (david-mclean .club in DNS Lookup)", "ET MALWARE CozyDuke APT Possible SSL Cert 5", "ET MOBILE_MALWARE Android APT-C-23 (new .filetea .me in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (myboon .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (harrykane .online in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-src .net)", "ET MALWARE ZuoRAT send_http_msg_php Call to dns.php", "ET MALWARE APT28/Sednit DNS Lookup (updatecenter .name)", "ET MALWARE APT28/Sednit DNS Lookup (pakistan-mofa .net)", "ET MALWARE APT28/Sednit DNS Lookup (driversupdate .info)", "ET MALWARE DNS query for known Anunak APT Domain (paradise-plaza.com)", "ET MALWARE CozyDuke APT Possible SSL Cert 6", "ET MALWARE RocketKitten APT Checkin", "ET MALWARE Possible APT30 or Win32/Nuclear HTTP Framework POST", "ET MOBILE_MALWARE Android APT-C-23 (engin-altan .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (pmi-pna .com in TLS SNI)", "ET MALWARE APT/Bitter Related CnC Activity", "ET MALWARE Donot (APT-C-35) Stage 1 Requesting Main Payload", "ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .minzdravros .com)", "ET MOBILE_MALWARE Android APT-C-23 (bbc-learning .com in DNS Lookup)", "ET MALWARE MuddyWater Payload CnC Checkin", "ET MALWARE Possible APT30 or Win32/Nuclear HTTP Framework", "ET MALWARE Likely Arid Viper APT Advtravel Campaign GET Keepalive", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 20", "ET MALWARE APT DarkHydrus DNS Lookup 20", "ET MALWARE CozyDuke APT Possible SSL Cert 7", "ET MALWARE Arid Viper APT DNS Lookup (mediahitech.info)", "ET MOBILE_MALWARE Android APT-C-23 (account-googlc .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (katie .party in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 15", "ET MOBILE_MALWARE Android APT-C-23 (caroline-nina .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (katie .party in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (aryastark .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (alain .ps in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (exvsnomy .club in DNS Lookup)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 6", "ET MALWARE APT DarkHydrus DNS Lookup 22", "ET MALWARE PawnStorm Java Class Stage 2 M2 Aug 28 2015", "ET MOBILE_MALWARE Android APT-C-23 (black-honey .club in TLS SNI)", "ET MALWARE OSX/OceanLotus / ELF/RotaJakario CnC Checkin", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (int-secure .org)", "ET MALWARE Win32/Ispen BADNEWS CnC Beacon", "ET MALWARE APT33/CharmingKitten Shellcode Communicating with CnC", "ET MOBILE_MALWARE Android APT-C-23 (kaniel-outis .info in DNS Lookup)", "ET MALWARE Desert Falcon Related APT DNS Lookup (nauss-lab.com)", "ET MALWARE Sofacy DNS Lookup microsof-update.com", "ET MALWARE Possible Winnti TLS Certificate Observed", "ET MALWARE Fake Virtually SSL Cert APT1", "ET MALWARE SeaDuke CnC Beacon", "ET MALWARE MiniDuke CnC Beacon (string1_slide_3_1)", "ET MOBILE_MALWARE Android APT-C-23 (donna-paulsen .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (debra-morgan .com in DNS Lookup)", "ET MALWARE Possible NK APT SLICKSHOES Host Checkin", "ET MALWARE SUR SSL Cert APT1", "ET MOBILE_MALWARE Android APT-C-23 (hotmailme .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (natemunson .com in DNS Lookup)", "ET MALWARE Sofacy DNS Lookup", "ET PHISHING APT SWC PluginDetect Landing Cookie 2015-10-15", "ET MALWARE Sofacy DNS Lookup secnetcontrol.com", "ET MOBILE_MALWARE Android APT-C-23 (mygift .website in DNS Lookup)", "ET MALWARE Possible OceanLotus Time Check to Microsoft.com", "ET MALWARE CozyDuke APT HTTP CnC Beacon Response", "ET MALWARE APT28 SEDNIT Variant CnC

	Beacon 3", "ET MOBILE_MALWARE Android APT-C-23 (cecilia-gilbert .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (miwakosato .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (harvey-ross .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (camilleoconnell .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (jon-snow .pro in TLS SNI)", "ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC Check Response", "ET MALWARE APT28/Sednit DNS Lookup (trend-news .org)", "ET MALWARE Observed Turla/APT34 CnC Domain Domain (dubaiexpo2020 .cf in TLS SNI)", "ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (bootstraplink .com)", "ET MALWARE CommentCrew Possible APT crabdance backdoor base64 head", "ET MALWARE Candiru Related Domain in DNS Lookup (cuturl .space)", "ET MALWARE APT SuperhardCorp DNS Lookup (ohio.sysbloger.com)", "ET MOBILE_MALWARE Android APT-C-23 (alisonparker .club in DNS Lookup)", "ET MALWARE W32/BaneChant.APT Initial CnC Beacon", "ET MALWARE WEBC2-UGX User-Agent (Windows+NT+5.x) APT1", "ET MOBILE_MALWARE Android APT-C-23 (alisonparker .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (cassy-gray .club in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (softwaresupportsv .com)", "ET MALWARE APT28 SEDNIT Variant CnC Beacon 4", "ET POLICY APT User-Agent to BackTrack Repository", "ET MALWARE APT DarkHydrus DNS Lookup 12", "ET MALWARE SSL/TLS Certificate Observed (APT32 METALJACK)", "ET MALWARE Drovorub file Module Server Response", "ET MALWARE APT28/Sednit DNS Lookup (virusdefender .org)", "ET MALWARE DNS query for known Anunak APT Domain (coral-trevel.com)", "ET MALWARE APT CozyCar SSL Cert 2", "ET MALWARE Activity related to APT.Seinup Checkin 1", "ET MALWARE APT Lurker POST CnC Beacon", "ET MALWARE Arid Viper APT DNS Lookup (mixedwork.com)", "ET MALWARE Desert Falcon APT DNS Lookup (iwork-sys.com)", "ET MOBILE_MALWARE Android APT-C-23 (namybotter .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (pml-help .site in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (iugur .live)", "ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (office)", "ET MALWARE REvil Exfil SFTP Certificate Inbound", "ET MALWARE APT32 Win32/Ratsnif POSTing Log Message to CnC", "ET MALWARE CommentCrew Possible APT c2 communications get system", "ET MOBILE_MALWARE Android APT-C-23 (gmailservice .us in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (1jve .com in DNS Lookup)", "ET MALWARE ZuoRAT Windows Loader Shellcode Retrieval", "ET MOBILE_MALWARE Android APT-C-23 (ososezo .site in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (moneymotion .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (fatehmedia .site in DNS Lookup)", "ET MALWARE Possible DeadlyKiss APT CnC Domain Observed in DNS Query", "ET EXPLOIT Targeted Attack from APT Actor Delivering HT SWF Exploit RIP", "ET MALWARE Hades APT Downloader Attempting to Retrieve Stage 2 Payload", "ET MOBILE_MALWARE Android APT-C-23 (nightchat .live in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (lyanna-stark .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (face-book-support .email in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (oriential .website in DNS Lookup)", "ET MALWARE Win32/Final1stspy CnC Checkin (Reaper/APT37 Stage 1 Payload)", "ET MOBILE_MALWARE Android APT-C-23 (matthew-stevens .club in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (dailypoliticsnews .com)", "ET MOBILE_MALWARE Android APT-C-23 (ezofiezo .website in DNS Lookup)", "ET MALWARE APT33/CharmingKitten DDNS Overlap Domain in DNS Lookup M2", "ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (linksis.info)", "ET MALWARE APT28/Sednit DNS Lookup (acledit .com)", "ET MALWARE APT28/Sednit DNS Lookup (theguardiannews .org)", "ET MALWARE Sofacy DNS Lookup securitypractic.com", "ET MALWARE Possible KONNI CnC Activity", "ET MALWARE MiniDuke CnC Beacon (string2_slide_2_1)", "ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC POST", "ET MALWARE APT28/Sednit DNS Lookup (dailyforeignnews .com)", "ET MALWARE Rhabdo CnC Activity M2", "ET MALWARE Sednit/AZZY Checkin", "ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (lol)", "ET MALWARE DarkHotel DNS Lookup (apply.ebizx.net)", "ET MOBILE_MALWARE Android APT-C-23 (natemunson .com in TLS SNI)", "ET MALWARE

	Red Leaves magic packet detected (APT10 implant)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 27", "ET MOBILE_MALWARE Android APT-C-23 (james-charles .club in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (govpk-mail .net)", "ET MALWARE Observed StrongPity CnC Domain (pulmonyarea .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (nissour-beton .com in DNS Lookup)", "ET MALWARE CommentCrew Possible APT crabdance backdoor base64 head 2", "ET MOBILE_MALWARE Android APT-C-23 (liz-keen .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (lord-varys .info in DNS Lookup)", "ET MALWARE MSIL APT28 Zebrocy/Zekapab Reporting to CnC M2", "ET MOBILE_MALWARE Android APT-C-23 (daario-naharis .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (lexi-branson .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (mygift .website in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 23", "ET MALWARE WEBC2-TABLE Checkin 2 - APT1 Related", "ET MALWARE APT28/Sednit DNS Lookup (dataclen .org)", "ET MOBILE_MALWARE Android APT-C-23 (mofa-help .site in DNS Lookup)", "ET MALWARE Observed DNS Query to APT10 Related CnC Domain", "ET MALWARE W32/Threebyte.APT Checkin", "ET MALWARE ZuoRAT CBeacon CnC", "ET MOBILE_MALWARE Android APT-C-23 (masuka .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (olivia-hartman .info in DNS Lookup)", "ET MALWARE APT32 CnC in DNS Lookup", "ET MOBILE_MALWARE Android APT-C-23 (octavia-blake .world in TLS SNI)", "ET MALWARE APT28 SEDNIT Variant CnC Beacon 2", "ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (Texsa)", "ET MOBILE_MALWARE Android APT-C-23 (arthursaito .club in TLS SNI)", "ET MALWARE Possible APT28 Maldoc CnC Checkin", "ET MALWARE Observed DNS Query to known Windshift APT Related Domain 2", "ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .miniboxmail .com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (filesrvr .net)", "ET MOBILE_MALWARE Android APT-C-23 (geny-wise .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (davina-claire .xyz in TLS SNI)", "ET MOBILE_MALWARE Possible Phenakite User-Agent", "ET MALWARE CommentCrew Possible APT c2 communications sleep3", "ET MALWARE APT.Fwits CnC Beacon M1", "ET MALWARE APT40/Dadstache Related DNS Lookup", "ET MOBILE_MALWARE Android APT-C-23 (eleanor-guthrie .info in DNS Lookup)", "ET MALWARE Sofacy DNS Lookup checkmalware.info", "ET MALWARE APT28/Sednit DNS Lookup (worldmilitarynews .org)", "ET MOBILE_MALWARE Android APT-C-23 (juana .fun in TLS SNI)", "ET MALWARE W32/Antifulai.APT CnC Beacon 2", "ET MALWARE APT28/Sednit DNS Lookup (militaryobserver .net)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (edu-cx .org)", "ET MOBILE_MALWARE Android APT-C-23 (leslie-barnes .website in TLS SNI)", "ET MALWARE APT SuperhardCorp DNS Lookup (np3.Jkub.com)", "ET MOBILE_MALWARE Android APT-C-23 (joycebyers .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (android-settings .info in TLS SNI)", "ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .miniboxmail .com)", "ET MALWARE MuddyWater Payload Registering with CnC", "ET MALWARE WEBC2-CSON Checkin - APT1 Related", "ET MALWARE Sofacy DNS Lookup msonlinelive.com", "ET MOBILE_MALWARE Android APT-C-23 (fasebookvideo .com in DNS Lookup)", "ET MALWARE Sofacy DNS Lookup adobeincorp.com", "ET MALWARE Sofacy DNS Lookup testservice24.net", "ET MOBILE_MALWARE Android APT-C-23 (max-eleanor .info in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (docuserve .ltd)", "ET MALWARE Bitter APT Domain in DNS Lookup (huandocimama .com)", "ET MOBILE_MALWARE Android APT-C-23 (accounts-googlc .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (mail-accout .club in TLS SNI)", "ET MALWARE Possible APT29 CozyBear/SeaDaddy SSL/TLS Certificate Observed", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 2", "ET MALWARE APT Cheshire Cat CnC Beacon", "ET MALWARE DarkHotel Downloader CnC Beacon 2", "ET MALWARE W32/Pgift.Backdoor APT CnC Beacon", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakmarines .com)", "ET MALWARE Observed DNS Query to known Windshift APT Related Domain 1", "ET MALWARE MSIL APT28 Zebrocy/Zekapab Reporting to CnC", "ET MALWARE Possible Trojan.APT.9002 POST", "ET MALWARE

	Observed StrongPity CnC Domain (hardwareoption .com in TLS SNI)", "ET MALWARE LAME SSL Cert APT1", "ET MALWARE CommentCrew UGX Backdoor initial connection", "ET MALWARE APT DarkHydrus DNS Lookup 6", "ET MALWARE APT28/Sednit DNS Lookup (reuters-press .com)", "ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (vie-en-islam .com)", "ET MOBILE_MALWARE Android APT-C-23 (firesky .site in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (leonard-kim .website in DNS Lookup)", "ET MALWARE APT CozyCar SSL Cert 8", "ET MALWARE APT SuperhardCorp DNS Lookup (docume.sysbloger.com)", "ET MOBILE_MALWARE Android APT-C-23 (accountforuser .website in DNS Lookup)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 18", "ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .minzdravros .com)", "ET MALWARE APT28/Sednit DNS Lookup (euronews24 .info)", "ET MALWARE Win32/SodaMaster domain observed in DNS query (www. rare-coisns. com)", "ET MOBILE_MALWARE Android APT-C-23 (jack-wagner .website in TLS SNI)", "ET MALWARE Rhabdo CnC Activity M1", "ET MALWARE Possible TransparentTribe APT CnC Activity", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ppinewsagency .live)", "ET MALWARE APT28/Sednit DNS Lookup (military-info .eu)", "ET MOBILE_MALWARE Android APT-C-23 (new .filetea .me in DNS Lookup)", "ET MALWARE METALJACK APT32 CnC Host Checkin", "ET MALWARE APT28/Sednit DNS Lookup (shurl .biz)", "ET MALWARE Miniduke Checkin", "ET MOBILE_MALWARE Android APT-C-23 (android-settings .info in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bahariafoundation .org)", "ET MALWARE APT28/Sednit DNS Lookup (inteldrv64 .com)", "ET MALWARE APT28/Sofacy Zebrocy Go Variant Checkin", "ET MALWARE APT28 DealersChoice DNS Lookup (zpfgr .com)", "ET MALWARE APT DarkHydrus DNS Lookup 4", "ET MALWARE CozyDuke APT HTTP POST CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (myboon .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (mediauploader .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (fasebock .info in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (cnnpolitics .eu)", "ET MALWARE APT DarkHydrus DNS Lookup 25", "ET MOBILE_MALWARE Android APT-C-23 (caroline-nina .com in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (nato-hq .com)", "ET MALWARE W32/DoubleTap.APT Downloader CnC Beacon", "ET MALWARE APT28/Sednit DNS Lookup (ausameetings .com)", "ET MOBILE_MALWARE Android APT-C-23 (heyapp .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (michael-keaton .info in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (fdn-trace .net)", "ET MALWARE BUILDINGCAN CnC Activity", "ET MOBILE_MALWARE Android APT-C-23 (bestbitloly .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (bbc-learning .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (leonard-kim .website in TLS SNI)", "ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (advtravel.info)", "ET MALWARE Turla DNS Lookup (vision2030 .cf)", "ET MALWARE Mini/Cosmic Duke variant FTP upload", "ET MALWARE Drovorub tunnel Module Server Response", "ET MALWARE APT SuperhardCorp DNS Lookup (drometic.suroot.com)", "ET MOBILE_MALWARE Android APT-C-23 (mail-presidency .com in DNS Lookup)", "ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin 2", "ET MALWARE APT28/Sednit DNS Lookup (windowscheckupdater .net)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ksew .org)", "ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike", "ET MALWARE APT DarkHydrus DNS Lookup 5", "ET MALWARE APT28 DealersChoice DNS Lookup (gtranm .com)", "ET MALWARE Possible APT17 CnC Content in Public Website", "ET MOBILE_MALWARE Android APT-C-23 (maria-bouchard .website in DNS Lookup)", "ET MALWARE APT28/Sofacy Zebrocy Go Variant Downloader Error POST", "ET MALWARE Lazarus APT Related Valefor/VSingle CnC Beacon", "ET MALWARE APT28/Sednit DNS Lookup (aljazeera-news .com)", "ET MOBILE_MALWARE Android APT-C-23 (dachfunny .club in TLS SNI)", "ET MALWARE Arid Viper APT Advtravel Campaign GET Request", "ET MOBILE_MALWARE Android APT-C-23 (dachfunny .us in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (graceygretchen .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (cerseilannister .info in TLS SNI)", "ET MALWARE GOLDBACKDOOR Domain (lit-peak-25706 .herokuapp .com) in TLS SNI", "ET

	MOBILE_MALWARE Android APT-C-23 (mygift .site in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (italk-chat .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (kaniel-outis .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (ososezo .site in DNS Lookup)", "ET MALWARE Miniduke variant C&C activity", "ET MALWARE APT28/Sednit DNS Lookup (microsoftsupp .com)", "ET MALWARE Win32.Sluegot.A Checkin WEBC2-YAHOO APT1 Related", "ET MOBILE_MALWARE Android APT-C-23 (jack-wagner .website in DNS Lookup)", "ET MALWARE Cobalt Strike Beacon Observed", "ET MOBILE_MALWARE Android APT-C-23 (mail-goog1e .com in TLS SNI)", "ET MALWARE APT29 Cache_DLL SSL Cert", "ET MOBILE_MALWARE Android APT-C-23 (freya .miranda-barlow .website in DNS Lookup)", "ET MALWARE APT DarkHydrus DNS Lookup 18", "ET MALWARE Sofacy DNS Lookup adawareblock.com", "ET MALWARE DarkHotel DNS Lookup (apply-wsu.ebizx.net)", "ET MALWARE MuddyWater Payload Requesting Command from CnC", "ET MALWARE APT28/Sednit DNS Lookup (euroreport24 .com)", "ET MOBILE_MALWARE Android APT-C-23 (bellamy-bob .life in TLS SNI)", "ET MALWARE CommentCrew Possible APT backdoor download logo.png", "ET MOBILE_MALWARE Android APT-C-23 (lets-see .site in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .info in DNS Lookup)", "ET MALWARE MuddyWater Payload Sending Command Output to CnC", "ET MALWARE APT_NGO_wuaclt", "ET MALWARE Arid Viper APT DNS Lookup (flushupdate.com)", "ET MOBILE_MALWARE Android APT-C-23 (clarke-taylor .life in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 7", "ET MALWARE APT28/Sednit DNS Lookup (kg-news .org)", "ET MALWARE APT32 Win32/Ratsnif Requesting Command from CnC", "ET MOBILE_MALWARE Android APT-C-23 (fatehmedia .site in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (harrykane .online in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (help-sec .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (eleanorguthrie .site in TLS SNI)", "ET DNS APT_NGO_wuaclt C2 Domain hotmal1.com", "ET MALWARE Possible APT40/Dadstache Stage 2 Payload Beacon", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (kdf-mail .com)", "ET MOBILE_MALWARE Android APT-C-23 (donna-paulsen .info in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (cloudflarecdn .com)", "ET MALWARE Kimsuky KGH Malware Suite Checkin M1", "ET MALWARE EMAIL SSL Cert APT1", "ET MALWARE APT DarkHydrus DNS Lookup 27", "ET MALWARE Kimsuky KGH Backdoor Secondary Payload Download Request", "ET MALWARE APT28/SEDNIT Uploader Variant DNS Lookup", "ET MOBILE_MALWARE Android APT-C-23 (heyapp .website in DNS Lookup)", "ET MALWARE Candiru Related Domain in DNS Lookup (bitly .tel)", "ET MALWARE MiniDuke CnC Beacon (string2_slide_3_2)", "ET MALWARE Turla Kopiluwak User-Agent", "ET MALWARE DarkHotel Downloader CnC Beacon 1", "ET MALWARE Possible WEBC2-GREENCAT Response - Embedded CnC APT1 Related", "ET MOBILE_MALWARE Android APT-C-23 (masuka .club in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (nato-news .com)", "ET MALWARE WEBC2-TABLE Checkin 1 - APT1 Related", "ET MOBILE_MALWARE Android APT-C-23 (marklavi .com in TLS SNI)", "ET MALWARE Arid Viper APT Possible User-Agent (Skypee)", "ET MOBILE_MALWARE Android APT-C-23 (apkapps .pro in TLS SNI)", "ET MALWARE Sofacy Request Outbound", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bitlyy .me)", "ET MOBILE_MALWARE Android APT-C-23 (easyshow .fun in DNS Lookup)", "ET MALWARE APT28 Uploader Variant CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (mofa-help .site in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 8", "ET MOBILE_MALWARE Android APT-C-23 (accountforusers .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (hotimael .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (aryastark .info in DNS Lookup)", "ET MALWARE ToddyCat Ninja Backdoor CnC Domain in DNS Lookup (eohsdnsaaojrhnqo .windowshost .us)", "ET MOBILE_MALWARE Android APT-C-23 (help-sec .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (mediauploader .info in TLS SNI)", "ET MALWARE CozyDuke APT Possible SSL Cert 8", "ET MOBILE_MALWARE Android APT-C-23 (christopher .fun in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (jimmykudo .online in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (accounts-gocgle .com in TLS SNI)", "ET MALWARE NCSC XAgent itwm beacon v1", "ET MOBILE_MALWARE

	Android APT-C-23 (flirtymania .fun in TLS SNI)", "ET MALWARE ZuoRAT send_http_msg_php Call to ssid.php", "ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (img .elliotterusties .com)", "ET MALWARE GOLDBACKDOOR Domain (main .dailynk .us) in TLS SNI", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 25", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakgov .org)", "ET MOBILE_MALWARE Android APT-C-23 (cassy-gray .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (max-mayfield .com in DNS Lookup)", "ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT TCP Keep-Alive", "ET MALWARE APT28/Sednit DNS Lookup (politicalreview .eu)", "ET MOBILE_MALWARE Android APT-C-23 (juana .fun in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (appchecker .us in DNS Lookup)", "ET MALWARE Observed StrongPity CnC Domain (resolutionplatform .com in TLS SNI)", "ET MALWARE Sednit/APT28/Sofacy Delphocy CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (karenwheeler .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (graceygretchen .info in DNS Lookup)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 5", "ET MALWARE DNS query for known Anunak APT Domain (great-codes.com)", "ET MALWARE W32/Ke3chang.MyWeb.APT Campaign CnC Beacon", "ET MALWARE [PTsecurity] Possible Cobalt Strike payload", "ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (cdn-ampproject .com)", "ET MALWARE Sofacy DNS Lookup updatesoftware24.com", "ET MALWARE APT29 Implant8 - Evil Twitter Callback", "ET MALWARE XDMonitor Checkin Activity", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (sd1-bin .net)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 17", "ET MOBILE_MALWARE Android APT-C-23 (jimmykudo .online in DNS Lookup)", "ET MALWARE DNSpionage Requesting Config", "ET MALWARE Donot (APT-C-35) Stage 1 Requesting Persistence Setup File", "ET MOBILE_MALWARE Android APT-C-23 (mail-accout .club in DNS Lookup)", "ET MALWARE Observed Sofacy CnC Domain (ndpmedia24 .com in DNS Lookup)", "ET MALWARE APT28 Komplex DNS Lookup (appleupdate .com)", "ET MOBILE_MALWARE Android APT-C-23 (maxlight .us in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (men-ana .fun in DNS Lookup)", "ET MALWARE Possible click2play bypass Oct 19 2015 as observed in PawnStorm", "ET MOBILE_MALWARE Android APT-C-23 (hareyupnow .club in TLS SNI)", "ET MALWARE Desert Falcon Related APT DNS Lookup (tvgate.rocks)", "ET MALWARE Arid Viper APT Exfiltrating files", "ET MOBILE_MALWARE Android APT-C-23 (harper-monty .site in TLS SNI)", "ET MALWARE APT CozyCar SSL Cert 3", "ET MOBILE_MALWARE Android APT-C-23 (account-gocgle .com in TLS SNI)", "ET MALWARE APT29 Implant8 - MAL_REFERER", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (moma-pk .org)", "ET MALWARE APT DarkHydrus DNS Lookup 26", "ET MALWARE TA428 Tmanger Checkin", "ET MALWARE Arid Viper APT Possible User-Agent (SK)", "ET MOBILE_MALWARE Android APT-C-23 (appchecker .us in TLS SNI)", "ET MALWARE Desert Falcon Related APT DNS Lookup (abuhmaid.net)", "ET MALWARE Miniduke Variant CnC Beacon via WebDAV", "ET MALWARE Observed StrongPity CnC Domain (applicationrepo .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paknvay-pk .net)", "ET MOBILE_MALWARE Android APT-C-23 (accountforusers .website in DNS Lookup)", "ET MALWARE DarkHotel Initial Beacon", "ET MALWARE Turla Snake OSX DNS Lookup (car-service .effers.com)", "ET MALWARE W32/Antifulai.APT CnC Beacon 1", "ET MOBILE_MALWARE Android APT-C-23 (karenwheeler .club in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cr20g .org)", "ET MALWARE Sofacy DNS Lookup windows-updater.com", "ET MOBILE_MALWARE Android APT-C-23 (account-googlc .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (pmi-pna .com in DNS Lookup)", "ET MALWARE APT SuperhardCorp DNS Lookup (books.mrface.com)", "ET MALWARE Red Leaves magic packet response detected (APT10 implant)", "ET MALWARE MINEBRIDGE CnC Request", "ET MALWARE Possible Charming Kitten Backdoor Checkin", "ET MALWARE Observed Turla Domain (vision2030 .tk in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (militaryadviser .org)", "ET MALWARE APT28/Sednit DNS Lookup (windowsappstore .net)", "ET MOBILE_MALWARE Android APT-C-23 (octavia-blake .world in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pafwa .info)", "ET

	MALWARE GOLDBACKDOOR Domain in DNS Lookup (main .dailynk .us)", "ET MALWARE APT CozyCar SSL Cert 1", "ET MOBILE_MALWARE Android APT-C-23 (italk-chat .com in DNS Lookup)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 11", "ET MOBILE_MALWARE Android APT-C-23 (italk-chat .com in TLS SNI)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 14", "ET MOBILE_MALWARE Android APT-C-23 (apkapps .site in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (katesacker .club in TLS SNI)", "ET MALWARE Backdoor.Linux.Turla Download", "ET MOBILE_MALWARE Android APT-C-23 (buymicrosft .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (apkapps .pro in DNS Lookup)", "ET MALWARE APT DarkHydrus DNS Lookup 9", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (s3-cdn .net)", "ET MALWARE PawnStorm Java Class Stage 2 M1 Aug 28 2015", "ET MOBILE_MALWARE Android APT-C-23 (assets-acc .club in DNS Lookup)", "ET MALWARE Arid Viper APT Transmitting Serial", "ET MOBILE_MALWARE Android APT-C-23 (namybotter .info in DNS Lookup)", "ET MALWARE EvilGrab or APT.9002 DNS Lookup (secvies.com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-edu .net)", "ET MALWARE APT CozyCar SSL Cert 6", "ET MALWARE WEBC2-KT3 Intial Connection Beacon Server Response APT1 Related", "ET MALWARE Cobalt Group SSL Certificate Detected", "ET MALWARE CobaltStrike DNS Beacon Response", "ET MALWARE FAKE YAHOO SSL Cert APT1", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (d01fa .net)", "ET MALWARE APT28 Zebrocy/Zekapab Reporting to CnC M3", "ET MOBILE_MALWARE Android APT-C-23 (eleanor-guthrie .info in TLS SNI)", "ET MALWARE WEBC2-KT3 Intial Connection Beacon APT1 Related", "ET MOBILE_MALWARE Android APT-C-23 (help-live .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (1jve .com in TLS SNI)", "ET MALWARE Arid Viper APT DNS Lookup (pstcmedia.com)", "ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .microtreely .com)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cvix .live)", "ET MOBILE_MALWARE Android APT-C-23 (easyshow .fun in TLS SNI)", "ET MALWARE APT1 WEBC2-UGX Related Pingbed/Downbot User-Agent (Windows+NT+5.x)", "ET MALWARE TA402/Molerats Pierogi Backdoor Activity", "ET MALWARE XDMonitor Sending Debug Messages", "ET MOBILE_MALWARE Android APT-C-23 (camilleoconnell .website in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (biocpl .org)", "ET MALWARE CosmicDuke Exfiltrating Data via FTP STOR", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (aspbin .net)", "ET MOBILE_MALWARE Android APT-C-23 (matthew-stevens .club in TLS SNI)", "ET MALWARE CommentCrew Possible APT c2 communications get command client key", "ET MALWARE Sofacy DNS Lookup microsofi.org", "ET MALWARE Sofacy HTTP Request microsof-update.com", "ET MALWARE APT SideWinder CnC Domain in DNS Lookup (cdn-dl. cn)", "ET MALWARE APT Backspace CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (aslaug-sigurd .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (accuant-googlc .com in DNS Lookup)", "ET MALWARE MiniDuke CnC Beacon (string2_slide_2_2)", "ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .microtreely .com)", "ET MALWARE ToddyCat Ninja Backdoor CnC", "ET MALWARE W32/Antifulai.APT CnC Beacon 3", "ET MOBILE_MALWARE Android APT-C-23 (max-mayfield .com in TLS SNI)", "ET MALWARE [GIGAMON_ATR] FIN8 BADHATCH Remote Shell Banner", "ET MOBILE_MALWARE Android APT-C-23 (hoopoechat .com in DNS Lookup)", "ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC GET", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 26", "ET MOBILE_MALWARE Android APT-C-23 (mail-goog1e .com in DNS Lookup)", "ET MALWARE Kimsuky CSPY Downloader Activity", "ET MALWARE Inception APT malware", "ET MALWARE CommentCrew Possible APT c2 communications download client.png", "ET MALWARE APT SuperhardCorp DNS Lookup (kieti.ipsecsl.net)", "ET MOBILE_MALWARE Android APT-C-23 (max-eleanor .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (everyservices .space in DNS Lookup)", "ET MALWARE WEBC2-CLOVER Checkin APT1 Related", "ET MALWARE Possible DarkHotel Landing M2", "ET MALWARE Observed StrongPity CnC Domain (hostoperationsystems .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (mauricefischer .club in TLS SNI)", "ET MALWARE Kimsuky KGH Backdoor CnC Activity", "ET MALWARE DNS query for known Anunak APT

	Domain (update-java.net)", "ET MALWARE W32/Antifulai.APT CnC Beacon 4", "ET MOBILE_MALWARE Android APT-C-23 (katesacker .club in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (vpn-secure .co)", "ET MALWARE APT33 CnC Domain in DNS Lookup", "ET MALWARE Arid Viper APT Transmitting Date", "ET MALWARE Observed StrongPity CnC Domain (uppertrainingtool .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-aws .net)", "ET MOBILE_MALWARE Android APT-C-23 (jorah-mormont .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (kate-austen .info in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (nrots .net)", "ET MALWARE Possible APT28 Xtunnel Activity", "ET MALWARE APT CozyCar SSL Cert 5", "ET MOBILE_MALWARE Android APT-C-23 (nissour-beton .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (namyyeatop .club in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (mod-pk .com)", "ET MOBILE_MALWARE Android APT-C-23 (appuree .info in TLS SNI)", "ET MOBILE_MALWARE Phenakite Image Upload CnC activity", "ET MALWARE APT28/Sednit DNS Lookup (unian-news .info)", "ET MOBILE_MALWARE Android APT-C-23 (lord-varys .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (margaery-tyrell .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (accuant-googlc .com in TLS SNI)", "ET MALWARE Arid Viper APT DNS Lookup (plmedgroup.com)", "ET MOBILE_MALWARE Android APT-C-23 (lincoln-blake .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (esofiezo .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (men-ana .fun in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (lindamullins .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (kristy-milligan .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (fasebookvideo .com in TLS SNI)", "ET MALWARE Observed StrongPity CnC Domain (hierarchicalfiles .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (lagertha-lothbrok .info in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 19", "ET MOBILE_MALWARE Android APT-C-23 (oriential .website in TLS SNI)", "ET MALWARE APT_NGO_wuaclt PDF file", "ET MOBILE_MALWARE Android APT-C-23 (bob-turco .website in DNS Lookup)", "ET MALWARE Trojan.APT.9002 CnC Traffic", "ET MOBILE_MALWARE Android APT-C-23 (buymicrosft .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .club in DNS Lookup)", "ET MALWARE APT DarkHydrus DNS Lookup 16", "ET DNS APT_NGO_wuaclt C2 Domain micorsofts.net", "ET MOBILE_MALWARE Android APT-C-23 (david-moris .website in DNS Lookup)", "ET MALWARE Possible APT-12 Related C2", "ET MALWARE Possible DarkHotel Landing M3", "ET MALWARE W32/DoubleTap.APT Downloader Socks5 Setup Request", "ET MOBILE_MALWARE Android APT-C-23 (accountusers .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (freya .miranda-barlow .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (nightchat .fun in DNS Lookup)", "ET MALWARE Arid Viper APT DNS Lookup (ahmedfaiez.info)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (csd-pk .co)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (gov-mail .net)", "ET MOBILE_MALWARE Android APT-C-23 (fasebook .cam in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakgov .net)", "ET MALWARE DNS query for known Anunak APT Domain (financialnewsonline.pw)", "ET MOBILE_MALWARE Android APT-C-23 (davina-claire .xyz in DNS Lookup)", "ET MALWARE Possible Charming Kitten Backdoor CnC Activity", "ET MALWARE Suspected Sidewinder APT Phishing Activity - Landing Page URI Pattern", "ET MALWARE APT_NGO_wuaclt C2 Check-in", "ET MALWARE Possible DarkHotel Landing M1", "ET MALWARE Win32/SodaMaster CnC HTTPS Checkin M2", "ET MALWARE CozyDuke APT HTTP GET CnC Beacon", "ET MALWARE APT32 Win32/Ratsnif CnC Checkin", "ET MALWARE Fake IBM SSL Cert APT1", "ET MALWARE Carbanak APT CnC Beacon 2", "ET MOBILE_MALWARE Android APT-C-23 (help-live .club in DNS Lookup)", "ET MALWARE Cobalt Strike Exfiltration", "ET MOBILE_MALWARE Android APT-C-23 (hotmailme .website in DNS Lookup)", "ET MALWARE W32/BaneChant.APT Winword.pkg Redirect", "ET MOBILE_MALWARE Android APT-C-23 (bitgames .world in TLS SNI)", "ET MALWARE Possible Kimsuky APT Connectivity Check via Document", "ET MOBILE_MALWARE

	Android APT-C-23 (firesky .site in TLS SNI)", "ET MALWARE StrongPity Host Checkin", "ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (viedechretien .org)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 1", "ET MALWARE Possible KONNI URI Path Observed", "ET MOBILE_MALWARE Android APT-C-23 (mail-presidency .com in TLS SNI)", "ET MALWARE Arid Viper APT Checkin 2", "ET MALWARE APT DarkHydrus DNS Lookup 1", "ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (leprotestant .com)", "ET MOBILE_MALWARE Android APT-C-23 (hitmesanjjoy .pro in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 3", "ET MALWARE Candiru Related Domain in DNS Lookup (url-tiny .co)", "ET MALWARE W32/Waterspout.APT Backdoor CnC Beacon", "ET MALWARE APT28/Sednit DNS Lookup (thediplomat-press .com)", "ET MALWARE APT28/Sednit DNS Lookup (kenlynton .com)", "ET MALWARE CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)", "ET MALWARE APT32 Komprogo DNS Lookup", "ET MOBILE_MALWARE Android APT-C-23 (miwakosato .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (harvey-ross .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (bestbitloly .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (billy-bones .info in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (unitednationsnews .eu)", "ET MALWARE Zebrocy Screenshot Upload", "ET MOBILE_MALWARE Android APT-C-23 (cerseilannister .info in DNS Lookup)", "ET MALWARE MiniDuke CnC Beacon (string1_slide_2_2)", "ET MALWARE MiniDuke CnC Beacon (string2_slide_3_1)", "ET MALWARE Sofacy DNS Lookup check-fix.com", "ET EXPLOIT_KIT DRIVEBY Sednit EK IE Exploit CVE-2013-1347 M1", "ET MALWARE Win32/COOKIEBAG Cookie APT1 Related", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (tin-url .com)", "ET MOBILE_MALWARE Android APT-C-23 (james-charles .club in TLS SNI)", "ET MALWARE TransparentTribe APT Maldoc CnC Checkin", "ET MALWARE APT28/Sednit DNS Lookup (ciscohelpcenter .com)", "ET MALWARE APT12 THREEBYTE DNS Lookup", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (krlwin .org)", "ET MOBILE_MALWARE Android APT-C-23 (miranda-barlow .website in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (microsofthelpcenter .info)", "ET MALWARE SERVER SSL Cert APT1", "ET MALWARE APT SuperhardCorp DNS Lookup (specs.dnsrd.com)", "ET MALWARE APT28 SEDNIT Variant CnC Beacon 1", "ET MALWARE DonotGroup APT DNS Lookup (bulk .fun)", "ET MOBILE_MALWARE Android APT-C-23 (login-yohoo .com in TLS SNI)", "ET MALWARE CommentCrew Possible APT c2 communications sleep2", "ET MOBILE_MALWARE Android APT-C-23 (gmailservice .us in TLS SNI)", "ET MALWARE APT Hellsing Proxy Checker Checkin", "ET MOBILE_MALWARE Android APT-C-23 (aamir-khan .site in TLS SNI)", "ET MALWARE Win32/Roficor.A (Darkhotel) Checkin 1", "ET MOBILE_MALWARE Android APT-C-23 (dardash .live in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (lindamullins .info in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (osce-press .org)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 23", "ET MOBILE_MALWARE Android APT-C-23 (jorah-mormont .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (kate-austen .info in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-top .net)", "ET MALWARE WEBC2-UGX Embedded CnC Response APT1", "ET MALWARE APT28/Sednit DNS Lookup (microsoftdriver .com)", "ET MOBILE_MALWARE Android APT-C-23 (leslie-barnes .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (cecilia-gilbert .com in DNS Lookup)", "ET MALWARE APT33/CharmingKitten JS/HTA Stage 1 CnC Checkin", "ET MALWARE Miniduke variant FTP upload", "ET MOBILE_MALWARE Android APT-C-23 (hotimael .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (arthursaito .club in DNS Lookup)", "ET MALWARE APT.Fwits CnC Beacon M2", "ET MALWARE [eSentire] Cobalt Strike Beacon", "ET MALWARE ComRAT CnC Domain in DNS Lookup", "ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (img .elliotterusties .com)", "ET MOBILE_MALWARE Android APT-C-23 (fasebook .cam in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (pml-help .site in TLS SNI)", "ET MALWARE APT DarkHydrus DNS Lookup 21", "ET MALWARE APT28/Sednit DNS Lookup (updmanager .com)", "ET MOBILE_MALWARE Android APT-C-23 (dachfunny .club in DNS Lookup)", "ET MALWARE Win32/Tosct.B UA Mandiant APT1 Related", "ET MALWARE TA428 Infostealer CnC Host Checkin", "ET MALWARE APT DarkHydrus DNS

	Lookup 17", "ET MALWARE CozyDuke APT Possible SSL Cert 3", "ET MALWARE APT OSX.XSLCmd CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (olivia-hartman .info in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (miranda-barlow .website in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .info in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (osce-info .com)", "ET MALWARE W32/Ke3chang.MovieStar.APT Campaign CnC Beacon", "ET MALWARE Win32/Chopstick Checkin (APT28 Related)", "ET MOBILE_MALWARE Android APT-C-23 (jon-snow .pro in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (lagertha-lothbrok .info in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (defenceiq .us)", "ET MALWARE W32/Ke3chang.Snake.APT Campaign CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (joycebyers .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (davos-seaworth .info in DNS Lookup)", "ET MALWARE APT28 DealersChoice.B DNS Lookup (appexsrv .net)", "ET MALWARE APT29 Domain in DNS Lookup (pandorasong .com)", "ET MALWARE APT28/Sednit DNS Lookup (mscoresvw .com)", "ET MALWARE Possible CVE-2015-2424 RTF Dropping Sofacy", "ET MALWARE Candiru Related Domain in DNS Lookup (llink .link)", "ET MALWARE CozyDuke APT Possible SSL Cert 4", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (dawnpk .org)", "ET MOBILE_MALWARE Android APT-C-23 (engin-altan .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (hitmesanjjoy .pro in DNS Lookup)", "ET MALWARE CommentCrew Possible APT c2 communications sleep5", "ET MALWARE W32/LetsGo.APT Sleep CnC Beacon", "ET MOBILE_MALWARE Android APT-C-23 (mary-crawley .com in TLS SNI)", "ET MALWARE NCSC XAgent itwm beacon v2", "ET MALWARE APT Related - BLACKCOFFEE Command Delimiters in HTTP Response M2", "ET MOBILE_MALWARE Android APT-C-23 (assets-acc .club in TLS SNI)", "ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (chretiendaujoudhui .com)", "ET MOBILE_MALWARE Android APT-C-23 (mygift .site in DNS Lookup)", "ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC Command Response", "ET MOBILE_MALWARE Android APT-C-23 (fasebcck .com in DNS Lookup)", "ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (fpupdate.info)", "ET MALWARE Sednit Connectivity Check 0 Byte POST", "ET MOBILE_MALWARE Android APT-C-23 (nightchat .live in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (face-book-support .email in DNS Lookup)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (chrom3 .net)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .fun in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (symantecsupport .org)", "ET MALWARE Desert Falcon Related APT DNS Lookup (blogging-host.info)", "ET MALWARE Candiru Related Domain in DNS Lookup (instagrarn .co)", "ET MALWARE MuddyWater Payload Sending Screenshot to CnC", "ET MALWARE APT28/Sofacy Zebrocy Secondary Payload CnC Checkin", "ET MALWARE W32/Ke3chang.Dream.APT Campaign CnC Beacon 2", "ET MOBILE_MALWARE Android APT-C-23 (harper-monty .site in DNS Lookup)", "ET MALWARE APT29/Wellness CnC Host Checkin", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 21", "ET MOBILE_MALWARE Android APT-C-23 (dardash .fun in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (billy-bones .info in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (updatesystems .net)", "ET MOBILE_MALWARE Android APT-C-23 (geny-wise .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (meet-me .chat in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (liz-keen .website in DNS Lookup)", "ET MALWARE Possible Winnti TLS SNI Observed", "ET MOBILE_MALWARE Android APT-C-23 (accountusers .website in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (natopress .com)", "ET MOBILE_MALWARE Android APT-C-23 (maria-bouchard .website in TLS SNI)", "ET MALWARE ZuoRAT GoBeacon CnC", "ET MALWARE APT Related - BLACKCOFFEE Command Delimiters in HTTP Response M1", "ET MALWARE W32/BaneChant.APT Data Exfiltration POST to CnC", "ET MALWARE Sofacy DNS Lookup symanttec.org", "ET MALWARE Red Leaves HTTP CnC Beacon (APT10 implant)", "ET MALWARE Hades APT Domain in DNS Lookup (findupdatems .com)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 16", "ET MALWARE MiniDuke CnC Beacon (string1_slide_3_2)", "ET MOBILE_MALWARE Android APT-C-23 (davos-seaworth .info in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (capisp .com)", "ET MALWARE

	PawnStorm Sednit DL Aug 28 2015", "ET MOBILE_MALWARE Android APT-C-23 (ezofiezo .website in TLS SNI)", "ET MALWARE WEBC2-TABLE Checkin 3 - APT1 Related", "ET MALWARE XDUpload Sending File Upload Progress", "ET MOBILE_MALWARE Android APT-C-23 (hcttmail .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (nightchat .fun in TLS SNI)", "ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (widgets-wp .com)", "ET MALWARE Drovorub monitor Module Server Response", "ET MALWARE Carbanak APT CnC Beacon 1", "ET MALWARE APT28/Sednit DNS Lookup (advpdxapi .com)", "ET MALWARE APT28 DealersChoice DNS Lookup", "ET MALWARE APT DarkHydrus DNS Lookup 24", "ET MALWARE Win32/Small.XR Checkin 2 WEBC2-CSON APT1 Related", "ET MALWARE Win32/Coreshell Checkin (APT28 Related)", "ET MALWARE APT32 Win32/Ratsnif Submitting Output of Command to CnC", "ET MALWARE NS SSL Cert APT1", "ET MOBILE_MALWARE Android APT-C-23 (fasebcck .com in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (flirtymania .fun in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (ososezo .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (accounts-gocgle .com in DNS Lookup)", "ET MALWARE APT.Agtid callback", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 7", "ET MALWARE APT28/Sednit DNS Lookup (diplomatnews .org)", "ET MALWARE DNS query for known Anunak APT Domain (ddnservice11.ru)", "ET MALWARE APT DarkHydrus DNS Lookup 10", "ET MOBILE_MALWARE Android APT-C-23 (esofiezo .website in TLS SNI)", "ET MALWARE Kimsuky KGH Malware Suite Checkin M2", "ET MALWARE Drovorub cloud.auth Module Server Response", "ET MALWARE Desert Falcon APT DNS Lookup (androcity.com)", "ET MOBILE_MALWARE Android APT-C-23 (namyyeatop .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (chat-often .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pkrepublic .org)", "ET MALWARE APT28/Sednit DNS Lookup (stratforglobal .net)", "ET MALWARE Arid Viper APT DNS Lookup (flushupate.com)", "ET MOBILE_MALWARE Android APT-C-23 (marklavi .com in DNS Lookup)", "ET MALWARE GOLDBACKDOOR Domain in DNS Lookup (lit-peak-25706 .herokuapp .com)", "ET MALWARE Win32/Ispen BADNEWS Fake User-Agent", "ET MALWARE APT SuperhardCorp DNS Lookup (ns8.ddns1.com)", "ET MOBILE_MALWARE Android APT-C-23 (michael-keaton .info in DNS Lookup)", "ET MALWARE Sofacy DNS Lookup testsnetcontrol.com", "ET MALWARE OceanLotus System Profiling JavaScript HTTP Request", "ET MOBILE_MALWARE Android APT-C-23 (aslaug-sigurd .info in TLS SNI)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 19", "ET MALWARE CommentCrew Possible APT backdoor stage 2 download base64 update.gif", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bbcnew .cn)", "ET MOBILE_MALWARE Android APT-C-23 (dardash .live in TLS SNI)", "ET MALWARE Desert Falcon Related APT DNS Lookup (facebook-emoticons.bitblogoo.com)", "ET MOBILE_MALWARE Android APT-C-23 (lincoln-blake .website in TLS SNI)", "ET MALWARE APT CozyCar SSL Cert 7", "ET MALWARE MiniDuke CnC Beacon (string1_slide_1_2)", "ET MOBILE_MALWARE Android APT-C-23 (parrotchat .co in TLS SNI)", "ET MALWARE Possible Dragonfly APT Activity HTTP URI OPTIONS", "ET MOBILE_MALWARE Android APT-C-23 (accounts-googlc .com in TLS SNI)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 13", "ET MALWARE CobaltStrike SMB P2P Default Msagent Named Pipe Interaction", "ET MALWARE CozyDuke APT Possible SSL Cert 1", "ET MALWARE APT28/Sednit DNS Lookup (nortonupdate .org)", "ET MOBILE_MALWARE Android APT-C-23 (activedardash .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (bob-turco .website in TLS SNI)", "ET MALWARE APT28 CnC Domain DNS Lookup", "ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin 1", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (kpt-pk .net)", "ET MOBILE_MALWARE Android APT-C-23 (accountforuser .website in TLS SNI)", "ET MALWARE StrongPity APT SSL Certificate Detected", "ET MALWARE APT28/Sofacy Zebrocy Go Variant CnC Activity", "ET MALWARE Kimsuky Related Host Data Exfil M3", "ET MALWARE APT33/CharmingKitten Encrypted Payload Inbound", "ET MALWARE Possible Dragonfly APT Activity - SMB credential harvesting", "ET MALWARE Sofacy DNS Lookup checkmalware.org", "ET MALWARE DarkHotel Payload Uploading to CnC", "ET MOBILE_MALWARE Android APT-C-23 (cecilia-dobrev .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (fileserve .work)", "ET MALWARE

	Sidewinder APT Related Domain in DNS Lookup (gov-pok .net)", "ET MALWARE Possible Winnti DNS Lookup", "ET MALWARE Reaper (APT37) DNS Lookup (kmbr1 .nitesbr1 .org)", "ET MALWARE DarkHotel CnC Domain in DNS Lookup", "ET MALWARE Possible APT28 DOC Uploader SSL/TLS Certificate Observed", "ET MALWARE MINEBRIDGE CnC Response", "ET MALWARE DNS query for known Anunak APT Domain (worldnewsonline.pw)", "ET MALWARE APT SideWinder CnC Domain in DNS Lookup (cdn-in. net)", "ET MALWARE Sofacy DNS Lookup updatepc.org", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 24", "ET MOBILE_MALWARE Android APT-C-23 (bitgames .world in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (activedardash .club in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (lyanna-stark .info in TLS SNI)", "ET MALWARE Volex - OceanLotus System Profiling JavaScript (linkStorage.x00SOCKET)", "ET MOBILE_MALWARE Android APT-C-23 (accaunts-googlc .com in TLS SNI)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-pak .net)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 10", "ET MALWARE Arid Viper APT File information", "ET MALWARE TwoFace WebShell Detected", "ET MALWARE SideWinder APT antibot script", "ET MALWARE Sofacy DNS Lookup malwarecheck.info", "ET MALWARE Troj_Yahoya Variant CnC Checkin", "ET MALWARE CommentCrew downloader without user-agent string exe download without User Agent", "ET MOBILE_MALWARE Android APT-C-23 (maxlight .us in DNS Lookup)", "ET MALWARE APT DarkHydrus DNS Lookup 28", "ET EXPLOIT [ConnectWise CRU] Java ECDSA (Psychic) TLS Signature (CVE-2022-21449)", "ET MALWARE Possible UNC1878 Cobalt Strike CnC SSL Cert Inbound (Mountainvew)", "ET MOBILE_MALWARE Android APT-C-23 (parrotchat .co in DNS Lookup)", "ET MALWARE W32/Ke3chang.MyWeb.APT Eourdegh Campaign CnC Beacon", "ET EXPLOIT_KIT DRIVEBY Sednit EK Landing", "ET MALWARE NCSC XAgent Beacon", "ET MOBILE_MALWARE Android APT-C-23 (david-mclean .club in TLS SNI)", "ET MALWARE XDUpload Uploading Files", "ET MALWARE APT28/Sednit DNS Lookup (natoint .com)", "ET MALWARE APT33/CharmingKitten DDNS Overlap Domain in DNS Lookup M1", "ET MALWARE W32/Ke3chang.BMW.APT Campaign CnC Beacon", "ET MALWARE Kimsuky KGH Backdoor CnC Activity M2", "ET MOBILE_MALWARE Android APT-C-23 (apkapps .site in DNS Lookup)", "ET MALWARE APT28/Sednit SSL Cert", "ET MOBILE_MALWARE Android APT-C-23 (kik-com .com in DNS Lookup)", "ET MALWARE XDUpload Uploading Directory Listting", "ET MALWARE Desert Falcon APT DNS Lookup (linkedim.in)", "ET MALWARE Desert Falcon Related APT DNS Lookup (nice-mobiles.com)", "ET MALWARE Likely Arid Viper APT Advtravel Campaign POST", "ET MALWARE Sofacy DNS Lookup checkwinframe.com", "ET MOBILE_MALWARE Android APT-C-23 (kik-com .com in TLS SNI)", "ET MALWARE DNSpionage Commands Embedded in Webpage Inbound", "ET MALWARE Volex - OceanLotus JavaScript Fake Page URL Builder Response", "ET MOBILE_MALWARE Android APT-C-23 (cecilia-dobrev .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (chat-often .com in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (worldpoliticsnews .org)", "ET MOBILE_MALWARE Android APT-C-23 (daario-naharis .info in DNS Lookup)", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 8", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ministry-pk .net)", "ET MOBILE_MALWARE Android APT-C-23 (margaery-tyrell .info in DNS Lookup)", "ET MALWARE APT DNSpionage/Karkoff CnC Domain in DNS Lookup", "ET MALWARE Arid Viper APT Checking filename", "ET EXPLOIT_KIT DRIVEBY Sednit EK IE Exploit CVE-2014-1776 M1", "ET MALWARE PawnStorm Java Class Stage 1 M1 Aug 28 2015", "ET MOBILE_MALWARE Android APT-C-23 (account-gocgle .com in DNS Lookup)", "ET MALWARE APT28/Sednit DNS Lookup (bbc-press .org)", "ET MOBILE_MALWARE Android APT-C-23 (debra-morgan .com in TLS SNI)", "ET MALWARE MiniDuke CnC Beacon (string1_slide_1_1)", "ET MALWARE APT28 Komplex DNS Lookup (itunes-helper .net)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pak-gov .com)", "ET MALWARE DonotGroup APT CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Android APT-C-23 (meet-me .chat in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (aamir-khan .site in DNS Lookup)", "ET MALWARE WEBC2-AUSOV Checkin Response - Embedded CnC APT1 Related", "ET MALWARE Candiru Related Domain in

	DNS Lookup (cuturl .app)", "ET MALWARE MiniDuke CnC Beacon (string2_slide_1_1)", "ET MALWARE Win32/SodaMaster CnC HTTPS Checkin M1", "ET MOBILE_MALWARE Android APT-C-23 (lets-see .site in DNS Lookup)", "ET MALWARE Arid Viper APT DNS Lookup (ineltdriver.com)", "ET MALWARE WEBC2-TABLE Checkin Response - Embedded CnC APT1 Related", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 9", "ET MALWARE CozyDuke APT Possible SSL Cert 2", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 15", "ET MALWARE AridViper CnC Domain in SNI", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 4", "ET MOBILE_MALWARE Android APT-C-23 (dachfunny .us in TLS SNI)", "ET MOBILE_MALWARE Phenakite Audio Upload CnC", "ET MALWARE APT28/Sednit DNS Lookup (politicsinform .com)", "ET MALWARE DNS query for known Anunak APT Domain (adguard.name)", "ET MOBILE_MALWARE Android APT-C-23 (alain .ps in TLS SNI)", "ET MALWARE APT33/CharmingKitten Retrieving New Payload (flowbit set)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pak-web .com)", "ET MALWARE RedLeaves HOGFISH APT Implant CnC", "ET MALWARE Sofacy DNS Lookup azureon-line.com", "ET MOBILE_MALWARE Android APT-C-23 (hcttmail .com in TLS SNI)", "ET MALWARE [401TRG] PS/PowDesk Checkin (APT34)", "ET MOBILE_MALWARE Android APT-C-23 (moneymotion .club in TLS SNI)", "ET MALWARE TEMP.Periscope APT Domain in DNS Lookup", "ET MALWARE APT DarkHydrus DNS Lookup 2", "ET MALWARE Win32/Namsoth.A Checkin/NEWSREELS APT1 Related", "ET MALWARE Turla SHIRIME DNS Lookup", "ET MALWARE Kimsuky APT Related Host Data Exfil M4", "ET MALWARE Volex - OceanLotus JavaScript Load (connect.js)", "ET MOBILE_MALWARE Android APT-C-23 (exvsnomy .club in TLS SNI)", "ET MALWARE APT28 Uploader Variant Fake Request to Google", "ET MOBILE_MALWARE Android APT-C-23 (fasebock .info in DNS Lookup)", "ET MALWARE Drovorub shell Module Server Response", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 22", "ET EXPLOIT_KIT DRIVEBY Generic CollectGarbage in JJEncode (Observed in Sednit)", "ET MALWARE APT DarkHydrus DNS Lookup 14", "ET MALWARE ZuoRAT send_http_msg_php Call to arp.php", "ET MALWARE CommentCrew Possible APT c2 communications html return 1", "ET MALWARE NCSC APT28 - Web/request -FILE- contenttype", "ET MOBILE_MALWARE Android APT-C-23 (everyservices .space in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (defencereview .eu)", "ET MALWARE Desert Falcon APT DNS Lookup (liptona.net)", "ET MOBILE_MALWARE Android APT-C-23 (clarke-taylor .life in DNS Lookup)", "ET MALWARE WEBC2-QBP Checkin Response 1 - Embedded CnC APT1 Related", "ET MALWARE Sofacy DNS Lookup scanmalware.info", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paf-gov .net)", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cloud-apt .net)", "ET MOBILE_MALWARE Android APT-C-23 (mary-crawley .com in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (italk-chat .info in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (lexi-branson .website in DNS Lookup)", "ET MALWARE FAKE AOL SSL Cert APT1", "ET MALWARE APT Lurker GET CnC Beacon", "ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ap1-port .net)", "ET MALWARE CommentCrew Possible APT c2 communications sleep", "ET MALWARE MiniDuke CnC Beacon (string2_slide_1_2)", "ET MALWARE Arid Viper APT Possible User-Agent (Skype)", "ET MOBILE_MALWARE Android APT-C-23 (christopher .fun in DNS Lookup)", "ET MOBILE_MALWARE Android APT-C-23 (black-honey .club in DNS Lookup)", "ET MALWARE APT DarkHydrus DNS Lookup 11", "ET MALWARE Arid Viper APT Checkin 1", "ET MOBILE_MALWARE Android APT-C-23 (ososezo .club in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (bellamy-bob .life in DNS Lookup)", "ET DNS APT_NGO_wuaclt C2 Domain micorsofts.com", "ET MOBILE_MALWARE Android APT-C-23 (hoopoechat .com in TLS SNI)", "ET MALWARE APT28/Sednit DNS Lookup (timezoneutc .com)", "ET MOBILE_MALWARE Android APT-C-23 (david-moris .website in TLS SNI)", "ET MOBILE_MALWARE Android APT-C-23 (appuree .info in DNS Lookup)", "ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (sskimresources .com)", "ET MOBILE_MALWARE Android APT-C-23 (login-yohoo .com in DNS Lookup)", "ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)", "ET MALWARE APT28 Komplex DNS Lookup (apple-iclouds .net)", "ET MALWARE XDUpload Sending Screenshot Upload Progress", "ET MALWARE ShellCrew.APT StreamEx DNS

	Lookup 3", "ET MALWARE DNS query for known Anunak APT Domain (ddnservice10.ru)", "ET MALWARE APT DarkHydrus DNS Lookup 13", "ET MOBILE_MALWARE Android APT-C-23 (mauricefischer .club in DNS Lookup)", "ET MALWARE Win32/SodaMaster domain observed in TLS SNI (www. rare-coisns. com)", "ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT TCP Checkin 1", "ET MALWARE ShellCrew.APT StreamEx DNS Lookup 12", "ET MALWARE MiniDuke CnC Beacon (string1_slide_2_1)", "ET MOBILE_MALWARE Android APT-C-23 (eleanorguthrie .site in DNS Lookup)"
Блокирование утечек информации	"ET INFO UPnP Discovery Search Response vulnerable UPnP device 3", "ET POLICY WebRTC IP tracking Javascript", "ET WEB_SERVER Successful DD-WRT Information Disclosure", "ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (linux style)", "ET INFO UPnP Discovery Search Response vulnerable UPnP device 1", "ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (BSD style)", "ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (BSD style)", "ET INFO UPnP Discovery Search Response vulnerable UPnP device 2", "ET WEB_SERVER WEB-PHP phpinfo access", "ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)", "ET ATTACK_RESPONSE passwd file Outbound from WEB SERVER Linux"
Чёрный список IP-адресов	"IP blocklist"
Блокирование активности троянских программ	"ET SCAN ZmEu Scanner User-Agent Inbound", "ET MALWARE Potentially Unwanted Program RebateInformerSetup.exe Download Reporting", "ET MALWARE Jupyter Stealer Reporting System Information", "ET MALWARE InfoBot Sending LAN Details", "ET MALWARE TA471/UNC2589 Related Activity (GET)", "ET MALWARE Win64/Vabushky.A Malicious driver download", "ET MALWARE Win32/ChromeBack Browser Hijacker Query Redirection", "ET MALWARE Evil JS Ransomware", "ET WEB_CLIENT DRIVEBY GENERIC ShellExecute in URLENCODE", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (hardwarecloseout .com)", "ET MALWARE ELF/BASHLITE vbot Variant CnC", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (netpixelds .com)", "ET MALWARE Linux/Tsunami DNS Request (updates.absentvodka.com)", "ET WEB_SERVER DNS Query for Suspicious 33db9538.com Domain - Anuna Checkin - Compromised PHP Site", "ET MALWARE Observed DNS Query to Budminer Domain (tw .americanunfinished .com)", "ET MALWARE Possible CopyKitten DNS Lookup (fdgdsg .xyz)", "ET MALWARE RezoStealer CnC Checkin", "ET MALWARE Observed DNS Query to Certishell Domain (freetips .php5 .sk)", "ET MALWARE Win32/SaintStealer Data Exfiltration Attempt M1", "ET MOBILE_MALWARE Android Malvertising Communication", "ET MALWARE Observed TraderTraitor Domain (tokenais .com) in TLS SNI", "ET MALWARE Win32/Bisonal Backdoor CnC Activity (POST)", "ET MALWARE Possible Kelihos.F EXE Download Common Structure", "ET MALWARE Zlader Ransomware Worm Propagating Over SMB v1 ASCII", "ET MALWARE ENV Variable Data Exfiltration Attempt (HTTP POST)", "ET MALWARE DNS Reply Sinkhole - Microsoft - 199.2.137.0/24", "ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B643 Oct 19 2017", "ET MALWARE Ponmocup HTTP Request (generic) M8", "ET MALWARE Legion Loader Activity Observed (neva-project)", "ET MALWARE Win32/Zemot Requesting PE", "ET MALWARE Gamaredon Related VBS Activity (GET)", "ET HUNTING SUSPICIOUS .PIF File Inside of Zip", "ET MALWARE PingPull ICMP Activity (Outbound)", "ET MALWARE Sharik/Smoke Loader Microsoft Connectivity check", "ET MALWARE Windows WMIC OS get Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Win32/Neutrino Cookie", "ET POLICY Likely PCTools.com Installer User-Agent (Installer Ping)", "ET MALWARE Observed Malicious DNS Query (ReactGet Group)", "ET HUNTING Suspicious Accept in HTTP POST - Possible Alphacrypt/TeslaCrypt", "ET MALWARE GravityRAT CnC Domain (strongbox .in in DNS Lookup)", "ET EXPLOIT GitLab Unauthenticated Remote ExifTool Command Injection (CVE-2021-24563)", "ET MALWARE Observed DNS Query to Impersoni-fake-ator (uc .ejalase .org)", "ET MALWARE Win32/Ficker Stealer Activity", "ET MALWARE Android/AhMyth RAT Command Inbound (Files Manager)", "ET ATTACK_RESPONSE Hostile FTP Server Banner (Reptile)", "ET EXPLOIT D-Link Remote Code Execution Attempt (CVE-2022-26258)", "ET CURRENT_EVENTS [Fireeye]

	Backdoor.HTTP.BEACON.[Yelp Request]", "ET MALWARE PowerTrick download ver2 bot", "ET MALWARE AgentTesla Exfil Via SMTP", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 10", "ET EXPLOIT Remote Command Execution via Android Debug Bridge", "ET MALWARE ELF/muBoT IRC Activity 6 (SOCKS)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (subsidiaryohio .linkpc.net)", "ET MALWARE Scarlet Mimic DNS Lookup 20", "ET MALWARE OneLouder Common URI Struct", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (edicupd002 .com)", "ET MOBILE_MALWARE NSO Related Domain 39", "ET MALWARE Villain C2 Framework HTTP Server Response", "ET MALWARE StrifeWater Rat CnC Activity", "ET MALWARE Observed DNS Query to Budminer Domain (accountinfo .ssl443 .org)", "ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (Checkupdate)", "ET MALWARE Win32 Dialer Variant", "ET MALWARE Zloader Related Download Activity (GET)", "ET ATTACK_RESPONSE Unusual FTP Server Banner (freeFTPd)", "ET MALWARE Possible CopyKitten DNS Lookup (primeminister-goverment-techcenter .tech)", "ET MALWARE Aerial Keylogger DNS Request", "ET MALWARE SLUB Domain in DNS Lookup", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (msfbckupsc .com)", "ET MALWARE Campo Loader Activity (GET)", "ET HUNTING SUSPICIOUS wsqmocn.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Sidewinder APT Related Malware Activity M2 (GET)", "ET MALWARE SSL/TLS Certificate Observed (Various Crimeware)", "ET MALWARE Pingback Shell Command Issued", "ET MALWARE IRC potential reptile commands", "ET INFO maas.io Image Download Flowbit Set", "ET MALWARE Possible Pegasus Related DNS Lookup (asrararablya .com)", "ET POLICY DNS Query to .onion proxy Domain (torman2.com)", "ET MALWARE CCleaner Backdoor DGA Domain (ab23660730bca .com) Dec 2018", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns2.hostasa.org)", "ET MALWARE Observed DNS Query to Budminer Domain (av .phdfa .com)", "ET USER_AGENTS Suspicious User-Agent (Forthgoner) - Possible Trojan Downloader GET Request", "ET WEB_SERVER c99 Shell Backdoor Var Override URI", "ET USER_AGENTS Suspicious User-Agent (HTTPTEST) - Seen used by downloaders", "ET MALWARE OSX/Proton.C/D Domain (handbrakestore .com in TLS SNI)", "ET MALWARE LokiBot Related DNS query", "ET WEB_CLIENT Possible FFSniff Inject Observed", "ET WORM W32/Rimecud wg.txt Checkin", "ET MALWARE Win32/XFILES Stealer Data Exfiltration Attempt", "ET MALWARE DangerousPassword APT Style Request (GET)", "ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain", "ET MALWARE Win32/Phorpiex Template 4 Active - Outbound Malicious Email Spam", "ET PHISHING Suspicious SSN Parameter in HTTP POST - Possible Phishing", "ET MOBILE_MALWARE Android/Ozotshielder.A Checkin", "ET MALWARE JS/Nemucod requesting EXE payload 2016-02-06", "ET INFO SimpleTDS go.php (sid)", "ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M3", "ET MALWARE LuminosityLink - Data Channel Server Response", "ET MALWARE W32/Zbot.InfoStealer WindowsUpdate Connectivity Check With Opera UA", "ET MALWARE DarkComet-RAT init connection", "ET MALWARE MSIL/GenKryptik.FQRH Download Request", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (onlinesoft .space)", "ET MALWARE Mashigoom/Tranwos/RevProxy ClickFraud - hello", "ET MALWARE Cryptolocker Payment Page (4nauizsaaopuj3qj)", "ET MALWARE [PTsecurity] Bladabindi/njRAT (HAMAD versions)", "ET MALWARE SystemdMiner CnC Activity", "ET MALWARE Observed DNS Query to Budminer Domain (bigbank .cnkk .org)", "ET MALWARE CCleaner Backdoor DGA Domain (ab1abad1d0c2a .com) Jul 2017", "ET MALWARE MSIL/CrimsonRAT Activity (POST)", "ET MALWARE Zbot .onion Proxy Domain", "ET MALWARE D1onis Stealer Sending Data to CnC", "ET ATTACK_RESPONSE Hostile FTP Server Banner (Bot Server)", "ET MALWARE Observed Karen Ransomware Powershell Loader", "ET MALWARE SocGholish Domain in DNS Lookup (brooklands .harteverything .com)", "ET MALWARE TA452 Related Backdoor Activity (POST)", "ET MOBILE_MALWARE Android/Locker.B Checkin 1", "ET MALWARE Trojan-Dropper.MSIL CnC Traffic - GET", "ET MALWARE SolarBot Plugin Download ComputerInfo", "ET MALWARE KeyBase Keylogger Uploading Screenshots", "ET MALWARE Zberp/ZeusVM receiving config via image file (steganography)", "ET MALWARE Blackmagic

	Ransomware Checkin Activity (GET)", "ET MALWARE OSX/Mughthesec/SafeFinder/OperatorMac DNS Query Observed", "ET MALWARE UNC2628 Malicious MSHTA Activity (GET)", "ET MALWARE JS/Cloud9 Domain (zmsp .top) in DNS Lookup", "ET WEB_SERVER Possible Custom Content Type Manager WP Backdoor Access", "ET MALWARE Legion Loader Activity Observed (YourUserAgent)", "ET MALWARE PingPull ICMP Activity M2 (Outbound)", "ET MALWARE Common Downloader Install Count Tracking URL (partner)", "ET MALWARE Win32/Trojan.Valyria.6015 CnC Activity (GET)", "ET MALWARE Win32.ClipBanker.uhn Exfil", "ET MALWARE Mirai Variant Domain (blacklister .nl in DNS Lookup)", "ET MALWARE FastPOS Reporting Error Code", "ET MALWARE Unknown Trojan Downloading PE via MSSQL Connection to Non-Standard Port", "ET MALWARE Possible Dyre SSL Cert M1 (L O)", "ET MALWARE FastPOS Successful Software Update Request", "ET MALWARE Possible Net Crawler SMB Share Access ascii (Operation Cleaver)", "ET MALWARE CCleaner Backdoor DGA Domain (ab3c2b0d28ba6 .com) Jan 2018", "ET MALWARE NetBackdoor User-Agent (.net backdoor)", "ET MALWARE AHK/BKDR_HTV.ZKGD-A Fake HTTP 500 Containing Encoded Commands Inbound", "ET MALWARE Win32.Bicololo Response 2", "ET MALWARE Bancos/Banker Info Stealer Post", "ET MALWARE NSO Group Pegasus Related Data Exfil (POST) M2", "ET MALWARE Sourtoff Download Simda Request", "ET MALWARE Suspected TeamTNT Linux Miner Activity", "ET MALWARE Win32/Caypnamer.A RAT CnC Initial Checkin", "ET MALWARE Possible Babar POST Request", "ET MALWARE Win32/HackTool.Agent.CS SMTP activity", "ET MALWARE Win32/DarkWatchman Checkin Activity (POST)", "ET MALWARE Suspected Ares Loader Activity (GET)", "ET MALWARE Possible CopyKittens DNS Lookup (mywindows24.in)", "ET MALWARE Possible Kaseya VSA Exploit Activity Inbound M2", "ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (zupertech .com)", "ET HUNTING Terse Unencrypted Request for Google - Likely Connectivity Check", "ET MALWARE Observed DNS Query to TA444 Domain (privacysign .org)", "ET ATTACK_RESPONSE Metasploit Meterpreter Reverse HTTPS certificate", "ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (databasegalore .com)", "ET MALWARE Neverquest/Vawtrak Posting Data", "ET MALWARE Observed Lazarus Domain (market .contradecapital .com in TLS SNI)", "ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mamsolutions .us)", "ET MALWARE IRC potential bot commands", "ET MALWARE Darkness DDoS Common Intial Check-in Response wtf", "ET MALWARE WinGo/Go-rod signInUrls Failed Data Exfiltration attempt", "ET MALWARE HermeticWizard - SMB Spreader - File Copy via SMB1 (NT Create AndX Request)", "ET MALWARE Observed IcedID Domain (deactivate .best in TLS SNI)", "ET MALWARE Java/Jacksbot Check-in", "ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v2", "ET MALWARE OSX/Proton.C/D Domain (handbrake .cc) in DNS Lookup", "ET EXPLOIT Possible ECLIPSEDWING RPCTOUCH MS08-067", "ET USER_AGENTS Suspicious UA Observed (Quick Macros)", "ET MALWARE Win32/TrojanDownloader.VB.RTN Payload Delivery Request", "ET MALWARE Observed DNS Query to Budminer Domain (oop .govtw .servernux .com)", "ET MALWARE Vicious Panda Checkin", "ET MALWARE Win32/Filecoder Ransomware Variant .onion Proxy Domain (tkj3higtqlvohs7z)", "ET MALWARE ELF/muBoT IRC Activity 5", "ET MALWARE Observed DNS Query to Budminer Domain (video .itsaol .com)", "ET MALWARE Subterranean Crimson Rat - FileManager List Command", "ET INFO Suspicious Windows NT version 7 User-Agent", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (mediamobilereg .com in DNS Lookup)", "ET MALWARE Ransomware Locky Possible Payment Page", "ET MALWARE Linux/dtool IRC Command (RAW)", "ET WEB_SERVER Win32/SessionManager2 Backdoor PING Command (Inbound)", "ET MALWARE MSIL.Kraken.v2 HTTP Pattern", "ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 1)", "ET MALWARE CryptoDefense DNS Domain Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (smtpgov .eSMTP .biz)", "ET MALWARE ZeroLocker Activity", "ET MALWARE CCleaner Backdoor DGA Domain (ab890e964c34 .com) Oct 2017", "ET MALWARE JS/Nemucod requesting EXE payload 2016-01-28", "ET MALWARE Observed DNS Query to Budminer Domain (global

	.smart-house .ga)", "ET POLICY External Host Creating Docker Image", "ET MALWARE ELF/Facefish Client Response (202)", "ET MALWARE Win32.VB.tdq - Fake User-Agent", "ET MALWARE ProjectSauron Remsec DNS Lookup (rapidcomments.com)", "ET MALWARE MWI Maldoc Stats Callout Aug 18 2015", "ET MALWARE Observed DNS Query to Budminer Domain (duth .ahfree .net)", "ET POLICY Observed SSL Cert (URL Shortener Service - tiny .cc)", "ET MALWARE Kraken Ransomware Start Activity 1", "ET MALWARE Possible PHP.MAILER WebShell Generic Request Inbound", "ET MALWARE Win32/Chinad Retrieving Config", "ET MALWARE HVNC BOT Detected", "ET WEB_SERVER Win32/SessionManager2 Backdoor DELETEFILE Command (Inbound)", "ET MALWARE Sidecopy APT Backdoor Related Activity (POST)", "ET MALWARE Observed DNS Query to Budminer Domain (tipo .dns-dns .com)", "ET MALWARE Zbot Generic URI/Header Struct .bin", "ET MALWARE linux.backdoor.wordpressexploit.2 JS backdoor retrieval", "ET MALWARE ELF/Emptiness v1.1 HTTP Flood Command Inbound", "ET MALWARE Observed DNS Query to Budminer Domain (bigbang .myddns .com)", "ET MALWARE Possible Winnti-related DNS Lookup (job .yoyakuweb .technology)", "ET MALWARE MacOS/UpdateAgent.A CnC Activity M1", "ET MALWARE Linux/Onimiki DNS trojan activity long format (Inbound)", "ET MALWARE Wide HTA with PowerShell Execution Inbound", "ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)", "ET MALWARE Observed DNS Query to Budminer Domain (oop .ddns .us)", "ET MALWARE Cknife Shell Command Struct Inbound (aspx)", "ET PHISHING Suspected TA445 Spearphishing Related Domain (i .ua-passport .space in TLS SNI)", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M9", "ET MALWARE Observed TA444 Domain (bankofamerica .tel in TLS SNI)", "ET MOBILE_MALWARE AdWare.AndroidOS.Ewind.cd Response", "ET MALWARE Bitter APT Related Activity (GET)", "ET EXPLOIT Adobe PDF Zero Day Trojan.666 Payload libarext32.dll Second Stage Download POST", "ET MALWARE Possible Pegasus Related DNS Lookup (manoraonline .net)", "ET MALWARE Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses", "ET MALWARE Win32/Dipverdle.A Activity", "ET MALWARE Reply Sinkhole - irc-sinkhole.cert.pl", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (truecrypte .org)", "ET MALWARE Lazarus Decafett DNS Lookup 2", "ET MALWARE Win32/Kelihos.F exe Download 2", "ET MALWARE Observed DNS Query to ShadowPad Domain (greatsong .soundcast .me)", "ET WEB_SERVER ATTACKER WebShell - 1337w0rm - cPanel Cracker", "ET MALWARE Kimsuky Related Maldoc Activity (POST)", "ET MALWARE Powershell Octopus Backdoor Activity (GET)", "ET MALWARE CargoBay CnC Activity", "ET DNS Reply Sinkhole - 106.187.96.49 blacklistthisdomain.com", "ET MALWARE DNS Query to Jaff Domain (orhangazitur . com)", "ET MALWARE Observed DNS Query to Budminer Domain (liveupdate .Jkub .com)", "ET P2P BearShare P2P Gnutella Client User-Agent (BearShare 6.x.x.x)", "ET MALWARE SSL/TLS Certificate Observed (StrongPity)", "ET MALWARE Win32.TrojanProxy Configuration file Download", "ET MALWARE User-Agent (Xmaker)", "ET HUNTING Suspicious exe.exe request - possible downloader/Oficla", "ET MALWARE MICROPSIA CnC Checkin", "ET MALWARE Netwire RAT Check-in (set)", "ET MALWARE Possible Pegasus Related DNS Lookup (icrcworld .com)", "ET MOBILE_MALWARE NSO Related Domain 18", "ET MALWARE Observed DNS Query to TA444 Domain (careers .bankofamerica .nyc)", "ET MALWARE Possible IRCBot.DDOS Common Commands", "ET MALWARE Observed DNS Query to TA455 Domain (microsoftdefender .info)", "ET MALWARE Win.Trojan.Chewbacca connectivity check", "ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.", "ET MALWARE Fake AV GET", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (issat .us)", "ET MALWARE APT29/CloakedUrsa Related Domain in DNS Lookup (crossfity .com)", "ET WEB_SERVER Perl/Mambo.WebShell Spreader IRC Open Ports Message", "ET MALWARE Possible Pegasus Related DNS Lookup (aalaan .tv)", "ET MALWARE Possible CopyKitten DNS Lookup (chromeupdates .online)", "ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .magicalgirlonlive .com)", "ET MALWARE Observed Malicious DNS Query (Mirrorthief Group)", "ET MALWARE Observed DNS Query to Budminer Domain (gpu .wikaba .com)", "ET USER_AGENTS Suspicious User-Agent (runPatch.html)", "ET MALWARE SMS-Bomber Activity", "ET MALWARE XDR33 CnC Server SSL Certificate

	Observed", "ET INFO NetSupport Remote Admin Checkin", "ET MALWARE Suspected Smokeloader Activity (POST)", "ET MALWARE LiteDuke Domain Observed", "ET MALWARE Mimikatz x86 Mimidrv.sys Download Over HTTP", "ET MOBILE_MALWARE NSO Related Domain 3", "ET MALWARE Obitel Downloader Request", "ET MALWARE JS/Nemucod requesting EXE payload 2015-12-01", "ET EXPLOIT IBM Data Risk Manager Arbitrary File Download Attempt", "ET MALWARE [401TRG] Backdoor.BEACON SSL Cert Inbound (infinitysoftwares .com)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 15", "ET MALWARE CCleaner Backdoor DGA Domain (ab693f4c0bc7 .com) Nov 2018", "ET MALWARE FakeAV oms.php Data Post", "ET MALWARE Observed DNS Query to Ursnif Domain (prises .cyou)", "ET HUNTING SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to lcomputers .com", "ET MALWARE Xbagger Macro Encrypted DL Jun 13 2016", "ET MALWARE SunSeed Downloader Retrieving Binary (set)", "ET MALWARE Kpang.com Related Trojan User-Agent (alertup)", "ET MALWARE Win32/Spy.Agent.QAQ Variant CnC Activity", "ET WEB_CLIENT pshell dl/execute primitives in wideb64 1", "ET HUNTING Suspicious Invalid HTTP Accept Header of ?", "ET MALWARE Possible VMWare NSX Manager Remote Code Execution Exploit Attempt (CVE-2021-39144)", "ET MALWARE Wintervivern Activity M2 (GET)", "ET MALWARE Generic.Malware.SFL User-Agent (Rescue/9.11)", "ET MOBILE_MALWARE Android Brunhilda Dropper (protectionguardapp .club in DNS Lookup)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (rotter2 .publicvm.com)", "ET MALWARE Observed DNS Query to TA455 Domain (remgrogroup .com)", "ET POLICY GridinSoft.com Software Version Check", "ET MALWARE Scarlet Mimic DNS Lookup 41", "ET MALWARE Possible Pegasus Related DNS Lookup (fb-accounts .com)", "ET MALWARE Generic Stealer Config Download Request", "ET MALWARE Limitless Logger Sending Data over SMTP 2", "ET MALWARE PS/PSRansom Client Checkin (GET)", "ET MALWARE Loki Locker Ransomware User-Agent", "ET MALWARE Observed DNS Query to Budminer Domain (sceyf .ibmmt .net)", "ET MALWARE Win32/Fireball Activity", "ET MALWARE Possible Asprox Pizza", "ET MALWARE Possible CopyKitten DNS Lookup (newsfeeds-microsoft .press)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (wantddantiprot .space in DNS Lookup)", "ET MALWARE Jupyter Stealer Reporting System Information M2", "ET MALWARE Gamaredon Style MalDoc .dot Download on freedynamicdns .org", "ET MALWARE Win32.Cerberus RAT Server ping", "ET INFO PowerShell DownloadFile Command Common In Powershell Stagers", "ET MALWARE GCleaner Downloader Activity M1", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (8as1s2 .com)", "ET MALWARE Observed DNS Query to Ursnif Domain (binchfog .xyz)", "ET MALWARE Win32/TrickBot CnC Initial Checkin M2", "ET MALWARE DonotGroup Maldoc Activity (GET)", "ET HUNTING SUSPICIOUS taskmgr.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Kimsuky Maldoc Activity (GET)", "ET MALWARE [Fireeye] Backdoor.BEACON M1", "ET MALWARE Observed DNS Query to Pegasus Domain (news-now .co)", "ET MALWARE Volatile Cedar DNS Lookup (dotnetexplorer.info)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher Sending Credit Card Info", "ET MALWARE Win32/MagicRAT Additional Payload URI M3", "ET MALWARE FrauDrop UA LETITGO", "ET MALWARE Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 1", "ET INFO JAVA - Java Class Download By Vulnerable Client", "ET MALWARE JS/Nemucod.M.gen downloading EXE payload", "ET MALWARE Win32/CrimsonRAT Variant Sending Command (inbound)", "ET MALWARE Fake Variation of Mozilla 4.0 - Likely Trojan", "ET INFO PowerShell Base64 Encoded Content Command Common In Powershell Stagers M1", "ET MALWARE Known Hostile Domain ilo.brenz .pl Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (aimimi .xxuz .com)", "ET MALWARE Restylink Domain in DNS Lookup (spffusa .org)", "ET MALWARE CryptoWall Check-in", "ET MALWARE Arkei/Vidar/Mars Stealer Variant DLL GET Request", "ET MALWARE Operation Blockbuster User-Agent (Mozillar)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Bookmarks Firefox.txt) M2", "ET MALWARE Possible Pegasus Related DNS Lookup (smsmensaje .mx)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (rootkit .tools)", "ET MALWARE CCleaner Backdoor DGA Domain

	(ab6d54340c1a .com) Feb 2017", "ET WEB_SERVER WebShell Generic eval of gzuncompress", "ET MALWARE ChaChi RAT Client CnC (POST)", "ET ATTACK_RESPONSE Backdoor reDuh http tunnel", "ET MALWARE Dosenjo/Kvadr Proxy Trojan Activity", "ET MOBILE_MALWARE NSO Related Domain 25", "ET MALWARE Cyborg Ransomware - Downloading Desktop Background", "ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (puccino .altervista .org)", "ET INFO Suspicious Windows NT version 8 User-Agent", "ET MALWARE Lockbit Ransomware Related Domain in DNS Lookup (ppaauuaa11232 .cc)", "ET MALWARE DarkGate Domain in DNS Lookup (hardwarenet .cc)", "ET MALWARE Hiloti loader installed successfully request", "ET MALWARE Possible Pegasus Related DNS Lookup (icloudcacher .com)", "ET HUNTING Suspicious User-Agent Containing .exe", "ET HUNTING Possible Obfuscator io JavaScript Obfuscation Exclusion", "ET MALWARE [Fireeye] Backdoor.BEACON M2", "ET MALWARE FruityArmor DNS Lookup (shelves-design .com)", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to thedoccloud .com", "ET MALWARE Vidar/Arkei/Megumin Stealer Keywords Retrieved", "ET MALWARE Possible Pegasus Related DNS Lookup (uaenews .online)", "ET MALWARE TA408 Related Activity (GET)", "ET MOBILE_MALWARE Android.Trojan.HiddenApp.OU Checkin", "ET MALWARE Win32/ElectricFish Authentication Packet Observed", "ET MOBILE_MALWARE NSO Related Domain 32", "ET MALWARE TellYouThePass Ransomware Checkin Activity (GET)", "ET INFO Obfuscated Eval String 3", "ET MALWARE MoneroPay Ransomware Payment Activity", "ET MALWARE Win32/Agent.UWW Variant Activity (Sending System Information)", "ET MALWARE Backdoor.Win32.Dorkbot.AR Join IRC channel", "ET MALWARE LokiBot File Exfiltration Detected", "ET CNC Feodo Tracker Reported CnC Server group 18", "ET MALWARE Observed DNS Query to Budminer Domain (H0TMAIL .ddns .info)", "ET MALWARE Banker.Delf User-Agent (hhh)", "ET MALWARE Windows Command Prompt OUTBOUND", "ET USER_AGENTS Metafisher/Goldun User-Agent (z)", "ET MALWARE Observed DNS Query to TA455 Domain (updateservices .co)", "ET INFO PowerShell DownloadData Command Common In Powershell Stagers", "ET MALWARE MSIL/Matrix Ransomware Sending Encrypted Filelist", "ET MALWARE Windows set Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE HackerDefender Root Kit Remote Connection Attempt Detected", "ET EXPLOIT SolusVM 1.13.03 SQL injection", "ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M1", "ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (onetwostep .at)", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (gh.dsaj2a1.org)", "ET MALWARE Bedep Connectivity Check M2", "ET MALWARE Potential Juniper Path Traversal RCE Attempt (CVE-2022-22245)", "ET WEB_SERVER WebShell - GODSpy - MySQL", "ET MALWARE Observed GandCrab Ransomware Domain (ransomware .bit in DNS Lookup)", "ET MALWARE TA453 Related Activity (FTP)", "ET MALWARE Observed DNS Query to Impersoni-fake-ator (fcanet .microsoftshop .org)", "ET MALWARE Possible PowerShell Empire Activity Outbound", "ET MALWARE Possible Upatre or Dyre SSL Cert Jan 22 2015", "ET MALWARE Likely Linux/Xorddos DDoS Attack Participation (xxxatat456.com)", "ET MALWARE Remote Utility Access Tool Key SMTP Exfil", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (googie .ph)", "ET MALWARE Win32.Sality User-Agent (DEBUT.TMP)", "ET MALWARE Python Library Backdoor Domain (wasp .plague .fun) in DNS Lookup", "ET MALWARE Ares Activity (POST)", "ET MALWARE HTTP Request to a *.su domain with direct request/fakebrowser (multiple families flowbit set)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (api .vmwareapi .net)", "ET HUNTING Microsoft Powershell Banner Output - Decimal Encoded", "ET ATTACK_RESPONSE Matahari client", "ET MALWARE Pony Downloader HTTP Library MSIE 5 Win98", "ET MALWARE Trojan.MyDNS DNSChanger - HTTP POST", "ET MALWARE Spy-Net Trojan Connection", "ET MALWARE Win32/StoredBt.A Activity", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (jourrapid .com)", "ET MALWARE Vidar Stealer CnC Domain in DNS Lookup", "ET MALWARE LogPOS Sending Data", "ET MALWARE Lazarus APT Related Maldoc Activity (GET)", "ET MALWARE Dridex DL Pattern Feb 18 2016", "ET EXPLOIT Possible Magento Directory Traversal Attempt", "ET MALWARE Snatch Ransomware Checkin (POST)", "ET MALWARE Winnti Payload - XORed Check-in

	to Infected System (0xd4413890)", "ET MALWARE ELF/Emptiness v2 XOR DNS Flood Command Inbound", "ET CURRENT_EVENTS [Fireeye] HackTool.UDP.Rubeus.[nonce 2]", "ET MALWARE Symbiote CnC Domain in DNS Lookup (bancodobrasil .dev)", "ET MALWARE Cobalt Strike Beacon Activity (GET)", "ET MALWARE Win32/NetDooka Framework RAT Sending System Information M1", "ET MOBILE_MALWARE AndroidOS/Basbanke.A Activity (POST)", "ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M2", "ET MALWARE Sality Variant Downloader Activity (3)", "ET MALWARE Win32.Small.qh/xSock User-Agent Detected", "ET MALWARE Lazarus APT Related Activity (GET)", "ET CNC Feodo Tracker Reported CnC Server group 4", "ET MALWARE Possible Pegasus Related DNS Lookup (topcontactco .com)", "ET MALWARE DNS Reply Sinkhole Microsoft NO-IP Domain", "ET MALWARE WARP Win32/Barkiofork.A", "ET WEB_SERVER Win32/SessionManager2 Backdoor PUTFILE Command (Inbound)", "ET WEB_SERVER c99 Shell Backdoor Var Override Cookie", "ET MALWARE Observed DNS Query to Budminer Domain (bidsd .justdied .com)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (aplikacje .ron-mil .space)", "ET MALWARE Observed IcedID Domain (bruzilovv .top in TLS SNI)", "ET MALWARE x0Proto Download Cmd", "ET MALWARE ELF/Mirai Variant UA Inbound (Tsunami)", "ET MALWARE Zeus.Downloader Campaign Second Stage Executable Request", "ET MALWARE ProjectSauron Remsec DNS Lookup (flowershop22.110mb.com)", "ET MALWARE Mustang Panda APT Related Activity (GET)", "ET MALWARE Wintervivern Activity M4 (GET)", "ET MALWARE Bitter APT ZxxZ Downloader CnC Checkin", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded Credential ConfigSyncProc System Details Request", "ET MALWARE Maldoc Downloading from Dropbox via API", "ET MALWARE HTML/Xbash Hex Encoded PS WebClient Object Inbound - Stage 1", "ET CURRENT_EVENTS [Fireeye] POSSIBLE HackTool.TCP.Rubeus.[User32LogonProcesss]", "ET MALWARE Observed DNS Query to Budminer Domain (dayan .onedumb .com)", "ET MALWARE Observed DNS Query to Certishell Domain (limousine-service .cz)", "ET WEB_SERVER WebShell - ASPyder - Auth Prompt", "ET MALWARE Egspy Infection Report Email", "ET MALWARE US-CERT TA14-353A Proxy Tool 1", "ET MALWARE Trojan Related Lame Updater User-Agent", "ET WEB_SERVER Win32/SessionManager2 Backdoor S5READ Command (Inbound)", "ET MALWARE MICROPSIA HTTP Failover Reporting Infected System Information and RAT Version", "ET MALWARE Observed DNS Query to Budminer Domain (iPhone .linkWebSock .ZoneID .uk .to)", "ET POLICY User Agent Ryeol HTTP Client Class", "ET HUNTING SUSPICIOUS msctcd.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Observed DNS Query to TA455 Domain (exprogroup .org)", "ET MALWARE Mimikatz x86 Executable Transfer Over SMB", "ET MALWARE Common Downloader Install Report URL (pid - mac)", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to highdatabase .com", "ET MOBILE_MALWARE Android.Dropper.Abd Checkin", "ET MALWARE SharpPanda APT Downloader Activity (GET)", "ET MALWARE MSIL/Spy.Agent.CSS Exfil", "ET MALWARE LDPinch SMTP Password Report", "ET MALWARE Observed SluttyPutty Maldoc User-Agent", "ET MALWARE Suspected Jobcrypter Ransomware Exfil (SMTP)", "ET MALWARE Linux DarkRadiation Ransomware Telegram Activity", "ET MALWARE Win32/Throwback Server Response (Incoming)", "ET MALWARE MSSQL maggie backdoor sysinfo Query Observed", "ET WEB_CLIENT Possible Injected JS Form Stealer Checking Page Contents M1", "ET MALWARE ELF/Mirai Variant UA Inbound (lessie)", "ET MALWARE Darkness DDoS HTTP Target/EXE", "ET MALWARE Win32/Tiggre!rfn Zipped Exfil", "ET MALWARE Observed DNS Query to Budminer Domain (info .chemoimmunity .top)", "ET MALWARE Suspected APT-Q-37 Related Activity (Outbound)", "ET MALWARE Win32/Neutrino CC dump", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded Credential ConfigSyncProc Login Attempt", "ET MALWARE Andromeda Downloading Module", "ET MALWARE Hoic.zip retrieval", "ET MALWARE Win32/Lumma Stealer Data Exfiltration Attempt M2", "ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate15.com)", "ET MALWARE Symbiote CnC Domain in DNS Lookup (caixa .wf)", "ET PHISHING Suspicious Minimal HTTP Refresh to Googledrive.com - Possible Phishing", "ET MALWARE Observed Win32/Ymacco.AA36 User-Agent", "ET MALWARE Maldoc Second Stage VBS

	Downloader with URL Padding", "ET MALWARE Observed DNS Query to Budminer Domain (iphone .site .web .fbs .ezua .com)", "ET MALWARE SocGholish Domain in DNS Lookup (collapse .tradingiswar .com)", "ET MALWARE Possible Dyre SSL Cert M2 (L CN)", "ET MALWARE TA401 Arid Viper CnC Domain in DNS Lookup (sknzy-mysl .vip)", "ET MALWARE JS/GootLoader CnC Exfil", "ET USER_AGENTS Suspicious User-Agent (FULLSTUFF)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (mmimdown .oss-cn-hongkong .aliyuncs .com)", "ET MALWARE DNS Possible User trying to visit POSHCODER.A .onion link outside of torbrowser", "ET WORM Win32.Socks.s HTTP Post Checkin", "ET MALWARE Observed Trojan.Verblecon Related Domain (jonathanhardwick .me in TLS SNI)", "ET MALWARE Observed DNS Query to Win32/TrojanDownloader.Agent.GEM Domain", "ET MALWARE WildPressure/Milum CnC Activity", "ET MALWARE Windows Scriptlet Invoking Powershell Likely Malicious", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (kazaboldu .net)", "ET MALWARE Gaboc Trojan Check-in", "ET MALWARE Observed MassLogger Domain in TLS SNI (ecigroup-tw .com)", "ET MALWARE GCleaner Downloader Activity M8", "ET MALWARE Zlob Updating via HTTP", "ET MALWARE Ponmocup Redirection from infected Website to Trojan-Downloader", "ET MALWARE Observed DNS Query to Budminer Domain (ktwords .lflink .com)", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (devciscoprograms .com)", "ET MALWARE MSIL/Crimson Receiving Command (ping) M1", "ET MALWARE Observed TA444 Domain (docuprivacy .com in TLS SNI)", "ET INFO NetSupport Remote Admin Response", "ET MALWARE Rogue.Win32/Winwebsec Install 2", "ET MALWARE Observed Ursnif Domain in TLS SNI (giantos .xyz)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 16", "ET MALWARE Cryptolocker Payment Page (krfdnhfnsai3d)", "ET MALWARE Pony DLL Download M2", "ET EXPLOIT Possible Successful ETERNALROMANCE MS17-010 - Windows Executable Observed", "ET EXPLOIT Possible Metasploit Java Exploit", "ET POLICY External Host Creating Docker Container", "ET MALWARE [PTsecurity] MSIL/Biskvit.A Check-in", "ET MALWARE Generic Request to gate.php Dotted-Quad", "ET MALWARE Hong Kong SWC Attack DNS Lookup (aoemvp.com)", "ET MALWARE W32/Lalus Trojan Downloader User Agent (Message Center)", "ET USER_AGENTS Suspicious User-Agent (miip)", "ET USER_AGENTS Suspicious User-Agent (DownloadMR)", "ET MALWARE Observed DNS Query to Budminer Domain (yahoo .ddns .name)", "ET MALWARE Possible Heliconia Noise Landing Page Response", "ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v1 Unicode", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (gvgnci .com)", "ET MALWARE Win32/Injector.BBYK Checkin", "ET MALWARE ASNAROK Related Domain in TLS SNI", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (cloud .skypecloud .net)", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 11", "ET MALWARE Observed Cobalt Strike User-Agent", "ET MALWARE Win32/Bisonal DNS Lookup 5", "ET WEB_SERVER WebShell Generic eval of base64_decode", "ET MALWARE Observed DNS Query to TA455 Domain (defenderupdate .ddns .net)", "ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound 3", "ET MALWARE Observed Ursnif Domain in TLS SNI (mamount .cyou)", "ET MALWARE Possible PHP.MAILER WebShell Register Shutdown Function Request Inbound", "ET MALWARE Possible Malicous Macro DL EXE Jul 01 2016 (userdir dotted quad)", "ET MALWARE Sourtoff Receiving Simda Payload", "ET MALWARE Win32/Cryptbot V2 Data Exfiltration Attempt", "ET MALWARE O97M/Sadoca.C!ml Checkin", "ET MALWARE Drive Receiving IP DDoS instructions", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (project2anub .xyz in DNS Lookup)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (seconddoxed .space in DNS Lookup)", "ET MALWARE TA450 Nagual/STARWHALE Beacon Activity (POST)", "ET MALWARE Powershell commands sent when remote host claims to send an image", "ET MALWARE MSIL/BISKVIT DNS Lookup (secured-links .org)", "ET MALWARE DirtJumper Activity", "ET MALWARE Observed DNS Query to Hilal RAT Domain (signin .dedyn .io)", "ET MALWARE Tinba Server Response", "ET PHISHING WalletConnect Stealer Landing Page 2022-11-23", "ET MALWARE Possible Pegasus Related DNS Lookup (y0utube .com.mx)", "ET EXPLOIT Possible ETERNALBLUE MS17-

	010 Echo Request (set)", "ET MALWARE Driveby Exploit Attempt Often to Install Monkif", "ET MALWARE Win32/Korplug.HQ CnC Activity", "ET MALWARE Scarlet Mimic DNS Lookup 15", "ET MALWARE Suspected Praying Mantis Threat Actor Activity", "ET MALWARE Unknown Actor Targeting Minority Groups Activity (POST)", "ET MALWARE W32/Echmark/MarkiRAT CnC Host Checkin", "ET SMTP Possible ComputerCop Log Transmitted via SMTP", "ET MALWARE OSX/Flashback.K/I User-Agent", "ET MALWARE Win32.Hyteod.acox Domain Generation Algorithm (DGA) Lookup NXDOMAIN Response", "ET MALWARE Observed DNS Query to Budminer Domain (dns .dymantic .service .fbs .ocry .com)", "ET MALWARE ELF/Mirai Variant UA Outbound (Shaolin)", "ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 1", "ET USER_AGENTS Suspicious User-Agent (ReadFileURL)", "ET MALWARE Observed DNS Query to Budminer Domain (nscnet .tk)", "ET MALWARE Observed TA444 Domain (bankofamerica .offerings .cloud in TLS SNI)", "ET MALWARE Suspicious UA Mozilla / 4.0", "ET MALWARE Observed MageCart Group 12 Domain (pathc .space in TLS SNI)", "ET MALWARE Possible Sharik/Smoke Loader 7zip Connectivity Check", "ET MALWARE SpamBanker message", "ET MALWARE HermeticWizard - WMI Spreader - File Copy via SMB1 (NT Create AndX Request)", "ET MALWARE Possible Net Crawler SMB Share Access unicode (Operation Cleaver)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(UPHTTP)", "ET MALWARE Possible Bedep Connectivity Check", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (topgamse .com)", "ET MALWARE Kimsuky Related Activity (POST)", "ET EXPLOIT CVE-2017-0199 Common Obfus Stage 2 DL", "ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M4", "ET MALWARE Dorkbot GeoIP Lookup to wipmania", "ET MALWARE Observed Malicious FIN12 Related SSL Cert", "ET MALWARE Win32/Shuckworm CnC Exfil M1", "ET MALWARE Observed Magecart Skimmer Domain (analiticsweb .site in TLS SNI)", "ET MALWARE Observed DNS Query to Budminer Domain (googledrivercould .serveuser .com)", "ET MALWARE LURK Trojan Communication Protocol detected", "ET MALWARE Win32.Riberow.A (postit3)", "ET MALWARE Possible Pegasus Related DNS Lookup (ooredoodeals .com)", "ET MALWARE CryptoWall Check-in M2", "ET MALWARE IcedID/Emotet Certificate Observed M1", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (myrappid .com)", "ET MALWARE Lazarus Decafett DNS Lookup 1", "ET MALWARE ELF/muBoT IRC Activity 7 (bindshell)", "ET EXPLOIT CVE-2014-6332 Sep 01 2016 (HFS Actor) M1", "ET MALWARE TROJ_PROX.AFV POST", "ET MALWARE Worm.VBS.Jenxcus.H User Agent", "ET ADWARE_PUP NivesroCheat CnC Activity M2", "ET POLICY WMIC WMI Request Over SMB - Likely Lateral Movement", "ET MALWARE Observed DNS Query for MageCart Data Exfil Domain", "ET CNC Feodo Tracker Reported CnC Server group 21", "ET MALWARE FakeAV Landing Page (aid sid)", "ET MOBILE_MALWARE iOS/Xsser checking library version", "ET ATTACK_RESPONSE MalDoc/Generik.ILNMZZB Payload Inbound", "ET MALWARE Libyan Scorpions Adwind DNS Lookup (collge .myq-see.com)", "ET MALWARE CCleaner Backdoor DGA Domain (abf09fc5abba .com) Jul 2018", "ET MALWARE Suspicious Zipped Filename in Outbound POST Request (Passwords.txt)", "ET MALWARE ProjectSauron Remsec DNS Lookup (sx4-ws42 .yi.org)", "ET WEB_CLIENT DRIVEBY Social Engineering Toolkit JAR filename detected", "ET MALWARE Win32/Predator Variant Dropper Activity", "ET MOBILE_MALWARE Worm.AndroidOS.Selfmite.a Checkin", "ET MALWARE Possible CopyKitten DNS Lookup (microsoft-security .host)", "ET SCAN WebHack Control Center User-Agent Inbound (WHCC/)", "ET MALWARE Possible Derusbi/Winnti Receiving Configuration", "ET MALWARE Possible Pegasus Related DNS Lookup (alljazeera .co)", "ET INFO Obfuscated Eval String (Single Q) 6", "ET MALWARE Sn0wsLogger CnC Exfil M2", "ET EXPLOIT HT SWF Exploit RIP", "ET HUNTING SUSPICIOUS Crystalize Filter in Uncompressed Flash", "ET MALWARE Shady RAT Send Status Result", "ET MALWARE Possible CopyKitten DNS Lookup (cloudmicrosoft .net)", "ET MALWARE Observed Ursnif Domain in TLS SNI (tornton .xyz)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (webfile .myq-see.com)", "ET MALWARE Filename svchost.exe Download - Common Hostile Filename", "ET WEB_CLIENT Evil Redirector Sep 29 2015", "ET MALWARE MAGICHOUND-related DNS Lookup (briefl .ink)", "ET PHISHING Data Submitted to Webeden.co.uk - Possible Phishing", "ET MOBILE_MALWARE

	ANDROIDOS_LEAKERLOCKER.HRX DNS Lookup", "ET MALWARE Subterranean Crimson Rat - AssignID Command", "ET MALWARE Win32/QuasarRAT CnC Traffic", "ET MALWARE MuddyWater APT Related Maldoc Checkin M1", "ET CURRENT_EVENTS [Fireeye] Backdoor.SSL.BEACON.[CSBundle Ajax]", "ET MALWARE Trojan/Win32.FraudPack User-Agent (Downloader MLR 1.0.0)", "ET CNC Feodo Tracker Reported CnC Server group 9", "ET POLICY External Host Sending Docker Swarm Join Command", "ET MALWARE SunSeed Download Retrieving Binary", "ET MALWARE Observed DNS Query to TA455 Domain (khaleejtimes .co)", "ET MALWARE Win32/Onliner Template 1 Active - Malicious Outbound Email Spam", "ET MALWARE Windows executable base64 encoded in XML", "ET MALWARE Linux DarkRadiation Ransomware Activity (wget)", "ET MALWARE Wintervivern Retrieving Task", "ET MALWARE Mera Keylogger POSTing keystrokes", "ET USER_AGENTS Suspicious User-Agent (CFS Agent)", "ET MALWARE Polonium CreepyDrive Client CnC Response", "ET WEB_SERVER Win32/SessionManager Backdoor ReadFile Command (Inbound)", "ET MALWARE Win32/Grimagent CnC Activity", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 6", "ET POLICY Abnormal User-Agent No space after colon - Likely Hostile", "ET MALWARE Known Malicious Redirector in DNS Lookup (by007 .cn)", "ET MALWARE Observed DNS Query to Ursnif Domain (damnater .com)", "ET MALWARE GravityRAT CnC Domain (sake .mozillaupdates .us in DNS Lookup)", "ET INFO Obfuscated Eval String (Single Q) 1", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (virtualdataserver .com)", "ET MALWARE Various Ransomware/Stealer Style External IP Address Check (myip .ch)", "ET MALWARE GravityRAT CnC Domain (nortonupdates .online in DNS Lookup)", "ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M3", "ET EXPLOIT Eir D1000 Modem CWMP Exploit Retrieving Wifi Key", "ET MALWARE Likely PadCrypt Locker PKG DL", "ET MALWARE IMDDOS Botnet User-Agent IAMDDOS", "ET MALWARE Likely Bot Nick in IRC (USA +..)", "ET MALWARE OSX/Flashback.K/I reporting failed infection", "ET MALWARE Observed DNS Query to Budminer Domain (members .viaopen .net)", "ET MALWARE WSHRAT Keylogger Module Download Command Inbound", "ET MALWARE Win32/AppleJeus CnC Checkin (POST)", "ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 2", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (wx .go890 .com)", "ET MALWARE Observed GandCrab Domain (gandcrab .bit)", "ET MALWARE OSX/Mami Possible DNS Query to Evil DNS Server", "ET MALWARE Banload User-Agent Detected (ExampleDL)", "ET WEB_SERVER PHP.//Input in HTTP POST", "ET MALWARE Observed DNS Query to Winnti Domain", "ET MALWARE W32/Citadel Infection or Config URL Request", "ET MALWARE Zeus.Downloader Campaign Second Stage Executable Request 10/4/2014", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (havan .qhigh.com)", "ET INFO Java Serialized Data", "ET MALWARE Possible CopyKitten DNS Lookup (qoldenlines .net)", "ET MALWARE SideCopy Group Activity (GET)", "ET MALWARE Win32/Gatak.DR Payload Instructions", "ET MALWARE Observed DNS Query to Budminer Domain (cart .skyseaweb .org)", "ET MALWARE Observed DNS Query to TA455 Domain (cloudgoogle .co)", "ET WEB_SERVER suhosin.simulation PHP config option in uri", "ET MALWARE Suspected fraud-bridge DNS Tunnel", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (pallomnareraebrazo .com)", "ET MALWARE FAKBEN Ransomware", "ET MALWARE TheTrick Banking Trojan User-Agent", "ET MALWARE EICAR File Sent With X-Powered By Kaspersky Labs 2022-11-03", "ET MALWARE Mac User-Agent Typo INBOUND Likely Hostile", "ET MOBILE_MALWARE Kimsuky AppleSeed CnC Checkin", "ET MALWARE Possible CopyKittens DNS Lookup (windows-kernel.in)", "ET MALWARE SocGholish Domain in DNS Lookup (founder .carflower .pics)", "ET MALWARE OSX/Proton.B DNS Lookup", "ET MALWARE dlink router access attempt", "ET MALWARE Operation Interception Beacon", "ET MOBILE_MALWARE NSO Related Domain 4", "ET POLICY Suspicious User Agent UpdateSoft", "ET MALWARE Polonium CreepyDrive Upload Request", "ET MALWARE FakeAV Install", "ET MALWARE Observed DNS Query to Budminer Domain (kuangd .new .hack-inter .net)", "ET MALWARE Fake AV Downloader.Onestage/FakeAlert.ZR User-Agent (AV1)", "ET MALWARE ChromeLoader CnC Checkin M2", "ET EXPLOIT_KIT Spelevo Download Payload Landing",

	"ET MALWARE Qasar Variant Domain (datapeople-cn .com in DNS Lookup)", "ET MALWARE Quant Loader Download Response M2", "ET MALWARE Suspected BTC Swapper Activity (GET)", "ET MALWARE TontoTeam APT Related Bisonal CnC Activity", "ET MALWARE Win32/BumbleBee Loader Activity (GET)", "ET MALWARE Hacking Team Scout Windows Implant Exfiltration", "ET MALWARE Shady RAT Get File Command", "ET WEB_SERVER IIS ISN BackDoor Command Delete Log", "ET MALWARE Trojan.Win32.Jorik.Totem.vg HTTP request", "ET MALWARE Downloader.Win32.Banload Reporting", "ET MALWARE Vawtrak/NeverQuest .onion Proxy Domain (llgerw4plyyff446)", "ET MALWARE Sn0wsLogger CnC Exfil M1", "ET MALWARE Observed DNS Query to Budminer Domain (wlks .ServeUsers .com)", "ET MALWARE Win32/SVCReady Loader Requesting Payload", "ET MALWARE Win32/Agent.VAZ Bot CnC Checkin M1", "ET USER_AGENTS Suspicious User-Agent Moxilla", "ET WEB_CLIENT Watering Hole Redirect Inject Jun 28 2017", "ET MALWARE Trojan.Kwampirs Outbound GET request", "ET MALWARE Win32/POWERPLANT CnC Exfil (Query)", "ET MALWARE Observed DNS Query to Budminer Domain (update .mefound .com)", "ET MALWARE Observed DNS Query to Budminer Domain (sorry .iownyour .biz)", "ET MALWARE Observed Ursnif Domain in TLS SNI (binchfog .xyz)", "ET MALWARE MSIL/PSW.Discord.AIY CnC Exfil", "ET MALWARE Ozone/Darktrack RAT Variant - Client Hello (set)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (adobe .name)", "ET MALWARE Linux/dtool IRC Command (EXEC)", "ET MALWARE ELF/Miner Activity (GET)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (twethujsnu .cc in DNS Lookup)", "ET MALWARE Observed Godlua Backdoor Domain (helegedada .github .io in TLS SNI)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (mircrosoftscoulds .com)", "ET MALWARE Ursnif Variant Retrieving Payload (x32)", "ET MALWARE Observed DNS Query to AppleJeus Domain (oilycargo .com)", "ET MALWARE DecebalPOS User-Agent", "ET MALWARE Win32/Webdor.NAC Variant CnC Activity", "ET MALWARE W32/NetShare User-Agent", "ET MALWARE Suspected Jupyter Stealer Related Activity (GET)", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M6", "ET MALWARE Observed DNS Query to Budminer Domain (bbwlkszb .organiccrap .com)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (wallanews .sytes.net)", "ET HUNTING Suspicious User-Agent (record)", "ET MALWARE Zbot .onion Proxy domain in SNI Aug 04 2014", "ET MALWARE Torpig Reporting User Activity (x25)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cmps .58sky .com)", "ET MOBILE_MALWARE DNS Android/Spy.Feabme.A Query", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M7", "ET MALWARE Observed Princess Ransomware Payment Domain (royal25fphqilqft in DNS Lookup)", "ET MALWARE MuddyWater APT Related Telegram Activity", "ET HUNTING Suspicious Request for Pdf.exe Observed in Zeus/Luminosity Link", "ET MALWARE SocGholish Domain in DNS Lookup (exclusive .milonopensky .store)", "ET MALWARE Possible Pegasus Related DNS Lookup (solo-hoy .com)", "ET MALWARE Virtumod/Agent.ufv/Virtumonde Get Request", "ET MOBILE_MALWARE NSO Related Domain 29", "ET MALWARE Laplas Clipper - SetOnline CnC Checkin", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server 3]", "ET MALWARE Observed DNS Query to Budminer Domain (most .gov .allowed .org)", "ET MALWARE Suspected Sidewinder APT Maldoc Activity", "ET MALWARE Observed DNS Query to Budminer Domain (oop .gov .minecraftr .us)", "ET MALWARE Evil Monero Cryptocurrency Miner Request Pools", "ET MALWARE EtumBot Registration Request", "ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (umpulumpu .ru)", "ET MOBILE_MALWARE Android/FakeKakao checkin 3", "ET MALWARE MUROFET/Licat Trojan", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain", "ET MALWARE Possible Winnti-related DNS Lookup (google-statics .com)", "ET MALWARE Woody RAT CnC Checkin", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Stager]", "ET MALWARE Observed IcedID Domain (deactivate .pw in TLS SNI)", "ET MALWARE Win32/Ymacco.AA67 CnC Activity", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (helpyoume .linkpc.net)", "ET MALWARE Kuluoz/Asprox Activity", "ET MALWARE SunOrcal Reaver Domain

	Observed (tashdqdxp .com) in DNS Lookup", "ET MALWARE Likely CryptoWall 2.0 .onion Proxy domain lookup", "ET MALWARE Restylink Domain in DNS Lookup (mbusabc .com)", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M8", "ET MALWARE Polonium CreepyDrive Download Request", "ET USER_AGENTS Win32.OnLineGames User-Agent (BigFoot)", "ET MALWARE Trojan Internet Connectivity Check", "ET MALWARE Observed Magecart Skimmer Domain (googie-analitycs .site in TLS SNI)", "ET MALWARE Observed DNS Query to TA455 Domain (online-audible .com)", "ET MALWARE Observed DNS Query to Budminer Domain (news .onmypc .org)", "ET MALWARE DDoS.Win32.Agent.bay Covert Channel (VERSONEX and Mr.Black)", "ET MALWARE Win32/Matanbuchus Loader Activity (POST)", "ET POLICY Majestic12 User-Agent Request Outbound", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns4.hostasa.org)", "ET MALWARE Backdoor/Win.Gh0stRAT CnC Exfil", "ET MALWARE Dark Halo/SUNBURST CnC Domain (globalnetworkissues .com in TLS SNI)", "ET MALWARE JS/Nemucod.M.gen requesting PDF payload 2015-10-07", "ET MALWARE US-CERT TA14-353A Proxy Tool 3", "ET MALWARE Observed DNS Query to Budminer Domain (mptudp .pw)", "ET MALWARE oRAT Related CnC Domain in DNS Lookup", "ET MALWARE Observed DNS Query to TA455 Domain (thefreemovies .net)", "ET MALWARE Casbaneiro CnC Host Checkin M2", "ET MALWARE Dark Halo/SUNBURST CnC Domain (webcodez .com in TLS SNI)", "ET MALWARE Observed DNS Query to Default Brute Ratel C2 Domain (evasionlabs .com)", "ET MALWARE Backdoor.Elise Style IP Check", "ET MALWARE Observed DNS Query to TA455 Domain (sauditourismguide .com)", "ET MALWARE Possible Pony DLL Download", "ET MALWARE Observed IcedID Domain in DNS Lookup (spkdeutshnewsupp .com)", "ET MALWARE Backdoored MSI Afterburner Payload Delivery Domain (git .git .skblxin .matrizauto .net) in DNS Lookup", "ET MALWARE Ursnif Variant Retrieving Payload (x64)", "ET MALWARE Chanitor Variant .onion Proxy Domain", "ET MALWARE Kaspersky Sinkhole DNS Reply", "ET MALWARE Kraken Ransomware End Activity", "ET MALWARE Cobalt Strike Malleable C2 Profile (extension.css)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (ftpserverit .otzo.com)", "ET WEB_CLIENT Possible eDellRoot Rogue Root CA", "ET MALWARE Windows WMIC NETLOGIN get Microsoft Windows DOS prompt command exit OUTBOUND", "ET USER_AGENTS Suspicious User-Agent (Installer)", "ET MALWARE MuddyWater APT Related Activity (GET)", "ET MALWARE Observed DNS Query to Budminer Domain (trademoea .onmypc .net)", "ET INFO JAR Containing Executable Downloaded", "ET MALWARE Possible Pegasus Related DNS Lookup (newtarrifs .net)", "ET MALWARE Windows sc query Microsoft Windows DOS prompt command exit OUTBOUND", "ET HUNTING Suspicious HTTP Referer C Drive Path", "ET EXPLOIT Possible CVE-2017-0199 HTA Inbound M2", "ET MALWARE DNSMessenger Payload (TXT base64 gzip header)", "ET MOBILE_MALWARE NSO Related Domain 22", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (daji8 .me)", "ET MALWARE Win32/Stealerium Stealer Checkin via Discord", "ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 2", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (comsecurityessentials .support)", "ET MALWARE GravityRAT CnC Domain (daily .windowsupdates .eu in DNS Lookup)", "ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate17.com)", "ET MALWARE Win32.FakeAV POST datan.php", "ET MALWARE Suspected Gamaredon APT Related Maldoc Activity (GET)", "ET WEB_SERVER disable_functions PHP config option in uri", "ET MALWARE MalDoc Requesting Payload 2020-04-21", "ET MOBILE_MALWARE Arid Viper (calculator-1e016 .appspot .com in DNS Lookup)", "ET MALWARE ZeroAccess udp traffic detected", "ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M2", "ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M2", "ET MALWARE Observed DNS Query to Certishell Domain (vavave .xf .cz)", "ET MOBILE_MALWARE Android/Updtkiller Sending Device Information", "ET MALWARE Ruskill/Palevo KCIK IRC Command", "ET MALWARE Bazaloader Variant Activity", "ET MALWARE Mustang Panda/RedDelta Activity", "ET MALWARE Magecart/Skimmer Domain in DNS Lookup (yzxi .net)", "ET MALWARE FinSpy Related Flash Installer Activity", "ET MOBILE_MALWARE Android/KungFu Package Delete Command", "ET MALWARE Win32/GrandaMisha Sending System

	Information (POST)", "ET MALWARE Filename server.exe Download - Common Hostile Filename", "ET MALWARE Observed DNS Query to Budminer Domain (bigbigbig .servehttp .com)", "ET MALWARE Python/PBot Browser Hijacker Activity", "ET MALWARE DarkGate Domain in DNS Lookup (akamai .la)", "ET MALWARE Possible Pegasus Related DNS Lookup (redcrossworld .com)", "ET MALWARE Win64/Spy.Agent.EE CnC Checkin Server Response", "ET MALWARE W32.Qakbot Webpage Infection Routine POST", "ET MALWARE Win32/Gh0st RAT Variant CnC Checkin response", "ET MALWARE Possible Graftor EXE Download Common Header Order", "ET MALWARE Downloader-5265/Torpig/Anserin/Sinowal Unique UA (MSID)", "ET MALWARE Observed TraderTraitor Domain (creaideck .com) in TLS SNI", "ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 5", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B643", "ET MALWARE Possible Bedep Connectivity Check (2)", "ET MALWARE Observed DNS Query to Budminer Domain (youtobeother .twbbs .org)", "ET MALWARE Observed Ursnif Domain in TLS SNI (dodstep .cyou)", "ET MALWARE Donkeyp2p Update Detected", "ET MALWARE Mirai Botnet Domain Observed", "ET MALWARE Suspicious Fake Opera 10 User-Agent", "ET MALWARE ShadowHammer DNS Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .dns-dns .tw)", "ET MOBILE_MALWARE Android/GoldDream Uploading Watch Files", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (adobe-flash .wiki)", "ET MALWARE Common Upatre URI/Headers Struct", "ET INFO PowerShell Base64 Encoded Content Command Common In Powershell Stagers M2", "ET MALWARE JST Perl IrcBot download", "ET MALWARE Observed DNS Query to Ursnif Domain (daydayvin .xyz)", "ET MALWARE Observed TA444 Domain (mufg .us .org in TLS SNI)", "ET MALWARE MICROPSIA HTTP Failover Response M1", "ET MALWARE BlackEnergy v2.x Plugin Download Request", "ET MALWARE XCodeGhost DNS Lookup", "ET MALWARE x0Proto Client Info", "ET HUNTING SUSPICIOUS Firesale gTLD IE Flash request to set non-standard filename (some overlap with 2021752)", "ET MOBILE_MALWARE Possible Android CVE-2014-6041", "ET MALWARE Subterranean Security Domain in DNS Lookup", "ET MALWARE W32.Dreambot File Upload (No Data Sent)", "ET MALWARE Observed DNS Query to Budminer Domain (kaspersky .apchnetinfo .com)", "ET MALWARE Win32/ClipBanker.OC CnC Activity M1", "ET HUNTING suspicious - gzipped file via JAVA - could be pack200-ed JAR", "ET MALWARE Parrot TDS Cleared Response", "ET MALWARE DonotGroup Pult Downloader Activity (POST)", "ET MALWARE Georbot requesting update", "ET USER_AGENTS Suspicious User-Agent Fragment (WORKED)", "ET MALWARE Possible W32/VBKlip BAN Download", "ET MALWARE MuddyWater APT Related Activity (POST)", "ET MALWARE TrueBot/Silence.Downloader Keep-Alive", "ET MALWARE MAGICHOUND.MPK Activity via IRC", "ET USER_AGENTS Suspicious User-Agent (QQ)", "ET MALWARE Possible Winnti-related DNS Lookup (vps2java .securitytactics .com)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (quickbooktechnicalsupport .org)", "ET MALWARE Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed DNS Query to Budminer Domain (blizzard .apchnetinfo .com)", "ET MALWARE [PTsecurity] Ursnif Encoded Payload Inbound", "ET MALWARE ELF/Emptiness v2 XOR HTTP Flood Command Inbound", "ET MALWARE Observed DNS Query to TA455 Domain (alharbitelecom .co)", "ET WORM TheMoon.linksys.router 1", "ET HUNTING Suspicious User-Agent (Random String)", "ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M1", "ET WEB_SERVER ATTACKER WebShell - Weevely - Cookie", "ET MALWARE Ursnif Payload Request (grab64.rar)", "ET MALWARE SocGholish Domain in DNS Lookup (taxes .rpacx .com)", "ET MALWARE EXE Download Request To Wordpress Folder Likely Malicious", "ET MALWARE TA569 sczriptzzbn JavaScript Inject", "ET WEB_CLIENT Fake Java Installer Landing Page Oct 21", "ET MALWARE Observed DNS Query to Budminer Domain (exchanger-online-thalesgroup .zyns .com)", "ET MALWARE Powershell Octopus Backdoor Activity (POST)", "ET MALWARE ELF/muBoT IRC Activity 3", "ET MALWARE W32/Witch.3FA0!tr CnC Activity M3", "ET MALWARE Observed TA444 Domain (docs .azurehosting .co in TLS SNI)", "ET USER_AGENTS SFML User-Agent (libsfml-network)", "ET MALWARE Evil PDF

	Retrieving Emotet Payload", "ET MALWARE IsSpace/Zacom Connectivity Check", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 7", "ET MALWARE Citadel Activity POST", "ET MALWARE GravityRAT CnC Domain (zen .mozillaupdates .us in DNS Lookup)", "ET MALWARE Symbiote CnC Domain in DNS Lookup (dpf .fm)", "ET MALWARE Arkei Stealer Config Download Request", "ET MALWARE Potential Juniper XPATH Injection Attempt (CVE-2022-22244)", "ET MALWARE PowerTrick download ver1 bot", "ET MALWARE Optix Pro Trojan/Keylogger Reporting Installation via HTTP-Email Post", "ET WEB_CLIENT Fake Flash Update Mar 23", "ET MALWARE Possible FakeAV Binary Download (Security)", "ET MALWARE BlueShtorm Infostealer Data Exfiltration", "ET MALWARE Observed DNS Query to Budminer Domain (msnlive .25u .com)", "ET MALWARE Golang Aurora Stealer Exfil Activity", "ET HUNTING Suspicious User-Agent (Agent and 5 or 6 digits)", "ET MOBILE_MALWARE Android/SlemBunk.Banker Phished Credentials Upload", "ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Passwords", "ET MALWARE Kimsuky Related Activity (GET)", "ET MALWARE Socks666 Connect Command Packet", "ET MALWARE Windows TaskList Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed Trojan.Verblecon Related Domain (verble .software in TLS SNI)", "ET MALWARE Java Archive sent when remote host claims to send an image", "ET MALWARE Observed DNS Query to LOADOUT Domain", "ET HUNTING Suspicious Script Loaded from Pastebin", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (soap .crmdev .org)", "ET WORM Possible Worm Sohanad.Z or Other Infection Request for setting.nql", "ET MALWARE Linux/DDoS.M Admin console status", "ET MALWARE GravityRAT CnC Domain (teraspace .co .in in DNS Lookup)", "ET MALWARE Observed DNS Query to IcedID Domain (dogotungtam .com)", "ET POLICY Spyware.Agent.elbb lava.cn Game Exe Download", "ET MALWARE Possible AMSI Powershell Bypass Attempt B641", "ET MALWARE ATTACKER IRCBot - net add PRIVMSG Command", "ET WEB_CLIENT Malicious iframe", "ET MALWARE Libyan Scorpions Netwire RAT DNS Lookup (wininit .myq-see.com)", "ET MALWARE Observed DNS Query to TA444 Domain (perseus .bond)", "ET MALWARE Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 3", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 22", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iranwatch .tech)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ccdata.txt) M1", "ET INFO Anyplace Remote Access Initial Connection Attempt (005)", "ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M3", "ET MALWARE Win32/DataStealer.P CnC Checkin", "ET MOBILE_MALWARE XML Style POST Of IMEI International Mobile Equipment Identity", "ET MALWARE Harvester Group Downloader Activity (GET)", "ET MALWARE HTML/Qbot Dropper (.zip)", "ET MALWARE Suspected RULER.Hacktool HTML Payload", "ET MALWARE Observed DNS Query to Budminer Domain (ey .acaro .org)", "ET MOBILE_MALWARE NSO Related Domain 6", "ET MALWARE Ponmocup Post Infection DNS Lookup fasternation", "ET MOBILE_MALWARE Android Fancy Bear Checkin 3", "ET WEB_SERVER Possible CVE-2016-5118 Exploit MVG attempt M2", "ET WEB_SERVER Possible Compromised Webserver Retriving Inject", "ET MALWARE Maldoc Retrieving Payload 2021-07-06", "ET WEB_CLIENT Fake Adobe Software Update Landing", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (thedoccloud .com)", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.tk)", "ET MALWARE Possible Malicious PowerSploit PowerShell Script Observed over HTTP", "ET MALWARE SteamStealer DNS Lookup (lightalex)", "ET POLICY owncloud .online Hosted Site Observed in TLS SNI", "ET MALWARE Win32/Darkme Trojan Checkin M2", "ET MALWARE IrcBot Downloading .old", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (screenshot.) M1", "ET MOBILE_MALWARE Arid Viper (es-last-telegram .appspot .com in DNS Lookup)", "ET MALWARE SideCopy APT MargulasRAT Related Activity", "ET MALWARE Skeleton Key Filename in SMB Traffic (Unicode)", "ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M3", "ET MALWARE MewsSpy.AE Onion Domain (cxkefbwo7qcmlelb in DNS Lookup)", "ET MALWARE Lurk Click fraud Template Request", "ET MALWARE Ozone/Darktrack RAT Variant - Server Hello", "ET WEB_CLIENT Generic HeapSpray Construct", "ET MALWARE Linux/dtool IRC Command

	Complete 1", "ET MALWARE Possible CopyKittens DNS Lookup (windows-10patch.in)", "ET MALWARE GravityRAT CnC Domain (wesharex .net in DNS Lookup)", "ET MALWARE Suspicious User-Agent (WindowsNT) With No Separating Space", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 19", "ET MALWARE CryptoWall CryptoWall 3.0 Check-in", "ET MALWARE APT34 Related Activity (GET)", "ET MALWARE CBReplay.P Ransomware", "ET WEB_CLIENT [eSentire] Fake Flash Update 2018-07-09", "ET MALWARE W32/AntiBreach Possible Activation Attempt", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (dynamicipaddress .linkpc.net)", "ET MALWARE Koobface HTTP Request (2)", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (kb63vhjuk3wh4ex7)", "ET MALWARE NetWire / Ozone / Darktrack Alien RAT - Client KeepAlive", "ET WEB_SERVER WebShell - Pouya - URI - raiz", "ET MALWARE SocGholish Domain in DNS Lookup (soendorg .top)", "ET MALWARE KeyBoy Backdoor Login", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (webcodez .com)", "ET MALWARE Win32/ChromeBack Browser Hijacker Home Beacon", "ET MALWARE SocGholish Domain in DNS Lookup (restructuring .breatheinnew .life)", "ET WEB_SERVER Compromised WordPress Server pulling Malicious JS", "ET MALWARE Office Macro Emotet Download URI Nov 24 2021", "ET WEB_SERVER WebShell - GODSpy - Auth Prompt", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.SmForw/SlemBunk/SLocker Checkin", "ET MALWARE Win32/LingyunNet.A Heartbeat Response", "ET MALWARE PingPull Related Activity (POST)", "ET MALWARE IIS Backdoor CnC Command Inbound", "ET MALWARE GravityRAT CnC Domain (enigma .net .in in DNS Lookup)", "ET MOBILE_MALWARE Android/RatMilad CnC Checkin", "ET MALWARE Possible WannaCry DNS Lookup 2", "ET MALWARE Observed DNS Query to TA455 Domain (listen-books .com)", "ET MALWARE Possible CopyKitten DNS Lookup (ads-youtube .online)", "ET MALWARE Downloaded .PNG With Embedded File (.sh)", "ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker Payment)", "ET MALWARE Observed DNS Query to Budminer Domain (privilegecom .theesponsibility .crabdance .com)", "ET MALWARE Observed DNS Query to UNC3890 Domain (pfizerpoll .com)", "ET MALWARE Observed DNS Query to Ursnif Domain (pinki .cyou)", "ET MALWARE Fake Google Chrome Notifications Installer", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 8", "ET WEB_SERVER WebShell - GODSpy - GODSpy title", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 8", "ET MALWARE TinyNuke VNC Checkin M2", "ET MALWARE Suspected APT32/OceanLotus Activity", "ET MALWARE Observed DNS Query to Budminer Domain (mitac_com .dns05 .com)", "ET MALWARE MalDoc Request for Payload (TA505 Related)", "ET MALWARE Win32/ArtraDownloader CnC Activity (GET)", "ET USER_AGENTS Suspicious User-Agent (56)", "ET CNC Feodo Tracker Reported CnC Server group 14", "ET MALWARE Win32.Razy.azv Downloading Content", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (iq3ahijcfeont3xx)", "ET HUNTING Download file with BITS via LNK file (Likely Malicious)", "ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 2)", "ET MALWARE Laplas Clipper - GetAddress CnC Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (bigkszb .twgogo .org)", "ET MALWARE Observed DNS Query to TA455 Domain (globaltalent .in)", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to digitalcollege .org", "ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B641 Oct 19 2017", "ET MALWARE Win32/Formgrabber Data Exfil", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (kubecloud .com)", "ET MALWARE Possible Raspberry Robin Activity (GET)", "ET MALWARE MalDoc Retrieving Payload May 23 2017 2", "ET MALWARE Cobalt Strike Activity (POST)", "ET MALWARE Win32/Sephora Related Activity (GET)", "ET MALWARE Likely GandCrab Ransomware Domain in HTTP Host M2", "ET MALWARE Cryptmen FakAV page Title", "ET MALWARE Win32/DolphinCape Activity (POST)", "ET MALWARE Possible CopyKitten DNS Lookup (microsoft-ds .com)", "ET MALWARE Trojan.BlackRev Registration Rev3", "ET MALWARE Hacking Team Android Implant Exfiltration", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M2", "ET MALWARE Observed DNS Query to TA455 Domain (linkedinz .me)", "ET MALWARE TA450 Nagual/STARWHALE GoLang Beacon Activity (POST)", "ET MALWARE Loki Locker Ransomware CnC Activity", "ET

	MALWARE FinSpy Related WinRAR Activity", "ET MALWARE Cobalt Strike Stager Time Check M2", "ET MALWARE Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M2", "ET HUNTING Suspicious User Agent (_)", "ET MALWARE [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message Header Local", "ET WEB_SERVER Perl/Mambo.WebShell Spreader IRC Scanning Message", "ET MALWARE CBeplay Downloading Design", "ET INFO Probably Evil Long Unicode string only string and unescape 2", "ET POLICY Possible IP Check curlmyip.com", "ET MALWARE MSIL/BISKVIT DNS Lookup (bigboss .x24hr .com)", "ET MALWARE Likely CryptoWall .onion Proxy domain in SNI", "ET MALWARE Win32/Banbra Banking Trojan Communication", "ET MALWARE SocGholish Domain in DNS Lookup (prompt .zonashoppers .academy)", "ET MALWARE BadRabbit Ransomware Payment Onion Domain", "ET WEB_SERVER Possible SQLi Attempt in User Agent (Inbound)", "ET MALWARE Patchwork Domain (randreports .org in DNS Lookup)", "ET POLICY IRC Channel JOIN on non-standard port", "ET MALWARE DCRAT Activity (GET)", "ET MALWARE MSIL/Crimson Receiving Command (dirs list)", "ET MALWARE Observed DNS Query to Fodcha Bot Domain", "ET MALWARE [ESET] TA410 APT LookBack HTTP Server Response", "ET MALWARE [PTsecurity] Black Stealer Exfil System Info", "ET MALWARE Restylink Domain in DNS Lookup (disknxt .com)", "ET MOBILE_MALWARE Android Trojan MSO.PJApps checkin 1", "ET MALWARE AHK.CREDSTEALER.A CnC Activity", "ET MALWARE Scarlet Mimic DNS Lookup 25", "ET MALWARE PS/PSRansom Server Status Check (GET)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (antivirusphonenumber .org)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 5", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup", "ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST)", "ET MALWARE Win32/Throwback CnC Activity (POST)", "ET MALWARE Upatre Common URI Struct Feb 12 2015", "ET MALWARE Perfect Keylogger FTP Initial Install Log Upload (Null obfuscated)", "ET MALWARE Observed DNS Query to Budminer Domain (madicity .org)", "ET MALWARE Zlob User Agent - updating (internetsecurity)", "ET MALWARE Win32/Variant.Babar.74963 CnC Exfil", "ET MALWARE Linux/Tsunami DNS Request (eggstrawdinarry.mylittlerepo.com)", "ET MALWARE Gamaredon/Armageddon CnC Activity (Sending Windows System Information)", "ET MALWARE Observed Pirate Stealer Domain in DNS Lookup (wearenotbbystealer .nl)", "ET MALWARE Iron Tiger DNSTunnel DNS Lookup (xssok.blogspot.com)", "ET MALWARE MintStealer Discord Activity (GET)", "ET MALWARE TorrentLocker DNS Lookup (walkingdead32.ru)", "ET MALWARE Win32/Bisonal DNS Lookup 4", "ET MALWARE Win32.Chroject.B Retrieving encoded payload", "ET USER_AGENTS Suspicious User-Agent (hi)", "ET MALWARE ELF/Mirai Variant UA Inbound (Cakle)", "ET MALWARE HTTPRevShell Initial CnC Checkin", "ET MOBILE_MALWARE IOS_XAGENT UA", "ET MALWARE NetSupport RAT with System Information", "ET MALWARE PSRansom File Exfiltration (POST)", "ET MALWARE Observed DNS Query to TA455 Domain (helpdesk-product .com)", "ET MALWARE Win32.Stealer.alwu Data Exfiltration Attempt", "ET MALWARE ReverseRAT Activity (POST) M3", "ET MALWARE Win32/ModernLoader Activity (POST)", "ET MALWARE Win32/Spy.Socelars.S CnC Activity M4 (GET)", "ET MALWARE Win32/Eternity Stealer Activity (POST)", "ET MALWARE Locky Ransomware Writing Instructions via SMB", "ET MALWARE SysJoker Related Domain in DNS Lookup (office360-update .com)", "ET MALWARE Patchwork DNS Tunneling (nsn1.winodwsupdates .me)", "ET MALWARE Possible Malicous Macro DL EXE Jul 01 2016 (dll generic custom headers)", "ET WEB_SERVER auto_prepend_file PHP config option in uri", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (galaxy-s .com)", "ET MALWARE Possible CopyKittens DNS Lookup (windowssup.in)", "ET MALWARE Scieron DNS Lookup (coastnews.darktech.org)", "ET MALWARE Windows quser Microsoft Windows DOS prompt command exit OUTBOUND", "ET MOBILE_MALWARE Android/Smsilence.A Successful Install Report", "ET MALWARE Known Malicious Redirector in DNS Lookup (vip.rm028 .cn)", "ET MALWARE Konni Related Activity", "ET MALWARE Observed DNS Query to Hilal RAT Domain (market .vinam .me)", "ET MALWARE TA444 Domain in DNS Lookup (sharedrive .ink)", "ET INFO Suspicious Windows NT version 0 User-Agent", "ET MALWARE Mimikatz x64

	Mimidrv.sys File Transfer Over SMB", "ET MALWARE Win32/LNK/Agent.GX Javascript Downloader M1", "ET MALWARE Send-Safe Bulk Mailer SSL Cert - Observed in Spam Campaigns", "ET USER_AGENTS Suspicious User-Agent (GOOGLE)", "ET MALWARE Win32/Qbot/Quakbot Downloader - Requesting Secondary Download", "ET MALWARE PoisonIvy RAT/Backdoor follow on POST Data PUSH Packet", "ET MALWARE Possible Malicious Invoice EXE", "ET MALWARE Magecart/Skimmer - _try_action Exfil Attempt", "ET MALWARE Wintervivern Activity (GET) M3", "ET MALWARE NoMercy Data Exfiltration M1", "ET MALWARE Observed DNS Query to Budminer Domain (emailfromsm .mpsdtupdsda .ezua .com)", "ET MALWARE ELF/Mirai Variant UA Outbound (muhstik)", "ET MALWARE MalDoc Retrieving Payload March 30 2017", "ET MALWARE IoT_reaper DNS Lookup M2 (hl859 .com)", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to kubecloud .com", "ET USER_AGENTS Suspicious User-Agent (Trojan.Hijack.IrcBot.457 related)", "ET MALWARE Successful Cobalt Strike Shellcode Download (x64) M2", "ET MALWARE W32/Agent.XXZBEN Downloader Activity", "ET MALWARE Win32/Neutrino ping", "ET MALWARE Possible BACKSWING JS Framework POST Observed", "ET MALWARE Win32/Eternity Ransomware Retrieving Image (GET)", "ET MALWARE TA444 Related Domain in DNS Lookup (web .shconstmarket .com)", "ET SCAN HTExploit Method", "ET MALWARE KeyBoy DNS Lookup (www .backus.myftp.name)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (update .adobe .wiki)", "ET MALWARE RedControle Probing Infected System", "ET MALWARE Pegasus Domain in DNS Lookup", "ET MALWARE DustySky Payload Link Request", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (epmhyca5ol6plmx3)", "ET MALWARE MewsSpy/NionSpy .onion Proxy Domain (z3mm6cupmtw5b2xx)", "ET MALWARE Possible Metasploit Java Payload", "ET USER_AGENTS Suspicious User-Agent (HTTP Downloader)", "ET MALWARE Observed DNS Query to Budminer Domain (widcards .abousts .fabioabreu .net)", "ET WEB_SERVER WebShell - ASPyder - File Upload - Response", "ET MOBILE_MALWARE Android Spy APT-C-23 (scott-chapin .com in TLS SNI)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES GET]", "ET MALWARE Conficker/MS08-067 Worm Traffic Outbound", "ET MALWARE US-CERT TA14-353A Wiper 2", "ET MALWARE Inbound PowerShell Saving Base64 Decoded Payload to Temp M2 2018-11-29", "ET MALWARE Linux DarkRadiation Ransomware Activity (curl)", "ET MALWARE Known Malicious Server in DNS Lookup (updatecache .com)", "ET MALWARE Suspected Lockscreen Ransomware Activity", "ET MALWARE Observed Thanatos Ransomware Variant Pico User-Agent", "ET MALWARE SocGholish Domain in DNS Lookup (canonical .fmunews .com)", "ET MALWARE W32/Trojan-Gypikon Sending Data", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (7tno4hib47vlep5o)", "ET MALWARE IMDDOS Botnet User-Agent i am ddos", "ET MALWARE Unicorn Stealer Activity (POST)", "ET INFO Suspicious Purported MSIE 7 with terse HTTP Headers GET to PHP", "ET MALWARE Observed DNS Query to Budminer Domain (gov .organiccrap .com)", "ET MALWARE Ponmocup Post Infection DNS Lookup intohave", "ET MALWARE MSIL/SkidRat User-Agent Observed", "ET WEB_SERVER WebShell ASPXShell - Title", "ET MALWARE Observed DNS Query to Budminer Domain (sososb .twbbs .org)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (liongracem .com)", "ET MALWARE W32/Kazy User-Agent (Windows NT 5.1 \; v.) space infront of semi-colon", "ET MALWARE Ponmocup HTTP Request (generic) M3", "ET MALWARE Win32/Orchard Botnet Activity M2", "ET MALWARE Observed DNS Query to Budminer Domain (mbank .moneyhome .biz)", "ET MALWARE KHRAT DNS Lookup (upload-dropbox .com)", "ET MALWARE Pegasus Domain in DNS Lookup (akhbar-almasdar .com)", "ET MALWARE TA457 Related Activity (POST)", "ET MALWARE Likely Infected HTTP POST to PHP with User-Agent of HTTP Client", "ET MALWARE Win32/LOADOUT CnC Activity", "ET MALWARE Win32.Agent.pt User-Agent Detected", "ET MALWARE OSX/WireLurker HTTP Request for manhuaba.com.cn", "ET MALWARE Possible Pegasus Related DNS Lookup (smscentro .com)", "ET MALWARE SupremeLogger CnC Checkin", "ET CHAT Gadu-Gadu Chat Client Checkin via HTTP", "ET MALWARE Suspected Powershell Empire POST M1", "ET MALWARE Possible Win32/SysJoker Retrieving CnC Information (GET)", "ET MALWARE Observed DNS Query to UNC3890 Domain

	(naturaldolls .store)", "ET WEB_SERVER WebShell Generic eval of gzinflate", "ET MALWARE VenusLocker Associated User-Agent Activity", "ET MALWARE Malicious Chrome Extension Domain Request (change-request .info in DNS Lookup)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (srv .payamradio .com)", "ET MALWARE Observed DNS Query to Budminer Domain (yahoo .mailweb .sxn .us)", "ET MALWARE Win32/Voltron/Spectre Stealer Checkin Activity (GET)", "ET MOBILE_MALWARE Android Fancy Bear Checkin 6", "ET MALWARE Observed DNS Query to TA455 Domain (supportskype .com)", "ET MOBILE_MALWARE Android/Kemoge Checkin", "ET MALWARE Suspected Powershell Empire GET M1", "ET MALWARE MacOS/UpdateAgent.A CnC Activity M2", "ET MALWARE JS/Batloader Payload Request (GET)", "ET MALWARE Win32/Wacatac.B!ml CnC Checkin", "ET MALWARE Win32/Aurora Stealer Accept Command", "ET MALWARE Observed BlackGuard_v2 Domain (win .mirtonewbacker .com) in TLS SNI", "ET MALWARE CCleaner Backdoor DGA Domain (ab1de19d80ae6 .com) in DNS Lookup", "ET MALWARE OSX/Proton.C/D Domain (eltima .in) in DNS Lookup", "ET MALWARE Suspected Bizarro Banker Activity (POST)", "ET MALWARE Pandemiya User-Agent", "ET MALWARE Possible IndigoDrop/Cobalt Strike Download", "ET MALWARE Possible DarkTequila SSL/TLS Certificate Observed", "ET MALWARE Likely Bot Username in IRC (XP-..)", "ET MALWARE ROMCOM RAT Campaign Domain (wveeam .com) in DNS Lookup", "ET MALWARE Volatile Cedar DNS Lookup (xploreredotnet.info)", "ET MALWARE Win32/Ursnif Connectivity Check", "ET MALWARE W32/Trojan-Gypikon Server Check-in Response", "ET MALWARE Observed Default CobaltStrike SSL Certificate", "ET MALWARE GravityRAT CnC Domain (bollywoods .co .in in DNS Lookup)", "ET MALWARE Bitter APT CHM Activity (GET) M3", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup", "ET MALWARE Win32/FFDroider CnC Activity", "ET EXPLOIT CVE-2014-6332 Sep 01 2016 (HFS Actor) M2", "ET MALWARE Possible ShadowHammer DNS Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (RdAccount .dns1 .us)", "ET MALWARE [eSentire] VBS Retrieving Malicious Payload", "ET MOBILE_MALWARE NSO Related Domain 40", "ET MALWARE Possible CopyKittens DNS Lookup (haaretz.link)", "ET MALWARE Powershell Octopus Backdoor Sending System Information (POST)", "ET EXPLOIT Possible $MFT NTFS Device Access in HTTP Response", "ET MALWARE Win32/Wacatac.B!ml Data Exfiltration", "ET MALWARE CryptoLocker EXE Download", "ET MALWARE [Fireeye] Backdoor.SUNBURST M1", "ET MALWARE Observed DNS Query to Budminer Domain (taitra .fartit .com)", "ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Domain Fetch", "ET MALWARE Shamoon v3 64bit Propagating Internally via SMB", "ET MALWARE Suspicious user agent (V32)", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to panhardware .com", "ET MALWARE IoT_reaper DNS Lookup M4 (cbk99 .com)", "ET MALWARE Codesoft PW Stealer Email Report Outbound", "ET MOBILE_MALWARE Observed Android/IRATA Domain (rimotgozaran .tk) in TLS SNI", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M1", "ET MALWARE Vidar/Arkei Stealer Client Data Upload", "ET MALWARE Win32/Bisonal DNS Lookup 2", "ET MALWARE Steganographic Encoded WAV File Inbound via HTTP M1", "ET MALWARE [PTsecurity] Possible Malicious (HTA-VBS-PowerShell) obfuscated command", "ET MALWARE Win32/Spy.Banker.AAXV Retrieving key from Pinterest", "ET MALWARE MSIL/TrojanDownloader.Small.CLJ CnC Activity", "ET MALWARE NanoLocker Check-in (ICMP) M1", "ET USER_AGENTS Suspicious User-Agent (winlogon)", "ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1", "ET MALWARE PowerShell/CustomRAT CnC Traffic", "ET MALWARE Loki Locker Ransomware Server Response (Public Key) M1", "ET MALWARE Possible Pegasus Related DNS Lookup (cnn-africa .co)", "ET MALWARE Iron Tiger Likely PlugX DNS Lookup (chrome.servehttp.com)", "ET USER_AGENTS Suspicious User-Agent (MadeByLc)", "ET POLICY DNS Lookup for Upaste Paste Site", "ET MALWARE Bitter APT Activity (GET)", "ET MALWARE Observed DNS Query to TA444 Domain (salt1ending .com)", "ET MALWARE Powersploit Framework Script Downloaded", "ET MALWARE Shady RAT Put File Command", "ET MALWARE IIStealer Inbound Exfil Request M2", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (v8.f1122.org)", "ET WEB_CLIENT

	Likely MS12-004 midiOutPlayNextPolyEvent Heap Overflow Midi Filename Requested baby.mid", "ET MALWARE Possible CopyKittens DNS Lookup (main.windowskernel14.com)", "ET MALWARE Win32/Ymacco.AA1C Activity", "ET MALWARE FOX-SRT ShimRat check-in (Yuok)", "ET PHISHING Data Submitted to ukit domain - Possible Phishing M1 2016-06-29", "ET MALWARE Observed Godlua Backdoor Domain (d .heheda .tk in TLS SNI)", "ET MALWARE Observed Ursnif Domain in TLS SNI (damnater .com)", "ET MALWARE Win32/SiMay RAT Activity (GET)", "ET MALWARE Observed DNS Query to Budminer Domain (skyfd .com)", "ET PHISHING Successful Bank of America Credential Phish 2022-08-25", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .yahoo-inc .DSMTP .COM)", "ET MALWARE Win32/Scieron-A UA (HTClient)", "ET MALWARE Unknown Chinese Threat Actor Malicious Redirect Activity", "ET MALWARE Possible Tinba DGA NXDOMAIN Responses (2)", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M1", "ET MALWARE TorrentLocker DNS Lookup (bigcrashcar.net)", "ET MOBILE_MALWARE NSO Group Domain in DNS Lookup (free247downloads .com)", "ET MALWARE ELF/muBoT User-Agent (I'm a mu mu mu ?)", "ET USER_AGENTS Suspicious User-Agent (HttpDownload)", "ET ATTACK_RESPONSE HTML Smuggling Powershell Payload In href", "ET MALWARE Legion Loader Activity Observed (lilith)", "ET MALWARE Scanbox Sending Host Data", "ET MALWARE SharpPanda APT Maldoc Activity", "ET MALWARE Suspected Polonium CnC Initial Checkin M2", "ET MALWARE PlugX/Destory HTTP traffic", "ET MALWARE Win32/Antilam.2_0 Sending Data over SMTP", "ET MALWARE Observed DNS Query to Budminer Domain (infor .nttcom .tk)", "ET MALWARE Gamania Trojan Check-in", "ET MALWARE Polonium APT CREEPYSNAIL Backdoor Related Activity (GET)", "ET MALWARE WORM_VOBFUS Requesting exe", "ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS PerlBot Version Message", "ET MALWARE Chinotto CnC Activity (command)", "ET MALWARE Downeks/Quasar DNS Lookup (download .data-server .cloudns .club)", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (navert0p.com)", "ET MALWARE APT-C-48 Related Activity Retrieving ConsoleHost (GET)", "ET MALWARE Observed Ursnif Domain in TLS SNI (lionnik .xyz)", "ET POLICY Powershell Activity Over SMB - Likely Lateral Movement", "ET MALWARE TA410 APT FlowCloud Dependency Download M2", "ET MALWARE Observed DNS Query to IcedID Domain (ajerlakerl .online)", "ET MALWARE Parite Setup Connection (tqzn.com related)", "ET MALWARE [401TRG] Observed Backdoor.SUNBURST CnC Domain (infinitysoftwares .com in TLS SNI)", "ET USER_AGENTS Suspicious User-Agent (Version 1.23)", "ET MALWARE Pingback Exep Command Issued", "ET MALWARE Poweliks Abnormal HTTP Headers high likelihood of Poweliks infection", "ET MALWARE Observed DNS Query to Comm100 Trojan Domain (amazonawsreplay .com)", "ET MALWARE Lazarus Decafett DNS Lookup 3", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (trendingonfeed .com)", "ET WEB_SERVER Possible CVE-2016-5118 Exploit SVG attempt M2", "ET MALWARE ELF_BASHLITE.SMB Dropping Files", "ET MALWARE Win32/Vidar Variant/Mars Stealer CnC Exfil", "ET MALWARE Observed DNS Query to Budminer Domain (symantecAnti .ItemDB .com)", "ET MALWARE Suspected DonotGroup Maldoc Activity (GET)", "ET MALWARE MalDoc Retrieving Qbot Payload 2022-06-14", "ET MALWARE Drive Receiving IP2 DDoS instructions", "ET MALWARE Gamarue/Andromeda Downloading Payload", "ET MALWARE [PTsecurity] Kraken Ransomware Start Activity 2", "ET USER_AGENTS Suspicious User-Agent (xfilesreborn)", "ET MALWARE DNS Reply Sinkhole - IP - 161.69.13.44", "ET MALWARE Common Upatre Header Structure 2", "ET MALWARE Kimsuky Related Activity Sending Windows Information (POST)", "ET MALWARE Possible Win32/Travnet.A Internet Connection Check (microsoft.com)", "ET MALWARE Scieron DNS Lookup (apple.dynamic-dns.net)", "ET MALWARE Observed BlackGuard_v2 Domain (umpulumpu .ru) in TLS SNI", "ET EXPLOIT Possible CVE-2016-2209 Symantec PowerPoint Parsing Buffer Overflow M1", "ET MALWARE Possible malicious Office doc hidden in XML file", "ET MALWARE Mimikatz x86 Executable Download Over HTTP", "ET MALWARE Possible SSH Linux.Fokirtor backchannel command", "ET MALWARE Possible DANDERSPRITZ HTTP Beacon", "ET MALWARE Observed DNS Query to Budminer Domain (list .googlebook .mrbonus .com)", "ET MALWARE System Progressive

	Detection FakeAV (AuthenticAMD)", "ET MALWARE Infostealer.Banprox Proxy.pac Download 3", "ET MALWARE Vawtrak/NeverQuest Posting Data", "ET MALWARE Linux/B1txor20 Backdoor Connectivity Check", "ET MALWARE Possible Outbound WebShell JPEG", "ET MALWARE Observed DNS Query to Budminer Domain (rocky3288 .changeip .org)", "ET MALWARE Observed Ursnif Domain in TLS SNI (gigeram .com)", "ET MALWARE Gazer DNS query observed (mydreamhoroscope . com)", "ET MALWARE DazzleSpy Related Domain in DNS Lookup", "ET MALWARE Suspicious User-Agent (Asteria md5)", "ET MALWARE Gamaredon APT Maldoc Related Activity (GET)", "ET MALWARE Sharik/Smoke Loader Adobe Connectivity check", "ET MALWARE Ponmocup HTTP Request (generic) M2", "ET MALWARE Tandem Espionage CnC Domain (rwwmefkauiaa .ru) in DNS Lookup", "ET MALWARE BadRabbit Ransomware Activity Via WebDAV (infpub)", "ET MALWARE Win32/Vodkagats Loader Requesting Payload", "ET MALWARE Mimikatz x64 Executable Transfer Over SMB", "ET MALWARE Possible JKDDOS download ddos.exe", "ET MALWARE KL-Remote / Cryp_Banker14 RAT response", "ET MALWARE Patchwork Domain (rannd .org in DNS Lookup)", "ET MALWARE ELF/Mirai Variant UA Outbound (Tsunami)", "ET MALWARE Observed DNS Query to IcedID Domain (coldcreekranch .com)", "ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup", "ET MALWARE Win32/RecordBreaker Checkin M2", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to solartrackingsystem .net", "ET MALWARE Suspected VileRAT Related Request Activity (GET)", "ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Jul 2020- Jan 2021) (set)", "ET EXPLOIT Unk.IoT IPCamera Exploit Attempt Inbound", "ET MALWARE IRC Potential bot update/download via ftp command", "ET MALWARE Kaseya VSA Exploit Activity M2 (SET)", "ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound 2", "ET WEB_SERVER WebShell - ASPyder -File Upload - POST Structure", "ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M1", "ET HUNTING Suspicious SWF filename movie(dot)swf in doc root", "ET MALWARE Generic - 8Char.JAR Naming Algorithm", "ET MOBILE_MALWARE NSO Related Domain 16", "ET MALWARE Remcos Builder License Check", "ET MALWARE Possible Zeus P2P Variant DGA NXDOMAIN Responses July 11 2014", "ET MALWARE Observed DNS Query to Budminer Domain (kgoogfsd .freetcp .com)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iransec .services)", "ET MALWARE Unk Spam Bot Template 1 Active - Outbound Malicious Email Spam", "ET MALWARE Win32/DarkCloud Exfil Over SMTP (Body)", "ET MALWARE ErbiumStealer Variant CnC Activity (getstub)", "ET MALWARE Hawkeye Keylogger SMTP Beacon", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cfg .jipinwan .com)", "ET INFO PowerShell Internet Connectivity Check via Network GUID Inbound", "ET USER_AGENTS Suspicious User-Agent (Kvadrlson 1.0)", "ET MALWARE ELF/Facefish Session Closing (400)", "ET MALWARE Ursnif Payload Request (cook64.rar)", "ET MALWARE Mimikatz x64 Mimidrv.sys Download Over HTTP", "ET USER_AGENTS suspicious user-agent (REKOM)", "ET USER_AGENTS Suspicious User-Agent (App4)", "ET MALWARE Virtumonde Variant Reporting to Controller via HTTP (3)", "ET MALWARE LDPinch SMTP Password Report with mail client The Bat!", "ET MALWARE JS/Cloud9 Domain (download .loginserv .net) in DNS Lookup", "ET MALWARE DNS Query for Cloud Atlas ecolines.es", "ET MALWARE ViperSoftX HTTP CnC Activity", "ET MALWARE Win32/Unknown VBScript Backdoor Activity (GET)", "ET INFO PowerShell NoProfile Command Received In Powershell Stagers", "ET MALWARE Packed Perl with Eval Statement", "ET MALWARE Observed DNS Query to Budminer Domain (article .phdfa .com)", "ET MALWARE Trickbot Payload Request", "ET EXPLOIT Obfuscation Technique Used in CVE-2014-0322 Attacks", "ET USER_AGENTS Suspicious User-Agent Detected (Compatible)", "ET MALWARE DATA-BROKER BOT Activity", "ET MALWARE Redline Stealer TCP CnC - Id1Response", "ET MALWARE Parrot TDS Malicious Response", "ET MALWARE Cobalt Strike Beacon Activity", "ET MALWARE carberp check in", "ET PHISHING Possible Phish - Mirrored Website Comment Observed", "ET MOBILE_MALWARE NSO Related Domain 17", "ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 1", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (shopingchina .net)", "ET MALWARE Win32/Youtube Bot - CnC Checkin", "ET MALWARE Nemucod Downloading Payload 2", "ET MALWARE

	Windows Executable Downloaded With Image Content-Type Header", "ET WEB_SERVER Win32/SessionManager2 Backdoor S5CLOSE Command (Inbound)", "ET MALWARE Win32/TrojanDownloader.Chekafe.D User-Agent my_check_data On Off HTTP Port", "ET MALWARE MAGICHOUND-related DNS Lookup (chrome-up .date)", "ET MALWARE Possible Veil Powershell Encoder B641", "ET MALWARE ObliqueRAT CnC Checkin", "ET INFO PDF /FlateDecode and PDF version 1.0", "ET USER_AGENTS Suspicious User-Agent (chrome)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (info .fazlollah .net)", "ET MALWARE Win32/Necurs Common POST Header Structure", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns3.hostasa.org)", "ET MALWARE Windows Microsoft Windows DOS prompt command Error not recognized", "ET MALWARE Observed DNS Query to Budminer Domain (mimimi .VizVaz .com)", "ET MALWARE TSPY_BANKER.IDV/Infostealer.Bancos Module Download", "ET MALWARE Possible Malicious Macro DL EXE May 2016 (Mozilla compatible)", "ET POLICY Java EXE Download", "ET MALWARE eCh0raix/QNAPCrypt Successful Server Response", "ET MALWARE Single char EXE direct download likely trojan (multiple families)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 11", "ET MALWARE Downbot/Shady Rat Remote Shell Connection", "ET MOBILE_MALWARE Arid Viper (samehnew-10a7c .firebaseio .com in DNS Lookup)", "ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .net)", "ET MALWARE Observed DNS Query to Budminer Domain (moea .strangled .net)", "ET MALWARE RansomCrypt Intial Check-in", "ET MALWARE Win32/Grandoreiro Loader Checkin Activity (POST)", "ET MALWARE Kelihos.K Executable Download DGA", "ET MALWARE WBK Download from dotted-quad Host", "ET MALWARE Win32/Filecoder.GC CnC Credentials Exfil", "ET WEB_SERVER JSP.SJavaWebManage WebShell Pass 20-09-2018 1", "ET MALWARE ShellBot.C retrieval", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(nento)", "ET MALWARE Yandexbot Request Outbound", "ET MALWARE RedditC2 Related Activity (POST)", "ET MALWARE iKittens OSX MacDownloader DNS Lookup (officialswebsites .info)", "ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Logs", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Information.html) M2", "ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (jonathanhardwick .me)", "ET PHISHING Data Submitted to MyFreeSites.com - Possible Phishing", "ET MALWARE Tandem Espionage CnC Domain (cugdwpnykghx .ru) in DNS Lookup", "ET MALWARE BlackTech FlagPro Dropper Activity (GET)", "ET MALWARE Philis.J ICMP Sweep (Payload Hello World)", "ET WEB_CLIENT DRIVEBY FakeUpdate - URI - /styles/javaupdate.css", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (primecisco .com)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (projectpredator .space in DNS Lookup)", "ET MOBILE_MALWARE Apple iPhone Implant - Command Executed", "ET MALWARE Win32/Onliner Requesting Additional Modules", "ET MALWARE WinGO\Monitor.go CnC Checkin", "ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Server Response (CVE-2022-1388)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (wallet.dat) M2", "ET MALWARE ChromeLoader CnC Error", "ET MALWARE ATTACKER IRCBot - net user - PRIVMSG Command", "ET MALWARE Magecart/Skimmer - AngryBeaver Exfil Attempt", "ET MOBILE_MALWARE NSO Related Domain 36", "ET MALWARE Cobalt Strike Beacon Activity (Wordpress Profile)", "ET MALWARE OneLouder EXE download possibly installing Zeus P2P", "ET MOBILE_MALWARE Android/Kemoge DNS Lookup", "ET MALWARE DNS Reply Sinkhole - Anubis - 195.22.26.192/26", "ET MALWARE Socks666 Connection Initial Packet", "ET MALWARE W2KM_BARTALEX Downloading Payload M2 (set)", "ET MALWARE Win32/H0lyGh0st Ransomware CnC Response", "ET MALWARE Win32/BLUELIGHT OAuth Login Attempt M2", "ET MALWARE Malicious Chrome Extension Requesting Websocket", "ET MALWARE Locky Ransomware Renaming File via SMB", "ET MALWARE Gamaredon APT Related Activity (POST)", "ET MALWARE JS/Ostap CnC Activity", "ET MALWARE Linux/dtool IRC Command (TCPFLOOD)", "ET MALWARE Observed Win32/SVCReady Loader User-Agent", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (viralonspot .com)", "ET MALWARE CenterPOS User Agent Observed", "ET MALWARE Observed DNS Query to Budminer Domain

	(toolbar .DSMTP .COM)", "ET MALWARE Symbiote CnC Domain in DNS Lookup (assets .fans)", "ET MALWARE Kimsuky Related Activity (ping)", "ET MALWARE MAGICHOUND-related DNS Lookup (microsoftexplorerservices .cloud)", "ET MALWARE Win32/CryPy Ransomware Encrypting File", "ET MOBILE_MALWARE Android Spy APT-C-23 (amanda-hart .website in DNS Lookup)", "ET MALWARE Cybergate/Rebhip/Spyrat Backdoor Keepalive", "ET HUNTING Self-Signed Cert O=XX Observed", "ET MALWARE Observed DNS Query to Budminer Domain (faqtos .ignorelist .com)", "ET USER_AGENTS Suspicious UA Observed (IEhook)", "ET MALWARE PowerTrick Known Key 2", "ET MALWARE Observed DNS Query to TA444/Lazarus Domain (concrecapital .com)", "ET MALWARE Blue Bot DDoS Proxy Request", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Acecard.c Checkin", "ET MALWARE Suspected Kimsuky Activity (GET)", "ET USER_AGENTS Suspicious User-Agent (ErrCode)", "ET MALWARE TransparentTribe APT Related Activity (POST)", "ET MALWARE SharpNoPSExec EXE Lateral Movement Tool Downloaded", "ET MALWARE Observed DNS Query to TA444 Domain (ms .onlineshares .cloud)", "ET MALWARE Zacom/NFlog HTTP POST Connectivity Check", "ET MOBILE_MALWARE NSO Related Domain 19", "ET MALWARE Bedep Connectivity Check M3", "ET MALWARE Zberp/ZeusVM receiving config via image file (steganography) 2", "ET MALWARE Possible CopyKittens DNS Lookup (windowsupup.com)", "ET MOBILE_MALWARE Android/Xnore Fake Facebook Login Credentials Collected", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original POST]", "ET MALWARE Win32/PurpleFox Related Activity (GET)", "ET MALWARE Windows systeminfo Microsoft Windows DOS prompt command exit OUTBOUND", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (google_chrome_default_) M1", "ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .nyc)", "ET MALWARE Teerac/CryptoFortress .onion Proxy Domain (3v6e2oe5y5ruimpe)", "ET MALWARE Observed Ursnif Domain in TLS SNI (minotos .xyz)", "ET CURRENT_EVENTS [Fireeye] Backdoor.DNS.BEACON.[CSBundle DNS]", "ET MALWARE Observed DNS Query to TA455 Domain (savemoneytrick .com)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (rewujisaf .com)", "ET MOBILE_MALWARE Unknown Redirector Nov 17 2016", "ET MALWARE IRC channel topic misc bot commands", "ET MALWARE HTML/Xbash Hex Encoded WScript.Shell Inbound - Stage 1", "ET HUNTING Suspicious User-Agent (C slash)", "ET MALWARE Bitter APT Related Domain in DNS Lookup (diyefosterfeeds .com)", "ET MALWARE Inbound PowerShell Saving Base64 Decoded Payload to Temp M1 2018-11-29", "ET MALWARE Trickbot/Anchor ICMP Request", "ET MALWARE [401TRG] Backdoor.BEACON SSL Cert Inbound (bigtopweb .com)", "ET MALWARE Win32/Limbozar Ransomware Activity (POST)", "ET MALWARE Observed Godlua Backdoor Domain (dd .heheda .tk in TLS SNI)", "ET POLICY DNS Query to .onion proxy Domain (torwoman.com)", "ET WEB_SERVER Win32/SessionManager2 Backdoor CMD Command (Inbound)", "ET MALWARE W32/Bapy.Downloader PE Download Request", "ET MALWARE SocGholish Domain in DNS Lookup (library .covebooks .com)", "ET MALWARE Possible Dyre SSL Cert Jan 22 2015", "ET MALWARE Qarallax RAT Downloading Modules", "ET MALWARE Win32/ChromeBack CnC Checkin", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 3", "ET MALWARE Observed Ursnif Domain in TLS SNI (pinki .cyou)", "ET USER_AGENTS VBS/Kimsuky UA Observed", "ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern", "ET MALWARE Win32/Filecoder.OJC CnC Checkin", "ET MALWARE NSO Group Pegasus Related Data Exfil (POST) M3", "ET MALWARE Observed DNS Query to Budminer Domain (pqsl .servernux .com)", "ET MALWARE Observed DNS Query to Budminer Domain (getadobe .dns-dns .com)", "ET MALWARE Observed DNS Query to EvilProxy Domain (pua75npooc4ekrkkppdglaleftn5mi2hxsunz5uuup6uxqmen4deepyd .onion)", "ET MALWARE Observed DNS Query to Budminer Domain (enjoyit .longmusic .com)", "ET MALWARE Possible IoT_reaper ELF Binary Download", "ET MALWARE Win32/LockScreen.BW Payment Info 2", "ET MALWARE OSX/LamePyre Screenshot Upload", "ET MALWARE ATTACKER IRCBot - PRIVMSG Response - Directory Listing", "ET MALWARE Innostealer Domain (windows11-upgrade .com) in TLS SNI", "ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cloud-sources .com)", "ET POLICY DNS

	Query For Browser Cryptocurrency Mining Domain", "ET MALWARE Backdoor.Win32.DarkComet Keepalive Outbound", "ET MALWARE SluttyPutty isDebuggerPresent in Fake Putty Executable", "ET MALWARE NetWire Variant - Client Hello", "ET MALWARE Observed DNS Query to Budminer Domain (mysweetpig .news .minecraftnoob .com)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (exmail .googie .com .ph)", "ET INFO PowerShell DownloadString Command Common In Powershell Stagers", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mainlytrendy .com)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (uwannaplaygame .space in DNS Lookup)", "ET MALWARE Win32/IcedID Request Cookie", "ET MOBILE_MALWARE TransparentTribe AhMyth RAT Variant Activity (POST)", "ET MALWARE Suspected Lazarus APT Related Backdoor Activity (POST) M1", "ET EXPLOIT Observed Orange LiveBox Router Information Leakage Attempt (CVE-2018-20377)", "ET WEB_SERVER WebShell - ASPyder - Auth Creds", "ET MALWARE Win32.Jadtre Retrieving Cfg File", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (shileyfetwell .com in DNS Lookup)", "ET MALWARE Drive Receiving POST1 DDoS instructions", "ET MALWARE Zlob User Agent (securityinternet)", "ET MALWARE MSIL/Lightning Stealer Exfil Activity", "ET MALWARE Observed DNS Query to UNC3890 Domain (celebritylife .news)", "ET MALWARE Observed DNS Query to UNC3890 Domain (rnfacebook .com)", "ET MALWARE Observed GandCrab Ransomware Domain (zonealarm .bit in DNS Lookup)", "ET POLICY Rebate Informer User-Agent (REBATEINF)", "ET MALWARE DPRK APT Related Maldoc Activity (POST) M2", "ET MALWARE Win32/SocksTroy Session Initiation Attempt M1", "ET HUNTING Suspicious X-mailer Synapse Inbound to SMTP Server", "ET HUNTING SUSPICIOUS wimhost.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Pegasus Domain in DNS Lookup (akhbarnew .com)", "ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .org)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (upservicemc .com)", "ET MALWARE Grandoreiro Downloader Activity", "ET MALWARE Possible Zeus GameOver Connectivity Check 2", "ET MALWARE MSIL/NR42 Bot Parsing Config From Webpage", "ET MALWARE Win32/NetDooka Framework RAT Sending System Information M2", "ET MALWARE Observed DNS Query to TA455 Domain (microsoftcdn .co)", "ET EXPLOIT Netgear R6260 Mini_httpd Buffer Overflow Attempt - Possible RCE (CVE-2021-34979)", "ET MALWARE Potential Juniper PHP Local File Inclusion Attempt (CVE-2022-22246)", "ET MALWARE TeleBots BCS-server User-Agent", "ET MALWARE Win32/RecordBreaker CnC Checkin - Server Response", "ET MALWARE Kimsuky Related Activity (down)", "ET MALWARE Observed TA444 Domain (perseus .bond in TLS SNI)", "ET MALWARE Win32/Logger RAT CnC Checkin", "ET MALWARE Observed TA471/UNC2589 Go Downloader User-Agent (-hobot-)", "ET MALWARE Observed DNS Query to TA444 Domain (docuprivacy .com)", "ET MALWARE Possible CopyKittens DNS Lookup (patch7-windows.com)", "ET MALWARE Possible Deep Panda User-Agent", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (flash .wy886066 .com)", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to deftsecurity .com", "ET MALWARE Windows WMIC STARTUP get Microsoft Windows DOS prompt command exit OUTBOUND", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (minielectronic .in)", "ET EXPLOIT TrendMicro node.js (Remote Debugger)", "ET MALWARE Observed DNS Query to Alibaba2044 Domain (utente .service-fatturecloud .de)", "ET MALWARE Observed DNS Query to Budminer Domain (happy .MyNetAV .ORG)", "ET MALWARE Suspected Tunna Proxy M4", "ET MALWARE TA401 Arid Viper Related Activity (POST)", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B642", "ET MOBILE_MALWARE WireX Botnet DNS Lookup", "ET P2P BearShare P2P Gnutella Client HTTP Request", "ET MALWARE Scarlet Mimic DNS Lookup 6", "ET MALWARE Observed DNS Query to Budminer Domain (newsda .opsdatus .greatfinder .org)", "ET MALWARE Win32/Vflooder.C Connectivity Check", "ET MALWARE Malware Delivery Landing Page via JS Redirect (2021-06-24)", "ET EXPLOIT Adobe PDF Zero Day Trojan.666 Payload libarhlp32.dll Second Stage Download POST", "ET WEB_CLIENT Blatantly Evil JS Function", "ET MALWARE WindowsEnterpriseSuite FakeAV Reporting via POST", "ET USER_AGENTS Suspicious

	User-Agent (CFS_DOWNLOAD)", "ET MALWARE HawkEye Keylogger Report SMTP", "ET MALWARE KeyBase Keylogger HTTP Pattern", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (2kjb7.net)", "ET MALWARE DNSTrojan FakeAV Dropper Activity Observed (2)", "ET MALWARE ELF/Mirai Variant UA Outbound (Ouija_x.86)", "ET MALWARE KL-Remote / Cryp_Banker14 RAT connection", "ET MALWARE Win32.Zbot.ivgw Downloading EXE", "ET MALWARE Win32/Poweliks GET Request", "ET MALWARE SSL/TLS Certificate Observed (Quasar Related)", "ET MALWARE Possible Schneebly Posting ScreenShot", "ET MALWARE Regin Hopscotch Module Accessing SMB2 Named Pipe (Unicode) 1", "ET MALWARE Suspected DNS2TCP Auth", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 6", "ET MALWARE CoinVault POST M2", "ET MALWARE URI Struct Observed in Pawn Storm CVE-2015-2950", "ET MALWARE Observed DNS Query to Pegasus Domain (helpusfind .biz)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (gamestoplay .bid)", "ET POLICY Installshield One Click Install User-Agent Toys File", "ET MALWARE Downloader Retrieving Malicious Powershell in DNS Response", "ET MALWARE GandCrab Style External IP Check (Spoofed Yahoo Host)", "ET MALWARE JackPOS XOR Encoded HTTP Client Body (key AA)", "ET MALWARE SuperFish Possible SSL Cert Signed By Compromised Root CA", "ET MALWARE Observed Malicious FIN12 Related SSL Cert (serviceswork .net)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (firstdoxed .space in DNS Lookup)", "ET MALWARE Possible Pegasus Related DNS Lookup (sabafon .info)", "ET MALWARE NOBELIUM Win32/VaporRage Loader CnC Checkin", "ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-a.space)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 9", "ET MALWARE Covenant Framework Default HTTP Beacon", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to incomeupdate .com", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access getGalleryImage", "ET MALWARE ABUSE.CH Ransomware Domain Detected", "ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP", "ET MALWARE JS/Cloud9 Domain (download .agency) in DNS Lookup", "ET MALWARE PRISM Backdoor", "ET MALWARE SFG Client Information POST", "ET MALWARE Kimsuky Related FTP File Download", "ET MALWARE Maldoc OneDrive Download Activity (GET)", "ET MALWARE Win32/TrickBot maserv Module Command", "ET MALWARE Win32/Covagent Checkin", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 2", "ET MALWARE Observed DNS Query to Budminer Domain (idb .dns-dns .com)", "ET POLICY Tor2Web .onion Proxy Service SSL Cert (2)", "ET MALWARE Possible Infection Report Mail - Indy Mail lib and Nome do Computador in Body", "ET MALWARE Possible CopyKittens DNS Lookup (img.gmailtagmanager.com)", "ET MALWARE Observed DNS Query to ErbiumStealer Domain (erbium .ml)", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (combinedresidency .org)", "ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .qhigh .com)", "ET MALWARE MSIL.Orion Stealer Exfil via FTP", "ET MALWARE RegHelper Installation", "ET USER_AGENTS Possible QBot User-Agent", "ET MALWARE Kimsuky Related Script Activity (GET)", "ET MALWARE Win32/RM3Loader Activity (set)", "ET MALWARE Win32/Variant.Zusy.402698 Checkin", "ET USER_AGENTS Tear Application User-Agent Detected", "ET MALWARE Generic Win32.Autorun HTTP Post", "ET MALWARE SocGholish Domain in DNS Lookup (kinematics .starmidwest .com)", "ET MALWARE Win32/Loli Stealer CnC Activity", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.so)", "ET MALWARE linux.backdoor.wordpressexploit.1 CnC Checkin", "ET MALWARE Unk.VBSLoader Retrieving Payload", "ET MALWARE Win32/Ficker Stealer Activity M2", "ET MALWARE Brontok User-Agent Detected (Brontok.A3 Browser)", "ET MALWARE Maldoc Checkin Activity (GET)", "ET MALWARE Win32/Tofsee Connectivity Check M2", "ET PHISHING Possible Successful Generic Phish (set) 2020-09-03", "ET MALWARE [PTsecurity] QRat.Java.RAT (state_alive)", "ET MALWARE Datoploader Activity M2 (GET)", "ET MALWARE Observed DNS Query to VBS/Agent.PUK Domain", "ET MALWARE Observed DNS Query to TA444 Domain (tptf .cloud)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ProcessInfo_Log.txt) M2", "ET WEB_SERVER Win32/SessionManager2 Backdoor GETFILE Command (Inbound)", "ET MALWARE Suspected Tunna Proxy M2 (Outbound)", "ET MALWARE Observed DNS Query to Budminer Domain (rt .skymeto .com)", "ET

	MALWARE Trojan-Dropper.MSIL CnC Traffic - POST", "ET MALWARE Generic Trojan with /? and Indy Library User-Agent", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (help2014 .linkpc.net)", "ET MALWARE METALJACK APT32 DNS Lookup (vitlescaux.com)", "ET MALWARE Limitless Logger Sending Data over SMTP", "ET MALWARE ABCbot CnC Instruction (syn)", "ET MALWARE Win32.Cerberus RAT Client pong", "ET WEB_SERVER Possible OpenX Backdoor Backdoor Access POST to flowplayer", "ET MALWARE Possible Pegasus Related DNS Lookup (mobile-analytics .netweb-cloud-services .com)", "ET USER_AGENTS Peppy/KeeOIL User-Agent (ekeoil)", "ET MALWARE Pony Downloader check-in response STATUS-IMPORT-OK", "ET MALWARE FIN12 Related WEIRDLOOP/Cobalt Strike Beacon Activity (GET)", "ET MALWARE JS/Spy.Agent.AW Download", "ET MALWARE Unknown Rootkit Checkin Activity (getSystemInfo)", "ET MALWARE NSO Group Pegasus Related Data Exfil (POST)", "ET MALWARE [PTsecurity] WeChat (Ransomware/Stealer) HttpHeader", "ET MALWARE Downadup/Conficker A or B Worm reporting", "ET MALWARE Known Hostile Domain .ntkrnlpa.info Lookup", "ET MALWARE Possible IoT_reaper ELF Binary Request M3 (set)", "ET MALWARE TA452 Related Backdoor Activity (GET)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (i .ua-passport .space)", "ET MALWARE Win32.Agent.OSCF CnC Checkin", "ET MALWARE W32/Vundo.Downloader Reporting User Website Session Information", "ET MALWARE ELF/Mirai Variant UA Outbound (ph0ne)", "ET EXPLOIT Access To mm-forms-community upload dir (Inbound)", "ET MALWARE MAZE Ransomware Payment Domain in DNS Lookup", "ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (drproxy .pro in DNS Lookup)", "ET USER_AGENTS Suspicious User-Agent (WinProxy)", "ET INFO Suspicious MSIE 10 on Windows NT 5", "ET MALWARE Win32/RecordBreaker - Observed UA M2", "ET MALWARE Suspected Tunna Proxy M3", "ET MALWARE Possible CopyKitten DNS Lookup (nameserver .win)", "ET MALWARE Shuckworm Backdoor Screenshot Upload Attempt", "ET MALWARE GCleaner Related Downloader User-Agent", "ET MALWARE MyKings Bootloader Variant Requesting Payload M2", "ET MALWARE X-Tag Zeus Mitmo user agent", "ET MALWARE Downeks/Quasar DNS Lookup (moreoffer .life)", "ET MALWARE Warzone RAT Response (Inbound)", "ET MALWARE Observed DNS Query to Budminer Domain (family .mobwork .net)", "ET MALWARE MSIL/InfoStealer Variant Activity (POST)", "ET MALWARE Windows Microsoft Windows DOS prompt command Error not found", "ET MALWARE Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-3)", "ET MALWARE Observed DNS Query to Budminer Domain (american .ddns .us)", "ET MALWARE Innostealer Domain in DNS Lookup (seventyfor .site)", "ET MALWARE Kaseya VSA Exploit Activity M1 (SET)", "ET USER_AGENTS Ufasoft bitcoin Related User-Agent", "ET MALWARE Win32/Coldstealer Sending System Information (POST)", "ET WEB_CLIENT CookieBomb 2.0 In Server Response Jan 29 2014", "ET MALWARE Observed DNS Query to Budminer Domain (aolmail .ddns .info)", "ET MOBILE_MALWARE iOS/Xsser sending GPS info", "ET MALWARE Covenant Framework HTTP Hello World Server Response", "ET MALWARE JS/Ostap Maldoc Check-in", "ET MALWARE GravityRAT CnC Domain (melodymate .co .in in DNS Lookup)", "ET USER_AGENTS Suspicious User-Agent Detected (GetUrlSize)", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (solartrackingsystem .net)", "ET MALWARE Win32/Aurora Stealer Thanks Command", "ET MALWARE [PTsecurity] Gozi/Ursnif Payload v14", "ET MALWARE RAMNIT.A M1", "ET MALWARE Scarlet Mimic DNS Lookup 34", "ET USER_AGENTS Suspicious User-Agent (hacker)", "ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Clipboard", "ET MALWARE DonotGroup CnC Observed in DNS Query", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 10", "ET MALWARE Win32/ViperSoftX Stealer Activity M3 (POST)", "ET USER_AGENTS W32/OnlineGames User-Agent (LockXLS)", "ET MALWARE Win32/Ymacco.AA60 Checkin", "ET MALWARE Windows nbtstat -a Microsoft Windows DOS prompt command exit OUTBOUND", "ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (number update)", "ET MALWARE PLATINUM Steganographic HTTP Response Page Inbound", "ET MALWARE Observed DNS Query to TA444 Domain (azure-protection .cloud)", "ET MALWARE Kimsuky Maldoc Activity", "ET MALWARE Observed TA444 Domain (mufg .ink in TLS SNI)", "ET MALWARE Grandoreiro Banking Trojan DGA

	Domain in DNS Lookup (freedynamicdns. org)", "ET MALWARE IMDDOS Botnet User-Agent YTDDOS", "ET MALWARE Banker.Delf User-Agent (MzApp)", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 1", "ET MALWARE Win32/Zemot URI Struct", "ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-akamaihd.com)", "ET MALWARE [PTsecurity] Gozi/Ursnif Payload v12", "ET MALWARE Powershell commands sent B64 2", "ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-a.xyz)", "ET MALWARE Observed DNS Query to Budminer Domain (Facebook .ddns .ms)", "ET MALWARE Windows Executable Sent When Remote Host Claims to Send a RAR Archive", "ET MALWARE Banker.Delf Infection variant 4 - Sending Initial Email to Owner", "ET MALWARE Win32/Tapazom.A", "ET MALWARE Win32/PlagueBot User-Agent", "ET MALWARE JS/Nemucod.M.gen downloading PDF payload", "ET MALWARE Win32/TrickBot Anchor Variant Style External IP Check", "ET MALWARE Win32/DCRat CnC Exfil", "ET MALWARE Win32/Shrine.A CnC Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (google_service .ns01 .us)", "ET MALWARE Windows executable base64 encoded", "ET MALWARE Observed GET Request to Jaff Domain (orhangazitur . com)", "ET MALWARE Observed Qbot Style SSL Certificate", "ET MALWARE Dridex POST Retrieving Second Stage M2", "ET MALWARE Lyceum Golang HTTP Backdoor Submitting Data to CnC", "ET MALWARE Windows net start Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed Compromised Domain (cryptoarenastore .com in TLS SNI) (2021-11-12)", "ET MALWARE W32.Qakbot Update Request", "ET POLICY RunDll Request Over SMB - Likely Lateral Movement", "ET CURRENT_EVENTS Possible Crypto Drainer Enumerate", "ET PHISHING Successful Phish OWA Credentials 2022-06-20", "ET POLICY Win32/Sogou User-Agent (SOGOU_UPDATER)", "ET MALWARE Oficla Downloader Activity Observed", "ET MALWARE Minirem", "ET MALWARE OSX Backdoor Quimitchin DNS Lookup", "ET MALWARE Win32/Pykspa.C Public IP Check", "ET INFO Obfuscated Eval String 1", "ET MALWARE Win32/CollectorStealer CnC Exfil M2", "ET MALWARE Parrot TDS Check", "ET MALWARE Win32/Termite Agent Implant Keep-Alive", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (63ghdye17.com)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (printertechnicahelp .com)", "ET MALWARE Chanitor .onion Proxy Domain (l7gbml27czk3kvr5)", "ET MALWARE Observed DNS Query to TA455 Domain", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (kolabdown .sytes.net)", "ET MALWARE Observed DNS Query to Budminer Domain (fareastone .my03 .com)", "ET MALWARE Observed DNS Query to Budminer Domain (trends .crabdance .com)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (fbi .am)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (bandtester .com)", "ET MALWARE Malicious Browser Installer Domain in DNS Lookup (tor-browser .io)", "ET MALWARE Observed DNS Query to Budminer Domain (name .itsaol .com)", "ET MALWARE Observed DNS Query to TA444 Domain (cloud .tptf .ltd)", "ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .fastpaymentser-vice .com)", "ET HUNTING SUSPICIOUS EXE Download from specific file share site (used in recent maldoc campaign)", "ET MALWARE Possible SKyWIper/Win32.Flame POST", "ET MALWARE Win32/CandyOpen/UniClient Activity (GET)", "ET MALWARE Shifr Ransomware Malicious Domain in SNI Observed", "ET MALWARE LolliCrypt Ransomware Sending Data to CnC", "ET WEB_CLIENT Malicious Chrome Extension Domain Request (lite-bookmarks .info in DNS Lookup)", "ET MALWARE Observed DNS Query to Budminer Domain (moea .toythieves .com)", "ET MALWARE AgentTesla HTML System Info Report Exfil via FTP", "ET MALWARE Likely CryptoWall .onion Proxy DNS lookup", "ET MALWARE W32/Zeus.InfoStealer Infection Campaign Heap.exe Request", "ET MOBILE_MALWARE DNS Trojan-Banker.AndroidOS.Marcher.i Query", "ET MALWARE Machete FTP activity", "ET MALWARE UPDATE Protocol Trojan Communication detected on http ports 2", "ET USER_AGENTS Suspicious User-Agent (sickness29a/0.1)", "ET MALWARE Win32/RecordBreaker - Library Request", "ET MALWARE Socks666 Successful Connect Packet Packet", "ET MALWARE Observed DNS Query to Ursnif Domain (astope .xyz)", "ET MALWARE Dridex POST Retrieving Second Stage", "ET MALWARE Observed DNS Query to Alibaba2044 Domain (downloadpdf-fattura .de)",

	"ET USER_AGENTS DanaBot Specific UA Observed", "ET WEB_CLIENT Fake Adobe Flash Player malware binary requested", "ET MALWARE Common Upatre Header Structure 3", "ET MALWARE Gozi/Ursnif/Papras Grabftp Module Download", "ET MALWARE ArcDoor User-Agent (ALIZER)", "ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)", "ET MALWARE User-Agent (Visbot)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle USAToday GET]", "ET MALWARE Dridex Base64 Executable", "ET USER_AGENTS Suspicious User-Agent (MS Internet Explorer)", "ET MALWARE VBS/Dojos Downloader Activity M2", "ET MALWARE Observed TA444 Domain (cloud .tptf .ltd in TLS SNI)", "ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration", "ET MALWARE ARM Binary Requested via WGET to Known IoT Malware Domain", "ET PHISHING Possible Glitch.me Phishing Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookie.txt) M1", "ET MALWARE Possible Variant.Kazy.53640 Malformed Client Hello SSL 3.0 (Cipher_Suite length greater than Client_Hello Length)", "ET MALWARE Win32/Sality.NBA Exfil", "ET MALWARE Gamaredon Maldoc Remote Template Retrieval (GET)", "ET MALWARE Observed Ursnif Domain in TLS SNI (gigiman .xyz)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (thespeedoflite .com)", "ET MALWARE Scieron DNS Lookup (yellowblog.flnet.org)", "ET MALWARE AtomLogger Exfil via FTP", "ET MALWARE ELF/Facefish Server Response (201)", "ET MALWARE Android/AhMyth RAT Command Inbound (Contacts Manager)", "ET MALWARE MSIL/Lordix Stealer Exfiltrating Data", "ET MALWARE Suspected Lazarus APT Related Backdoor Activity (POST) M2", "ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 3", "ET MALWARE Win64/CobaltStrike.Beacon.J CnC Checkin", "ET MALWARE Innostealer Domain in DNS Lookup (windows11-upgrade .com)", "ET MALWARE Win32/SVCReady Loader CnC Activity", "ET HUNTING SUSPICIOUS winhosts.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE SocGholish Domain in DNS Lookup (squad .incumetrics .com)", "ET MALWARE Likely GandCrab Ransomware Domain in HTTP Host M1", "ET MALWARE Tibs/Harnig Downloader Activity", "ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .ro .lt)", "ET MALWARE Observed DNS Query to Budminer Domain (lookup .ns02 .us)", "ET MALWARE Suspected Malicious VBS Script Activity", "ET MALWARE Regin Hopscotch Module Accessing SMB Named Pipe (Unicode) 2", "ET MALWARE Win32/Delf.TJJ CnC Checkin M1", "ET EXPLOIT Possible ETERNALROMANCE MS17-010", "ET USER_AGENTS Suspicious User-Agent (API-Guide test program) Used by Several trojans", "ET MALWARE Nitro Stealer Exfil Activity (Response)", "ET MALWARE Dialer.Trojan Activity", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (aka7newmalp23 .com)", "ET MALWARE SocGholish Domain in DNS Lookup (subscribe .3gbling .com)", "ET MOBILE_MALWARE Android/IRATA Data Exfiltration Attempt", "ET MALWARE Possible AMSI Powershell Bypass Attempt B642", "ET MALWARE Observed DNS Query to Budminer Domain (youtobebig .cnkk .org)", "ET MALWARE VBA/Agent.ADT Checkin", "ET MALWARE Possible Satan Cryptor GeoIP Lookup", "ET MALWARE MSIL/JobCrypter Ransomware Checkin via SMTP", "ET MALWARE Win32/Sephora Related Activity (POST)", "ET MALWARE Observed Ursnif Domain in TLS SNI (fishenddog .xyz)", "ET MALWARE SunOrcal Reaver Domain Observed (weryhstui .com) in DNS Lookup", "ET MALWARE Dridex/Bugat/Feodo Cookie", "ET MALWARE Win64/Agent.qwiakk CnC Checkin", "ET MALWARE CopyKittens Matryoshka DNS Lookup 2 (twiter-statics . info)", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to deftsecurity .com", "ET MALWARE Orca RAT URI Struct 4", "ET MALWARE Probable Keylogger Report SMTP", "ET WEB_SERVER AnonGhost PHP Webshell", "ET MALWARE TA453 ClumsyCover Maldoc Activity (GET)", "ET MALWARE PE EXE or DLL Windows file download Text M2", "ET MALWARE Aurora Stealer Admin Console In HTTP Response", "ET MALWARE Gamaredon APT Backdoor Related Activity", "ET MALWARE Ponmocup HTTP Request (generic) M7", "ET MALWARE Gozi/Ursnif/Papras Connectivity Check", "ET MALWARE Hupigon User Agent Detected (??)", "ET MALWARE MegalodonHTTP/LuciferHTTP Client Action", "ET MALWARE Storm C&C with typo'd User-Agent (Windoss)", "ET MALWARE Powershell commands sent B64 3", "ET MALWARE W32/Scar Downloader Request", "ET MALWARE MSSQL maggie backdoor ListIP Query Observed", "ET MALWARE Orca

	RAT URI Struct 2", "ET MALWARE Compromised Chat Application Related User-Agent (Chrorne)", "ET MALWARE Cybergate/Rebhip/Spyrat Backdoor Keepalive Response", "ET MALWARE Downeks/Quasar DNS Lookup (ping .topsite .life)", "ET PHISHING Form Data Submitted to yolasite.com - Possible Phishing", "ET MALWARE Win32/Wacapew CnC Checkin", "ET MALWARE DNS Query to TOX Ransomware onion (toxicola7qwv37qj)", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 5", "ET MALWARE Possible Duqu 2.0 Accessing backdoor over 443", "ET MALWARE Matrix Max Stealer Exfiltration Observed", "ET MALWARE TorrentLocker DNS Lookup", "ET MALWARE BIOPASS RAT Python Activity (GET)", "ET MALWARE GoLang Popping Eagle Trojan Related Activity (POST)", "ET MALWARE Password Stealer - User-Agent (Ucheck)", "ET MALWARE Possible Malicious Macro DL EXE Feb 2016 (WinHTTPRequest)", "ET MALWARE Malicious Browser Installer Domain in DNS Lookup (torbrowser .io)", "ET MALWARE Observed DNS Query to Ursnif Domain (fineg .xyz)", "ET MALWARE China Chopper Command Struct", "ET MALWARE Possible PlugX DNS Lookup (googlemanage.com)", "ET MALWARE GravityRAT CnC Domain (nightly .windowsupdates .eu in DNS Lookup)", "ET MALWARE Possible Kimsuky Related Malicious VBScript", "ET WEB_SERVER WebShell - ASPyder - File Browser - POST Structure", "ET USER_AGENTS Downloader User-Agent HTTPGET", "ET MALWARE Linux/dtool IRC Command (HTTPFLOOD)", "ET MALWARE Observed DNS Query to Budminer Domain (googlemailinforma .orge .pl)", "ET MALWARE OSX/WireLurker HTTP Request for www.comeinbaby.com", "ET INFO Suspicious Windows NT version 2 User-Agent", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (gameoolines .com)", "ET MALWARE Magecart CnC Domain Observed in DNS Query", "ET MALWARE US-CERT TA14-353A Listening Implant 7", "ET MALWARE Win32/Nivdort Posting Data 1", "ET PHISHING Data Submitted to Weebly.com - Possible Phishing", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M6", "ET MALWARE Observed Ursnif Domain in TLS SNI (isteros .com)", "ET WEB_CLIENT Possible BadRabbit Driveby Download M1 Oct 24 2017", "ET MALWARE DarkGate Domain in DNS Lookup (awsamazon.cc)", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M8", "ET MALWARE Win32/Expiro.CD Check-in", "ET MALWARE JS/Nemucod requesting EXE payload 2016-02-01", "ET MALWARE FruityArmor DNS Lookup (weekendstrips .net)", "ET MALWARE MalDoc Retrieving Possible Ostap Payload", "ET MALWARE Observed Godlua Backdoor Domain (c .cloudappconfig .com in TLS SNI)", "ET MALWARE Win32/Filecoder.STOP Variant Public Key Download", "ET MALWARE Observed DNS Query to TA444 Domain (unchained-capital .co)", "ET MALWARE Fake/Short Google Search Appliance UA Win32/Ranbyus and Others", "ET MALWARE MSIL/GX Stealer/GravityRAT Uploading File", "ET WEB_SERVER Possible CVE-2016-5118 Exploit SVG attempt M1", "ET MALWARE Possible CopyKittens DNS Lookup (wheatherserviceapi.info)", "ET MALWARE Agent Tesla Keylogger Report SMTP", "ET MALWARE MWI Maldoc Posting Host Data", "ET EXPLOIT Metasploit Browser Exploit Server Plugin Detect", "ET MALWARE Galock Ransomware Command", "ET MALWARE Observed Evrial Domain (projectevrial .ru in DNS Lookup)", "ET MALWARE SocGholish Domain in DNS Lookup (hair .2topost .com)", "ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v1 ASCII", "ET MALWARE JSSLoader Initial Checkin", "ET MALWARE Win32/Nivdort Posting Data 2", "ET MALWARE Suspicious User-Agent build - possibly Delf/Troxen/Zema", "ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cdn-filestorm .com)", "ET MALWARE Malicious Dropper Activity (GET)", "ET MALWARE TorrentLocker DNS Lookup (server38.info)", "ET MALWARE Observed DNS Query to TA455 Domain (cortanaupdate .co)", "ET MOBILE_MALWARE NSO Related Domain 5", "ET MALWARE Kimsuky Related Malicious VBScript Inbound M4", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 4", "ET MALWARE ABCbot CnC Instruction (stop)", "ET MALWARE Suspected Chinese Based APT Malware Retrieving File (GET)", "ET MALWARE Backdoor Win32/Hupigon.CK Server Idle", "ET MALWARE Suspicious Zipped Filename in Outbound POST Request (Passwords.txt) M2", "ET MOBILE_MALWARE NSO Related Domain 7", "ET MALWARE Suspicious Download Setup_ exe", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 6", "ET MALWARE Downloader/Win.MalXll.R466354

	Payload Request", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (androidsmedia .com in DNS Lookup)", "ET MALWARE Possible WannaCry DNS Lookup 1", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (panhardware .com in TLS SNI)", "ET MALWARE TDTESS Backdoor User-Agent", "ET MALWARE Possible Kelihos Infection Executable Download With Malformed Header", "ET MALWARE Higasia CnC Activity", "ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Screenshot", "ET MALWARE Trojan.Win32.A.FakeAV Reporting", "ET MALWARE Panda Banker Injects Domain (urimchi3dt4 .website in TLS SNI)", "ET USER_AGENTS Downloader User-Agent Detected (Windows Updates Manager|3.12|...)", "ET MALWARE GravityRAT CnC Domain (nightlybuild .mozillaupdates .com in DNS Lookup)", "ET CNC Feodo Tracker Reported CnC Server group 7", "ET MALWARE Win32/Farfli.CUY Downloader", "ET MALWARE Observed DNS Query to Budminer Domain (kuangd .new .privatedns .org)", "ET MALWARE IoT_reaper DNS Lookup M1 (hl852 .com)", "ET MALWARE Kimsuky Related Activity (init)", "ET MALWARE Win32/RecordBreaker - Observed UA M4 (20112211)", "ET USER_AGENTS suspicious user agent string (changhuatong)", "ET USER_AGENTS Suspicious user agent (mdms)", "ET MALWARE Observed DNS Query to Ursnif Domain (giantos .xyz)", "ET MALWARE Suspected Polonium CnC Initial Checkin M1", "ET MALWARE Request for Malicious .dat File", "ET MALWARE Tandem Espionage CnC Domain (ckrddvcveumq .ru) in DNS Lookup", "ET MALWARE Upatre Downloader 2p (Zeus) May 07 2014", "ET MALWARE Subterranean Crimson Rat - GetClientLog Command", "ET WEB_SERVER Compromised Wordpress Install Serving Malicious JS", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (progsupdate .com)", "ET MALWARE Operation Cobra Venom WSF Stage 1 - File Decode Completed", "ET MALWARE Win32/TrojanDropper.Agent.SSQ Checkin", "ET MALWARE Win32/Comotor.A!dll Reporting 1", "ET MALWARE JS.ElectronBot Payload Inbound", "ET MALWARE [PTsecurity] Win32/Spy.RTM/Redaman IP Check", "ET MALWARE ELF/Muhstik Scanner Module Activity", "ET MALWARE Win32/TrojanDropper.Agent.SRM Exfil via Discord", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 2", "ET MALWARE Spoofed MSIE 8 User-Agent Likely Ponmocup", "ET MALWARE Fasec/FakeAV Alert/Keylogger/Dropper/DNSChanger Possible Rootkit - HTTP GET", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES POST]", "ET MALWARE Win32/Tapazom.A 2", "ET MALWARE Volatile Cedar DNS Lookup (explorerdotnt.info)", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access postToSocial", "ET MALWARE Kriptovor SMTP Traffic", "ET MALWARE Unknown Actor Targeting Minority Groups Activity (GET)", "ET MALWARE RevProxy Java Settings", "ET MALWARE Scarlet Mimic DNS Lookup 47", "ET MALWARE Observed DNS Query to POWERPLANT Domain", "ET MALWARE MSSQL maggie backdoor sp_addextendedproc Command Observed", "ET INFO Inbound PowerShell Checking for Virtual Host (Win32_PointingDevice WMI)", "ET WEB_CLIENT W32/Caphaw DriveBy Campaign Statistic.js", "ET MALWARE Skeleton Key Filename in SMB2 Traffic", "ET MALWARE Emotet v2 Exfiltrating Outlook information", "ET MALWARE MSIL/G1 Stealer/GravityRAT Requesting Payload", "ET MALWARE Observed DNS Query to TA455 Domain (mideasthiring .com)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 1", "ET MALWARE Possible Tunna Proxy Activity (Response)", "ET MALWARE Possible Maldoc Retrieving Dridex from pastebin", "ET CNC Feodo Tracker Reported CnC Server group 17", "ET MOBILE_MALWARE NSO Related Domain 33", "ET MALWARE Possible CopyKittens DNS Lookup (kernel4windows.in)", "ET MALWARE Possible Win32/Hupigon ip.txt with a Non-Mozilla UA", "ET MALWARE US-CERT TA14-353A Proxy Tool 2", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES Server]", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (938jss .com)", "ET MALWARE FakeAV FakeSmoke HTTP POST check-in", "ET MALWARE SocGholish Domain in DNS Lookup (chess .north-atlantic .com)", "ET MALWARE a310Logger Stealer Exfil (SMTP)", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 10", "ET MALWARE SC-KeyLog Keylogger Installed - Sending Log Email Report", "ET HUNTING Possible PHP Backdoor Command Execution", "ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Google)", "ET MALWARE

	Observed AHK Downloader Request Structure", "ET MALWARE Observed DNS Query to Budminer Domain (intweb .mobwork .net)", "ET MALWARE BernhardPOS Possible Data Exfiltration via DNS Lookup (29a.de)", "ET MALWARE SteamStealer DNS Lookup (steamdesktopauthenticator)", "ET MALWARE AntiVirus exe Download Likely FakeAV Install", "ET MALWARE SEASALT Server Response", "ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)", "ET MALWARE Win32/Kuluoz.B Request", "ET MALWARE Observed DNS Query to Ursnif Domain (logotep .xyz)", "ET MALWARE Trojan.BlackRev V1.Botnet HTTP Login POST Flood Traffic Outbound", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (daj8 .me)", "ET MALWARE Possible AMSI Powershell Bypass Attempt", "ET MALWARE ELF/Mirai Variant UA Inbound (Yowai)", "ET MALWARE Variant.Strictor Dropper", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (ananoka .com)", "ET MALWARE PandoraRat/Refroso.bsp Activity", "ET MALWARE Win32/TrickBot maserv Module CnC Activity", "ET MALWARE Win32/Wacatac Ransomware Variant Retrieving File (GET)", "ET MALWARE SocGholish CnC Domain in DNS Lookup (* .shrubs .emptyisland .pics)", "ET MALWARE Observed DNS Query to Certishell Domain (hotel-boss .eu)", "ET MALWARE [Fireeye] Backdoor.BEACON M6", "ET MALWARE Query for Known Hostile *test.3322.org.cn Domain", "ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup", "ET MALWARE Suspected SmokeLoader Retrieving Next Stage (GET)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (tissat .us)", "ET EXPLOIT Pulse Secure SSL VPN - Arbitrary File Read (CVE-2019-11510)", "ET USER_AGENTS Suspected Mekotio User-Agent (4M5yC6u4stom5U8se3r)", "ET MALWARE LokiBot Cryptocurrency Wallet Exfiltration Detected", "ET MALWARE SSL Cert Associated with Lazarus Downloader (JEUSD)", "ET MALWARE Malicious Chrome Extension Click Fraud Activity via Websocket", "ET MALWARE MSSQL maggie backdoor ls Query Observed", "ET MALWARE Havoc Framework CnC Request", "ET MALWARE ELF/Mirai Variant UA Outbound (b3astmode)", "ET MALWARE TA444 Related Domain (thecloudnet .org) in DNS Lookup", "ET MALWARE Virut Counter/Check-in", "ET MALWARE Win32/Grandoreiro Related Activity (GET)", "ET HUNTING SUSPICIOUS connhost.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Win32/Phoenix Keylogger Exfil via SMTP - Generic", "ET MALWARE Observed Evrial Domain (cryptoclipper .ru in DNS Lookup)", "ET MALWARE GravityRAT CnC Domain (gyzu .mozillaupdates .us in DNS Lookup)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (wallanews .publicvm.com)", "ET MALWARE DNS Query to Jaff Domain (fkksjobnn43 . org)", "ET MALWARE Cobalt Strike Related Activity (GET)", "ET MALWARE Win32/Trojan.Agent.FSTT CnC Activity", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (whoamis .info)", "ET MALWARE ATTACKER IRCBot - net localgroup - PRIVMSG Command", "ET CNC Feodo Tracker Reported CnC Server group 13", "ET MOBILE_MALWARE NSO Group Domain in DNS Lookup (urlpush .net)", "ET WEB_CLIENT pshell dl/execute primitives in wideb64 2", "ET MALWARE Operation SpoofedScholars Activity (GET)", "ET MALWARE Possible Java/Downloader Observed in Pawn Storm CVE-2015-2590 1", "ET MALWARE Win32/Spy.Mekotio.EY Payload Request", "ET MALWARE Observed DNS Query to Budminer Domain (backupcoa .serveftp .com)", "ET MALWARE Win32/Hancitor Checkin", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server 2]", "ET MOBILE_MALWARE SslCrypt Server Communication", "ET USER_AGENTS Suspicious User-Agent (RestoroMainExe)", "ET MALWARE Innostealer Domain (windows-11info .com) in TLS SNI", "ET USER_AGENTS Suspicious User Agent (agent)", "ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS Attack Done Message", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (exportball .servegame.org)", "ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query", "ET MALWARE Libyan Scorpions Adwind DNS Lookup (sara2011 .no-ip.biz)", "ET MALWARE PlugX or EvilGrab DNS Lookup (websecexp.com)", "ET USER_AGENTS Observed Suspicious UA (PhoneMonitor)", "ET MALWARE Shamoon v3 32bit Propagating Internally via SMB", "ET HUNTING ARM Binary Downloaded via WGET Containing Suspicious Netcat Command - Possible IoT Malware", "ET MALWARE Windows nbtstat -s Microsoft Windows DOS prompt command exit OUTBOUND", "ET MOBILE_MALWARE

	Android/Spy.Agent.AON / Glancelove DNS Lookup 2 (glancelove .com)", "ET ATTACK_RESPONSE Backdoor reDuh http initiate", "ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Sending System Information (POST)", "ET MALWARE Possible Worm W32.Svich or Other Infection Request for setting.xls", "ET MALWARE SocGholish Domain in DNS Lookup (shipwrecks .ggentile .com)", "ET MALWARE Blackshades Payload Download Command", "ET MALWARE Win32.UFRStealer.A issuing MKD command FTP", "ET MALWARE TorrentLocker DNS Lookup (allwayshappy.ru)", "ET MALWARE Possible Locky VB/JS Loader Download Sep 08 2017", "ET MALWARE Kimsuky APT Related Activity (GET)", "ET MALWARE Sinowal/sinonet/mebroot/Torpig infected host POSTing process list", "ET MALWARE Netbounce Related Activity (Program Wrapper)", "ET MALWARE Spy Banker Outbound Communication Attempt", "ET HUNTING SUSPICIOUS Word DOCX with Many ActiveX Objects and Media", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 7", "ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B641", "ET WEB_SERVER WebShell - GODSpy - GOD Hacker", "ET MALWARE SysJoker Related Domain in DNS Lookup (graphic-updater .com)", "ET MALWARE Observed DNS Query to Comm100 Trojan Domain (microsoftfileapis .com)", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.in)", "ET MALWARE ELF/Kinsing Payload Request M1", "ET MALWARE Known Skunkx DDOS Bot User-Agent Cyberdog", "ET MALWARE AHK.CREDSTEALER.A CnC Exfil", "ET MALWARE IMDDOS Botnet User-Agent STORMDDOS", "ET MALWARE Win32/Phoenix Grabber Sending System Information (POST)", "ET MALWARE Linux/dtool IRC Command (RESTART)", "ET MALWARE Win32/Wacapew.C!ml CnC Checkin", "ET MOBILE_MALWARE Android Spy APT-C-23 (david-gardiner .website in TLS SNI)", "ET MALWARE Spytector Domain DNS Lookup (mail .spytector .com)", "ET EXPLOIT Zollard PHP Exploit UA Outbound", "ET MALWARE UPDATE Protocol Trojan Communication detected on non-http ports 2", "ET MALWARE Yoda's Protector Packed Binary - VERY Likely Hostile", "ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 3 (autoandroidup .website)", "ET MALWARE Win32/Drokbk Checkin Activity (GET)", "ET MALWARE Possible Pegasus Related DNS Lookup (accounts .mx)", "ET DNS Reply Sinkhole - Georgia Tech (2)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice Server]", "ET MALWARE Linux/Denonia DNS Request Over HTTPS (denonia .xyz) M1", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 3", "ET MALWARE TA444 Related Activity (POST)", "ET MALWARE IoT_reaper DNS Lookup M5 (bbk80 .com)", "ET MALWARE [Flashpoint] Possible CVE-2018-4878 Check-in", "ET MALWARE Observed DNS Query to Budminer Domain (ktwods .lflink .com)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 18", "ET MALWARE Observed Certificate Containing Possible Base64 Encoded Powershell Inbound", "ET MALWARE Observed DNS Query to Ursnif Domain (lionnik .xyz)", "ET MALWARE Win32/CrimsonRAT Variant Sending Command M2 (inbound)", "ET MALWARE Win32/Delf.BLL Variant CnC Activity (Inbound)", "ET MALWARE PlugX variant", "ET MALWARE Win32/Enchanim Check-in Response", "ET MALWARE Dyreza RAT Ex-filtrating Data", "ET MALWARE ELF/Mirai Variant UA Inbound (Solar)", "ET MALWARE Ursnif Payload Request (cook32.rar)", "ET MALWARE Possible CopyKittens DNS Lookup (patch8-windows.com)", "ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (win .mirtonewbacker .com)", "ET MALWARE Observed DNS Query to EvilProxy Domain (msdnmail .net)", "ET MALWARE Kimsuky Related Domain in DNS Lookup", "ET ATTACK_RESPONSE Windows LMHosts File Download - Likely DNSChanger Infection", "ET ATTACK_RESPONSE Unusual FTP Server Banner (warFTPd)", "ET MALWARE Win32/Irafau Backdoor CnC Activity (POST)", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 14", "ET POLICY Microsoft user-agent automated process response to automated request", "ET MALWARE Operation EvilTraffic Initial Redirect M2", "ET MALWARE Win32/Infostealer.Snifula File Upload", "ET MALWARE Linux/ShellshockCampaign.DDOSBot Reporting IP", "ET MALWARE Suspicious user-agent (f**king)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (netstreamag .publicvm.com)", "ET MALWARE Cobalt Strike Malleable C2 Profile wordpress_ Cookie Test", "ET INFO PowerShell Hidden Window Command

	Common In Powershell Stagers M2", "ET MALWARE Netbounce User-Agent (Netbounce)", "ET MALWARE ProjectSauron Remsec DNS Lookup (we .q.tcow.eu)", "ET MOBILE_MALWARE [PTsecurity] Spyware.BondPath (PathCall/Dingwe) Check-in", "ET MALWARE Linux/Tsunami Remote Shell M2", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 9", "ET MALWARE Win32/ArmyOfUkraine Bot Activity", "ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M3", "ET MALWARE Bifrose Response from Controller", "ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check M3", "ET MALWARE Trojan.Proxy.Small.Z CnC Checkin", "ET MALWARE Alina User-Agent(Alina)", "ET MALWARE Windows netstat Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Win32/Spy.Socelars.S CnC Activity M3", "ET MALWARE Win32/Swizzor User-Agent (Swizz03r)", "ET MALWARE Subterranean Crimson Rat - GetInfo Command", "ET MALWARE Observed DNS Query to Budminer Domain (bulk .indonet .org)", "ET MALWARE SteamStealer DNS Lookup (steamdesktop)", "ET MALWARE MAGICHOUND-related DNS Lookup (ntg-sa .com)", "ET MALWARE ReverseRAT Activity (POST) M4", "ET MALWARE DarkComet-RAT server join acknowledgement", "ET WEB_CLIENT Evil JavaScript Injection Sep 29 2015", "ET USER_AGENTS Suspicious User-Agent (dBrowser CallGetResponse)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (down .downloadoneyoutube.co.vu)", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .kingdom .myddns .com)", "ET INFO JAVA - Java Archive Download By Vulnerable Client", "ET MALWARE Lyceum Golang HTTP Backdoor CnC Checkin", "ET MALWARE Covenant Framework HTTP Beacon", "ET MALWARE Trojan:Win32/WinLNK.APA!MTB Payload Request", "ET MALWARE Observed DNS Query to Budminer Domain (kilomier .2waky .com)", "ET INFO Obfuscated Eval String (Single Q) 2", "ET USER_AGENTS VPNFilter Related UA (Hakai/2.0)", "ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v1 Unicode", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (protect4juls .space in DNS Lookup)", "ET USER_AGENTS Suspicious User-Agent (Internet HTTP Request)", "ET MALWARE Subterranean Crimson Rat - Client Traffic", "ET MALWARE Win32/ProtonBot Stealer Activity", "ET MALWARE 000Stealer CnC Checkin", "ET MALWARE Possible Kelihos.F EXE Download Common Structure 2", "ET INFO Probably Evil Long Unicode string only string and unescape 3", "ET MALWARE Pingback Exec Command Issued", "ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement", "ET MALWARE Observed DNS Query to Budminer Domain (manated .dynamic-dns .net)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ccdata.txt) M2", "ET USER_AGENTS User-Agent (STEROID Download)", "ET MALWARE CCleaner Backdoor DGA Domain (ab8cee60c2d .com) Aug 2017", "ET MALWARE FakeAV Check-in purporting to be MSIE with invalid terse HTTP headers", "ET MALWARE Infostealer.Bancos Sending Stolen info SMTP", "ET EXPLOIT D-Link Remote Code Execution Attempt (CVE-2022-28958)", "ET MALWARE Bitter APT CHM CnC Activity M1 (GET)", "ET MALWARE DNS Query Possible Zbot Infection Query for networksecurityx.hopto.org", "ET MALWARE Win32/Sabsik.EN.D!ml CnC Checkin", "ET MALWARE Restylink Domain in DNS Lookup (youmiuri .com)", "ET USER_AGENTS Suspicious User-Agent (ms_ie) - Crypt.ZPACK Gen Trojan Downloader GET Request", "ET MALWARE x0Proto Pong", "ET MALWARE Win32/Neshta.A Posting Data", "ET MALWARE [401TRG] Observed Backdoor.SUNBURST CnC Domain (bigtopweb .com in TLS SNI)", "ET MALWARE Possible Malicious Macro DL BIN May 2016 (No UA)", "ET MALWARE Torpig Reporting User Activity (wur8)", "ET MALWARE Generic Downloader - HTTP POST", "ET MALWARE Legion Loader Activity Observed (satan)", "ET MALWARE ISMAgent DNS Tunneling (microsoft-publisher . com)", "ET MALWARE DNS Query Sykipot Domain rusview.net", "ET INFO Inbound PowerShell Checking for Virtual Host (Win32_Fan WMI)", "ET MALWARE Golang/Sandcat Plugin Activity (POST)", "ET MALWARE Drive Receiving POST2 DDoS instructions", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (globalnetworkissues .com)", "ET MALWARE Cryptowall 2.0 DL URI Struct Oct 2 2014", "ET MALWARE Observed DNS Query to Budminer Domain (Kmember .wikaba .com)", "ET MALWARE BePush/Kilim payload retrieval", "ET MALWARE DeathStalker APT Related Maldoc Activity (GET)", "ET

	MALWARE X-Files Stealer CnC Exfil Activity M1", "ET USER_AGENTS Suspicious User-Agent Detected (Downloader1.2)", "ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns", "ET USER_AGENTS Suspicious User-Agent (AutoHotkey)", "ET MALWARE Backdoor.Win32.Sykipot Put", "ET MALWARE Spora Ransomware DNS Query", "ET MOBILE_MALWARE Android.YzhcSms URL for Possible File Download", "ET USER_AGENTS Suspicious User-Agent (123)", "ET MALWARE Linux/Onimiki DNS trojan activity long format (Outbound)", "ET MALWARE MAGICHOUND.FETCH Retrieving Malicious PowerShell", "ET MALWARE TA444 Domain in DNS Lookup", "ET MALWARE Win32/TrojanDownloader.Waski.F Locker DL URI Struct Jul 25 2014", "ET MALWARE Possible Banload Downloading Executable", "ET MALWARE Suspected Zebrocy Downloader Traffic", "ET MALWARE Lazyscripter Related Activity (Inbound)", "ET MALWARE GreenDou Downloader User-Agent (hello crazyk)", "ET MALWARE Windows driverquery -v Microsoft Windows DOS prompt command exit OUTBOUND", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 13", "ET MALWARE Deathstalker/Evilnum Delivery Domain (bukjut11 .com) in TLS SNI", "ET MALWARE Scieron DNS Lookup (demon.4irc.com)", "ET MALWARE Observed DNS Query to Cobalt Strike Domain 2022-10-11 (pigahinilu .com)", "ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST) 3", "ET POLICY Terse Named Filename EXE Download - Possibly Hostile", "ET MALWARE JS/Cloud9 Domain (cloud-miner .de) in DNS Lookup", "ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2", "ET MALWARE Brute Ratel Fake User-Agent", "ET MALWARE Win32/Vermilion Stager Activity (GET)", "ET MALWARE Observed DNS Query to Budminer Domain (common .taiwan .twilightparadox .com)", "ET MALWARE Observed DNS Query to Ursnif Domain (dodsman .com)", "ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 1", "ET MALWARE SSL/TLS Certificate Observed (Get2 CnC)", "ET MALWARE Win32/a310Logger Variant Data Exfil via SMTP", "ET MALWARE Manjusaka CnC Server Response", "ET MALWARE Potential FakeAV HTTP GET Check-IN (/check)", "ET MALWARE Win32/Generik.BUTNSNA Checkin", "ET MALWARE Locky Intermediate Downloader", "ET DOS HOIC with booster outbound", "ET MALWARE Antinum HTTP Checkin", "ET MALWARE Backdoor Win32.Idicaf/Atraps", "ET MALWARE Malicious JS.Nemucod to PS Dropping PE Nov 14 M2", "ET MALWARE Observed DNS Query to TA455 Domain (microsoftedgesh .info)", "ET MALWARE Known Hostile Domain ant.trenz .pl Lookup", "ET MALWARE Aura Ransomware User-Agent", "ET MALWARE OSX/Mughthesec/SafeFinder/OperatorMac Rogue Search Engine DNS Query Observed", "ET MALWARE Possible IoT_reaper ELF Binary Request M1 (set)", "ET MALWARE Observed DNS Query to Budminer Domain (Kaccount .moneyhome .biz)", "ET MALWARE MSSQL maggie backdoor whoami Query Observed", "ET MALWARE Suspected Lazarus APT Related Activity (GET)", "ET MALWARE Win32/Nemty Ransomware Style Geo IP Check M1", "ET MALWARE MSIL/KeyRedirEx Banker Requesting Redirect/Inject List", "ET MALWARE Avzhan DDoS Bot User-Agent MyIE", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle CDN GET]", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M5", "ET MALWARE BIOPASS RAT Go Activity (GET)", "ET MALWARE DonotGroup Pult Downloader Activity (POST) M2", "ET MOBILE_MALWARE AdWare.AndroidOS.Ewind.cd Checkin", "ET MALWARE Win32.Riberow.A (listdir)", "ET INFO PowerShell NonInteractive Command Common In Powershell Stagers", "ET MALWARE Possible Gamaredon APT Related Malicious Shortcut Activity (GET)", "ET MALWARE Suspected PlugX Checkin Activity (GET)", "ET WEB_SERVER Observed FxCodeShell Web Shell Password", "ET WEB_CLIENT Fake Windows Security Warning - png", "ET MALWARE Swizzor-based Downloader - Invalid User-Agent (Mozilla/4.0 (compatible MSIE 7.0 na .NET CLR 2.0.50727 .NET CLR 3.0.4506.2152 .NET CLR 3.5.30729))", "ET MOBILE_MALWARE Android.Stealthgenie Checkin", "ET MALWARE CCleaner Backdoor DGA Domain (ab3d685a0c37 .com) Nov 2017", "ET MALWARE W32/Echmark CnC Activity M2", "ET MALWARE Win32/Voltron/Spectre Stealer CnC Activity (POST)", "ET MALWARE Backdoor.Win32.RShot Ping Outbound", "ET MALWARE Observed DNS Query to UNC3890 Domain (fileupload .shop)", "ET MALWARE SocGholish Domain in DNS Lookup", "ET WEB_SERVER ATTACKER WebShell - Weevely - Downloaded", "ET

	MALWARE Innostealer Domain in DNS Lookup (windows-11info .com)", "ET MALWARE LinPEAS Privilege Escalation Script Response (Without Banner)", "ET MALWARE Possible CopyKitten DNS Lookup (azurewebsites .tech)", "ET MALWARE Possible Inbound PowerShell via Invoke-PSImage Stego", "ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (bot update)", "ET MALWARE Win32/CONFUCIUS_B External IP Check to CnC M2", "ET MALWARE System Progressive Detection FakeAV (INTEL)", "ET MALWARE Possible Pegasus Related DNS Lookup (deportes24-7 .com)", "ET MALWARE MSIL/TrojanDownloader.Agent.KUO CnC Activity M1", "ET MALWARE Possible Pegasus Related DNS Lookup (twiitter .com.mx)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 12", "ET POLICY Possible Trojan File Download bad rar file header (not a valid rar file)", "ET POLICY Norton Update User-Agent (Install Stub)", "ET MALWARE Observed TA444 Domain (smbcgroup .us in TLS SNI)", "ET MALWARE Observed MageCart CnC Domain in TLS SNI", "ET MALWARE Urlzone/Bebloh Trojan Check-in", "ET MOBILE_MALWARE Android Marcher Trojan Download - BankAustria Targeting (set)", "ET MOBILE_MALWARE Android/GPlayed (sub1 .tdsworker .ru in DNS Lookup)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (11i .me)", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (true-crypte .website)", "ET MALWARE Possible CopyKittens DNS Lookup (wethearservice.com)", "ET CNC Feodo Tracker Reported CnC Server group 1", "ET MALWARE [PTsecurity] Adwind SSL Certificate Observed", "ET MOBILE_MALWARE Android/ShartBot CNC Domain (cdopea .store) in DNS Lookup", "ET MALWARE Tandem Espionage CnC Domain (zyzkikpfewuf .ru) in DNS Lookup", "ET MALWARE NoMercy Stealer CnC Checkin", "ET MALWARE CCleaner Backdoor DGA Domain (ab1145b758c30 .com) Sep 2017", "ET MALWARE Likely Malicious wininet UA Downloading EXE", "ET MALWARE Win32/WinDealer CnC Activity (Checkin)", "ET MALWARE Echelon/DarkStealer Variant CnC Exfil", "ET MALWARE Win32/Emotet CnC Activity (POST) M10", "ET MALWARE Quasar CnC Domain in DNS Lookup", "ET MALWARE Haxdoor Reporting User Activity", "ET MALWARE Poebot Related User Agent (SPM_ID=)", "ET MALWARE Observed MageCart Group 12 Domain (toolser .pw in TLS SNI)", "ET MALWARE Win32/PurpleWave Stealer CnC Exfil", "ET MALWARE TrojanSpy.KeyLogger.acqh User-Agent(EMSFRTCBVD)", "ET MALWARE Possible Win32/SillyFDC WordPress Traffic", "ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .crmdev .org)", "ET MALWARE Embedded ZIP/APK File With Fake Windows Executable Header - Possible AV Bypass Attempt", "ET CNC Feodo Tracker Reported CnC Server group 11", "ET MALWARE Dark Halo/SUNBURST CnC Domain (kubecloud .com in TLS SNI)", "ET MALWARE Ponmocup HTTP Request (generic) M1", "ET MALWARE Linux/dtool IRC Command (CHSERVER)", "ET MALWARE Observed DNS Query to Pegasus Domain", "ET MALWARE AlphaCrypt Connectivity Check 1", "ET MALWARE Perfect Keylogger Install Email Report", "ET EXPLOIT HT SWF Exploit RIP M2", "ET EXPLOIT SolusVM 1.13.03 Access to solusvmc-node setuid bin", "ET MALWARE W32.Virut.A joining an IRC Channel", "ET MALWARE OSX/WireLurker User-agent (globalupdate)", "ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (greenblguard .shop)", "ET MALWARE Cobalt Strike X-Client Header (notevil)", "ET MALWARE Observed DNS Query to Budminer Domain (kdbb .ourhobby .com)", "ET MALWARE Win32/Atraps Receiving Config via Image File (steganography)", "ET MALWARE APT Operation Sidecopy lnk Activity (GET)", "ET MALWARE Powershell with Decimal Encoded RUNPE Downloaded", "ET MALWARE Vidar Stealer IP Address in DNS Query Response", "ET MALWARE Smokeloader getsock Command", "ET MALWARE Trojan Downloader.Bancos Reporting", "ET MALWARE Win32/VBS.Sload Activity (GET)", "ET INFO possible .jpg download by VBA macro", "ET MALWARE SysJoker Related Domain in DNS Lookup (bookitlab .tech)", "ET MALWARE Trojan Downloader User-Agent (Tiny)", "ET WEB_CLIENT Malicious Chrome Extension Domain Request (nyoogle .info in DNS Lookup)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 10", "ET MALWARE Observed DNS Query to Budminer Domain (centers .allowed .org)", "ET MALWARE Observed TA444 Domain (azure-protection .cloud in TLS SNI)", "ET MALWARE Observed DNS Query to TA444 Domain (mizuhogroup .us)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Google Chrome.txt)

	M2", "ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 3", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice GET]", "ET MALWARE W32/Asprox.FakeAV Affiliate Second Stage Download Location Request", "ET MALWARE Win32/DanijBot User-Agent", "ET MALWARE Andromeda Check-in Response", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Stager 2]", "ET MALWARE TA402/Molerats Related VBS Retrieval", "ET MALWARE Gamaredon Maldoc Activity (GET)", "ET MALWARE Hangover related campaign Response", "ET MALWARE W32/Badur.Spy User Agent lawl", "ET MALWARE SocGholish Domain in DNS Lookup (extcourse .zurvio .com)", "ET MALWARE MageCart Exfil URI", "ET MALWARE Android/AhMyth RAT Command Inbound (Camera Manager)", "ET MALWARE Suspected Gamaredon Downloader Activity", "ET MALWARE Suspicious Email Attachment Possibly Related to Mydoom.L@mm", "ET ATTACK_RESPONSE Unusual FTP Server Banner (fuckFtpd)", "ET WEB_SERVER DNS Query for Suspicious e5b57288.com Domain - Anuna Checkin - Compromised PHP Site", "ET MALWARE Knockbot Proxy Response From Controller (empty command)", "ET MALWARE Win32.Riberow.A (fsize)", "ET MALWARE Possible MSIL/Solorigate.G!dha/SUPERNOVA Webshell Access Request", "ET MALWARE Observed DNS Query to Budminer Domain (asia .publiccosplay .org)", "ET MALWARE Win32/Ascrirac .onion proxy Domain (5sse6j4kdaeh3yus)", "ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (gaymers .ax)", "ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M3", "ET MALWARE Win32/NetDooka Framework RAT Sending Session ID", "ET MALWARE Ransomware/Cerber Onion Domain Lookup", "ET MALWARE VBulletin Backdoor CMD inbound", "ET MALWARE Danabot UA Observed", "ET MALWARE Observed Karen Ransomware CnC Checkin", "ET INFO Java Serialized Data via vulnerable client", "ET WEB_CLIENT Possible Malicious Redirect 8x8 script tag URI struct", "ET MALWARE Fake Software Download Redirect Leading to Malware M1", "ET MALWARE MSIL/Crimson Receiving Command (folders list)", "ET MALWARE Observed TA444 Domain (bankofamerica .nyc in TLS SNI)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 24", "ET USER_AGENTS VPNFilter Related UA (curl53)", "ET MALWARE Faked Russian Opera UA without Accept - probable downloader", "ET MALWARE Possible Win32/Dimegup.A Downloading Image Common URI Struct", "ET MALWARE Possible W32/KanKan tools.ini Request", "ET MALWARE TrochilusRAT DNS Lookup (security-centers.com)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (everyavenuetravel .site)", "ET USER_AGENTS Suspicious User-Agent (RBR)", "ET MALWARE Win32/Lilith Stealer getCommands Command", "ET MALWARE Win32/PurpleFox Retrieving File (GET)", "ET POLICY CCProxy in use remotely - Possibly Hostile/Malware", "ET MALWARE Known Sinkhole Response Header CERT.PL", "ET MALWARE [PTsecurity] Tinba (Banking Trojan) Check-in", "ET MALWARE Java/QRat Retrieving PE", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 6", "ET MALWARE Observed DNS Query to Budminer Domain (google .apchnetinfo .com)", "ET SCAN Hikvision DVR attempted Synology Recon Scan", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn1 .com)", "ET MALWARE Observed DNS Query to Budminer Domain (stonekiki .freeddns .com)", "ET MALWARE Observed Malicious Domain Targeting Minority Groups (officemodel .org in TLS SNI)", "ET MALWARE DDoS.Win32.Agent.bay Variant Covert Channel (VERSONEX)", "ET MALWARE Gameredon Loader Activity", "ET MALWARE Godlua Backdoor Stage-3 Server Heartbeat Reply (Sep 2020 - Nov 2023)", "ET MALWARE Possible Kimsuky Related Download", "ET MALWARE Comfoo Outbound Communication", "ET MALWARE Vobfus Check-in", "ET MOBILE_MALWARE NSO Related Domain 14", "ET MALWARE ChaChi RAT Server Response", "ET WEB_CLIENT CookieBomb Generic PHP Format", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 5", "ET WEB_CLIENT DRIVEBY Social Engineering Toolkit JAR Download", "ET MALWARE MSIL/Spy.Agent.CVT CnC Exfil", "ET MALWARE SysJoker Dropper Related Domain in DNS Lookup (github .url-mini .com)", "ET MALWARE Potential Juniper Reflected XSS Attempt (CVE-2022-22242)", "ET MALWARE Possible Puzzlemaker Remote Shell Activity (GET)", "ET MALWARE Trojan-Downloader Win32.Genome.AV", "ET MALWARE DNS Query Sykipot Domain

	insdet.com", "ET MALWARE Observed DNS Query to Budminer Domain (dirco .jetos .com)", "ET MALWARE Win32/LingyunNet.A Heartbeat", "ET MALWARE Observed DNS Query to Budminer Domain (news .rockspace .wang)", "ET MALWARE Stuxnet index.php", "ET MALWARE Wintervivern Checkin", "ET MALWARE BlackGuard_v2 Data Exfiltration Observed", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Steam_htmlcache.txt)", "ET MALWARE Possible BlackEnergy Accessing SMB/SMB2 Named Pipe (ASCII)", "ET MALWARE GravityRAT CnC Domain (savitabhabi .co .in in DNS Lookup)", "ET MALWARE Bitter APT AlmondRAT CnC Checkin", "ET MALWARE TA402/Molerats CnC Checkin", "ET MALWARE Win32/Sehyioa Variant Activity (POST)", "ET MALWARE Possible ICMP Backdoor Tunnel Command - whoami", "ET MALWARE Confucious APT CnC Checkin", "ET MALWARE SSL/TLS Certificate Observed (DiplomatLoader)", "ET MALWARE Possible PDF Dictionary Entry with Hex/Ascii replacement", "ET MALWARE Win32/Tiggre Variant Activity Sending System Files (POST)", "ET MALWARE Observed DNS Query to Budminer Domain (sacstartapples .mohwfreshman1 .otzo .com)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 12", "ET MALWARE ELF/Emptiness v2 XOR Exec Command Inbound", "ET MALWARE DonotGroup Related Domain in DNS Lookup (grapehister .buzz)", "ET MALWARE TA402/Molerats Payload Downloaded", "ET MALWARE ELF/Mirai Variant UA Outbound (Yakuza)", "ET MALWARE Backdoor.Win32.DarkComet Keepalive Inbound", "ET MALWARE Observed Godlua Backdoor Domain (d .cloudappconfig .com in TLS SNI)", "ET MALWARE Observed DNS Query to TA455 Domain (googleupdate .co)", "ET MALWARE Pegasus Domain in DNS Lookup (al-taleanews .net)", "ET MALWARE Win64/Agent.BP System Info Exfil", "ET MALWARE Win32/Packed.Themida.AAL Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (tpp .otzo .com)", "ET USER_AGENTS Suspicious User-Agent (up2dash updater)", "ET WEB_CLIENT Inbound JS with Possible 1px-1px Exfiltration Image", "ET MALWARE General Trojan Downloader", "ET MALWARE Observed Magecart Skimmer Domain (googie-analytics .online in TLS SNI)", "ET MALWARE Suspected Cobalt Strike Beacon Activity (DNS)", "ET MALWARE Win32/Unknown CnC Activity", "ET MALWARE [Fireeye] Backdoor.BEACON M3", "ET MALWARE ABUSE.CH TorrenLocker Payment Domain Detected", "ET MOBILE_MALWARE NSO Related Domain 35", "ET MOBILE_MALWARE Android Spy APT-C-23 (amanda-hart .website in TLS SNI)", "ET EXPLOIT Possible 2012-1533 altjvm RCE via JNLP command injection", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Mozilla_Firefox_Cookies) M1", "ET MALWARE DPRK APT Related Maldoc Activity (POST)", "ET MALWARE User-Agent in Referer Field - Likely Malware", "ET MALWARE Observed DNS Query to Budminer Domain (rfvg .karlosb .com)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ProcessInfo_Log.txt) M1", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (kalpoipolpmi .net)", "ET WEB_SERVER WebShell - ASPyder - File Browser - Interface", "ET MALWARE Win32/VB.PNU CnC Checkin", "ET MALWARE Ruskill/Palevo Download Command", "ET MALWARE Trojan.BlackRev Download Executable", "ET MALWARE Win32/Blacktech Plead CnC Activity (POST)", "ET MALWARE Sidewinder Stage 2 VBS Downloader Reporting Successful Infection", "ET POLICY User-Agent Recuva (Recuva)", "ET MALWARE Observed DNS Query to Budminer Domain (qtwlkszb .dynamicdns .org .uk)", "ET MALWARE W32.Netwire Connectivity Check", "ET MALWARE CopperStealer - Remote Desktop - Task Request", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadlog .linkpc.net)", "ET MALWARE RKO Remote File Upload Attempt", "ET USER_AGENTS suspicious user agent string (CholTBAgent)", "ET MALWARE Arkei/Vidar/Mars Stealer Variant CnC checkin commands", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (proxy .oracleapps .org)", "ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check M2", "ET MALWARE VBKlip/ClipBanker.P Status Update", "ET MALWARE Legion Loader Activity Observed (salmonella-symptome)", "ET MALWARE TorrentLocker DNS Lookup (updatemyhost.ru)", "ET MALWARE ELF/Mirai Variant UA Outbound (Hentai)", "ET MALWARE Probable OneLouder downloader (Zeus P2P)", "ET MALWARE Possible CopyKitten DNS Lookup (owa-microsoft .online)", "ET MALWARE CIA Ransomware Domain (cia .cookie-coin .xyz) in DNS Lookup", "ET MALWARE

	Win32/TrojanDownloader.AutoHK.MT CnC Checkin", "ET POLICY Monero Mining Pool DNS Lookup", "ET MALWARE BF Botnet CnC Checkin", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (zupertech .com in TLS SNI)", "ET MALWARE [PTsecurity] Win32/TinyNuke Payload ACF40 Inbound", "ET MALWARE Possible OSX/SHLAYER Checkin M2", "ET MALWARE LokiBot Keylogger Data Exfiltration Detected M1", "ET MALWARE MSIL/Crimson Receiving Command (files list)", "ET MALWARE DNS Reply Sinkhole - Microsoft - 131.253.18.11-12", "ET MALWARE Win32/FlyStudio.OJJ CnC Checkin", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (nod-update .it)", "ET MALWARE SocGholish Domain in DNS Lookup (people .fl2wealth .com)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 16", "ET MALWARE [401TRG] SUNBURST Related DNS Lookup to bigtopweb .com", "ET MALWARE DarkComet-RAT Client Keepalive", "ET MALWARE LokiBot User-Agent (Charon/Inferno)", "ET MALWARE Screenblaze SCR Related Backdoor - GET", "ET MALWARE Generic Stealer Config from Server", "ET MALWARE Observed DNS Query to TA444 Domain (edit .wpsonline .co)", "ET MALWARE MalDoc Retrieving msiexec Commands via DNS TXT", "ET WEB_CLIENT Fake 404 With Hidden Login Form", "ET MALWARE BlackTech Plead Encrypted Payload Inbound", "ET MALWARE Cryptowall .onion Proxy Domain", "ET MALWARE TA410 APT FlowCloud Hardcoded Request (POST)", "ET MALWARE Win32/Screenshotter Backdoor Payload Request (GET)", "ET MALWARE FAKEIE Minimal Headers (flowbit set)", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 9", "ET MALWARE Win32/Agent.USB Variant CnC Activity", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 3", "ET MALWARE APT29/CloakedUrsa Google Drive Authentication (POST)", "ET MALWARE Possible Duqu 2.0 Request", "ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (bukjut11 .com)", "ET MALWARE Possible Zendran ELF IRCBot Joining Channel", "ET MOBILE_MALWARE NSO Related Domain 37", "ET MALWARE Win32/JSWORM Ransomware Style Geo IP Check M1", "ET MALWARE Observed DNS Query to Budminer Domain (sci .dns1 .us)", "ET MOBILE_MALWARE Arid Viper (samehnew-10a7c .appspot .com in DNS Lookup)", "ET MALWARE Observed DNS Query to Comm100 Trojan Domain (windowstearns .com)", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (sharpion .org in DNS Lookup)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (ysl .jxwan .com)", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to thedoccloud .com", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (plastic .delldrivers .in)", "ET MALWARE W32/StealRat.SpamBot Email Template Request", "ET MALWARE Clipsa Stealer - Exfiltration Activity", "ET MALWARE CCleaner Backdoor DGA Domain (aba9a949bc1d .com) Mar 2017", "ET MALWARE Win32/H0lyGh0st Ransomware CnC Activity (GET Public Key)", "ET HUNTING SUSPICIOUS Possible WebShell Login Form (Outbound)", "ET MALWARE Possible Upatre Downloader SSL certificate", "ET MALWARE Observed Trojan.Verblecon Related Domain (gaymers .ax in TLS SNI)", "ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate16.com)", "ET MALWARE Observed DNS Query to Budminer Domain (symantec .apchnetinfo .com)", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to webcodez .com", "ET WEB_SERVER WebShell - GODSPy - Auth Creds", "ET MALWARE Skyfall fake Skype install link", "ET MALWARE Wapack Labs Sinkhole DNS Reply", "ET USER_AGENTS Suspicious User-Agent (msIE 7.0)", "ET POLICY trymedia.com User-Agent (Macrovision_DM)", "ET MALWARE Operation EvilTraffic Initial Redirect M1", "ET USER_AGENTS Suspicious User-Agent (Hello World)", "ET WEB_SERVER c99 Shell Backdoor Var Override Client Body", "ET MALWARE Woody RAT Payload Delivery Domain (garmandesar .duckdns .org) in DNS Lookup", "ET MALWARE Observed TraderTraitor Domain (aideck .net) in TLS SNI", "ET MALWARE Observed DNS Query to Budminer Domain (economy .ServeUser .com)", "ET MOBILE_MALWARE Arid Viper (calculator-1e016 .firebaseio .com in DNS Lookup)", "ET MALWARE Win32/WindowsDefender Bypass Download Request", "ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 3", "ET MALWARE Netbounce Proxy User-Agent (idk)", "ET MALWARE System Progressive Detection FakeAV (AMD)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (allmyad .com)", "ET MALWARE Observed Ursnif Domain in TLS SNI (gigimas .xyz)", "ET

	WEB_CLIENT Possible Injected JS Form Stealer Checking Page Contents M2", "ET MALWARE Iron Tiger HTTPBrowser DNS Lookup (trendmicro-update.org)", "ET USER_AGENTS MSIL/Peppy User-Agent", "ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (purple .m-ads .net in DNS Lookup)", "ET MALWARE PlugX DNS Lookup (mailsecurityservice.com)", "ET EXPLOIT Eir D1000 Modem CWMP Exploit RCE", "ET MALWARE Possible Adwind/jSocket SSL Cert (assylias.Inc)", "ET ATTACK_RESPONSE python shell spawn attempt", "ET MALWARE Win32.Virut - GET", "ET MALWARE Observed DNS Query to TA455 Domain (getadobe .net)", "ET USER_AGENTS Suspicious User-Agent (Mozil1a)", "ET MALWARE DonotGroup Template Download", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (udo .jxwan .com)", "ET MALWARE Observed DNS Query to TA444 Domain (ledger-cloud .com)", "ET USER_AGENTS MacShield User-Agent Likely Malware", "ET USER_AGENTS Suspicious User-Agent (Loands) - Possible Trojan Downloader GET Request", "ET WEB_SPECIFIC_APPS Wordpress Slideshow Gallery 1.4.6 - Shell Upload", "ET MALWARE Observed DNS Query to Budminer Domain (pic-yahoo .ddns .us)", "ET MALWARE Various Malicious AlphaNum DL Feb 10 2016", "ET POLICY URL Shortener Service Domain in DNS Lookup (tiny .cc)", "ET MALWARE Win32/Bisonal DNS Lookup 1", "ET MALWARE Possible Dridex Download URI Struct with no referer", "ET MALWARE ZeroLocker Downloading Config", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 16", "ET WEB_SERVER Possible CVE-2016-5118 Exploit MVG attempt M1", "ET MALWARE TransparentTribe Related CnC Activity", "ET MALWARE Possible CopyKitten DNS Lookup (trendmicro .tech)", "ET MALWARE Linux/Tsunami Remote Shell M1", "ET MALWARE Blackmoon/Banbra Configuration Request M2", "ET USER_AGENTS Long Fake wget 3.0 User-Agent Detected", "ET MOBILE_MALWARE Android Trojan Cloudsota HTTP Host", "ET MALWARE Solarbot Check-in", "ET MALWARE Kuluoz Activity", "ET MALWARE Wintervivern Activity (GET)", "ET MALWARE Observed Pegasus Domain (hooklevel .com in TLS SNI)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DEMO)", "ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 23", "ET USER_AGENTS Suspicious User-Agent (xr - Worm.Win32.VB.cj related)", "ET MALWARE Possible CopyKittens DNS Lookup (cacheupdate14.com)", "ET MALWARE Possible JKDDOS download cl.exe", "ET MALWARE Observed DNS Query to TA455 Domain (online-chess .live)", "ET MALWARE Observed DNS Query to IcedID Domain (acehphonnajaya .com)", "ET MALWARE HTTP Request for Possible ELF/LiLocked Ransomware Note", "ET MOBILE_MALWARE Apple iPhone Implant - Boundary Observed", "ET MALWARE APT34 Related DNS Tunneling Activity", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher DNS Lookup", "ET MALWARE Fodcha Botnet Style DNS Server Lookup", "ET MALWARE Win32/Vidar Variant/Mars CnC Activity (GET)", "ET MALWARE W32/DownloaderAgent.fajk Second Stage Download List Requested", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (smartsftp .pw)", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 1", "ET MALWARE Observed DNS Query to Budminer Domain (wlksbb .MrsLove .com)", "ET MALWARE Gamaredon Information Stealer Data Exfiltration Attempt", "ET MALWARE OSX/WizardUpdate CnC Activity", "ET USER_AGENTS Suspicious User-Agent (MYURL)", "ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (h4ck .cfd in TLS SNI)", "ET MALWARE Anuna PHP Backdoor Sucessful Exploit", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (newsforward .quest)", "ET MOBILE_MALWARE NSO Related Domain 1", "ET MALWARE Win32/Arkei Stealer CnC Checkin (GET)", "ET MOBILE_MALWARE Android/FakeWallet.D Activity (GET)", "ET MALWARE 404/Snake/Matiex Keylogger Style External IP Check", "ET MALWARE GravityRAT CnC Domain (titaniumx .co .in in DNS Lookup)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 2", "ET MALWARE Observed IcedID Domain (80frontluzkher .xyz in TLS SNI)", "ET MALWARE CCleaner Backdoor DGA Domain (abccc097dbc0.com) Sep 2018", "ET MALWARE HawkEye Keylogger FTP", "ET HUNTING FTP CWD to windows system32 - Suspicious", "ET WEB_SERVER Insomnia Shell HTTP Request", "ET MALWARE GravityRAT CnC Domain (click2chat .org in DNS Lookup)", "ET MALWARE Possible

	Andromeda download with fake Zip header (2)", "ET MALWARE Win32/Voltron/Spectre Stealer Sending OS Information (POST)", "ET MALWARE Observed DNS Query to Hilal RAT Domain (market .dedyn .io)", "ET POLICY DNS Query to .onion proxy Domain (onion.guide)", "ET MALWARE Observed DNS Query to Budminer Domain (biz .pcanywhere .NET)", "ET MALWARE Win32/Avaddon Ransomware Style External IP Address Check", "ET INFO Inbound PowerShell Checking for Virtual Host (Win32_BaseBoard WMI)", "ET POLICY .onion proxy Domain (onion .plus in DNS Lookup)", "ET ATTACK_RESPONSE JS/Comm100 Trojan Backdoor Inbound", "ET MALWARE Golang/Kaos/YamaBot CnC Activity M2 (POST)", "ET MALWARE Qtloader encrypted check-in Oct 19 M1", "ET WEB_SERVER open_basedir PHP config option in uri", "ET MALWARE VBS/Kimsuky.O Host Fingerprint Exfil", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M10", "ET MALWARE Revoyem Ransomware Activity", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (seobundlekit .com)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (worldchangeos .com)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle USAToday Server]", "ET HUNTING SUSPICIOUS .exe Downloaded from SVN/HTTP on GoogleCode", "ET MALWARE Shady RAT Retrieve and Execute Command", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 4", "ET MALWARE Win32/ChromeBack Browser Hijacker (getAd)", "ET MALWARE Win32/TrojanDownloader.Wauchos.A CnC Activity", "ET MALWARE Downloader.Win32.Adload (KaiXin Payload) Config Download", "ET MALWARE Win32/Ruckguv.A Requesting Payload", "ET MALWARE Tandem Espionage CnC Domain (dwrfqitgvmqn .ru) in DNS Lookup", "ET MALWARE Scarlet Mimic DNS Lookup 46", "ET MALWARE TeslaCrypt/AlphaCrypt Payment DNS Lookup", "ET MALWARE FastPOS RAM Scraper Sending Details", "ET MALWARE Win32/BazarLoader Activity (GET)", "ET MALWARE Win32/Agent.Fish Data Exfiltration", "ET POLICY DNS Query to .onion proxy Domain (torroadsters.com)", "ET MALWARE Common Zbot EXE filename Dec 09 2013", "ET MALWARE Mimikatz x64 Executable Download Over HTTP", "ET MALWARE Kimsuky Related Host Data Exfil", "ET MALWARE Spy/Infostealer.Win32.Embed.A Client Traffic", "ET MALWARE Vawtrak/NeverQuest - Post Data Form 01", "ET MALWARE SQUIRRELWAFFLE Loader Activity (POST)", "ET MALWARE Win32/Blacktech Plead CnC Activity (GET)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (info .payamradio .com)", "ET MOBILE_MALWARE iOS/Xsser sending files", "ET POLICY DNS Query to .onion proxy Domain (onion.city)", "ET MALWARE Win32/Gatak Activity", "ET MALWARE Observed DNS Query to TA444 Domain (docs .azurehosting .co)", "ET MALWARE Pegasus Domain in DNS Lookup (arabia-islamion .com)", "ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (purple .itraffic .click in DNS Lookup)", "ET MALWARE Win32/Neurevt.A/Betabot Check-in 4", "ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (WinInet)", "ET MALWARE ELF/Kinsing Payload Request M2", "ET MALWARE Possible ReactorBot .bin Download", "ET MALWARE Lazarus Related Maldoc Activity", "ET MALWARE Possible TA410 APT FlowCloud Dependency Download", "ET MOBILE_MALWARE Android/Koler.C Checkin", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to globalnetworkissues .com", "ET MALWARE Possible Windows executable sent when remote host claims to send a Text File", "ET MALWARE Possible IoT_reaper ELF Binary Request M2 (set)", "ET MALWARE Tandem Espionage CnC Domain (sinelnikovd .ru) in DNS Lookup", "ET MALWARE TA404/Zinc Trojanized KiTTY CnC Checkin", "ET MALWARE Observed DNS Query to Certishell Domain (sivpici .php5 .sk)", "ET MALWARE Inbound JasperLoader Using Array Push Obfuscation", "ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (session cookie delete)", "ET MALWARE LokiBot Screenshot Exfiltration Detected", "ET MALWARE Possible CopyKittens DNS Lookup (windows-drive20.com)", "ET MALWARE WRAT Dropper (TLS SNI)", "ET MALWARE Observed DNS Query to Hyperion Obfuscator Domain (plague .fun)", "ET MALWARE IceApple User-Agent observed", "ET MALWARE ProxyBox - ProxyBotCommand - I_AM", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to databasegalore .com", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(smaal)", "ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 1", "ET MALWARE ELF/muBoT IRC Activity 2", "ET MALWARE

	Win32/SaintStealer Data Exfiltration Attempt M2", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (wh47f2as19.com)", "ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 3)", "ET MALWARE NewPosThings Data Exfiltration", "ET MALWARE Gamaredon APT Maldoc Related Activity (POST)", "ET MALWARE ELF/Emptiness v1.1 DNS Flood Command Inbound", "ET MALWARE Possible Pegasus Related DNS Lookup (turkishairines .info)", "ET MALWARE EUPUDS.A Requests for Boleto replacement", "ET MALWARE SmokeLoader - Init 0x", "ET MOBILE_MALWARE Android Spy APT-C-23 (javan-demsky .website in TLS SNI)", "ET MALWARE Possible Winnti-related DNS Lookup", "ET MALWARE Observed GandCrab Ransomware Domain (chlenaverasiskihe .sex in DNS Lookup)", "ET MALWARE Sidecopy APT Related Backdoor Activity", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (mail .irir .org)", "ET MALWARE Filename explorer.exe Download - Common Hostile Filename", "ET MALWARE Powershell commands sent B64 1", "ET EXPLOIT Possible ETERNALROMANCE MS17-010 Heap Spray", "ET MALWARE SocGholish Domain in DNS Lookup (festival .robingaster .com)", "ET POLICY Software Install Reporting via HTTP - Wise User Agent (Wise) Sometimes Malware Related", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original GET]", "ET MALWARE Possible Zeus GameOver Connectivity Check", "ET MALWARE Win32/Zemot Config Download", "ET MALWARE Possible WannaCry DNS Lookup 4", "ET MALWARE eCh0raix/QNAPCrypt Requesting Key/Wallet/Note", "ET USER_AGENTS Suspicious user agent (asd)", "ET MALWARE Win32/MultiPasswordRecovery.A cs-crash PWS", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M3", "ET MALWARE ATTACKER IRCBot - PRIVMSG Response - ipconfig command output", "ET MALWARE Observed DNS Query to Budminer Domain (bnhxalex .organiccrap .com)", "ET MALWARE Possible Winnti-related DNS Lookup (css .google-statics .com)", "ET MALWARE Win32/PrivateLoader Related Domain in DNS Lookup (fouratlinks .com)", "ET MALWARE W32/Goolbot.E Checkin UA Detected iamx", "ET MALWARE Restylink Domain in DNS Lookup (differentfor .com)", "ET WEB_SERVER WebShell - ASPyder - File Create - POST Structure", "ET WEB_CLIENT Possible CookieBomb Generic JavaScript Format", "ET MALWARE SC-KeyLog Keylogger Installed - Sending Initial Email Report", "ET MALWARE Likely Evil Macro EXE DL mar 15 2016", "ET MALWARE Scarlet Mimic DNS Lookup 44", "ET MALWARE Win32/Delf.UUW CnC Keep-Alive", "ET MALWARE Observed DNS Query to Budminer Domain (big .qpoe .com)", "ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor Module Download Request", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access takeCameraPicture", "ET MALWARE EXE Download When Server Claims To Send Audio File - Must Be Win32", "ET MALWARE SunOrcal Reaver Domain Observed (olinaodi .com) in DNS Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (google .ddns .name)", "ET MALWARE Echelon/DarkStealer Variant CnC Exfil M2", "ET MALWARE Observed DNS Query to Budminer Domain (k1fsc .ax .lt)", "ET MALWARE TROJAN Win32-WebSec Reporting", "ET MALWARE PolyglotDuke Domain Observed", "ET P2P zzima_loader", "ET MALWARE Lazarus APT Related Domain in DNS Lookup (professiondesc .com)", "ET MALWARE Possible Pegasus Related DNS Lookup (bahrainsms .co)", "ET MALWARE Observed Ursnif Domain in TLS SNI (fineg .xyz)", "ET MOBILE_MALWARE Observed Android/IRATA Domain (rimot-anitain .tk) in TLS SNI", "ET MALWARE ELF/DarkNexus User-Agent", "ET MALWARE Observed Magecart Skimmer Domain (googie-analytics .website in TLS SNI)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (safara .sytes.net)", "ET ATTACK_RESPONSE 401TRG Perl DDoS IRCBot File Download", "ET MALWARE ELF/Mirai Variant UA Inbound (b3astmode)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b Apps List Exfil", "ET MALWARE MZRevenge Ransomware CnC", "ET MALWARE Blaze/Supreme Bot Activity", "ET WEB_SERVER WebShell - Pouya - Pouya_Server Shell", "ET MALWARE SocGholish Domain in DNS Lookup (consultant .meredithklemmblog .com)", "ET MALWARE OpenSSH in ICMP Payload - Possible Covert Channel", "ET MALWARE AHK.CREDSTEALER.A MalDoc Retrieving Payload", "ET MALWARE Alina Server Response Code", "ET MOBILE_MALWARE NSO Related Domain 15", "ET MALWARE Dark Halo/SUNBURST CnC Domain (lcomputers .com in TLS SNI)", "ET MALWARE Possible IceRat CnC Acitivty", "ET MALWARE Malicious XLS DDE rar Drop

	Fake 404 Response", "ET MALWARE DonotGroup Related Domain in DNS Lookup (officeframework .online)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(bugmaal)", "ET MALWARE W32/Woai.Dropper Config Request", "ET INFO AutoIt User-Agent Downloading ZIP", "ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3", "ET MALWARE APT29/CloakedUrsa Related Domain in DNS Lookup (techspaceinfo .com)", "ET MALWARE DNS Query for Operation Cleaver Domain", "ET MALWARE Deep Panda Downloader User-Agent (mozilla_horizon) GET request observed", "ET MALWARE Sality - Fake Opera User-Agent (Opera/8.89)", "ET INFO JAVA - Java Archive Download", "ET MALWARE Likely Bot Nick in IRC ([country|so version|CPU])", "ET MALWARE LinPEAS Privilege Escalation Script Response (With Banner)", "ET MALWARE MosesStaff APT Related Activity (POST)", "ET MALWARE MiniDuke Domain Observed", "ET MALWARE Win64/TrojanDownloader.Age Download Activity (GET)", "ET MALWARE Predator Pain Sending Data over SMTP", "ET MALWARE Observed DNS Query to UNC3890 Domain (xxx-doll .com)", "ET MOBILE_MALWARE Android Dropper Checkin Activity (POST)", "ET MALWARE GoBrut/StealthWorker Requesting Brute Force List (flowbit set)", "ET MALWARE Emotet Certificate Observed M2", "ET MALWARE BazaLoader Activity (GET)", "ET MALWARE SocGholish Domain in DNS Lookup (internship .ojul .com)", "ET MALWARE Observed DNS Query to TA455 Domain (googleservices .co)", "ET MALWARE Downloader/Linux.Agent CnC Domain (pateu .freevar .com) in DNS Lookup", "ET MALWARE PyPI Malicious Library Update Payload Checkin", "ET MALWARE Trojan.Bayrob Keepalive", "ET MALWARE Observed DNS Query to Budminer Domain (twmis .twgogo .org)", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 4", "ET MALWARE Observed DNS Query to Budminer Domain (update .madacity .top)", "ET MALWARE Likely Trojan Multi-part Macro Download M1", "ET MALWARE Win32/Shuckworm CnC Exfil M2", "ET MALWARE Win32/TyphonReborn Telegram CnC Checkin", "ET MALWARE FastPOS Sending Keystrokes", "ET MALWARE Observed DNS Query to Budminer Domain (healths .jumpingcrab .com)", "ET WEB_CLIENT Volexity - JS Sniffer Data Theft Beacon Detected", "ET MALWARE NetWire Variant - Server Directory Listing Request", "ET MALWARE Malicious XLS DDE rar Drop Attempt (.live)", "ET MALWARE Linux DarkRadiation Ransomware Activity Attack Check", "ET MALWARE Win32/Pteranodon CnC Exfil (POST)", "ET MALWARE Blackbeard Check-in", "ET MALWARE Win32/Gomorrah Stealer Data Exfiltration", "ET INFO Obfuscated Eval String (Single Q) 5", "ET CNC Feodo Tracker Reported CnC Server group 8", "ET MALWARE Observed Win32/CollectorStealer User-Agent M2", "ET HUNTING Suspicious Possible Process Dump in POST body", "ET MALWARE Scieron DNS Lookup (autocar.ServeUser.com)", "ET MALWARE Malicious VBS Sending System Information (POST)", "ET MALWARE ELF/Emptiness v1 DNS Flood Command Inbound", "ET USER_AGENTS Suspicious User-Agent (Our_Agent)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (glamorousfeeds .com)", "ET MALWARE ReverseRAT Activity (POST) M1", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (wijariief .space in DNS Lookup)", "ET MALWARE Magecart Skimmer Websocket Domain in DNS Lookup", "ET MALWARE W32.Berbew Check-in", "ET MALWARE CSharp SMB Scanner Assembly in PowerShell Inbound M2", "ET MALWARE Win32/Fujacks Activity", "ET MALWARE MyKings Bootloader Variant Requesting Payload M1", "ET EXPLOIT Possible CVE-2016-2209 Symantec PowerPoint Parsing Buffer Overflow M2", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 6", "ET MALWARE [Fireeye] Observed SUNBURST DGA Request", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 5", "ET MALWARE Spytector Domain (mail .spytector .com) in TLS SNI", "ET MALWARE Successful CargoBay Exfil", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 9", "ET MALWARE HB_Banker16 Get", "ET MALWARE Win32/MagicRAT CnC Activity M2", "ET MALWARE Possible SharpShooter Framework Generated Script", "ET MALWARE Observed GandCrab Ransomware Domain (carder .bit in DNS Lookup)", "ET CURRENT_EVENTS [Fireeye] HackTool.UDP.Rubeus.[nonce]", "ET SCAN Internal Dummy Connection User-Agent Inbound", "ET USER_AGENTS Suspicious User-Agent (Mozilla/3.0 (compatible))", "ET MALWARE CCleaner Backdoor DGA Domain (ab2e1b782bad .com) Mar 2018", "ET

	MALWARE TA471 Malicious AutoIT File Upload", "ET USER_AGENTS Suspicious User-Agent (angel)", "ET MALWARE Lyceum Group Activity (DNS)", "ET MALWARE Trojan/Downloader.Fosniw.sap Reporting via SMTP", "ET MALWARE Legion Loader Activity Observed (heil_satan)", "ET MALWARE [Fireeye] Backdoor.BEACON M5", "ET MALWARE Observed DNS Query to TA455 Domain (outlookdelivery .com)", "ET MALWARE Suspected Bitter APT Related Activity", "ET INFO Suspicious Windows NT version 3 User-Agent", "ET MALWARE Unknown CN Related APT Activity (GET)", "ET EXPLOIT WSO2 Server RCE (CVE-2022-29464)", "ET MALWARE Observed TA444 Domain (careersbankofamerica .us in TLS SNI)", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 5", "ET POLICY Powershell Command With Encoded Argument Over SMB - Likely Lateral Movement", "ET MALWARE Windows dir Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed DNS Query to Goofy Guineapig Domain (static .tcplog .com)", "ET MALWARE Observed Certificate Containing Double Base64 Encoded Executable Inbound", "ET MALWARE CopperStealer - Browser Stealer Exfil via Telegram", "ET MALWARE Nerbian RAT Data Exfiltration", "ET MALWARE SharpPanda APT Activity (GET)", "ET MALWARE Win32/DarkWatchman Activity (POST)", "ET USER_AGENTS ErbiumStealer UA Observed", "ET MALWARE Atom Logger exfil via SMTP", "ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response", "ET MALWARE Observed DNS Query to TA444 Domain (smbcgroup .us)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (agph .ivi66 .net)", "ET PHISHING Phishery Phishing Tool - Default SSL Certificate Observed", "ET WEB_CLIENT JS ShellWindows/AddInProcess Win10 DeviceGuardBypass Inbound", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .hinet .dns-dns .com)", "ET MALWARE GORGON APT Download Activity M2", "ET MALWARE Blaze/Supreme Bot Activity M2", "ET MALWARE Observed DNS Query to Budminer Domain (customs .bot .nu)", "ET MALWARE Observed DNS Query to Budminer Domain (gov .toh .info)", "ET MALWARE ABCbot CnC Instruction (dns)", "ET MALWARE [Fireeye] Backdoor.SUNBURST M2", "ET MALWARE IoT_reaper DNS Lookup M6 (bbk86 .com)", "ET MALWARE DNS Query for Cloud Atlas blackberry-support.herokuapp.com", "ET USER_AGENTS Suspicious User-Agent (Inet_read)", "ET USER_AGENTS Dialer-967 User-Agent", "ET MALWARE Possible Winnti-related DNS Lookup (macos .exoticlol .com)", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access sendSMS", "ET MALWARE Win32/Delf.TJJ CnC Checkin M2", "ET MALWARE Observed BlackGuard_v2 Domain (greenblguard .shop) in TLS SNI", "ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (storangefilecloud .vip)", "ET MALWARE Suspected DonotGroup Dropper Activity", "ET MALWARE Suspected Polonium CnC Checkin (result.php - process list) M1", "ET MALWARE Observed DNS Query to TA455 Domain (edge-cloudservices .com)", "ET MALWARE Possible Dyre SSL Cert M3 (O CN)", "ET MALWARE Blue Bot DDoS Target Request", "ET MALWARE Cobalt Strike Activity (GET)", "ET MALWARE IRC Potential bot scan/exploit command", "ET MALWARE OSX/WireLurker DNS Query Domain manhuaba.com.cn", "ET USER_AGENTS Observed Bumblebee Loader User-Agent (bumblebee)", "ET MALWARE Possible Malicious Macro DL EXE Feb 2016", "ET MALWARE SSL/TLS Certificate Observed (WRAT)", "ET MALWARE Windows net statistics server Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Win32/44Caliber Stealer Discord Activity (POST)", "ET MALWARE Observed DNS Query to Ursnif Domain (gigiman .xyz)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (tissatweb .us)", "ET MALWARE MSIL/TrojanDownloader.Agent.KUO CnC Activity M2", "ET PHISHING Suspicious CVV Parameter in HTTP POST - Possible Phishing", "ET MALWARE CCleaner Backdoor DGA Domain (ab99c24c0ba9 .com) Feb 2018", "ET EXPLOIT Possible Elasticsearch CVE-2015-1427 Exploit Campaign SSL Certificate", "ET MALWARE Observed Ursnif Domain in TLS SNI (dodsman .com)", "ET MALWARE Observed DNS Query to IcedID Domain (baherlakerl .online)", "ET MALWARE Mazilla Suspicious User-Agent Jan 15 2015", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (polanicia .com)", "ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .us .org)", "ET MALWARE Observed DNS Query to Budminer Domain (zcrd .twgogo .org)", "ET MALWARE Observed DNS Query to Budminer Domain (ey .uk .to)", "ET POLICY

	HTMLGET User Agent Detected - Often Linux utility based", "ET MALWARE Observed Ursnif Domain in TLS SNI (astope .xyz)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iredugov .wiki)", "ET MALWARE Zeus Spam Campaign pdf.exe In ZIP - 26th Feb 2014", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (nihaobrazzzahit .top in DNS Lookup)", "ET MALWARE Android/AhMyth RAT Command Inbound (SMS Manager)", "ET MALWARE ProjectSauron Remsec DNS Lookup (bikessport.com)", "ET MALWARE Observed DNS Query to Budminer Domain (TheoreticalModel .onmypc .us)", "ET MALWARE Observed DNS Query to Ursnif Domain (fishenddog .xyz)", "ET MALWARE TA569 Fake Browser Update Domain in DNS Lookup (profi-stom .com)", "ET MALWARE Possible SharpShooter Framework Generated VBS Script", "ET MALWARE Gamaredon APT Related Maldoc Activity (GET)", "ET MALWARE Win32/Wacatac.B Payload Download", "ET MALWARE MustangPanda APT Dropper Activity (POST)", "ET MALWARE Innostealer Domain (seventyfor .site) in TLS SNI", "ET MALWARE Observed DNS Query to Budminer Domain (iphone-ex .info .tm)", "ET MALWARE ELF/Emptiness v2 XOR Update Command Inbound", "ET MOBILE_MALWARE Android Spy APT-C-23 (linda-gaytan .website in DNS Lookup)", "ET MALWARE ClipBanker Variant Activity (POST)", "ET USER_AGENTS Suspicious User-Agent (Fire-Cloud)", "ET USER_AGENTS User-Agent (single dash)", "ET MALWARE CCleaner Backdoor DGA Domain (ab2d02b02bb3 .com) May 2018", "ET MALWARE Observed DNS Query to TA444 Domain (documentshare .info)", "ET MALWARE Maldoc Retrieving Payload 2022-06-15", "ET MALWARE Win32/Caypnamer.A RAT CnC Keepalive", "ET MALWARE TorrentLocker DNS Lookup (worldnews247.net)", "ET MALWARE GravityRAT CnC Domain (chat2hire .net in DNS Lookup)", "ET MALWARE FIN7 JSSLoader Variant Activity (POST)", "ET ATTACK_RESPONSE JS/Comm100 Trojan CnC Payload Inbound", "ET MALWARE MAGICHOUND-related DNS Lookup (analytics-google .org)", "ET MALWARE Observed DNS Query to Budminer Domain (Liveupdate .jkub .com)", "ET MALWARE Observed DNS Query to TA455 Domain (sharepointnotify .com)", "ET USER_AGENTS Suspicious User-Agent (firefox)", "ET MALWARE Observed DNS Query to TA455 Domain (updatedefender .net)", "ET MALWARE DNS Query for a known malware domain (sektori.org)", "ET MALWARE W32/Badlib Connectivity Check To Department of Defense Intelligence Information Systems", "ET MALWARE Likely Evil Request for uac.exe With Minimal Headers", "ET MALWARE ASCII Executable Inside of MSCOFF File DL Over HTTP", "ET MALWARE ELF/Win32 Lucky Ransomware Encryption Process Started", "ET WEB_CLIENT Android Fake AV Download Landing Mar 06 2017", "ET MALWARE PlayMP3z.biz Related Spyware/Trojan Install Report", "ET MALWARE Chinotto CnC Activity (result)", "ET MALWARE Observed TA444 Domain (share .anobaka .info in TLS SNI)", "ET MALWARE Observed DNS Query to Budminer Domain (kcg2 .gov .tw .allowed .org)", "ET MALWARE Deep Panda Domain in DNS Lookup (svn1 .smi1egate .com)", "ET EXPLOIT Windows Defender POWERLIKS Detection Bypass", "ET MALWARE Cycbot POST", "ET MALWARE Likely Evil Macro EXE DL mar 28 2016", "ET MALWARE [PTsecurity] Trojan.Downloader VBA Script obfuscation (binary_getter)", "ET MALWARE eleethub .com Domain in DNS Lookup (eleethub .com)", "ET MALWARE Mustang Panda APT TONESHELL Related Activity", "ET MALWARE Win32/BLUELIGHT OAuth Login Attempt", "ET MALWARE Colibri Loader Domain in DNS Lookup (securetunnel .co)", "ET MALWARE ProjectSauron Remsec DNS Lookup (asrgd-uz .weedns.com)", "ET MALWARE Danabot Associated Activity (GET)", "ET MALWARE Win32/Gatak.DR Activity", "ET MALWARE TinyNuke VNC Checkin M3", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (aserogeege .space in DNS Lookup)", "ET WEB_SERVER WebShell Generic eval of str_rot13", "ET MOBILE_MALWARE NSO Related Domain 28", "ET MALWARE Innostealer Domain (windows11-infoserver .com) in TLS SNI", "ET MALWARE Observed DNS Query to TA444 Domain (globiscapital .co)", "ET MALWARE Observed DNS Query to Budminer Domain (moea .dsmtp .com)", "ET MALWARE Vidar Stealer Payload Delivery Domain (audacitya .org) in DNS Lookup", "ET MALWARE TA444 Related Domain (azure-security .online) in DNS Lookup", "ET MALWARE MSIL/Crimson Receiving Command (getavs)", "ET MALWARE Fake Software Download Redirect Leading to Malware M2", "ET MALWARE Observed DNS Query to Budminer Domain

	(download .longmusic .com)", "ET MALWARE Ponmocup Post Infection DNS Lookup messagewild", "ET MALWARE Known Malicious Doc Downloading Payload Dec 06 2016", "ET MALWARE Observed DNS Query to Budminer Domain (cier .edu .tw .us .to)", "ET HUNTING SUSPICIOUS waulct.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE W32/Quasar 1.3/Venom RAT Connectivity Check 3", "ET MALWARE APT/FamousSparrow Activity (POST)", "ET MALWARE JS/Cloud9 Cookie Exfiltration Attempt", "ET SCAN Suspicious User-Agent inbound (bot)", "ET MALWARE Arkei/Vidar/Mars Stealer Variant Data Exfiltration Attempt", "ET MALWARE Villain C2 Framework HTTP Command Response", "ET MALWARE MagikPOS Downloader Retrieving Payload", "ET MALWARE Suspicious X-mailer Synapse", "ET MALWARE PowerTrick Known Key 1", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher.a Checkin", "ET MOBILE_MALWARE iOS DualToy Checkin", "ET MALWARE Cobalt Strike Malleable C2 Amazon Profile Variant (GET)", "ET USER_AGENTS Suspicious User-Agent (Clever Internet Suite)", "ET MALWARE CCleaner Backdoor DGA Domain (ab2da3d400c20 .com) Apr 2017", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 15", "ET MALWARE Possible DACLS RAT Log Collector Download", "ET HUNTING Suspicious Proxifier DL (non-browser observed in maldoc campaigns)", "ET MALWARE Patchwork APT Related Activity M2 (POST)", "ET MALWARE KHRAT DragonOK DNS Lookup (inter-ctrip .com)", "ET USER_AGENTS Suspicious User-Agent (WebForm 1)", "ET MALWARE W32/Safe User Agent Fantasia", "ET MALWARE EtumBot Ping", "ET WEB_SERVER c0896 Hacked Site Response Hex (Outbound)", "ET MALWARE Known Hostile Domain citi-bank.ru Lookup", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (humaantouch .com)", "ET MALWARE Observed DNS Query to Budminer Domain (airbus .zyns .com)", "ET MALWARE Observed Ursnif Domain in TLS SNI (logotep .xyz)", "ET MALWARE [FIREEYE] PULSECHECK Webshell Access Outbound", "ET MALWARE Win32/Criminal RAT CnC Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (bigbang .ddns .ms)", "ET MALWARE RedLine Stealer TCP CnC net.tcp Init", "ET MALWARE W32/iGrabber Info Stealer FTP Upload", "ET MALWARE W32/SecVerif.Downloader Second Stage Download Request", "ET MALWARE Observed DNS Query to TA455 Domain (outlookde .live)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 8", "ET MOBILE_MALWARE NSO Related Domain 10", "ET MALWARE Observed DNS Query to Budminer Domain (workstation .mypop3 .org)", "ET MALWARE Observed DNS Query to Budminer Domain (ofa .fartit .com)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (ukgames .tech)", "ET MALWARE TA444 Related Domain in DNS Lookup (wordonline .cloud)", "ET MALWARE Win32/Dynamer Trojan Dropper User-Agent VB Http", "ET WEB_CLIENT CookieBomb Generic HTML Format", "ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (https)", "ET MALWARE Galock Ransomware Check-in", "ET MALWARE Observed TA453 Domain (washingtonlnstitute .org in TLS SNI)", "ET MALWARE SocGholish Domain in DNS Lookup (deposit .coveprice .com)", "ET WORM TheMoon.linksys.router 3", "ET INFO Inbound PowerShell Checking for Virtual Host (MSAcpi_ThermalZoneTemperature WMI)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 4", "ET MALWARE OSX/Proton.C/D Domain (handbrakestore .com) in DNS Lookup", "ET MALWARE Pegasus Domain in DNS Lookup (alrainew .com)", "ET MALWARE CORESHELL Malware Response from server", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .newmc .dns-dns .com)", "ET MALWARE Observed Karen Ransomware Domain (karen .h07 .wlh .io in TLS SNI)", "ET EXPLOIT Metasploit FireFox WebIDL Privileged Javascript Injection", "ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M2", "ET MALWARE VBA/TrojanDownloader.Agent.PAC Retreiving Malicious VBScript", "ET MALWARE VBS/Wimmie.A Set", "ET MALWARE VenusLocker Activity", "ET MALWARE Lurk Downloader Check-in", "ET MALWARE Possible DNS Tunneling Observed", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (wicommerece .com)", "ET MALWARE Win32/TrojanDownloader.Agent.GEM Maldoc Remote Template Request M1", "ET MALWARE [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon", "ET MALWARE Win32/Valyria Maldoc Payload Request M2", "ET MALWARE VBS/Agent.PUK Data Exfiltration Request M2", "ET MALWARE Observed DNS Query to

	Ursnif Domain (higmon .cyou)", "ET MALWARE Gozi Communication 2", "ET MALWARE MontysThree HTTPTransport Module Activity", "ET MOBILE_MALWARE NSO Pegasus iOS Activity (GET)", "ET MALWARE Observed DNS Query to Ursnif Domain (minotos .xyz)", "ET MALWARE Tandem Espionage CnC Domain (rhjebiuujydv .ru) in DNS Lookup", "ET MALWARE ElectroRAT CnC Checkin", "ET MALWARE Possible CopyKitten DNS Lookup (jguery .online)", "ET MALWARE Legion Loader Activity Observed (Mylegion666)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (linux .wy01 .com)", "ET MALWARE iebar Spyware User Agent (iebar)", "ET MALWARE Observed Win32/CollectorStealer User-Agent M1", "ET MALWARE Polonium APT PAPACREEP Backdoor Related Activity", "ET MALWARE GravityRAT CnC Domain (msoftserver .eu in DNS Lookup)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Mozilla_Firefox_Cookies) M2", "ET MALWARE GhostWriter APT Related Cobalt Strike Activity (GET)", "ET MALWARE ELF/Emptiness v2 XOR UDP Flood Command Inbound", "ET MALWARE MSIL/Unk.CoinMiner Downloader", "ET MALWARE Atya Dropper Possible Rootkit - HTTP GET", "ET MALWARE Win32/Oliga Fake User Agent", "ET MALWARE Jadtree Downloader rar", "ET MALWARE Win32/Borr Stealer Variant Sending System Information", "ET MALWARE Win32/Farfli.BAL CnC Activity", "ET MALWARE Hupigon User Agent Detected (VIP2007)", "ET MALWARE Havoc Framework CnC Response", "ET MALWARE Observed DNS Query to Ursnif Domain (rorfog .com)", "ET MALWARE Linux/Tsunami DNS Request (linuxmint.kernel-org.org)", "ET MALWARE MAGICHOUND-related DNS Lookup (com-ho .me)", "ET MALWARE Observed TA444 Domain (tptf .cloud in TLS SNI)", "ET EXPLOIT Remote Command Execution via Android Debug Bridge 2", "ET MALWARE Observed DNS Query to UNC3890 Domain (office365update .live)", "ET DOS HOIC with booster inbound", "ET MALWARE Observed DNS Query to Ursnif Domain (tornton .xyz)", "ET MOBILE_MALWARE AndroidOS/Lotoor.Q", "ET MALWARE Trojan Generic - POST To gate.php with no referer", "ET INFO Anyplace Remote Access Checkin (051)", "ET MALWARE Observed DNS Query to Budminer Domain (mails .grousp .allowed .org)", "ET MALWARE Emotet Style Request Activity (GET)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 4", "ET USER_AGENTS Suspicious User-Agent (MSIE)", "ET CURRENT_EVENTS Possible Crypto Drainer Fetch", "ET MALWARE Win32/RecordBreaker CnC Checkin M1", "ET MALWARE Backdoor.Elise Style IP Check M2", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (mynetenergy .com)", "ET MALWARE ELF/Mirai Variant UA Outbound (lessie)", "ET MALWARE Luder.B User-Agent (Mozilla/4.0 (SPGK)) - GET", "ET MOBILE_MALWARE Android Spy APT-C-23 (linda-gaytan .website in TLS SNI)", "ET WEB_CLIENT Generic Attempted Executable Drop via VBScript", "ET MALWARE Observed DNS Query to Budminer Domain (nditd .top)", "ET MALWARE Unknown Webserver Backdoor", "ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M1", "ET MALWARE Powershell/CustomRAT CnC Domain in DNS Lookup (kleinm .de)", "ET MALWARE TA569 Domain in DNS Lookup (luxurycompare .com)", "ET MALWARE TA410 APT FlowCloud Dependency Download M1", "ET MALWARE Suspected Solarwinds Serv-U Backdoor (Incoming)", "ET MALWARE Win32/Voltron/Spectre Stealer Download Activity (GET)", "ET MALWARE MSIL/KeyRedirEx Banker Receiving Redirect/Inject List", "ET MALWARE Observed Ursnif Domain in TLS SNI (mainwog .xyz)", "ET MALWARE Rostpay Downloader User-Agent", "ET MALWARE VBS/Agent.PUK Data Exfiltration Request M1", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M2", "ET USER_AGENTS Suspicious User-Agent Sample", "ET MOBILE_MALWARE SMSSend Fake flappy bird APK", "ET MALWARE Possible CopyKitten DNS Lookup (alkamaihd .net)", "ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 2", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 4", "ET MALWARE Possible Outbound WebShell GIF", "ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Identity Check Activity (GET)", "ET MALWARE Possible CopyKittens DNS Lookup (alhadath.mobi)", "ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M2", "ET MALWARE TA453 Domain in DNS Lookup (washingtonlnstitute .org)", "ET MALWARE Win32/Phorpiex Template 5 Active - Outbound Malicious Email Spam", "ET MALWARE Win32/LockScreen.BW Payment

	Info", "ET EXPLOIT CVE-2016-0189 Exploit", "ET DOS SMBLoris NBSS Length Mem Exhaustion Attempt (PoC Based)", "ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful", "ET MALWARE Zbot downloader Installing Zeus", "ET USER_AGENTS Suspicious User-Agent (USERAGENT)", "ET MALWARE Possible Pegasus Related DNS Lookup (asrarrarabiya .com)", "ET MALWARE Windows WMIC SERVICE get Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE SocGholish Domain in DNS Lookup (premiere .4tosocialbeginners .com)", "ET USER_AGENTS Observed Suspicious UA (h55u4u4u5uii5)", "ET MALWARE Subterranean Crimson Rat - FileManager pwd Command", "ET MALWARE Win32/Darkme Trojan Checkin M1", "ET MALWARE Netwire RAT Check-in", "ET MALWARE Observed DNS Query to Budminer Domain (news .mynews .photo-frame .com)", "ET INFO Obfuscated Eval String (Single Q) 4", "ET MALWARE TrickBot Related Activity (GET)", "ET MALWARE Observed DNS Query to Alibaba2044 Domain (service-fatturecloud .de)", "ET MALWARE Win32/Zemot Fake Search Page", "ET MALWARE Win32/ChromeBack Browser Hijacker Sync", "ET MALWARE Observed DNS Query to Ursnif Domain (gigeram .com)", "ET MALWARE Possible CopyKitten DNS Lookup (akamaitechnology .com)", "ET MALWARE Likely Geodo/Emotet Downloading PE", "ET MALWARE Observed DNS Query to ShadowPad Domain (supermarket .ownip .net)", "ET MALWARE Possible CopyKittens DNS Lookup (windows24-kernel.in)", "ET MALWARE Win32/Agent.XXZ Checkin", "ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .supapureigemu .com)", "ET USER_AGENTS Suspicious User-Agent (SERVER2_03)", "ET USER_AGENTS Win32/Feebs.kw Worm User-Agent Detected", "ET MOBILE_MALWARE CoolReaper User-Agent", "ET MALWARE Waledac FACEPUNCH Traffic Detected", "ET MALWARE Observed DNS Query to Ursnif Domain (reaso .xyz)", "ET MALWARE Possible Veil Powershell Encoder B643", "ET MALWARE Redline Stealer TCP CnC Activity", "ET MALWARE HermeticWizard - WMI Spreader - Remote Process Creation M2", "ET MALWARE CopperStealer - Remote Desktop - Initial Checkin", "ET MALWARE W32/TCYWin.Downloader User-Agent", "ET MALWARE Successful Cobalt Strike Shellcode Download (x64) M1", "ET MALWARE Naikon DNS Lookup (greensky27.vicp.net)", "ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 4", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M9", "ET MALWARE Possible IoT_reaper ELF Binary Request M5 (set)", "ET MALWARE FRAT Downloader Activity", "ET MALWARE FinFisher Malware Connection Handshake", "ET MALWARE Kimsuky Related Maldoc Activity (GET)", "ET MALWARE W32/Zbot.Variant Fake MSIE 6.0 UA", "ET USER_AGENTS Suspicious User-Agent (HardCore Software For)", "ET MALWARE SocGholish Domain in DNS Lookup (fittingroom .gibbsjewelry .com)", "ET MALWARE Possible Pegasus Related DNS Lookup (emiratesfoundation .net)", "ET MALWARE Potential Dridex.Maldoc Minimal Executable Request", "ET POLICY archive.org heritix Crawler User-Agent (Outbound)", "ET MALWARE Win32/Screenshotter Backdoor CnC Activity (GET)", "ET MALWARE Observed Ursnif Domain in TLS SNI (higmon .cyou)", "ET MALWARE Tandem Espionage CnC Domain (wzqyuwtdxyee .ru) in DNS Lookup", "ET MALWARE Observed DNS Query to Budminer Domain (yahoo .serveuser .com)", "ET MALWARE Android/AhMyth RAT Command Inbound (Location Manager)", "ET MALWARE APT15/NICKEL KETRUM CnC Activity (POST)", "ET MALWARE Brute Ratel CnC Activity (json-c2) M1", "ET MALWARE Observed TA444 Domain (careers .bankofamerica .nyc in TLS SNI)", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access sendMail", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (gc .wb51 .com)", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (secandroid .com in DNS Lookup)", "ET MOBILE_MALWARE Android/Kemoge Checkin 2", "ET MALWARE Godlua Backdoor Downloading Encrypted Lua", "ET MALWARE GuLoader Domain in DNS Lookup (zoneofzenith .com)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(FMBVDFRESCT)", "ET MALWARE Operation Cobra Venom Stage 1 DNS Lookup", "ET MALWARE Ponmocup HTTP Request (generic) M6", "ET MALWARE J-Spy JSP webshell request", "ET MALWARE Observed DNS Query to Budminer Domain (jjj .ns02 .us)", "ET MALWARE Matanbuchus Loader CnC M4", "ET MALWARE ObliqueRAT CnC Heartbeat Packet", "ET MALWARE WindowsEnterpriseSuite FakeAV

	get_product_domains.php", "ET MALWARE Restylink Domain in DNS Lookup (sseekk .xyz)", "ET MALWARE Smokeloader getproxy Command", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Wroba Lure (Package Delivery)", "ET MALWARE Observed DNS Query to Budminer Domain (moea .jumpingcrab .com)", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(yez2o5lwqkmlv5lc)", "ET MALWARE Possible WannaCry DNS Lookup 5", "ET MALWARE Possible Zeus P2P Variant Check-in", "ET MALWARE Orca RAT URI Struct 3", "ET MALWARE Bitter APT Backdoor Related Activity", "ET MALWARE Observed DNS Query to AppleJeus Domain (wirexpro .com)", "ET MOBILE_MALWARE Android Spy APT-C-23 (frances-thomas .com in TLS SNI)", "ET MALWARE Shylock Module Data POST", "ET MALWARE Observed DNS Query to Budminer Domain (bitcom .polaczyk .com)", "ET MALWARE x0Proto Init", "ET MALWARE ReverseRAT Activity (POST) M2", "ET MALWARE Cryptolocker Payment Domain (3qbyaoohkcqkzrz6)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (feedsonbudget .com)", "ET MALWARE Neverquest Request URI Struct", "ET MOBILE_MALWARE NSO Related Domain 11", "ET MALWARE Possible CopyKittens DNS Lookup (walla.link)", "ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M5", "ET MALWARE EncryptorRaas .onion Proxy Domain", "ET MALWARE Netbounce Proxy Activity", "ET MALWARE Umbra/Multibot Loader User-Agent (umbra)", "ET MALWARE Linux/dtool IRC Command Complete 3", "ET MALWARE Possible MalDoc Retrieving Payload 2021-11-01", "ET CNC Feodo Tracker Reported CnC Server group 2", "ET MALWARE ELF/Mirai Variant UA Outbound (Damien)", "ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .getkiplayer .com)", "ET MALWARE Android/AhMyth RAT Command Inbound (Call Manager)", "ET MALWARE Innostealer Domain in DNS Lookup windows-server031 .com)", "ET MALWARE Hakbit/Thanos Ransomware Exfil via FTP", "ET MALWARE Possible Covenant Framework Grunt Stager HTTP Download (DynamicInvoke)", "ET WEB_CLIENT pshell dl/execute primitives in wideb64 6", "ET MALWARE Linux/Xnote Keep-Alive", "ET MALWARE Win32/DanaBot Harvesting Email Addresses 1", "ET MALWARE Banker.Delf Infection - Sending Initial Email to Owner", "ET MALWARE Limitless Logger RAT HTTP Activity", "ET MALWARE Downloaded .bat Disables Windows Defender", "ET MALWARE Suspected TA404 APT Related Activity M2", "ET MALWARE Request for fake postal receipt from e-mail link", "ET WEB_CLIENT c0896 Hacked Site Response Hex (Inbound)", "ET MALWARE x0Proto Ping", "ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (panhardware .com)", "ET MALWARE Win32/Tofsee Connectivity Check M3", "ET MALWARE PWSteal.Bancos Generic Banker Trojan SCR Download", "ET MALWARE Hupigon User Agent Detected (RAV1.23)", "ET HUNTING suspicious - uncompressed pack200-ed JAR", "ET MALWARE ISMAgent DNS Lookup (msoffice-cdn . com)", "ET MALWARE RansomCrypt Getting Template", "ET MALWARE KeyBoy DNS Lookup (tibetvoices .com)", "ET USER_AGENTS Suspicious Win32 User Agent", "ET MALWARE ELF/Emptiness v1.1 UDP Flood Command Inbound", "ET MALWARE Trojan.Delf-5496 New Infection Report", "ET MALWARE Observed DNS Query to TA444 Domain (shconstmarket .com)", "ET MALWARE Observed DNS Query to Budminer Domain (oop .uk .to)", "ET MALWARE Possible CopyKittens DNS Lookup (windowskernel14.com)", "ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Yahoo)", "ET MOBILE_MALWARE Oscorp/UBEL Activity", "ET MALWARE Gimmiv Infection Ping Outbound", "ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v2", "ET MALWARE Banker.Delf User-Agent (Ms)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server]", "ET MALWARE Observed DNS Query to Win32/TrojanDropper.Agent.SLC Domain", "ET MALWARE Scarlet Mimic DNS Lookup 42", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 5", "ET MALWARE Possible Pegasus Related DNS Lookup (bulbazaur .com)", "ET MALWARE Linux/Denonia DNS Request Over HTTPS (denonia .xyz) M2", "ET MALWARE Dark Halo/SUNBURST CnC Domain (seobundlekit .com in TLS SNI)", "ET MOBILE_MALWARE Android Trojan MSO.PJApps checkin 2", "ET USER_AGENTS Suspicious User-Agent (Presto)", "ET MALWARE Executable contained in DICOM Medical Image PACS DICOM Protocol Transfer", "ET MALWARE Observed DNS Query to Budminer Domain (mofa .ignorelist .com)", "ET MALWARE ElectroRAT

	Command from Server (Get folder content)", "ET MALWARE Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack)", "ET MALWARE Observed DNS Query to AppleJeus Domain (bloxholder .com)", "ET MALWARE W32/SpyBanker Infection Confirmation Email 2", "ET MALWARE Arid Viper APT Related Activity (POST)", "ET MALWARE ELF/MachO.Netwire Connectivity Check", "ET MALWARE Win32/RecordBreaker CnC Exfil (Cookies)", "ET MALWARE Observed DNS Query to AppleJeus Domain (telloo .io)", "ET ATTACK_RESPONSE HTML Smuggling Powershell Payload In iframe", "ET POLICY DNS request for Monero mining pool", "ET POLICY Possible SQLi Attempt in User Agent (Outbound)", "ET MALWARE JavaRAT Keep-Alive (inbound)", "ET MALWARE 000Stealer Data Exfiltration M2", "ET MALWARE Backdoor.Perl.Shellbot.cd IRC Bot that have DoS/DDoS functions", "ET MALWARE Generic Password Stealer User Agent Detected (RookIE)", "ET MALWARE ConstructorWin32/Agent.V", "ET USER_AGENTS Observed Malicious VBS Related UA", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 13", "ET MALWARE WinGo/YT Stealer CnC Checkin", "ET MALWARE Win32/Lilith Stealer uploadFile Data Exfiltration Attempt", "ET MALWARE dYdX NPM Package Backdoor Exfiltration Domain (api .circle-cdn .com) in DNS Lookup", "ET MALWARE Possible Pegasus Related DNS Lookup (pickuchu .com)", "ET MALWARE Win32/MagicRAT CnC Checkin M2", "ET MALWARE Nerbian RAT CnC Checkin", "ET MALWARE PandoraRat/Refroso.bsp Directory Listing Sent To Server", "ET MALWARE ZeroAccess P2P Module v6 Reporting", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (hdfuckedin18 .top in DNS Lookup)", "ET MALWARE Sharik/Smoke Loader Adobe Connectivity Check 2", "ET MALWARE Possible Astaroth User-Agent Observed", "ET MALWARE JS/HTA Downloader Behavior M3", "ET MOBILE_MALWARE Android Spy APT-C-23 (david-gardiner .website in DNS Lookup)", "ET MALWARE Observed DNS Query to TA455 Domain (getadobe .ddns .net)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mvpconsultant .us)", "ET INFO PowerShell Hidden Window Command Common In Powershell Stagers M1", "ET MALWARE GO/Titan Stealer Data Exfiltration Attempt", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn2 .com)", "ET MALWARE Win32/CrimsonRAT Variant Sending System Information (outbound)", "ET MALWARE Possible Stitur Secondary Download", "ET MALWARE ELF/Muhstik Attempting to Download Payload", "ET MOBILE_MALWARE Android.Tonclank JAR File Download", "ET MALWARE [PTsecurity] Tinba (Banking Trojan) HTTP Header", "ET MALWARE DeimosC2 TCP Agent Heartbeat", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (globalnews .cloud)", "ET MALWARE CCleaner Backdoor DGA Domain (ab1c403220c27 .com) Jun 2017", "ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Mozilla JS Class Creation", "ET MALWARE Possible Winnti-related Destination", "ET USER_AGENTS Suspicious User-Agent (chek)", "ET MALWARE Kimsuky Related Maldoc Activity (HEAD)", "ET MALWARE GravityRAT CnC Domain (microsoftupdate .in in DNS Lookup)", "ET CNC Feodo Tracker Reported CnC Server group 10", "ET MALWARE CloudAtlas APT Maldoc Activity (GET)", "ET MALWARE TrojanDownloader Win32/Harnig.gen-P Reporting", "ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value Snkz", "ET MALWARE DNS query for Known OphionLocker Domain", "ET MALWARE ABUSE.CH Locky Payment Domain Detected", "ET MALWARE Generic Dropper Installing PUP 1", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (databasegalore .com in TLS SNI)", "ET MALWARE Win32/CollectorStealer - Uploading System Information", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 20", "ET MALWARE Possible CopyKittens DNS Lookup (patchthiswindows.com)", "ET MALWARE Driveby Loader Request List.php", "ET MALWARE Suspected Win32/Hancitor Checkin", "ET MALWARE Snake rootkit usermode-centric encrypted command from server", "ET MALWARE BKransomware Domain (3whyfziey2vr41yq in DNS Lookup)", "ET MALWARE WindowsEnterpriseSuite FakeAV check-in GET", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup", "ET MOBILE_MALWARE Android Spy APT-C-23 (javan-demsky .website in DNS Lookup)", "ET MALWARE JS/Nemucod.M.gen requesting PDF payload 2015-11-02", "ET MOBILE_MALWARE Android Syria-Twitter Checkin", "ET MALWARE Win32/Darkme CnC

	Domain in DNS Lookup (csmmmsp099q .com)", "ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (incomeupdate .com)", "ET HUNTING SUSPICIOUS lgfxsrvc.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Kimsuky Related Malicious VBScript Inbound M3", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (jmarrycs .com)", "ET MALWARE Volatile Cedar DNS Lookup (dotntexplorere.info)", "ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)", "ET MALWARE Gimemo Activity", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M1", "ET MALWARE PowerTrick download bot known key", "ET PHISHING Suspected TA445 Spearphishing Related Domain (aplikacje .ron-mil .space in TLS SNI)", "ET CNC Feodo Tracker Reported CnC Server group 12", "ET MALWARE Possible Pegasus Related DNS Lookup (asrararabiya .co)", "ET MALWARE RocketMan Win32/Drun", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (incomeudpate .com in TLS SNI)", "ET INFO Lockbit Ransomware Related Domain in DNS Lookup (lockbitapt)", "ET INFO Suspicious Windows NT version 9 User-Agent", "ET MOBILE_MALWARE NSO Pegasus iOS Megalodon Activity (GET)", "ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M2", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 2", "ET MALWARE Win32/LingyunNet.A CnC Checkin", "ET MALWARE APT15/NICKEL Related CnC Activity (POST)", "ET MALWARE W32/Lile.A DoS Outbound", "ET MALWARE Observed DNS Query to Budminer Domain (fsc-kd .ns01 .info)", "ET MOBILE_MALWARE NSO Related Domain 38", "ET CNC Feodo Tracker Reported CnC Server group 25", "ET MALWARE Observed Lazarus Related Domain (docs .gsheetpage .com in TLS SNI)", "ET MALWARE W32/SCKeyLog.InfoStealer Installation Confirmation Via SMTP", "ET MALWARE Zingo/GinzoStealer Data Exfiltration M2", "ET MALWARE Cayosin Botnet User-Agent Observed M1", "ET MALWARE Windows ipconfig Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE ELF/BASHLITE CnC Activity (Response)", "ET MOBILE_MALWARE Android/Spy.Agent.BEH Variant Activity (POST)", "ET MALWARE DonotGroup Activity (GET)", "ET MALWARE ReverseRat 2.0 CnC Checkin M2", "ET MALWARE GravityRAT CnC Domain (chuki .mozillaupdates .us in DNS Lookup)", "ET MALWARE ABCbot CnC Instruction (bigudp)", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (wangzongfacai.com)", "ET MALWARE APT28/FancyBear Related Activity (POST)", "ET MALWARE Observed DNS Query to Budminer Domain (pe .publiccosplay .org)", "ET MALWARE Observed DNS Query to Budminer Domain (kuangdao .serveftp .com)", "ET CNC Feodo Tracker Reported CnC Server group 16", "ET MALWARE Observed DNS Query to TA455 Domain (enerflex .ddns .net)", "ET WEB_SERVER JSP.SJavaWebManage WebShell Pass 20-09-2018 2", "ET MALWARE Trojan Downloader GetBooks UA", "ET MALWARE JAR/Qealler Stealer HTTP Headers Observed", "ET MALWARE Gamaredon File Stealer POST", "ET MALWARE Android/AhMyth RAT Init Checkin", "ET MALWARE SocGholish Domain in DNS Lookup (podcasts .momsgrabcoffee .com)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 21", "ET MALWARE Observed DNS Query to TA444 Domain (cloud .globiscapital .co)", "ET MALWARE Win32/MassLogger FTP Data Exfiltration", "ET MALWARE Suspicious bot.exe Request", "ET INFO WinHttpRequest (flowbits no alert)", "ET MALWARE ELF/Mirai Variant UA Outbound (Cakle)", "ET POLICY My2022/Beijing2022 App (DNS Lookup) 1", "ET USER_AGENTS Suspicious User-Agent (HELLO)", "ET HUNTING Suspicious User-Agent (NULL)", "ET USER_AGENTS Observed Malicious User-Agent (CobaltStrike)", "ET MALWARE IcedID WebSocket Request", "ET MALWARE Suspected Glupteba Download", "ET MALWARE Possible CopyKittens DNS Lookup (windowslayer.in)", "ET MALWARE Possible Covenant Framework Grunt PowerShell Stager HTTP Download", "ET MALWARE TA444 Related Domain (azure-security .site) in DNS Lookup", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (cisco-helpdesk .cf)", "ET MOBILE_MALWARE Android/FlyTrap Activity (POST)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (id .bigmir .space)", "ET POLICY Suspicious ToTok Mobile Application TLS Request", "ET MALWARE Observed DNS Query to Budminer Domain (web .stonekiki .freeddns .com)", "ET MALWARE Malicious VBE Script (COVID-19 Phish 2020-04-03)", "ET MALWARE SocGholish Domain in DNS Lookup

	(travel .dianatokaji .com)", "ET MALWARE SocGholish Domain in DNS Lookup (navyseal .digijump .online)", "ET MALWARE JavaRAT Sending Screenshot", "ET MALWARE Suspected Cobalt Strike Beacon User-Agent String", "ET MALWARE Spora Ransomware SSL Certificate Detected", "ET MALWARE Win32/Wacatac.B Loader CnC Checkin", "ET MALWARE Cobalt Strike Stager Time Check M1", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (androidssystem .com in DNS Lookup)", "ET MALWARE Trojan.BackDoor-DRV.gen.c Reporting-1", "ET USER_AGENTS User-agent DownloadNetFile Win32.small.hsh downloader", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (noredirecto .redirectme.net)", "ET MALWARE LuminosityLink - Data Channel Client Request", "ET MALWARE Malicious ELF Activity", "ET MALWARE AllcomeClipper CnC Checkin", "ET MALWARE Observed DNS Query to TA444 Domain (finxiio .com)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (am-reader .com)", "ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Check-in Activity (GET)", "ET MALWARE SocGholish Domain in DNS Lookup (repo .allgoodsnservices .com)", "ET HUNTING SUSPICIOUS winlog.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE JS/Skimmer Inbound (Likely MageCart) M2", "ET MOBILE_MALWARE NSO Related Domain 31", "ET MALWARE Possible Upatre Downloader SSL certificate (fake loc)", "ET MALWARE Eternity Stealer Screen Capture Activity", "ET MALWARE Observed IcedID Domain in DNS Lookup (bayernbadabum .com)", "ET MALWARE Carberp file download", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn3 .com)", "ET MALWARE GCleaner Downloader Activity M2", "ET MALWARE Observed DNS Query to TA455 Domain (careers-finder .com)", "ET MALWARE Windows route Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE TA450 GRAMDOOR Telegram CnC Activity (POST)", "ET MALWARE Ranscam Ransomware Contact Form", "ET MALWARE Deathstalker/Evilnum Delivery Domain (puccino .altervista .org) in TLS SNI", "ET MALWARE Innostealer Domain in DNS Lookup (windows11-infoserver .com)", "ET MALWARE GORGON APT Download Activity", "ET MALWARE Xilcter/Zeus related malware dropper reporting in", "ET MOBILE_MALWARE Android/TrojanDropper.Agent.EP HTTP Host", "ET MALWARE Waledac Beacon Traffic Detected", "ET P2P Phatbot Control Connection", "ET MALWARE Backdoor.Win32.Sykipot Get Config Request", "ET MALWARE Suspected DonotGroup Dropper Telegram API Activity", "ET MALWARE Possible Win32/Get2 Downloader Activity", "ET MALWARE Observed DecryptmyFiles Ransomware User-Agent (uniquesession)", "ET MALWARE W32.Duptwux/Ganelp FTP Username - onthelinux", "ET MALWARE Likely Linux/Xorddos DDoS Attack Participation (gggatat456.com)", "ET MALWARE Upatre Binary Download Jan 02 2014", "ET MALWARE Nim Based Downloader Activity (GET)", "ET MALWARE Pegasus Domain in DNS Lookup (al7erak247 .com)", "ET MALWARE Win32/Valyria Maldoc Payload Request M1", "ET MALWARE Win32/ClipBanker.OC CnC Activity M2", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Bookmarks Firefox.txt) M1", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 14", "ET MALWARE Shade Ransomware Payment Domain in DNS Lookup", "ET MALWARE Winquickupdates.com/Mycashloads.com Related Trojan Install Report", "ET MALWARE Maldoc Retrieving Binary", "ET USER_AGENTS Suspicious User-Agent (Testing)", "ET WEB_CLIENT pshell dl/execute primitives in wideb64 5", "ET MALWARE Proxychecker Lookup", "ET MALWARE Possible CopyKittens DNS Lookup (u.mywindows24.in)", "ET MALWARE HTA.BabyShark HTTP Exfil", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to avsvmcloud .com", "ET MALWARE Sharik/Smoke Loader Adobe Connectivity Check 3", "ET MALWARE Mylobot Receiving XOR Encrypted Config (0xde)", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (freescanonline .com in TLS SNI)", "ET CURRENT_EVENTS Sliver Related Domain in DNS Lookup", "ET USER_AGENTS Suspicious User Agent (BlackSun)", "ET MALWARE Powershell/PowHeartBeat CnC Checkin - HTTPS", "ET MALWARE Win32/Emotet CnC Activity (POST) M11", "ET MALWARE ELF/Mirai Variant UA Inbound (Damien)", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.to)", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (devcisco .com)", "ET MALWARE Observed DNS Query to

	W32/Filecoder.KY!tr.ransom Domain (e4c0660414bf .eu .ngrok .io)", "ET MALWARE Observed Evrial Domain (cryptoclipper .ru in TLS SNI)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cnwx .58ad .cn)", "ET MALWARE TraderTraitor AlticGO CnC Checkin (POST)", "ET MALWARE Arkei/Vidar/Mars Stealer Variant", "ET MALWARE Gamaredon/Armageddon Activity (Retrieving Remote .dot)", "ET MALWARE Win32/Generik.NWVMNHQ Variant Exfil (POST)", "ET USER_AGENTS suspicious User Agent (Lotto)", "ET MALWARE Possible BlackEnergy Accessing SMB/SMB2 Named Pipe (Unicode)", "ET MALWARE Banker.Delf User-Agent (WINDOWS_LOADS)", "ET MALWARE Win32/NetDooka Framework RAT Sending File", "ET WORM TheMoon.linksys.router 2", "ET USER_AGENTS Suspicious User-Agent (AVP2006IE)", "ET MALWARE Observed TA444 Domain (sharedrive .ink in TLS SNI)", "ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M3", "ET EXPLOIT Metasploit Random Base CharCode JS Encoded String", "ET MALWARE Suspicious User-Agent - Matcash related Trojan Downloader (Ismazo Advanced Loader)", "ET MALWARE Deathstalker/Evilnum Delivery Domain (storangefilecloud .vip) in TLS SNI", "ET MALWARE XLS.Unk DDE rar Drop Attempt (.online)", "ET MALWARE [Akamai] Panchan Miner Botnet Checkin", "ET MALWARE [Fireeye] Backdoor.SUNBURST M3", "ET MALWARE US-CERT TA14-353A Lightweight Backdoor 1", "ET MALWARE Banload Downloader Infection - Sending initial email to owner", "ET MALWARE LooCipher Ransomware Onion Domain", "ET MALWARE SocGholish Domain in DNS Lookup (pastor .cntcog .org)", "ET MALWARE Win32/Sabsik Config Downloader", "ET MALWARE SSL/TLS Certificate Observed (FIN7 JSSLoader)", "ET MALWARE METALJACK APT32 DNS Lookup (m.topiccore.com)", "ET MALWARE Maldoc Retrieving Remote Template (GET)", "ET MALWARE HermeticWizard - SMB Spreader - Remote Process Creation", "ET HUNTING SUSPICIOUS winhost(32|64).exe in URI", "ET MALWARE Linux.Mirai Login Attempt (xc3511)", "ET MALWARE Possible CopyKitten DNS Lookup (broadcast-microsoft .tech)", "ET MALWARE MSSQL maggie backdoor Query Observed (other functions)", "ET MALWARE Win32/Tnega Activity (GET)", "ET MALWARE PNScan.2 Inbound Status Check Response", "ET MALWARE CustomRAT DNS lookup", "ET MALWARE ASNAROK Related Domain in DNS Lookup", "ET MALWARE IcedID Fake Resume Server in DNS Lookup", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 3", "ET MALWARE Win32/MagicRAT Additional Payload URI M4", "ET MALWARE Observed Ursnif Domain in TLS SNI (fingerpin .cyou)", "ET EXPLOIT Possible ECLIPSEDWING MS08-067", "ET MALWARE Valyria Downloader Activity", "ET MALWARE Genome User-Agent (Http Down)", "ET MALWARE Observed DNS Query to Budminer Domain (taiwanmail .org .ignorelist .com)", "ET MALWARE DarkGate Domain in DNS Lookup (battlenet .la)", "ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (Comands)", "ET MALWARE W32.Tomiris C2 (init)", "ET MALWARE Common Downloader Install Count Tracking URL", "ET MALWARE Observed TraderTraitor Domain (cryptais .com) in TLS SNI", "ET MALWARE Observed Vidar Stealer Domain (computerprotect .me) in TLS SNI", "ET MALWARE Win32/Spy.Delf.QTL Data Exfiltration Attempt", "ET MALWARE Steam Stealer", "ET MALWARE Observed DNS Query to Budminer Domain (mybb .dns-dns .com)", "ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (dosandiq .space in DNS Lookup)", "ET MALWARE GravityRAT CnC Domain (sharify .co .in in DNS Lookup)", "ET MALWARE Linux/Tsunami DNS Request (updates.mintylinux.com)", "ET EXPLOIT Shenzhen TVT DVR/NVR/IPC ConfigSyncProc RCE Attempt", "ET MALWARE Possible CopyKittens DNS Lookup (windows-my50.com)", "ET USER_AGENTS Suspicious User-Agent (contains loader)", "ET P2P Bittorrent P2P Client HTTP Request", "ET MALWARE Possible CopyKitten DNS Lookup (jguery .net)", "ET MOBILE_MALWARE Android/SndApp.B Sending Device Information", "ET USER_AGENTS Eldorado.BHO User-Agent Detected (MSIE 5.5)", "ET MALWARE Suspected Gamaredon APT Related Activity (GET)", "ET MALWARE ELF/LiLocked Ransom Note in HTTP Response", "ET MALWARE Observed DNS Query to Hilal RAT Domain (bnt2 .live)", "ET POLICY DNSWatch.info IP Check", "ET MALWARE Win32/Eternity Activity (POST)", "ET MALWARE GoLinux/GoTrim CnC Checkin", "ET MALWARE MWI Maldoc Stats Callout Oct 28", "ET HUNTING Possible Kimsuky Related

	Malicious VBScript Inbound", "ET MALWARE BlackEnergy POST Request", "ET MALWARE Possible Pegasus Related DNS Lookup (mz-vodacom .info)", "ET MALWARE linux.backdoor.wordpressexploit file upload test", "ET MALWARE PyPI Malicious Library Payload Delivery Domain (python-release .com) in DNS Lookup", "ET MALWARE TinyNuke VNC Checkin", "ET MALWARE Trojan.Verblecon User Agent Observed", "ET MALWARE TA457 Related Activity M2 (POST)", "ET MALWARE Observed DNS Query to Ursnif Domain (gigimas .xyz)", "ET USER_AGENTS Suspicious User-Agent (checkonline)", "ET MALWARE Towerweb Ransomware Landing Page", "ET MALWARE Observed DNS Query to Budminer Domain (mosec .twgogo .org)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 4", "ET MALWARE Wintervivern Retrieving Commands", "ET WEB_SERVER WebShell - Pouya - URI - action=", "ET INFO tor2www .onion Proxy SSL cert", "ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory", "ET MALWARE Possible Maldoc Downloader Aug 18 2017", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (deftsecurity .com)", "ET MALWARE Jorik FakeAV GET", "ET WEB_SERVER WebShell - Generic - GIF Header With HTML Form", "ET INFO WinHttpRequest Downloading EXE", "ET MALWARE Drive Receiving UDP DDoS instructions", "ET MALWARE Patchwork APT Related Activity (POST)", "ET MALWARE rechnung zip file download", "ET MALWARE MSIL/G1 Stealer/GravityRAT Uploading File", "ET MALWARE Legion Loader Activity Observed", "ET MALWARE Observed DNS Query to TA455 Domain (librarycollection .org)", "ET MALWARE Windows qwinsta Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed ProtonBot User-Agent", "ET MALWARE Gamaredon APT Related Activity (GET)", "ET HUNTING SUSPICIOUS mssrs.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE DonotGroup Related Domain in DNS Lookup (mimeversion .top)", "ET EXPLOIT Zollard PHP Exploit UA", "ET MALWARE Win32/TrojanDownloader.Agent.GEM Maldoc Remote Template Request M2", "ET MALWARE Observed DNS Query to Budminer Domain (jgx .explorermaker .com)", "ET MALWARE Embedded Android Dalvik Executable File With Fake Windows Executable Header - Possible AV Bypass Attempt", "ET MALWARE PE EXE or DLL Windows file download disguised as ASCII", "ET MALWARE FOX-SRT ShimRat check-in (Data)", "ET MALWARE JavaRAT Requesting Screenshot", "ET MALWARE Polonium CreepyDrive Implant Request", "ET DNS Reply Sinkhole - Dr. Web", "ET CNC Feodo Tracker Reported CnC Server group 6", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Wroba.m Checkin", "ET MALWARE Possible DANDERSPRITZ Default HTTP Headers", "ET MALWARE Observed DNS Query to Ursnif Domain (pipap .xyz)", "ET MALWARE ChromeLoader CnC Checkin M1", "ET MALWARE Gamaredon Related Maldoc Activity (GET)", "ET MALWARE RedditC2 Related Activity M2 (POST)", "ET EXPLOIT Possible EXPLODINGCAN IIS5.0/6.0 Exploit Attempt", "ET MALWARE Win32/Nemty Ransomware Style Geo IP Check M2", "ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .live)", "ET MALWARE Win32/Bancos URL Structure", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to digitalcollege .org", "ET MALWARE Windows netsh advfirewall show allprofiles Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Observed Ursnif Domain in TLS SNI (rorfog .com)", "ET MALWARE PRG/wnspoem/Zeus InfoStealer Trojan Config Download", "ET POLICY HTTP Request to Lockbit Ransomware Payment Domain", "ET MALWARE Observed Godlua Backdoor Domain (c .heheda .tk in TLS SNI)", "ET MALWARE Win32/Fareit Variant Activity (POST)", "ET MALWARE Unk.CoinMiner Loader Checkin", "ET MALWARE Legion Loader Activity Observed (heil_moloch)", "ET MALWARE Win32/PurpleWave Stealer Requesting Config", "ET MALWARE SocGholish Domain in DNS Lookup (office .cdsigner .com)", "ET MALWARE XLS.Unk DDE rar Drop Attempt (.club)", "ET MALWARE TA569 Fake Browser Update", "ET MALWARE Pandorahvnc/Pikolo RAT Checkin Activity", "ET MALWARE TA453 Related Domain in DNS Lookup (litby .us)", "ET MALWARE Observed Buran Ransomware UA (GHOST)", "ET MALWARE VoidRay Downloader CnC Activity", "ET MALWARE Observed DNS Query to Budminer Domain (zoneprenuin .crabdance .com)", "ET MALWARE Scarlet Mimic DNS Lookup 24", "ET USER_AGENTS Suspicious User-Agent (INSTALLER)", "ET MALWARE Trojan.Nurjax Retrieving Domains via JS", "ET MALWARE Filez Downloader Checkin",

	"ET MALWARE Observed DNS Query to Budminer Domain (tdns .verydvcd .com)", "ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling", "ET MALWARE Win32/MereTam.A Ransomware CnC Checkin", "ET MALWARE PNScan.2 Inbound Status Check - set", "ET MALWARE Observed DNS Query to TA444 Domain (stablehouses .info)", "ET MALWARE Observed DNS Query to TA444 Domain (cooporatestock .com)", "ET MALWARE LokiBot Application/Credential Data Exfiltration Detected M2", "ET MALWARE Zhelatin npopup Update Detected", "ET MALWARE Observed DNS Query to Budminer Domain (wephone .us .to)", "ET MALWARE Observed DNS Query to Budminer Domain (bestcom .dns2 .us)", "ET MALWARE Win32.Blackbeard Downloader", "ET MALWARE Haxdoor Reporting User Activity 2", "ET MALWARE JS/Nemucod requesting EXE payload 2016-03-31", "ET MALWARE Win32/Spy.Obator .onion Proxy Domain", "ET MALWARE Win32/a310Logger Data Exfil via SMTP", "ET MALWARE US-CERT TA14-353A Listening Implant 6", "ET MALWARE W32/Quasar 1.3/Venom RAT Connectivity Check 2", "ET MALWARE Win32/DarkCloud Exfil Over SMTP (Subject)", "ET CNC Feodo Tracker Reported CnC Server group 5", "ET MALWARE Windows WMIC NIC get Microsoft Windows DOS prompt command exit OUTBOUND", "ET MOBILE_MALWARE NSO Related Domain 9", "ET MALWARE Observed DNS Query to Budminer Domain (mains .tainoetnde .bgphome .com)", "ET MALWARE Predator Pain Keylogger FTP", "ET MALWARE Win32.Tdss User Agent Detected (Mozzila)", "ET MALWARE BB Trojan Communication Protocol detected", "ET MALWARE Tandem Espionage CnC Domain (dvizhdom .ru) in DNS Lookup", "ET MALWARE FaceBook IM & Web Driven Facebook Trojan Posting Data", "ET EXPLOIT CVE-2016-0189 Exploit HFS Actor", "ET POLICY Snadboy.com Products User-Agent", "ET CURRENT_EVENTS Sliver Related Domain in DNS Lookup (saleforces-it .com)", "ET MALWARE Drive Receiving GET DDoS instructions", "ET MALWARE Cobalt Strike Activity", "ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M1", "ET MALWARE Observed Ursnif Domain in TLS SNI (pipap .xyz)", "ET MALWARE JS/Cloud9 Clipboard Exfiltration Attempt", "ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .tk)", "ET MALWARE [Fireeye] Backdoor.BEACON M4", "ET MALWARE ELF/Miner Loader Activity M2 (GET)", "ET MALWARE Unknown Rootkit Download Activity (GET)", "ET MALWARE Possible CopyKitten DNS Lookup (elasticbeanstalk .tech)", "ET MALWARE Snake Keylogger CnC Exfil via Telegram", "ET WEB_SERVER JSP.SJavaWebManage WebShell Access", "ET WEB_CLIENT Office Discovery HTA file Likely CVE-2017-0199 Request M2", "ET INFO Probably Evil Long Unicode string only string and unescape 1", "ET MALWARE Suspected Tunna Proxy M1 (Outbound)", "ET MALWARE Win32/Killav.CM CnC Response", "ET MALWARE IoT_reaper DNS Lookup M3 (hi8529 .com)", "ET EXPLOIT Metasploit Browser Exploit Server Plugin Detect 2", "ET MALWARE Possible WannaCry DNS Lookup 3", "ET MALWARE BlackEnergy v2.x HTTP Request with Encrypted Variables", "ET MALWARE ELF/muBoT IRC Activity 1", "ET MALWARE [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message", "ET MALWARE JS/Nemucod.M.gen requesting EXE payload 2015-11-02", "ET MALWARE TA569 Domain in DNS Lookup (luxury-limousine .com)", "ET MALWARE ATTACKER IRCBot - The command completed successfully - PRIVMSG Response", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .boonty .Got-Game .org)", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (srv .fazlollah .net)", "ET MALWARE Possible PlugX Common Header Struct", "ET MALWARE ELF/Mirai Variant UA Outbound (Solar)", "ET MALWARE DPRK HIDDEN COBRA DDoS Handshake Success", "ET MALWARE Drop.Agent.bfsv HTTP Activity (UsER-AgENt)", "ET MALWARE Win32/PurpleWave Stealer CnC Exfil M2", "ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M1", "ET MALWARE OSX/Shlayer Malicious Download Request", "ET MALWARE ABUSE.CH Ransomware Domain Detected (TeslaCrypt Payment)", "ET MALWARE Hacking Team Implant Exfiltration", "ET MALWARE Malicious VBS Downloader fake image zip", "ET MALWARE Malicious Mega Chrome Extension Exfil Domain (www .megaopac .host in DNS Lookup)", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to freescanonline .com", "ET MALWARE JS.ElectronBot.B.F7A4D930 Downloader (GET)", "ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce 2]", "ET MALWARE Possible Covenant Framework Grunt Stager HTTP Download

	(Grunt.GruntStager)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (screenshot.) M2", "ET MOBILE_MALWARE Android/GoldDream Task Information Retrieval", "ET MALWARE IoT_reaper DNS Lookup M7 (ha859 .com)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Joker Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (whlu .congci .info)", "ET MALWARE Observed ExecPS/Cobolt Domain (getfreshnews .com in DNS Lookup)", "ET MALWARE IOS.Oneclickfraud HTTP Host", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (linux .wy01 .vip)", "ET MALWARE Possible Pegasus Related DNS Lookup (secure-access10 .mx)", "ET MALWARE SteamStealer Domain in SNI", "ET MALWARE Unk.DPRK MalDoc SysInfo CnC Exfil", "ET MALWARE Ransomware Locky .onion Payment Domain (mphtadhci5mrdlju)", "ET WEB_SPECIFIC_APPS ManageEngine Desktop Central Administrator Account Creation", "ET MALWARE Win32/Teslacrypt Ransomware .onion domain (7hwr34n18.com)", "ET MALWARE Lucky Ransomware Reporting Successful File Encryption", "ET MALWARE HTTP Andromeda File Request", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 6", "ET MALWARE MAGICHOUND-related DNS Lookup (msservice .site)", "ET MALWARE Observed DNS Query to Budminer Domain (kdmm .t28 .net)", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (highdatabase .com in TLS SNI)", "ET MALWARE ELF/Miner Loader Activity M1 (GET)", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.hk)", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M4", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 2", "ET MALWARE MAGICHOUND-related DNS Lookup (timezone .live)", "ET MALWARE CCleaner Backdoor DGA Domain (ab33b8aa69bc4 .com) Oct 2018", "ET MALWARE Android/AhMyth RAT WebSocket Session", "ET MALWARE ProjectSauron Remsec DNS Lookup (wildhorses.awardspace.info)", "ET MOBILE_MALWARE Android/DwnlAPK-A Configuration File Request", "ET MALWARE IP2B Trojan Communication Protocol detected", "ET MALWARE Scieron DNS Lookup (logoff.ddns.info)", "ET MALWARE Observed DNS Query to Budminer Domain (Artor .terelation .com)", "ET MALWARE Suckfly/Nidiran Backdoor DNS Lookup", "ET POLICY FreeRide Games Some AVs report as TrojWare.Win32.Trojan.Agent.Gen", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a Checkin 2", "ET MALWARE MSIL/PSW.Agent.QJK Stealer Data Exfil Via HTTP", "ET MALWARE ABUSE.CH Locky Domain", "ET MALWARE Banker/Banbra Variant POST via x-www-form-urlencoded", "ET MALWARE Observed DNS Query to Ursnif Domain (dodstep .cyou)", "ET MALWARE OSX/MapperState CnC Activity", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (polussuo .com)", "ET MALWARE Magecart Exfil Domain in DNS Lookup (convert-server .com)", "ET MALWARE CCleaner Backdoor DGA Domain (ab3520430c23 .com) May 2017", "ET HUNTING Observed Malicious Filename in Outbound POST Request (Information.txt)", "ET MALWARE TorrentLocker DNS Lookup (tweeterplanet.ru)", "ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (python-release .com) in TLS SNI", "ET MALWARE FIN7 JSSLoader Activity (GET)", "ET MALWARE Possible Tinba DGA NXDOMAIN Responses", "ET MALWARE Observed DNS Query to ROMCOM RAT Domain (optasko .com)", "ET MALWARE Possible Drive DDoS Check-in", "ET MALWARE Win32/RecordBreaker - Observed UA M1", "ET MALWARE Likely MAGICHOUND.FETCH Receiving PowerSploit PowerShell over HTTP", "ET MALWARE Observed TA444 Domain (azure-protect .online in TLS SNI)", "ET MALWARE FortDisco Reporting Status", "ET MALWARE OSX/Proton.B Domain in SNI", "ET INFO Obfuscated Eval String 5", "ET MALWARE Win32/Aurora Stealer WORK Command", "ET MALWARE Observed DNS Query to Hilal RAT Domain (archery .dedyn .io)", "ET MALWARE MSIL/MosaiqueRAT CnC Checkin", "ET MALWARE Cryptolocker .onion Proxy Domain", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (wallet.dat) M1", "ET MOBILE_MALWARE Apple iPhone Implant - Upload Files", "ET MALWARE Conficker.b Shellcode", "ET MALWARE Generic gate .php GET with minimal headers", "ET MALWARE Konni APT MalDoc Activity (GET)", "ET WEB_CLIENT DRIVEBY Redirection - Injection - Modified Edwards Packer Script", "ET POLICY Petite Packed Binary Download", "ET MOBILE_MALWARE Android/Code4hk.A Checkin", "ET

	MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 4", "ET MALWARE MS Office Macro Dridex Download URI Jan 7 2015", "ET MALWARE Megumin v2 Stealer User-Agent", "ET MALWARE SWORD Sending Sword Marker", "ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .me)", "ET MALWARE [PTsecurity] Black Stealer Exfil FTP STOR", "ET MALWARE Observed DNS Query to Budminer Domain (specas .OurHobby .com)", "ET MALWARE TA453 Related Domain in DNS Lookup (de-ma .online)", "ET MALWARE Observed Pegasus Domain (api1r3f4 .redirectweburl .com in TLS SNI)", "ET MALWARE Observed DNS Query to TA444 Domain (tptf .fund)", "ET MOBILE_MALWARE Android BatteryBotPro Checkin 2", "ET MALWARE MSIL/Injector.VVP Downloader Activity M1", "ET MOBILE_MALWARE Android Brunhilda Dropper (multifuctionscanner .club in TLS SNI)", "ET MALWARE Possible FortDisco Reporting Hacked Accounts", "ET MALWARE Win32/NitroStealer/exoStub CnC Exfil", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (dingpsounda .space in DNS Lookup)", "ET MOBILE_MALWARE Android Trojan Fake10086 checkin 2", "ET USER_AGENTS Suspicious User-Agent (Session) - Possible Trojan-Clicker", "ET MALWARE Skeleton Key Filename in SMB Traffic (ASCII)", "ET MALWARE Observed DNS Query to Budminer Domain (yahoonews .twgg .org)", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (freescanonline .com)", "ET MALWARE Gazer DNS query observed (soligro . com)", "ET MALWARE Scarlet Mimic DNS Lookup 1", "ET USER_AGENTS Suspicious User-Agent (Accessing)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (google_chrome_default_) M2", "ET MOBILE_MALWARE Android Fancy Bear Checkin 4", "ET MALWARE Zeus Bot Connectivity Check", "ET MALWARE Possible DarkRats Tor Traffic", "ET MOBILE_MALWARE Android Marcher Trojan Download - Raiffeisen Bank Targeting (set)", "ET MALWARE Smokeloader getload Command", "ET MALWARE Win32/H0lyGh0st Ransomware Exfil Activity (POST)", "ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS Mambo Scanning Message", "ET MOBILE_MALWARE NSO Related Domain 2", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (scradm .in in DNS Lookup)", "ET MALWARE Possible Winnti-related Destination (google-searching .com)", "ET MALWARE GravityRAT CnC Domain (dailybuild .mozillaupdates .com in DNS Lookup)", "ET MALWARE MalDoc Retrieving Payload 2021-06-15", "ET WEB_CLIENT Likely Driveby Delivered Malicious PDF", "ET MALWARE Observed DNS Query to Pegasus Domain (start-anew .net)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (privateanbshouse .space in DNS Lookup)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(TCBFRVDEMS)", "ET MALWARE CSharp SMB Scanner Assembly in PowerShell Inbound M1", "ET INFO file possibly containing Serialized Data file", "ET MALWARE Bamital Connectivity Check", "ET MALWARE FIN7 JSSLoader Variant Activity (GET)", "ET MALWARE Dorkbot Loader Payload Request", "ET MALWARE Possible Emotet DGA NXDOMAIN Responses", "ET MALWARE Win32/Vulturi CnC Activity (GET)", "ET MALWARE Observed DNS Query to TA455 Domain (freechess .live)", "ET MALWARE SysJoker Related Domain in DNS Lookup (winaudio-tools .com)", "ET INFO DRIVEBY Generic - *.com.exe HTTP Attachment", "ET MALWARE TA444 Domain in DNS Lookup (dnx .capital)", "ET MALWARE Generic - POST To .php w/Extended ASCII Characters", "ET WEB_SERVER Jorgee Scan", "ET MALWARE Win32/Arkei Stealer CnC Checkin (POST)", "ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Jun 2019- Dec 2019) (set)", "ET MALWARE BACKCONFIG CnC Downloader Activity", "ET MALWARE Malicious Second Stage Payload Inbound 2021-02-19", "ET MALWARE GCleaner Downloader Activity M3", "ET MALWARE linux.backdoor.wordpressexploit.2 CnC Checkin", "ET USER_AGENTS Suspicious User-Agent (IE)", "ET HUNTING SUSPICIOUS EXE Download from Google Common Data Storage with no Referer", "ET MALWARE Observed SystemBC CnC Domain in DNS Query", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (oauth3 .html5100 .com in DNS Lookup)", "ET MALWARE Java EXE Download by Vulnerable Version - Likely Driveby", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DEMOMAKE)", "ET MALWARE NEODYMIUM Wingbird DNS Lookup (srv602 .ddns.net)", "ET MALWARE Win32/Enosch.A gtalk connectivity check", "ET MALWARE Observed Magecart Skimmer Domain (googletagsmanager .website in

	TLS SNI)", "ET MALWARE Possible Worm W32.Svich or Other Infection Request for setting.doc", "ET MALWARE Win32/Ficker Stealer Activity M3", "ET WEB_SERVER Win32/SessionManager2 Backdoor S5WRITE Command (Inbound)", "ET MALWARE Win32/Pripyat Activity (POST)", "ET MALWARE Observed TA444 Domain (ms .onlineshares .cloud in TLS SNI)", "ET WEB_CLIENT FoxxySoftware - Landing Page", "ET MOBILE_MALWARE Android Fancy Bear Checkin 2", "ET ATTACK_RESPONSE Zone-H.org defacement notification", "ET MALWARE Observed DNS Query to Budminer Domain (kelsdc .compress .to)", "ET MALWARE Observed DNS Query to TA455 Domain (etisalatonline .com)", "ET USER_AGENTS Suspicious User-Agent (Download App)", "ET MALWARE Buer - DomainInfo User-Agent", "ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Command Fetch", "ET MALWARE Transparent Tribe APT Related Backdoor Sending System Information", "ET MALWARE Octopus Malware Initial Connectivity Check", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (viewnet .better-than.tv)", "ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (StatusTime)", "ET MALWARE Possible AMSI Powershell Bypass Attempt B643", "ET MALWARE Linux/Torte Downloading Binary", "ET MALWARE Turla JS/Kopiluwak Sending Information (POST)", "ET MALWARE Suspected SandCat Related Communication (POST)", "ET MALWARE Suspected Win32/TinyNode Activity (Outbound)", "ET WORM Rimecud Worm checkin", "ET MALWARE Win32/MagicRAT Additional Payload URI M1", "ET MALWARE Observed DNS Query to W32/Filecoder.KY!tr.ransom Domain (ec2-3-125-223-134 .eu-central-1 .compute .amazonaws .com)", "ET MALWARE Possible Winnti-related DNS Lookup (google-searching .com)", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (helpzonecisco .com)", "ET MALWARE Fruspam polling for IP likely infected", "ET MALWARE Observed DNS Query to TA455 Domain (applytalents .com)", "ET MALWARE Win32/Napolar.A Getting URL", "ET WEB_SERVER China Chopper WebShell Observed Outbound", "ET MALWARE OSX/ZuRu Activity (POST)", "ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to seobundlekit .com", "ET MALWARE Observed DNS Query to Budminer Domain (wmdshr .3322 .org)", "ET MALWARE Win32/Pterodo CnC Activity (POST)", "ET MALWARE Interactsh Control Panel (DNS)", "ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (akademia-mil .space)", "ET MOBILE_MALWARE NSO Related Domain 34", "ET MALWARE [PTsecurity] JS.Trojan-Downloader.Nemucod.yo HTTP POST (:Exec:)", "ET MALWARE APT-C-23 Activity (POST)", "ET MALWARE Novaloader Stage 2 VBS Request", "ET MALWARE Stobox Connectivity Check", "ET MALWARE J-Spy JSP webshell response", "ET MALWARE DOC/TrojanDownloader.Agent.ARJ Payload Request", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Google Chrome.txt) M1", "ET MALWARE Fake Software Download Redirect Leading to Malware M3", "ET MALWARE Observed DNS Query to Budminer Domain (post .ourhobby .com)", "ET MALWARE W32/Nolja Trojan User-Agent (FileNolja)", "ET MALWARE Observed DNS Query to TA455 Domain (office-shop .me)", "ET MALWARE Maldoc CnC Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (security .MyNetAV .ORG)", "ET MOBILE_MALWARE NSO Related Domain 27", "ET MALWARE Observed TA444 Domain (tptf .fund in TLS SNI)", "ET MALWARE ABUSE.CH Cryptolocker Payment Page (de2nuvwegoo32oqv)", "ET MALWARE Brute Ratel CnC Activity (json-c2) M2", "ET MALWARE Windows WMIC SHARE get Microsoft Windows DOS prompt command exit OUTBOUND", "ET JA3 Hash - Trojan.AndroidOS.Jocker.snt 1", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(folderwin)", "ET MALWARE rat-test CnC Response", "ET MALWARE Observed Godlua Backdoor Domain (dd .cloudappconfig .com in TLS SNI)", "ET MALWARE Possible Evil Macro Downloading Trojan Dec 16 2015 Post to EXE", "ET MALWARE Win32/Malgent!MSR Dropper Requesting Payload", "ET MOBILE_MALWARE Android Fancy Bear Checkin", "ET MALWARE Win32/a310Logger Clipboard Exfil via SMTP", "ET WEB_SERVER ATTACKER WebShell - 1337w0rm - Landing Page", "ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (cspapop110 .com)", "ET WEB_CLIENT DRIVEBY EXE Embeded in Page Likely Evil M2", "ET DNS Reply Sinkhole FBI Zeus P2P 1 - 142.0.36.234", "ET MALWARE UIWIX Ransomware .onion Payment Domain (4ujngbdqqm6t2c53)", "ET

	MALWARE Win32/Emotet CnC Activity (POST) M9", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to websitetheme .com", "ET MALWARE Cashout Proxy Bot reg_DST", "ET MALWARE Suspected Tunna Proxy M2", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to virtualdataserver .com", "ET USER_AGENTS Suspicious User-Agent Possible Trojan Downloader Shell", "ET MALWARE Win32/Cryptbotv2 Activity (POST)", "ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .twnic .almostmy .com)", "ET MALWARE Woody RAT Payload Delivery Domain (fcloud .nciinform .ru) in DNS Lookup", "ET MALWARE Arid Gopher Related User-Agent (aimxxhwpcc)", "ET MALWARE DonotGroup Related Domain in DNS Lookup (ppadoaolnwod .xyz)", "ET MALWARE Blackmoon/Banbra Configuration Request", "ET MALWARE Observed TraderTraitor Domain (dafom .dev) in TLS SNI", "ET MALWARE Observed Malicious SSL Cert (Microsoft Security localhost)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a Checkin", "ET MALWARE Possible Dyre SSL Cert (fake state)", "ET MALWARE Observed Koadic Header Structure", "ET POLICY Powershell Command With Hidden Window Argument Over SMB - Likely Lateral Movement", "ET MALWARE SunSeed Lua Downloader Activity (GET)", "ET WEB_CLIENT Possible FortDisco Wordpress Brute-force Site list download 10+ wp-login.php", "ET MALWARE Downeks/Quasar DNS Lookup (signup .updatesforme .club)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (newsagent .quest)", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access registerMicListener", "ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 1", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (financialtrending .com)", "ET MALWARE Observed Trojan.Verblecon Related Domain (.verble .rocks in TLS SNI)", "ET MALWARE Netwire RAT Check-in 2", "ET MALWARE Wintervivern Activity M5 (GET)", "ET MOBILE_MALWARE Android Spyware Dowgin Checkin", "ET MALWARE StrongPity CnC Domain Observed in DNS Query", "ET MALWARE Observed DNS Query to Ursnif Domain (kidup .xyz)", "ET MALWARE TA444 Related CnC Payload Request", "ET INFO HTTP Request with Double Cache-Control", "ET MALWARE Win32/Spy.Tuscas", "ET MOBILE_MALWARE NSO Related Domain 30", "ET USER_AGENTS Suspicious User-Agent (opera)", "ET MALWARE System Information Being Sent in User-Agent", "ET MALWARE LokiBot Fake 404 Response", "ET MALWARE Vobus/Beebone Sinkhole DNS Reply", "ET MALWARE Suspected ExtraPulsar Backdoor", "ET MALWARE Corebot Module Download 2", "ET MALWARE MoneroOcean Installer Batch Script Inbound", "ET MALWARE Possible Pegasus Related DNS Lookup (smser .net)", "ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2", "ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M6", "ET MOBILE_MALWARE Android Golden Rat Checkin", "ET MALWARE Likely Evil EXE download from WinHttpRequest non-exe extension", "ET MALWARE Executioner Ransomware Reporting Infection via SMTP", "ET USER_AGENTS Suspicious User-Agent (MyAgent)", "ET MALWARE Observed TA444 Domain (dnx .capital in TLS SNI)", "ET MALWARE Observed DNS Query to TA455 Domain (elecresearch .org)", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[Build ID]", "ET MALWARE Kimsuky APT Related Host Data Exfil M5", "ET MALWARE Observed Blackguard_v3.5 Domain (ritmflow .online) in TLS SNI", "ET MALWARE Backdoor.Irc.MFV User Agent Detected (IRC-U)", "ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS Attacking Message", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (decfurnish .com)", "ET MALWARE Possible Kaseya VSA Exploit Activity Inbound M1", "ET MALWARE Trickbot Anchor ICMP Request", "ET MOBILE_MALWARE Android Marcher Trojan Download - Sparkasse Bank Targeting (set)", "ET USER_AGENTS Suspicious User-Agent VCTestClient", "ET MALWARE Netbounce Program Wrapper Download", "ET MALWARE Observed DNS Query to Pegasus Domain (reunionlove .net)", "ET MALWARE Observed DNS Query to Budminer Domain (soft .update .cloudns .info)", "ET MALWARE Python CTX Library Backdoor Domain in DNS Lookup (anti-theft-web .herokuapp .com)", "ET MALWARE Win32/Fynloski.AA CnC Checkin", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (selectnew25mode .space in DNS Lookup)", "ET MOBILE_MALWARE Android TrojanFakeLookout.A", "ET MALWARE HTran/SensLiceId.A

	response to infected host", "ET MALWARE Observed DNS Query to TA455 Domain (onedriveupdate .net)", "ET MALWARE ROMCOM RAT Campaign Domain (keepas .org) in DNS Lookup", "ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cddn .site)", "ET MALWARE Observed DNS Query to TA444 Domain (share .anobaka .info)", "ET MALWARE Observed DNS Query to Budminer Domain (info .IsASecret .com)", "ET USER_AGENTS Supicious User-Agent (RT/1.0)", "ET MALWARE Legion Loader Activity Observed (the devil)", "ET MALWARE HermeticWizard - WMI Spreader - Remote Process Creation M1", "ET MALWARE Pegasus Domain in DNS Lookup (akhbar-islamyah .com)", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M7", "ET MALWARE CenterPOS Delete Plugins", "ET MALWARE Observed ZLoader CnC Domain in SNI", "ET MALWARE Maldoc Activity (GET)", "ET MALWARE Likely Koobface Beaconing (getexe)", "ET MALWARE Possible Win32/Petya Conn Check", "ET MALWARE ELF.MrBlack DOS.TF Malformed Lookup (/lib32/libc.so.6)", "ET HUNTING SUSPICIOUS pony.exe in URI", "ET MALWARE TA569 Obfuscated sczriptzzb JavaScript Inject", "ET MALWARE MassLogger Client Exfil (POST) M3", "ET MALWARE Volatile Cedar DNS Lookup (erdotntexplore.info)", "ET MALWARE Possible CopyKittens DNS Lookup (haaretz-news.com)", "ET MALWARE CCleaner Backdoor DGA Domain (abce85a51bbd .com) Aug 2018", "ET MALWARE Win32/RecordBreaker - Observed UA M5 (23591)", "ET MALWARE Win32/QQPass Checkin", "ET MALWARE Chthonic Check-in", "ET POLICY Android.Plankton/Tonclank Successful Installation Device Information POST Message Body", "ET ADWARE_PUP AlphabetSoup Adware Extension CnC Checkin", "ET MALWARE GoldenSpy Domain Observed", "ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (lcomputers .com)", "ET ATTACK_RESPONSE Unusual FTP Server Banner (NzmxFtpd)", "ET MALWARE Worm.Win32.Ngrbot.lof Join IRC channel", "ET MALWARE Laplas Clipper - Regex CnC Request", "ET MALWARE Observed DNS Query to ShadowPad Domain (supership .dynv6 .net)", "ET MALWARE Maldoc Sending Windows System Information (POST)", "ET MALWARE Iron Tiger Gh0ST/PlugX/Various Backdoors DNS Lookup (gameofthrones.ddns.net)", "ET MALWARE Possible Pony Payload DL", "ET MALWARE Malware Connectivity Check to Google", "ET MALWARE CargoBay User-Agent", "ET MALWARE TraderTraitor dafom CnC Checkin M1 (POST)", "ET MALWARE WS/JS Downloader Mar 07 2017 M2", "ET MALWARE Supercharge Component Download (exe)", "ET MALWARE Babar POST Request", "ET MALWARE Observed DNS Query to Pirate Stealer Domain (mdvksublbpczqluqvvbytfprxdwakuke .nl)", "ET MALWARE JS/Nemucod.M.gen requesting EXE payload 2015-10-07", "ET MALWARE Vundo User-Agent Check-in", "ET MALWARE Win32/Trojan.Nymeria CnC", "ET MALWARE Transparent Tribe APT Related Backdoor Receiving Command (Inbound)", "ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Request (set)", "ET MALWARE [PTsecurity] Win32/Spy.Agent.PMJ (MICROPSIA)", "ET MALWARE AlphaCrypt .onion Proxy Domain (djdkduep62kz4nzx)", "ET MALWARE W32/Echmark/MarkiRAT CnC Request", "ET MALWARE Win32/CandyOpen/UniClient Activity (POST)", "ET PHISHING Nedbank Phishing Landing Page 2022-06-22", "ET MALWARE Mimikatz x86 Mimidrv.sys File Transfer Over SMB", "ET MALWARE [Fireeye] Backdoor.SUNBURST M4", "ET MALWARE CNRarypt Ransomware CnC Activity", "ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (bot registration)", "ET MALWARE Win32/Agent.UWW Variant Activity (Retrieving Commands)", "ET MOBILE_MALWARE Android/Spy.Kasandra.A Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (expiration .toythieves .com)", "ET MALWARE Executable contained in DICOM Medical Image SMB File Transfer", "ET MALWARE Possible Netwire RAT Client HeartBeat C1 (no alert)", "ET MALWARE Suspected Mustang Panda APT Related Activity (GET)", "ET CNC Feodo Tracker Reported CnC Server group 3", "ET MALWARE indux.php check-in", "ET MALWARE Win32/RocketX Stealer CnC Exfil", "ET MALWARE TorrentLocker DNS Lookup (ssl-server24.ru)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (foddylearn .com)", "ET POLICY Android.Plankton/Tonclank Successful Installation Device Information POST", "ET INFO JAVA - Java Class Download", "ET MALWARE Win32/Delfinject Check-in", "ET MALWARE FakeAV security_scanner.exe", "ET MALWARE W2KM_BARTALEX Downloading Payload

	2", "ET MALWARE Possible Pegasus Related DNS Lookup (track-your-fedex-package .org)", "ET MALWARE Win32/X-Files Stealer Activity", "ET MALWARE MSIL/Monitor.PCTattletale.A Checkin (POST)", "ET MALWARE ELF/Mirai Variant UA Inbound (Shaolin)", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (github .wiki)", "ET MALWARE Win32/MagicRAT Additional Payload URI M2", "ET MALWARE Phorpiex Botnet Downloader Activity (GET)", "ET WEB_SERVER WebShell Generic eval of convert_uudecode", "ET MALWARE Possible Winnti-related DNS Lookup (resume .immigrantlol .com)", "ET MALWARE ELF/Mirai Variant UA Outbound (Yowai)", "ET MALWARE Observed DNS Query to TA444 Domain (cloud .mufg .uk)", "ET MALWARE RedGuard Framework Related Request Activity", "ET MALWARE Possible Maldoc Downloading EXE Jul 26 2016", "ET MALWARE W32/Downloader Secondary Download Request - W32/Hupigon.Backdoor Likely Secondary Payload", "ET MALWARE Observed IcedID Domain (ldrtoyota .casa in TLS SNI)", "ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 2", "ET MALWARE TA410 APT FlowCloud Dependency Download M3", "ET POLICY DNS Query to .onion proxy Domain (onion .casa in DNS Lookup)", "ET MALWARE Possible Office Doc with Embedded VBA containing Reverse Meterpreter Shell", "ET POLICY Powershell Command With No Profile Argument Over SMB - Likely Lateral Movement", "ET MALWARE Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-2)", "ET WEB_SERVER allow_url_include PHP config option in uri", "ET MALWARE System Progressive Detection FakeAV (GenuineIntel)", "ET MALWARE BlackshadesRAT Reporting", "ET MALWARE Observed DNS Query to TA455 Domain (talktalky .azurewebsites .net)", "ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Oracle canada)", "ET MALWARE [TGI] Py.Machete FTP Exfil 2", "ET MALWARE Observed DNS Query to Budminer Domain (skype .mrbonus .com)", "ET MALWARE [PTsecurity] PS/TrojanDownloader.Agent.NNR XORed Zip payload (key 0x91)", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (thedoccloud .com in TLS SNI)", "ET MALWARE Downloader/Linux.Agent CnC Domain (wget .hostname .help) in DNS Lookup", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 14", "ET INFO Lock Emoji In Title - Possible Social Engineering Attempt", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (showsvc .com)", "ET MALWARE PennyWise Stealer Data Exfiltration", "ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Dec 2019- Jul 2020) (set)", "ET MALWARE Backdoor.Win32.Aldibot.A User-Agent (Aldi Bot)", "ET MALWARE Known Sinkhole Response abuse.ch", "ET MALWARE Observed DNS Query to Certishell Domain (googleprovider .ru)", "ET MOBILE_MALWARE NSO Related Domain 12", "ET MALWARE Sharik/Smoke Loader Microsoft Connectivity Check", "ET MALWARE Win32.Agent.kawe SMTP Stealer", "ET MALWARE Pegasus Domain in DNS Lookup (al-taleanewsonline .net)", "ET MALWARE JS.SocGholish CnC Activity (POST)", "ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cxizi .net)", "ET MALWARE Backdoor.Win32.Ixeshe", "ET MALWARE Windows Microsoft Windows DOS prompt command Error Invalid Argument", "ET MALWARE Banker.Delf User-Agent (Mz)", "ET MALWARE PoshC2 Downloader Activity (GET)", "ET MALWARE TA410 APT LookBack Client HTTP Activity (POST)", "ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (.verble .rocks)", "ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst", "ET MALWARE Black KingDom Ransomware Related Activity", "ET MALWARE Win32/Meimaii Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (loginlived .com)", "ET ATTACK_RESPONSE Trojan.Dropper.HTML.Agent Payload", "ET MALWARE Win32/Toby.N Multilocker Image Request", "ET MALWARE HompesA Activity", "ET USER_AGENTS Suspicious User-Agent Im Luo", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 7", "ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce]", "ET MALWARE OSX/Proton.C/D Domain (handbrake .cc) in TLS SNI", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice POST]", "ET MALWARE Observed DNS Query to TA444 Domain (1drvmicrosoft .com)", "ET MALWARE HTML/Xbash Hex Encoded PowerShell Args Inbound - Stage 1", "ET MALWARE Putter Panda 3PARA RAT initial beacon", "ET WEB_CLIENT DRIVEBY EXE Embeded in Page Likely Evil M1", "ET MALWARE Observed DNS Query to TA444 Domain (wps .wpsonline .co)", "ET

	MALWARE Win32/Darkme CnC Domain in DNS Lookup (muasaashshaj .com)", "ET MALWARE Observed TA444 Domain (cloud .mufg .uk in TLS SNI)", "ET USER_AGENTS Suspicious User-Agent _updater_agent", "ET MALWARE Downloaded .bat Disables Real Time Monitoring", "ET WEB_SERVER IIS ISN BackDoor Command Get Logpath", "ET MALWARE Observed BlackGuard_v2 Domain (onetwostep .at) in TLS SNI", "ET MALWARE Observed TA444 Domain (mizuhogroup .us in TLS SNI)", "ET MALWARE Legion Loader Activity Observed (Amen)", "ET INFO Obfuscated Eval String (Single Q) 7", "ET MALWARE Zbot .onion Proxy DNS lookup July 31 2014", "ET MALWARE GoLang Discord Token Grabber Exfil", "ET MALWARE Possible CopyKitten DNS Lookup (ssl-gstatic .online)", "ET MALWARE Observed Ursnif Domain in TLS SNI (kidup .xyz)", "ET USER_AGENTS Suspicious User-Agent (SomeTimes)", "ET MALWARE MASSLOGGER Client Data Exfil (POST) M2", "ET MALWARE Eternity Stealer Data Exfiltration Activity", "ET MALWARE WinPwn PenTesting Activity", "ET POLICY Possible IP Check ip-addr.es", "ET MALWARE Chinotto CnC Activity (file)", "ET MALWARE Win32.Lager Trojan Reporting", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 17", "ET USER_AGENTS Downloader User-Agent Detected (ld)", "ET POLICY Data POST to an image file (jpg)", "ET POLICY DNS Query to .onion proxy Domain (torforall.com)", "ET MALWARE Pingback OK Issued", "ET MALWARE Possible SombRAT Initial DNS Lookup", "ET MALWARE IRC Private message on non-standard port", "ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)", "ET MALWARE Cryptolocker Payment Page (aynfksddnnfwkd)", "ET MALWARE FastPOS Sending Status Logs", "ET MALWARE ELF/Emptiness v1 UDP Flood Command Inbound", "ET MALWARE ELF/muBoT IRC Activity 4", "ET MALWARE [AV] EarthWorm/Termite IoT Agent Reporting Infection", "ET MALWARE ELF/Mirai Variant UA Outbound (Rift)", "ET MALWARE W32.Razy Inject Domain in DNS Lookup", "ET MOBILE_MALWARE Android.Trojan.SMSSend.Y", "ET EXPLOIT Possible CVE-2014-6332 Arrays with Offset Dec 23", "ET PHISHING Suspected TA445 Spearphishing Related Domain (akademia-mil .space in TLS SNI)", "ET MALWARE DarkCrystal Rat Stealer Data Exfiltration Activity", "ET MALWARE W2KM_BARTALEX August 11 2015", "ET MALWARE Observed DNS Query to W32/Filecoder.KY!tr.ransom Domain (81 .59 .117 .34 .bc .googleusercontent .com)", "ET MALWARE Linux/dtool IRC Command Complete 2", "ET MALWARE Windows nbtstat -n Microsoft Windows DOS prompt command exit OUTBOUND", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[Yelp GET]", "ET MALWARE Volatile Cedar DNS Lookup (carima2012.site90.com)", "ET WEB_CLIENT DRIVEBY Redirection - Wordpress Injection", "ET MALWARE GravityRAT CnC Domain (gozap .co .in in DNS Lookup)", "ET MALWARE Possible Pegasus Related DNS Lookup (ideas-telcel .com.mx)", "ET MALWARE Observed DNS Query to TA444 Domain (cloud .wpic .ink)", "ET MALWARE Observed DNS Query to Budminer Domain (gmailgroup .mooo .com)", "ET MALWARE Observed DNS Query to Budminer Domain (toolbar .qpoe .com)", "ET MALWARE Lazarus Decafett DNS Lookup 4", "ET MALWARE Win32/Lilith Stealer registerBot CnC Checkin", "ET MALWARE Saint Bot CnC Activity", "ET WEB_CLIENT DRIVEBY GENERIC CollectGarbage in Hex String No Seps", "ET MALWARE JavaRAT Requesting Screen Size", "ET EXPLOIT F5 BIG-IP iControl REST authentication bypass attempt (CVE-2022-1388) M2", "ET MALWARE Ponmocup HTTP Request (generic) M9", "ET MALWARE Executable contained in DICOM Medical Image Received from PACS DICOM Device", "ET MALWARE MWI Maldoc Load Payload", "ET MALWARE Win32/NetDooka Framework Related Activity (POST) M2", "ET MALWARE CIA Ransomware - wallpaper/readme retrieval attempt", "ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (dajuw .com)", "ET MALWARE PyPI Phishing/Malware Data Exfiltration Domain (linkedopports .com) in DNS Lookup", "ET MALWARE DeepEnd Research Ransomware Domain Detected", "ET HUNTING Suspicious UA (^IE[\d\s])", "ET INFO Obfuscated Eval String (Single Q) 3", "ET WEB_SERVER Win32/SessionManager2 Backdoor S5CONNECT Command (Inbound)", "ET MALWARE Possible Andromeda download with fake Zip header (1)", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (svnservices .com)", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .lily .onmypc .net)", "ET HUNTING SUSPICIOUS alg.exe in URI Probable Process Dump/Trojan Download", "ET MALWARE Go/Anubis Registration Activity", "ET MALWARE Blue Bot DDoS Logger Request", "ET

	MOBILE_MALWARE Kimsuky AppleSeed CnC Checkin M2", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .wlksbb .MrsLove .com)", "ET MALWARE Win32/Nubjub.A HTTP Check-in", "ET MALWARE ELF/Emptiness v1 HTTP Flood Command Inbound", "ET MALWARE Nemucod JS Downloader Aug 01 2017", "ET MALWARE CCleaner Backdoor DGA Domain (ab1b0eaa24bb6 .com) Jun 2018", "ET MALWARE Observed DNS Query to Budminer Domain (airlinesflightleaving .thesizeofearth .ourhobby .com)", "ET MALWARE Observed DNS Query to TA455 Domain (onedrivelive .me)", "ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .microsoftshop .org)", "ET MALWARE LokiBot Keylogger Data Exfiltration Detected M2", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookies.txt) M2", "ET MALWARE Observed Buran Ransomware UA (BURAN)", "ET MALWARE LNK/Agent.GX CnC Traffic", "ET MALWARE Vawtrak/NeverQuest Posting Data 2", "ET MALWARE TA444 Related Domain (autoprotect .com .de) in DNS Lookup", "ET MALWARE TorrentLocker DNS Lookup (octoberpics.ru)", "ET MALWARE Win32/PrivateLoader Related Activity (GET)", "ET MALWARE Win32/Necurs", "ET MALWARE Brazilian Banker SSL Cert", "ET MALWARE Blackguard_v3.5 Domain in DNS Lookup (ritmflow .online)", "ET USER_AGENTS Unknown - Java Request - gt 60char hex-ascii", "ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (market .contradecapital .com)", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (taiprotectsq .xyz in DNS Lookup)", "ET MALWARE Banito/Agent.pb Pass Stealer Email Report Outbound", "ET MALWARE Possible CopyKittens DNS Lookup (gmailtagmanager.com)", "ET MALWARE Observed DNS Query to EvilProxy Domain (evilproxy .pro)", "ET MALWARE Suspected Golang/Zerobot Websocket Activity (GET)", "ET PHISHING PhishMe.com Phishing Exercise - Client Plugins", "ET WEB_CLIENT Internet Explorer Memory Corruption Vulnerability (CVE-2016-0063)", "ET MALWARE Win32/ChromeBack Extention Payload Fetch", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco .cf)", "ET MALWARE Win32/MSIL.Heracles Checkin", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco-helpdesk .ml)", "ET MALWARE HiddenTears Ransomware Activity (GET)", "ET USER_AGENTS Suspicious User-Agent (SUiCiDE/1.5)", "ET MALWARE Windows arp -a Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE SolarBot Plugin Download WalletSteal", "ET MALWARE ATTACKER IRCBot - PRIVMSG Response - net command output", "ET INFO AutoIt User Agent Executable Request", "ET MALWARE ATTACKER IRCBot - PRIVMSG Response - Directory Listing *nix", "ET DNS Reply Sinkhole - Georgia Tech (1)", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 3", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M2", "ET MALWARE Perfect Keylogger FTP Initial Install Log Upload", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[POST]", "ET WEB_CLIENT Malicious Chrome Extension Domain Request (stickies .pro in DNS Lookup)", "ET MALWARE Possible Windows executable sent when remote host claims to send html content", "ET MALWARE Gulpix/PlugX Client Request", "ET MALWARE Win32/Alpha Stealer v1.5 PWS Exfil via HTTP", "ET MALWARE Observed DNS Query to Budminer Domain (google .dynssl .com)", "ET MALWARE AgentTesla Exfil via FTP", "ET MALWARE Ransomware Locky .onion Payment Domain", "ET MALWARE Cobalt Strike Related Activity (POST)", "ET MALWARE SocGholish Domain in DNS Lookup (notes .fumcpittsburg .org)", "ET MALWARE Legion Loader Activity Observed (legion)", "ET MOBILE_MALWARE Android/FakeKakao checkin 1", "ET MALWARE Win32/Enchanim Process List Dump", "ET MALWARE Malicious lnk Activity", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (picture .efanshion .com)", "ET USER_AGENTS Suspicious User-Agent (INet)", "ET USER_AGENTS Suspicious User-Agent Detected (RLMultySocket)", "ET WEB_SERVER Win32/SessionManager2 Backdoor FILESIZE Command (Inbound)", "ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (StnyFtpd)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadmyhost .zapto.org)", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to freescanonline .com", "ET MALWARE Likely Linux/Tsunami DDoS Attack Participation (s-p-o-o-f-e-d.h-o-s-t.name)", "ET MALWARE Soraya Credit Card Exfiltration", "ET MALWARE

	[PTsecurity] Paradise Ransomware Check-in", "ET MALWARE Panda Banker Injects Domain (urimchi3dt4 .website in DNS Lookup)", "ET MALWARE Win32/H0lyGh0st CnC Activity", "ET MALWARE Maldoc Activity Sending Windows User Info (GET)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 15", "ET WEB_SERVER safe_mode PHP config option in uri", "ET MALWARE Fake Opera 8.11 UA related to Trojan Activity", "ET MALWARE Maldoc Activity (set)", "ET MALWARE Shark Pass Stealer Email Report", "ET MALWARE TA444 Related Domain (hoststudio .org) in DNS Lookup", "ET MALWARE OSX/SHLAYER CnC Activity M2", "ET MALWARE Win32/Sehyioa Variant Activity (Download)", "ET MALWARE Innostealer Domain (windows-server031 .com) in TLS SNI", "ET MALWARE Buran Ransomware Activity M1", "ET MALWARE Possible Java/Downloader Observed in Pawn Storm CVE-2015-2590 2", "ET MOBILE_MALWARE signed-unsigned integer mismatch code-verification bypass", "ET WEB_CLIENT Evil Keitaro Set-Cookie Inbound (85937)", "ET MALWARE Win32/Lumma Stealer Data Exfiltration Attempt M1", "ET MALWARE CryptoLocker .onion Proxy Domain (zoqowm4kzz4cvvvl)", "ET MALWARE Observed Ursnif Domain in TLS SNI (vavilgo .xyz)", "ET MALWARE Observed DNS Query to Budminer Domain (relationship .epac .to)", "ET WEB_SERVER Insomnia Shell Outbound CMD Banner", "ET MALWARE Observed TraderTraitor Domain (alticgo .com) in TLS SNI", "ET MALWARE Win32/Suspected Reverse Shell Connection", "ET USER_AGENTS Aria2 User-Agent", "ET MALWARE CopyKittens Matryoshka DNS Lookup 1 (winupdate64 . com)", "ET MALWARE Observed DNS Query to Certishell Domain (forummanazera .sk)", "ET MALWARE Win32/Unk.HRESQ! MultiDownloader Checkin M2", "ET EXPLOIT Possible DOUBLEPULSAR Beacon Response", "ET MALWARE Curso Banker Downloading Modules", "ET MALWARE Observed DNS Query to AppleJeus Domain (strainservice .com)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(sendFile)", "ET WEB_SERVER DNS Query for Suspicious 54dfa1cb.com Domain - Anuna Checkin - Compromised PHP Site", "ET MALWARE PlugX Activity (POST)", "ET MOBILE_MALWARE NSO Related Domain 24", "ET POLICY RemoteSpy.com Upload Detect", "ET MALWARE Possible Pegasus Related DNS Lookup (tpcontact .co.uk)", "ET MALWARE Linux/dtool IRC Command (AUTH)", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (deftsecurity .com in TLS SNI)", "ET MALWARE SocGholish Domain in DNS Lookup (montage .travelguidediva .com)", "ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)", "ET MALWARE Win32/Lilith Stealer getFile Command", "ET WEB_CLIENT DRIVEBY Generic URLENCODED CollectGarbage", "ET MOBILE_MALWARE Possible iOS WebView Auto Dialer 2", "ET MALWARE Observed DNS Query to Maldoc Domain (webnar .info)", "ET MALWARE Known Sinkhole Response Header INetSim", "ET MALWARE Observed DNS Query to Budminer Domain (money .terelation .com)", "ET WEB_SERVER ATTACKER WebShell - Weevely - POSTed", "ET MOBILE_MALWARE NSO Related Domain 8", "ET MALWARE MSIL/Almashreq Executing New Processes", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (aksconsulting .us)", "ET MALWARE SocGholish Domain in DNS Lookup (resort .reliablecommunityservices .com)", "ET MALWARE Observed DNS Query to known Avaddon Ransomware Payment Domain", "ET MALWARE JS Skimmer Domain in DNS Lookup", "ET MALWARE Possible Pegasus Related DNS Lookup (sms .webadv.co)", "ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (websitetheme .com in TLS SNI)", "ET MALWARE Impersoni-fake-ator backdoor CnC Checkin", "ET MALWARE Possible Pegasus Related DNS Lookup (univision .click)", "ET ATTACK_RESPONSE JS/Spy.Banker.LD Credit Card Skimmer Inbound", "ET MALWARE X-Malware-Sinkhole Header in HTTP Response", "ET MALWARE Possible Zbot Activity Common Download Struct", "ET MALWARE Observed DNS Query to Budminer Domain (oop .crabdance .com)", "ET MALWARE Tandem Espionage CnC Domain (aztkiryhetxx .ru) in DNS Lookup", "ET MALWARE Inbound PowerShell Executing Base64 Decoded VBE from Temp 2018-11-29", "ET MALWARE FBot Downloader Generic GET for ARM Payload", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (digitalcollege .org)", "ET MALWARE Win32/Urausy.C response", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (weeklylive .info)", "ET MALWARE HermeticWizard - WMI Spreader - File Copy via SMB2 (NT Create AndX Request)", "ET MALWARE

	ProxyBot Phone Home Traffic", "ET MALWARE Observed DNS Query to Budminer Domain (update .madicity .org)", "ET MALWARE ESPecter Bootkit Initialization Activity (GET)", "ET MALWARE Pult Downloader Activity", "ET MOBILE_MALWARE Android Spy APT-C-23 (frances-thomas .com in DNS Lookup)", "ET MALWARE Observed DNS Query to TA455 Domain (lukoil .in)", "ET MALWARE ErbiumStealer Response From CnC", "ET POLICY Explorer Shell CLSID COM Object Call Method Inbound via TCP", "ET MALWARE Win32/STEALBIT Data Exfiltration Tool Activity (PUT)", "ET MALWARE Observed DNS Query to Budminer Domain (renders .maninta .anichgroup .com)", "ET MALWARE Generic .bin download from Dotted Quad", "ET MOBILE_MALWARE NSO Related Domain 20", "ET MALWARE TA444 Related Domain (autoprotect .gb .net) in DNS Lookup", "ET INFO Tor2Web .onion Proxy Service SSL Cert (1)", "ET MALWARE Observed DNS Query to Ursnif Domain (mainwog .xyz)", "ET MALWARE Possible CopyKittens DNS Lookup (heartax.info)", "ET MALWARE Possible CopyKittens DNS Lookup (big-windowss.com)", "ET MALWARE Potential Juniper Phar Deserialization RCE Attempt (CVE-2022-22241)", "ET MALWARE Win32/Cryptrun.B Connectivity check", "ET MALWARE Unknown DPRK Threat Actor Activity (GET)", "ET MALWARE JavaRAT Sending Screen Size", "ET MALWARE ErbiumStealer Response From Panel", "ET MALWARE W32/VBS.SLoad.Backdoor Initial Base64 Encoded OK Server Response", "ET PHISHING Data Submitted to ukit domain - Possible Phishing M2 2016-06-29", "ET MALWARE MSIL/Agent.CTK Checkin", "ET EXPLOIT FireEye Appliance Unauthorized File Disclosure", "ET MALWARE Generic CMD Remote Shell", "ET MALWARE Observed DNS Query to Budminer Domain (photostw .twgogo .org)", "ET USER_AGENTS Suspicious User-Agent (runUpdater.html)", "ET MALWARE W32.Qakbot Request for Compromised FTP Sites", "ET MALWARE APT29/WellMess CnC Activity", "ET MALWARE Deep Panda CnC Check-In", "ET MALWARE Suspected MuddyWater Related CnC Activity", "ET USER_AGENTS Suspicious User-Agent (Errordigger.com related)", "ET MALWARE Observed Magecart Exfil Domain (imags .pw in TLS SNI)", "ET MALWARE Common Downloader Install Report URL (wmid - ucid)", "ET MALWARE Malicious lnk Downloader Activity (GET)", "ET MALWARE Win32/DuckLogs Malware Activity (GET)", "ET MALWARE ABCbot CnC Exfil", "ET MOBILE_MALWARE Android.Trojan.Marcher.U DNS Lookup", "ET MALWARE DLoader File Download Request Activity", "ET MALWARE Win32/Killav.CM Checkin M2", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M4", "ET MALWARE Successful Cobalt Strike Shellcode Download (x32)", "ET MALWARE Possible Malicious Tor Module Download", "ET INFO EXE Download With Content Type Specified As Empty", "ET MOBILE_MALWARE NSO Related Domain 13", "ET MALWARE Lethic - Client Alive", "ET MALWARE WP CharCode Inject", "ET MALWARE Suspected Tunna Proxy M3 (Outbound)", "ET MALWARE ZINC APT Related Backdoor Activity (POST)", "ET MALWARE Observed DNS Query to Budminer Domain (bing .ikwb .com)", "ET MALWARE MSIL/Spy.Agent.DYS Exfil", "ET MALWARE Observed DNS Query to Budminer Domain (ftp .ourfriends .sexxxy .biz)", "ET P2P Bittorrent P2P Client User-Agent (Bittorrent/5.x.x)", "ET MALWARE Predator Logger Sending Data over SMTP", "ET MALWARE Zingo/GinzoStealer Stealer Exfiltration Observed", "ET MALWARE Windows driverquery -si Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE TA444 Related Domain (updatezone .org) in DNS Lookup", "ET MALWARE Powershell/PowHeartBeat CnC Checkin - ICMP", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(MBESCVDFRT)", "ET MALWARE Pony Loader default URI struct", "ET MALWARE TA457 Related Activity M3 (POST)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (speedbind .com)", "ET MALWARE Brontok User-Agent Detected (Rivest)", "ET MALWARE Possible IRC Bot Common PRIVMSG Commands", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (a-techsolutions .us)", "ET MALWARE MSIL/Golroted.B Keylogger FTP", "ET MALWARE Kriptovor Retrieving RAR Payload", "ET WEB_CLIENT c0896 Hacked Site Response Octal (Inbound)", "ET MALWARE Outbound POST Request with ps PowerShell Command Output", "ET DNS Reply Sinkhole - sinkhole.cert.pl 148.81.111.111", "ET MALWARE Sality - Fake Opera User-Agent", "ET MALWARE Kimsuky APT PebbleDash Related Activity (GET)", "ET MALWARE Ursnif Payload Request (grab32.rar)", "ET MALWARE MSUpdater Connectivity Check to Google", "ET

	MALWARE FIN12 Related WHITEDAGGER/Cobalt Strike Beacon Activity (GET)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (bk .957wan .com)", "ET MALWARE ELF.MrBlack DOS.TF Variant", "ET MALWARE Trojan/Win32.Espy Report via SMTP", "ET MALWARE Pingback Download Command Issued", "ET MALWARE Legion Loader Activity Observed (suspira)", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 4", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 8", "ET MALWARE Observed DNS Query to Ursnif Domain (isteros .com)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 13", "ET MALWARE Malicious XSL file download (FTP)", "ET MALWARE APT/Bitter Maldoc Activity", "ET MALWARE FrauDrop UA single", "ET USER_AGENTS Suspicious User-Agent Detected (WINS_HTTP_SEND Program/1.0)", "ET MALWARE W32/Rovnix Activity", "ET MALWARE ELF/Mirai Variant UA Inbound (muhstik)", "ET MALWARE Observed DNS Query to Budminer Domain (lily .onmypc .net)", "ET MALWARE CCleaner Backdoor DGA Domain (ab253af862bb0 .com) Apr 2018", "ET WEB_CLIENT Evil Keitaro Set-Cookie Inbound (9487d)", "ET MALWARE ZeroAccess Outbound udp traffic detected", "ET MALWARE Win32/SocksTroy Session Initiation Attempt M2", "ET MALWARE Possible TDSS User-Agent CMD", "ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .offerings .cloud)", "ET MALWARE Linux/Tsunami Downloader", "ET EXPLOIT LastPass RCE Attempt", "ET MALWARE Win32/DownloadAdmin Activity", "ET MOBILE_MALWARE NSO Pegasus iOS Megalodon Gatekeeper Activity (GET)", "ET MALWARE W32/Asprox.FakeAV Affiliate Download Location Response - Likely Pay-Per-Install For W32/Papras.Spy or W32/ZeroAccess", "ET MALWARE Win32/Pteranodon CnC Exfil (POST) M2", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (windriversupport .com)", "ET MALWARE Slugin.A PatchTimeCheck.dat Request", "ET USER_AGENTS Suspicious User-Agent (svchost)", "ET MALWARE Dumador Reporting User Activity", "ET MALWARE Quant Loader Download Request", "ET MALWARE Win32/MereTam.A Ransomware CnC Init Activity", "ET MALWARE Saker UA", "ET MALWARE ELF/Facefish Empty Payload (set)", "ET MALWARE IRC Channel topic scan/exploit command", "ET MALWARE Win32.Beaugrit.gen.AAAA", "ET MALWARE Meterpreter or Other Reverse Shell SSL Cert", "ET MALWARE Hiloti loader requesting payload URL", "ET MALWARE Volatile Cedar DNS Lookup (saveweb.wink.ws)", "ET MALWARE Backdoor.Win32/Dervec.gen Connectivity Check to Google", "ET MALWARE Observed Nemty Ransomware Payment Page", "ET MALWARE sysrv.ELF Exploit Success Payload Request", "ET MALWARE TA453 Related Domain in DNS Lookup (tinyurl .ink)", "ET MALWARE BleachGap Ransomware Checkin (POST)", "ET MALWARE Deep Panda Domain in DNS Lookup (vpn2 .smi1egate .com)", "ET HUNTING SUSPICIOUS DOC Download from commonly abused file share site", "ET MALWARE Linux/dtool IRC Command (STOP)", "ET ADWARE_PUP Nivesro Cheat CnC Activity M1", "ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M1", "ET MALWARE W32/Zeus.InfoStealer Infection Campaign Wav.exe Request", "ET MALWARE Corebot Requesting Module", "ET MALWARE Observed Possible PowerSploit/PowerView .ps1 Inbound", "ET MALWARE Brute Ratel CnC Activity (xml-c2) M1", "ET MALWARE Common RAT Connectivity Check Observed", "ET MALWARE Suspected PlugX Checkin Activity (udp)", "ET MALWARE Common Trojan HTTP GET Logging", "ET MOBILE_MALWARE NSO Related Domain 21", "ET MALWARE Observed DNS Query to Budminer Domain (cca .us .to)", "ET MALWARE Possible CryptoLocker TorComponent DL", "ET MALWARE Gozi check-in / update", "ET MALWARE W2KM_BARTALEX Downloading Payload M2", "ET MALWARE KeyBoy DNS Lookup (www .eleven.mypop3.org)", "ET MALWARE Win32/RM3Loader Server Response", "ET MALWARE MSIL/KeyRedirEx Banker Receiving Exit Instruction", "ET HUNTING Powershell Get-ComputerInfo Output (WindowsBuildLabEx) - Decimal Encoded", "ET HUNTING Suspicious POST With Reference to WINDOWS Folder Possible Malware Infection", "ET MALWARE Observed DNS Query to Budminer Domain (common .taiwaninfoma .uk .to)", "ET MALWARE Win32/Khaosz.A!MTB Checkin - Command Retrieval", "ET MOBILE_MALWARE Android/FakeKakao checkin 2", "ET HUNTING PNG in HTTP POST (Outbound)", "ET MALWARE Scarlet Mimic DNS Lookup 17", "ET MALWARE Cobalt Strike Beacon Activity (UNC2447)", "ET MALWARE W32/Sality Executable Pack Digital Signature ASCII Marker", "ET MALWARE Mustang

	Panda/RedDelta Downloader Activity", "ET MALWARE Windows WMIC SYSACCOUNT get Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE SideCopy APT Related Activity (GET)", "ET MALWARE Linux/dtool IRC Command (UDPFLOOD)", "ET USER_AGENTS Suspicious User Agent (ScrapeBox)", "ET MALWARE Likely Mirai Related Outbound Shell Request", "ET ATTACK_RESPONSE webr00t WebShell Access", "ET MOBILE_MALWARE AndroRAT Bitter DNS Lookup (info2t .com)", "ET MALWARE Possible MalDoc Retrieving Payload 2021-07-19", "ET MALWARE Observed Magecart CnC Domain in TLS SNI", "ET USER_AGENTS Suspicious User-Agent (VMozilla)", "ET MALWARE Cayosin Botnet User-Agent Observed M2", "ET MALWARE Probable OneLouder downloader (Zeus P2P) exe download", "ET MALWARE SolarBot Plugin Download Server Response", "ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .chirigame .com)", "ET MALWARE FIN12 Related ICECANDLE/Cobalt Strike Activity (GET)", "ET MALWARE Midhos/Medfos downloader", "ET MALWARE Phonk Trojan CnC Checkin (POST)", "ET MOBILE_MALWARE Evil Eye Android Malware Beacon", "ET MALWARE Revoyem Ransomware Check-in", "ET MALWARE Steam Steal0r", "ET MALWARE Trojan Downloader User-Agent BGroom", "ET MALWARE PowerShell/Agent.A DNS Lookup (go0gIe.com)", "ET MALWARE Cobalt Strike Beacon (Amazon Profile) M2", "ET EXPLOIT SugarCRM Auth Bypass Attempt 2022-12-31", "ET MALWARE Observed DNS Query to TA455 Domain (appslocallogin .online)", "ET MALWARE W32/Dridex Binary Download Mar 23 2016", "ET MALWARE FRAT Downloader Error Report POST", "ET MALWARE Kimsuky Related CnC Activity", "ET MALWARE Win32/RecordBreaker CnC Checkin - Server Response M2", "ET INFO Inbound PowerShell Checking for Virtual Host (Win32_DiskDevice WMI)", "ET MALWARE Zbot/Beomok/PSW - HTTP POST", "ET MOBILE_MALWARE Adware.Adwo.A", "ET MALWARE Trojan Downloader User-Agent (NOPE)", "ET MALWARE Golang/Webbfustator DNS Tunneling Activity", "ET MALWARE Win32/GenKryptik.FKJZ CnC Exfil", "ET MALWARE Possible IoT_reaper ELF Binary Request M4 (set)", "ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky Payment)", "ET MALWARE SunOrcal Reaver Domain Observed (fyoutside .com) in DNS Lookup", "ET MALWARE NoMercy Data Exfiltration M2", "ET MALWARE TigerHunter DOTM CnC Checkin", "ET MALWARE njRAT v65.0 CnC Checkin", "ET MALWARE MAGICHOUND-related DNS Lookup (com-adm.in)", "ET MALWARE Trojan.Nurjax Downloading PE", "ET USER_AGENTS Suspicious User-Agent outbound (bot)", "ET USER_AGENTS Suspicious User-Agent (InfoBot)", "ET MALWARE 000Stealer Data Exfiltration M1", "ET MALWARE Observed GandCrab Payment Domain (gandcrab in DNS Lookup)", "ET MALWARE Win32/Atomsilo Ransomware Activity (POST)", "ET USER_AGENTS Suspicious User-Agent (ItIsMe)", "ET MALWARE Observed DNS Query to Certishell Domain (ms .rousinov .cz)", "ET MALWARE CyberGate RAT User-Agent (USER_CHECK)", "ET MALWARE Nemucod JS Downloader June 12 2017", "ET MALWARE Win32/Pottieq.A Check-in", "ET MALWARE Possible Godzilla Loader Base64 Filename", "ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 2", "ET MALWARE W32/Hupigon.B User Agent TSDownload", "ET MALWARE Rogue AV Downloader concat URI", "ET MALWARE Possible Tunna Proxy Closing Connection", "ET MALWARE Observed MageCart Group 12 Domain (zolo .pw in TLS SNI)", "ET WEB_CLIENT DRIVEBY Social Engineering Toolkit Web Clone code detected", "ET MALWARE Observed DNS Query to Budminer Domain (mobiles .chickenkiller .com)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies Firefox.txt) M2", "ET MALWARE Suspected Sidewinder Activity (GET)", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 7", "ET MALWARE TrueBot/Silence.Downlaoder Screenshot Post M1", "ET MALWARE Hakbit/Thanos Ransomware BMP Download", "ET EXPLOIT Possible Tor/Noscript JS Bypass", "ET INFO Secondary Flash Request Seen (no alert)", "ET MALWARE Deep Panda Domain in DNS Lookup (giga .gnisoft .com)", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 1", "ET MALWARE Win32/MagicRAT CnC Checkin M1", "ET MALWARE Possible Win32/Napolar.A URL Response", "ET MALWARE BadRabbit Ransomware Activity Via WebDAV (cscc)", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (cisco-help .cf)", "ET MOBILE_MALWARE Android/FluBot Trojan Sending Information (POST)", "ET MALWARE InfoBot Sending

	Machine Details", "ET EXPLOIT PHP Melody v3.0 SQL Injection Attempt", "ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 2", "ET MALWARE METALJACK APT32 DNS Lookup (jcdn.jsoid.com)", "ET INFO Obfuscated Eval String 7", "ET MALWARE Win32/Detplock Checkin via SMTP", "ET USER_AGENTS Suspicious user agent (Google page)", "ET HUNTING SUSPICIOUS .CPL File Inside of Zip", "ET MALWARE IRC Bot Download http Command", "ET MALWARE PingPull Related Activity (Outbound)", "ET MALWARE Known Sinkhole Response Header", "ET MALWARE SocGholish Domain in DNS Lookup (myfood .silverspringfoodproject .org)", "ET MALWARE Virut Family GET", "ET MALWARE GravityRAT CnC Domain (x-trust .net in DNS Lookup)", "ET MALWARE Suspected Polonium CnC Checkin (result.php - process list) M2", "ET MALWARE Suspected TA404 APT Related Activity M1", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (furnitureshopone .us)", "ET WEB_CLIENT Fake Adobe Flash Player update warning enticing clicks to malware payload", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to virtualdataserver .com", "ET MALWARE CryptoLocker .onion Proxy Domain (iezqmd4s2fflmh7n)", "ET MALWARE Observed DNS Query to TA455 Domain (cortanaservice .com)", "ET MALWARE ELF/Mirai Variant UA Inbound (Hentai)", "ET MALWARE Suspected Sliver DNS CnC", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(k7tlx3ghr3m4n2tu)", "ET MALWARE Observed Pirate Stealer Domain in DNS Lookup (socket .bby .gg)", "ET MALWARE Observed DNS Query to TA455 Domain (saipem .org)", "ET MALWARE Lyceum Golang HTTP Backdoor Requesting Commands", "ET MALWARE Zlob User Agent - updating (Winlogon)", "ET INFO Possibly Malicious VBS Writing to Persistence Registry Location", "ET WEB_CLIENT JS Browser Based Ransomware", "ET MALWARE Fraudload/FakeAlert/FakeVimes Downloader - POST", "ET MALWARE Possible Pegasus Related DNS Lookup (alawaeltech .com)", "ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Oracle America)", "ET MALWARE TraderTraitor dafom CnC Checkin M2 (POST)", "ET PHISHING Successful American First CU Credential Phish 2023-01-03", "ET MALWARE Peppy/KeeOIL Google Connectivity Check", "ET CNC Feodo Tracker Reported CnC Server group 22", "ET MALWARE OSX/Flashback.K/I reporting successful infection 2", "ET MALWARE Mekotio HTTP Method (111SA)", "ET MALWARE PowerShell Script Downloading Emotet DLL", "ET MOBILE_MALWARE Windows Phone PUA.Redpher (myservicessapps .com in DNS Lookup)", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (highdatabase .com)", "ET MALWARE Possible W32/KanKan Update officeaddinupdate.xml Request", "ET MALWARE Sakula DNS Lookup (inocnation.com)", "ET MALWARE Nobelium APT Related Activity (GET)", "ET INFO Hiloti Style GET to PHP with invalid terse MSIE headers", "ET MALWARE MSIL/Document Stealer Exfil", "ET MALWARE Brontok/Joseray User-Agent Detected (Joseray.A3 Browser)", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (websitetheme .com)", "ET MALWARE Possible CopyKitten DNS Lookup (sharepoint-microsoft .co)", "ET MALWARE W32/Echmark/MarkiRAT CnC Response", "ET MALWARE Brute Ratel CnC Activity (xml-c2) M2", "ET MALWARE Win32/Aurora Stealer Sending System Information", "ET USER_AGENTS Suspicious User-Agent (=Mozilla)", "ET MALWARE ABUSE.CH Cerber Ransomware Domain Detected", "ET MALWARE SocGholish Domain in DNS Lookup (modernism .designpaw .com)", "ET MALWARE Eternity Stealer CnC Domain in DNS Lookup (wasabiwallet .online)", "ET HUNTING Possible Obfuscator io JavaScript Obfuscation", "ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v1 ASCII", "ET MOBILE_MALWARE Arid Viper (dash-chat-c02b3 .firebaseio .com in DNS Lookup)", "ET MALWARE Observed DNS Query to EvilProxy Domain (rproxy .io)", "ET MALWARE Win32/Delf.BLL Variant CnC Activity (Outbound)", "ET MALWARE Win32/Kribat-A Downloader Activity", "ET MALWARE Generic Dropper Installing PUP 2", "ET MALWARE Sisproc update", "ET MALWARE DragonOK KHRAT Downloader Receiving Payload", "ET MOBILE_MALWARE Android/GoldDream Infected Device Registration", "ET MALWARE Chinotto CnC Activity (hello)", "ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to avsvmcloud .com", "ET MALWARE Win32/Winshow User Agent", "ET MALWARE METALJACK APT32 DNS Lookup (libjs.inquirerjs.com)", "ET HUNTING Windows nbtstat -r Microsoft Windows DOS

	prompt command exit OUTBOUND", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (newphoneapp .com)", "ET HUNTING Suspicious HTTP Request for gift.exe", "ET MALWARE JS/TrojanDownloader.Agent.TXV CnC Activity", "ET MALWARE Suspected Polonium CnC Checkin (get_cmd)", "ET PHISHING Suspected TA445 Spearphishing Related Domain (id .bigmir .space in TLS SNI)", "ET MALWARE OSX/Proton.C/D Domain (eltima .in in TLS SNI)", "ET INFO Microsoft Script Encoder Encoded File", "ET MALWARE [PTsecurity] MZRevenge Ransomware Server Response", "ET MALWARE Windows gpresult Microsoft Windows DOS prompt command exit OUTBOUND", "ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Response", "ET MALWARE Suspicious User-Agent (Post)", "ET MALWARE TorrentLocker DNS Lookup (deadwalk32.ru)", "ET MALWARE Observed TA444 Domain (privacysign .org in TLS SNI)", "ET MALWARE Loki Locker Ransomware Server Response (Public Key) M2", "ET MALWARE Possible CopyKittens DNS Lookup (windowkernel.com)", "ET MALWARE linux.backdoor.wordpressexploit.1 JS backdoor retrieval", "ET WEB_CLIENT Malicious Fake JS Lib Inject", "ET MALWARE GravityRAT CnC Domain (orangevault .net in DNS Lookup)", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns1.hostasa.org)", "ET MALWARE Observed DNS Query to TA444 Domain (cloud .jbic .us)", "ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 5 (updatemobapp .website)", "ET MALWARE Shady RAT Relay Command", "ET MALWARE BartCrypt Payment DNS Query to .onion proxy Domain (khh5cmzh5q7yp7th)", "ET MALWARE Tibs Trojan Downloader", "ET MALWARE Observed DNS Query to Budminer Domain (thesizeofearth .ourhobby .com)", "ET MALWARE OSX/Flashback.K/I reporting successful infection", "ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain", "ET CNC Feodo Tracker Reported CnC Server group 24", "ET MALWARE IcedID Observed Domain (loadfreeman .casa in TLS SNI)", "ET MALWARE ChromeLoader Activity (GET)", "ET EXPLOIT Possible ETERNALBLUE Exploit M3 MS17-010", "ET MALWARE Win32/Koubbeh Sending Windows System Info", "ET MOBILE_MALWARE Possible Trojan-Banker.AndroidOS.Sharkbot Activity (DNS Lookup) 2", "ET ACTIVEX Possible Follina Payload Delivery Page", "ET MALWARE Possible Pegasus Related DNS Lookup (iusacell-movil .com.mx)", "ET MOBILE_MALWARE Android BatteryBotPro Checkin", "ET MALWARE Win32/Toby.N Multilocker Request", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 6", "ET MALWARE DonotGroup Backdoor Activity (POST)", "ET MALWARE SocGholish Domain in DNS Lookup (passphrase .singinganewsong .com)", "ET MALWARE Win32/PlugX Related Activity", "ET WEB_CLIENT XHR POST Request - Possible Form Grabber Activity", "ET MALWARE Ransomware Locky .onion Payment Domain (5n7y4yihirccftc5)", "ET MALWARE Ponmocup HTTP Request (generic) M5", "ET MALWARE Observed DNS Query to Ursnif Domain (mamount .cyou)", "ET MALWARE Tandem Espionage CnC Domain (sanlygeljek .ru) in DNS Lookup", "ET MALWARE Banker.anv Generally Suspicious User-Agent (CustomExchangeBrowser)", "ET MALWARE Win32/Sabsik.FL.B!ml Exfil", "ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[SID1]", "ET MALWARE Malicious Mega Chrome Extension Exfil Domain (www .megaopac .host in TLS SNI)", "ET MALWARE Downloaded Script Disables Firewall/Antivirus", "ET MALWARE Possible CopyKitten DNS Lookup (dnsserv .host)", "ET MALWARE Downloader (P2P Zeus dropper UA)", "ET MALWARE Possible Variant.Kazy.53640 Malformed Client Hello SSL 3.0 (Session_Id length greater than Client_Hello Length)", "ET USER_AGENTS Win32/OnLineGames User-Agent (Revolution Win32)", "ET MALWARE Possible Malicious Macro EXE DL AlphaNumL", "ET MALWARE Iron Ransomware Domain (y5mogzal2w25p6bn .ml in DNS Lookup)", "ET MALWARE Suspicious User-Agent (GenericHttp/VER_STR_COMMA)", "ET MALWARE Observed DNS Query to Budminer Domain (find .usdc .ignorelist .com)", "ET MALWARE Likely Malware CnC Hosted on 000webhostapp - POST to gate.php", "ET MALWARE Likely Fake Antivirus Download InternetAntivirusPro.exe", "ET MALWARE Observed DNS Query to TA455 Domain (apply-jobs .com)", "ET HUNTING Download Request Containing Suspicious Filename - Crypted", "ET MALWARE Observed DNS Query to Budminer Domain (obicsystem .ntt-nexia .tk)", "ET MALWARE FastPOS Software Update Request", "ET MALWARE Win32/Girostat Stealer (POST)", "ET MALWARE [PTsecurity] Trickbot Data Exfiltration",

	"ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M1", "ET MALWARE Rouge Security Software Win32.BHO.egw", "ET MALWARE MAZE Ransomware Payment Domain DNS Lookup", "ET MALWARE Observed PyPI Phishing/Malicious Library Data Exfiltration Domain (linkedopports .com) in TLS SNI", "ET MOBILE_MALWARE Suspected Android Youzicheng Proxy Activity", "ET USER_AGENTS Suspicious User-Agent (Windows Explorer)", "ET MALWARE Restylink Domain in DNS Lookup (officehoster .com)", "ET MALWARE TransparentTribe APT Related Backdoor Activity", "ET POLICY Inbound PowerShell Capable of Enumerating Internal Network via WMI", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (mci .ejalase .org)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (www .58sky .com)", "ET MALWARE Cryptowall 3.0 .onion Proxy Domain", "ET MALWARE Vawtrak/NeverQuest Server Response", "ET MALWARE Observed DNS Query to Budminer Domain (prefers .kboyda .net)", "ET MALWARE Cobalt Strike Beacon (Bing Profile)", "ET MALWARE Known IoT Malware Domain", "ET MALWARE Win32/CollectorStealer - Returning Client GeoIP Information", "ET MALWARE Ddex Loader Check-in", "ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.cc)", "ET MALWARE Observed DNS Query to Budminer Domain (hinet .dns-stuff .com)", "ET MALWARE Observed DNS Query to Budminer Domain (zbAction .dynssl .COM)", "ET MALWARE Trojan.BlackRev Get Command Rev3", "ET MALWARE Observed DNS Query to EvilProxy Domain (top-cyber .club)", "ET MALWARE Gamaredon APT Related Domain in DNS Lookup", "ET MALWARE Zbot UA", "ET MOBILE_MALWARE NSO Related Domain 26", "ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .online)", "ET MALWARE Observed DNS Query to TA455 Domain (updatedns .ddns .net)", "ET MALWARE W32/VPEYE Trojan Downloader User-Agent (VP-EYE Downloader)", "ET MALWARE CCleaner Backdoor DGA Domain (ab70a139cc3a.com) Dec 2017", "ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .tel)", "ET MALWARE Group 21 Payload CnC Checkin", "ET MALWARE Malicious SSL Certificate detected (BoratRat)", "ET MALWARE Shylock Module Server Response", "ET MALWARE Win32/Agent Tesla SMTP Clipboard Exfil", "ET PHISHING Observed DNS Query to Nedbank Phishing Domain", "ET MALWARE HTML/TrojanDropper.Agent.T Payload Inbound", "ET MALWARE Ponmocup HTTP Request (generic) M4", "ET MALWARE Likely Geodo/Emotet Downloading PE - Fake UA", "ET MALWARE Bossabot DDoS tool RFI attempt", "ET MALWARE ELF/Mirai Variant UA Inbound (Rift)", "ET USER_AGENTS Suspected Mekotio User-Agent (MyCustomUser)", "ET MALWARE FakeM SSL DNS Lookup (islamhood .net)", "ET MALWARE Observed DNS Query to AppleJeus Domain (rebelthumb .net)", "ET MOBILE_MALWARE Android.HongTouTou Checkin", "ET WEB_SERVER WebShell Generic - ASP File Uploaded", "ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (aa.hostasa.org)", "ET MALWARE Win32/Numando Banker CnC Activity", "ET USER_AGENTS User-Agent (ChilkatUpload)", "ET MALWARE MASSLOGGER Client Data Exfil (POST)", "ET MALWARE Ousaban Related Maldoc Activity", "ET MALWARE StartPage Userclass HTTP Request", "ET USER_AGENTS User-Agent (Unknown)", "ET MALWARE Observed DNS Query to Budminer Domain (kingpsng .twgogo .org)", "ET MALWARE BestAntivirus2011 Fake AV reporting", "ET MALWARE FIN7/Carbanak Staging Domain in DNS Lookup (civilizationidium .com)", "ET MALWARE IrcBot Fantasy Name Gen", "ET HUNTING Suspicious VNC Remote Admin Request", "ET MALWARE Athena Bot Nick in IRC", "ET MALWARE DNSTrojan FakeAV Dropper Activity Observed (1)", "ET MALWARE Backdoor.Win32.Vertexbot.A User-Agent (VERTEXNET)", "ET MALWARE JS/RAA Ransomware check-in", "ET MALWARE W32/Liftoh.Downloader Get Final Payload Request", "ET EXPLOIT Metasploit Plugin-Detect Posting Data 2", "ET MALWARE ATTACKER IRCBot - netsh - PRIVMSG Command", "ET MALWARE Executable Download Purporting to be JavaScript likely 2nd stage Infection", "ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 4", "ET MALWARE BlackEnergy v2 POST Request", "ET MALWARE Dyreza RAT Fake Server Header", "ET MALWARE Pegasus Domain in DNS Lookup (al-nusr .net)", "ET MALWARE CryptoWall/TeslaCrypt Payment Domain", "ET MALWARE Possible CopyKitten DNS Lookup (1m100 .tech)", "ET WEB_SERVER IIS ISN BackDoor Command GetLog", "ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 3", "ET MALWARE Observed DNS

	Query to Budminer Domain (itunes .toythieves .com)", "ET USER_AGENTS Downloader User-Agent (AutoDL\/1.0)", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (datasamsung .com)", "ET MALWARE FIN7 JSSLoader Activity (POST)", "ET WEB_CLIENT Office UA FB SET", "ET MALWARE FOX-SRT ShimRat check-in (php)", "ET MALWARE Win32/Pterodo CnC Activity (GET)", "ET MALWARE SocGholish Domain in DNS Lookup (group5 .corralphacap .com)", "ET USER_AGENTS Suspicious User-Agent (ISMYIE)", "ET MALWARE Konni RAT Querying CnC for Commands", "ET MALWARE Steganographic Encoded WAV File Inbound via HTTP M2", "ET MALWARE Dalexis Downloading EXE", "ET MALWARE SocGholish Domain in DNS Lookup (perspective .abcbarbecue .xyz)", "ET MALWARE LuminosityLink - Data Channel Client Request 2", "ET MALWARE Observed DNS Query to Budminer Domain (mofamail .acmetoy .com)", "ET MALWARE [401TRG] SUNBURST Related DNS Lookup to infinitysoftwares .com", "ET MALWARE Observed DNS Query to Certishell Domain (msrousinov .cz)", "ET MALWARE KINS/ZeusVM Variant Retrieving Config", "ET COINMINER Observed Coin-Hive In Browser Mining Domain (coin-hive .com in TLS SNI)", "ET MALWARE TinyLoader.B1 Sending Processes", "ET MALWARE Observed DNS Query to TA444 Domain (vote .anobaka .info)", "ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 1 (goldncup .com)", "ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)", "ET MALWARE Observed Python CTX Library Backdoor Domain (anti-theft-web .herokuapp .com) in TLS SNI", "ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (news .alberto2011 .com)", "ET MALWARE Linkup Ransomware check-in", "ET MOBILE_MALWARE iOS/Xsser Checkin", "ET MALWARE ENV Variable Data Exfiltration Domain (ovz1 .j19544519 .pr46m .vps .myjino .ru) in DNS Lookup", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 3", "ET MALWARE Corebot Module Download", "ET MALWARE Bredolab Downloader Communicating With Controller (1)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookie.txt) M2", "ET WEB_SERVER WebShell - GODSpy - Cookie", "ET WEB_CLIENT pshell dl/execute primitives in wideb64 3", "ET WEB_SERVER HTTP POST Generic eval of base64_decode", "ET MALWARE Possible Pegasus Related DNS Lookup (whatsapp-app .com)", "ET INFO Potential Malicious PDF (EmbeddedFiles) improper case", "ET WEB_SPECIFIC_APPS Request to Wordpress W3TC Plug-in dbcache Directory", "ET MALWARE Nemty Ransomware Payment Page ID File Upload", "ET MALWARE Observed DNS Query to TA455 Domain (enerflex .org)", "ET MALWARE Win32.Lager Trojan Reporting (gcu)", "ET WEB_CLIENT Office Requesting .HTA File Likely CVE-2017-0199 Request", "ET MALWARE Observed DNS Query to Certishell Domain (profiit .fiit .stuba .sk)", "ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (dsk .5636 .com)", "ET MALWARE TorrentLocker DNS Lookup (doubleclickads.net)", "ET MALWARE Backdoor.Win32/Etumbot.B Requesting RC4 Key", "ET MALWARE ElectroRAT Command from Server (Screenshot)", "ET MALWARE Observed Ursnif Domain in TLS SNI (prises .cyou)", "ET MALWARE Win32/Hikit Server Authentication Response", "ET MALWARE FakeAV Landing Page", "ET MALWARE Echelon/Mist Stealer CnC Activity", "ET MALWARE Scarlet Mimic DNS Lookup 27", "ET MALWARE Win32/Sisproc", "ET MALWARE Observed Ursnif Domain in TLS SNI (reaso .xyz)", "ET USER_AGENTS Suspicious User-Agent (IE/1.0)", "ET MALWARE Unknown - Loader - Check .exe Updated", "ET MALWARE Win32/MagicRAT CnC Activity M1", "ET MALWARE Common Downloader Install Report URL", "ET MALWARE Anuna PHP Backdoor Attempt", "ET USER_AGENTS Suspicious User-Agent (cso)", "ET MALWARE Possible Encoded Wide PowerShell (IEX) in Certificate Inbound", "ET MALWARE Win32/DTStealer CnC Activity", "ET MOBILE_MALWARE Operation Pawn Storm IOS_XAGENT Checkin", "ET MOBILE_MALWARE Bahamut Group Fake VPN Payload Delivery Domain (thesecurevpn .com) in DNS Lookup", "ET MALWARE Win32/LNK/Agent.GX Javascript Downloader M2", "ET USER_AGENTS VPNFilter Related UA (Gemini/2.0)", "ET MALWARE MICROPSIA HTTP Failover Response M2", "ET MALWARE Dark Halo/SUNBURST CnC Domain (solartrackingsystem .net in TLS SNI)", "ET HUNTING Terse Request for WordPress Site ending in all digits", "ET MALWARE Ransomware CrypMIC Payment Onion Domain", "ET MALWARE ELF/Mirai Variant Activity (Outbound)", "ET MALWARE Possible Pegasus Related DNS Lookup

	(damanhealth .online)", "ET MALWARE [PTsecurity] Bladabindi/njRAT (Dd19271927)", "ET USER_AGENTS Suspicious User-Agent (NateFinder)", "ET MALWARE Scarlet Mimic DNS Lookup 45", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(vbusers)", "ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B642 Oct 19 2017", "ET MALWARE Volatile Cedar Win32.Explosive Fake User-Agent", "ET MALWARE Trojan.Win32.DLOADR.TIOIBEPQ CnC Traffic", "ET MALWARE Possible CopyKittens DNS Lookup (micro-windows.in)", "ET MALWARE Umbra/MultiBot Plugin access", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 12", "ET MALWARE Unknown Trojan with Fake Java User-Agent", "ET MALWARE Win32/Malgent!MSR User-Agent", "ET CNC Feodo Tracker Reported CnC Server group 19", "ET MALWARE Observed Evrial Domain (projectevrial .ru in TLS SNI)", "ET MALWARE PDF 0day Communication - agent UA Feb 14 2013", "ET MALWARE Smokeloader getgrab Command", "ET MALWARE LokiBot Application/Credential Data Exfiltration Detected M1", "ET MALWARE Win32/Filecoder.STOP Variant Request for Public Key", "ET MALWARE FinFisher Malware Connection Initialization", "ET MALWARE TA459 Related Activity (Inbound)", "ET MALWARE Win32/BlackMagic Ransomware Payload Request (GET)", "ET MALWARE Blue Bot DDoS Blog Request", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 11", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies Firefox.txt) M1", "ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (avsvmcloud .com)", "ET MALWARE Observed DNS Query to Budminer Domain (yahoofacebook .345 .pl)", "ET INFO External Host Probing for ChromeCast Devices", "ET POLICY DNS Query to .onion proxy Domain (onion.link)", "ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (WinFtpd)", "ET MALWARE Observed DNS Query to TA455 Domain (updateddns .ddns .net)", "ET MALWARE MS_D0wnl0ad3r Screenshot Upload", "ET CURRENT_EVENTS NATO Themed Maldoc Related Domain in DNS Lookup (am .my-zo .org)", "ET MALWARE Backdoor.Win32.VB.cfi (related) System Info Upload via FTP", "ET MALWARE TA404/Zinc Trojanized muPDF/Subliminal CnC Checkin", "ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 5", "ET MALWARE ATTACKER IRCBot - ipconfig - PRIVMSG Command", "ET MALWARE Possible Pegasus Related DNS Lookup (network190 .com)", "ET MALWARE Observed DNS Query to TA455 Domain (sparrowsgroup .org)", "ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b DNS Lookup", "ET MALWARE Observed Malicious SSL Cert (RedGuard Framework)", "ET MOBILE_MALWARE Android Spy APT-C-23 (scott-chapin .com in DNS Lookup)", "ET MOBILE_MALWARE MOONSHINE payload C2 activity", "ET HUNTING Suspicious User-Agent (c \windows)", "ET MALWARE HTTP Request to a *.pw domain with direct request/fake browser (multiple families flowbit set)", "ET MALWARE Observed PowerShell/CustomRAT Domain (kleinm .de) in TLS SNI", "ET MALWARE Sasfis Botnet Client Reporting Back to Controller After Command Execution", "ET WEB_CLIENT DRIVEBY FakeSupport - URI - windows-firewall.png", "ET MALWARE IIStealer Inbound Exfil Request", "ET MALWARE Trojan.BlackRev Registering Client", "ET MALWARE Possible CopyKittens DNS Lookup (windowskernel.in)", "ET MALWARE Observed DNS Query to Certishell Domain (reality .skarabeus .sk)", "ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(fwgrhsao3aoml7ej)", "ET MALWARE Maze/ID Ransomware Activity", "ET MALWARE Observed TA444 Domain (team .msteam .biz in TLS SNI)", "ET WEB_CLIENT DRIVEBY GENERIC ShellExecute in Hex No Seps", "ET ATTACK_RESPONSE VBA/Subdoc.B Obfuscated Payload Inbound", "ET MALWARE Observed DNS Query to XWorm RAT Domain (system6458 .ddns .net)", "ET MOBILE_MALWARE Android Marcher Trojan Download - Austrian Bank Targeting", "ET MALWARE Maldoc Retrieving Additional Resources (GET)", "ET MALWARE MSIL/NoCry Ransomware Checkin Via Discord", "ET MALWARE Possible CopyKitten DNS Lookup (1e100 .tech)", "ET MALWARE Observed DNS Query to Budminer Domain (kingdom .myddns .com)", "ET MALWARE Possible Passthru/Kshell Port Redirection Initiation", "ET MALWARE Tandem Espionage CnC Domain (zpuxmwmwdxxk .ru) in DNS Lookup", "ET MALWARE Possible Malicious Gzip PowerShell over HTTP", "ET MALWARE Win32.SpyEyes.bllw CnC Exfil", "ET INFO Suspicious Windows NT version 1 User-Agent", "ET MALWARE Win32/Bisonal DNS Lookup 3", "ET MALWARE Win32/CopperStealer CnC Activity M2", "ET MALWARE

	Sharik/Smoke Loader Receiving Payload", "ET EXPLOIT Possible CVE-2014-6332 DECS2", "ET USER_AGENTS Suspicious User-Agent String (AskPartnerCobranding)", "ET MALWARE Sharik/Smoke Loader Java Connectivity Check", "ET MALWARE Win32/SiMay RAT Activity M2 (GET)", "ET MALWARE FOX-SRT ShimRatReporter check-in", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco .gq)", "ET MALWARE Iron Tiger Backdoor.GTalkTrojan DNS Lookup (update.gtalklite.com)", "ET MALWARE TA453 Related Activity (POST)", "ET MOBILE_MALWARE Possible iOS WebView Auto Dialer 1", "ET MALWARE JS.InfectedMikrotik Injects Domain Observed in TLS SNI", "ET MALWARE Win32/Frosparf.B Downloading Hosts File", "ET MOBILE_MALWARE Suspected PROJECTSPY Cookie", "ET MALWARE WSF/JS Downloader Jan 30 2017 M1", "ET POLICY Cnet App Download and Checkin", "ET MALWARE Scarlet Mimic DNS Lookup 26", "ET MALWARE Win32.Chroject.B ClickFraud Request", "ET MALWARE Hacking Team Elite Windows Implant Exfiltration", "ET USER_AGENTS Suspicious User-Agent (IEMGR)", "ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (h4ck .cfd) Domain in DNS Lookup", "ET MALWARE Possible Veil Powershell Encoder B642", "ET INFO Obfuscated Eval String 6", "ET MALWARE SharpExec EXE Lateral Movement Tool Downloaded", "ET MALWARE W32/Coced.PasswordStealer User-Agent 5.0", "ET MALWARE Optix Pro Trojan/Keylogger Reporting Installation via Email", "ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 4 (mobilestoreupdate .website)", "ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST) 2", "ET MALWARE Symbiote CnC Domain in DNS Lookup (caixa .cx)", "ET MALWARE Observed DNS Query to Budminer Domain (oop .itsaol .com)", "ET MALWARE Observed DNS Query to Budminer Domain (saitama .map-shinai .com)", "ET USER_AGENTS Fake Mozilla User-Agent String Observed (M0zilla)", "ET MALWARE ELF/Mirai Variant UA Inbound (Yakuza)", "ET MALWARE Datoploader Activity (GET)", "ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray", "ET MALWARE HermeticWizard - File Copy via SMB", "ET MALWARE Observed DNS Query to Budminer Domain (micro .security .services .rebatesrule .net)", "ET MALWARE OilRig QUADAGENT DNS Tunneling", "ET WEB_CLIENT Observed DNS Query to Malicious Cookie Monster Roulette JS Cookie Stealer Exfil Domain", "ET WEB_SERVER Perl/Mambo.WebShell Spreader IRC No Open Ports Message", "ET WEB_CLIENT Malicious Redirect 8x8 script tag", "ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (log post)", "ET MALWARE Win32/POWERPLANT CnC Exfil (INIT)", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Firefox.txt) M1", "ET CNC Feodo Tracker Reported CnC Server group 15", "ET MALWARE Arkei Stealer IP Lookup", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookies.txt) M1", "ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mamsolution .us)", "ET MALWARE Observed DNS Query to Budminer Domain (mofir .twgg .org)", "ET MALWARE Trojan.SpamBanker Report via SMTP", "ET MALWARE Observed DNS Query to Budminer Domain (music .apchnetinfo .com)", "ET MALWARE W32/Renos.Downloader User Agent zeroup", "ET MALWARE Win32/NetDooka Framework Related Activity (POST)", "ET MALWARE Observed SocGholish Domain in TLS SNI", "ET MALWARE JavaRAT Keep-Alive (outbound)", "ET MALWARE IMDDOS Botnet User-Agent kav", "ET MALWARE Observed DNS Query to Budminer Domain (trace .leecantu .com)", "ET MALWARE FakeAV User-Agent XML", "ET MALWARE Upatre Common URI Struct Dec 01 2014", "ET MALWARE Suspicious User-Agent MyAgrent", "ET WEB_CLIENT Possible BadRabbit Driveby Download M2 Oct 24 2017", "ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access makeCall", "ET MALWARE Win32/TrojanDownloader.Agent.RFS Variant Checkin", "ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M2", "ET MALWARE Filename hkcmd.exe Download - Common Hostile Filename", "ET MALWARE Linux/AES.DDoS Sending Real/Fake CPU&BW Info", "ET MALWARE Observed Sidewinder APT User-Agent", "ET MALWARE Possible Pegasus Related DNS Lookup (mymensaje-sms .com)", "ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M5", "ET WEB_SERVER Mambo.PerlBot Spreader IRC DDOS Exploited Message", "ET MALWARE WSHRAT

	Credential Dump Module Download Command Inbound", "ET MALWARE Observed DNS Query to TA444 Domain (wpsonline .co)", "ET MALWARE KeyBoy DNS Lookup (www .about.jkub.com)", "ET MALWARE Spoofed MSIE 7 User-Agent Likely Ponmocup", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Information.html) M1", "ET INFO Obfuscated Eval String 4", "ET MALWARE Pushdo Update URL Detected", "ET DNS Reply Sinkhole - Zinkhole.org", "ET MALWARE Backdoor.Win32.Agent.myttae User-Agent", "ET MALWARE Sality Variant Downloader Activity (2)", "ET MALWARE TrueBot/Silence.Downlaoder Screenshot Post M2", "ET MALWARE Suspected Tunna Proxy M4 (Outbound)", "ET MALWARE Win32.Bicololo Response 1", "ET MALWARE Malicious Downloader Activity (GET)", "ET POLICY Powershell Command With Execution Bypass Argument Over SMB - Likely Lateral Movement", "ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound", "ET MALWARE Windows net statistics workstation Microsoft Windows DOS prompt command exit OUTBOUND", "ET MALWARE Win32.HLLW.Autoruner USA_Load UA", "ET POLICY Suspicious ToTok Mobile Application DNS Request", "ET EXPLOIT Access To mm-forms-community upload dir (Outbound)", "ET MALWARE SSL/TLS Certificate Observed (Magecart)", "ET MALWARE Win32/Sality.NBA CnC Checkin", "ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 3", "ET HUNTING HTTP Executable Download from suspicious domain with direct request/fake browser (multiple families)", "ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DSMBVCTFRE)", "ET MALWARE Observed DNS Query to Budminer Domain (ourfriends .sexxxy .biz)", "ET MALWARE Sharik/Smoke Fake 404 Response with Payload Location", "ET MALWARE JS/Cryxos Stealer Variant Sending Data to Telegram (POST)", "ET ATTACK_RESPONSE Hostile FTP Server Banner (StnyFtpd)", "ET MALWARE Win32/SaintStealer CnC Response", "ET MALWARE Win32/DanaBot Harvesting Email Addresses 2", "ET MALWARE Win32/NitroStealer CnC Exfil M2", "ET MALWARE Suspected DNS2TCP Connect", "ET MALWARE Zingo/GinzoStealer Data Command List Fetch", "ET MALWARE NORTHSTAR Client Data POST", "ET MALWARE Win32/PlugX/Talisman Activity (POST)", "ET MOBILE_MALWARE XML Style POST Of IMSI International Mobile Subscriber Identity", "ET MALWARE Hyperion Obfuscator Payload Inbound", "ET MALWARE MSSQL maggie backdoor Accessall Query Observed", "ET MALWARE MAGICHOUND-related DNS Lookup (servicesystem .serveirc.com)", "ET MALWARE Suspected Gootkit Activity", "ET MALWARE Possible MalDoc Payload Download Nov 11 2014", "ET MALWARE Win32/BanloadDownloader.XZY Retrieving Payload", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadtesting .com)", "ET MALWARE Win32/Corrempa/HZRAT CnC Checkin", "ET MALWARE JS/TrojanDropper.Agent.OHE CnC Checkin", "ET MALWARE Observed DNS Query to Budminer Domain (voicetube .citytalk .crabdance .com)", "ET MALWARE Scarlet Mimic DNS Lookup 16", "ET MALWARE W32/NSIS.TrojanDownloader Second Stage Download Instructions from Server", "ET CNC Feodo Tracker Reported CnC Server group 20", "ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B645W Oct 19 2017", "ET MALWARE Trojan Generic - POST To gate.php with no accept headers", "ET MALWARE Observed TA444 Domain (mufg .tokyo in TLS SNI)", "ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (informaxima .org)", "ET MALWARE Charming Kitten APT Related DNS Activity", "ET MALWARE Possible Kaseya VSA Exploit URI Structure Inbound", "ET MALWARE Avzhan DDOS Bot Outbound Hardcoded Malformed GET Request Denial Of Service Attack Detected", "ET MALWARE Unk.PSAttack Activity", "ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (galaxysupdates .com)", "ET MALWARE Win32/Grandoreiro Sending System Information (POST)", "ET MALWARE Observed DNS Query to Budminer Domain (software .acmetoy .com)", "ET MALWARE Win32/PSW.Papras.CK file upload", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 2", "ET MALWARE PE EXE or DLL Windows file download Text", "ET MALWARE CryptoWall .onion Proxy Domain (7oqnsnzwwnm6zb7y)", "ET MALWARE Win32/Phorpiex Template 3 Active - Outbound Malicious Email Spam", "ET MALWARE Proyecto RAT Variant - Yopmail Login attempt (set)", "ET MALWARE Mal/Ransom-CE Connectivity Check", "ET EXPLOIT Possible Cisco RV320 RCE Attempt (CVE-2019-1652)", "ET MALWARE Observed DNS Query to Budminer Domain (1122334 .zyns .com)", "ET

	INFO Obfuscated Eval String 2", "ET MALWARE Possible Tracur.Q HTTP Communication", "ET MALWARE Mirai Variant Domain (bigboatreps .pw in DNS Lookup)", "ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound", "ET MALWARE PROMETHIUM/StrongPity DNS Lookup (updatesync .com)", "ET MALWARE Trojan-Dropper.Win32.Agent.ksja", "ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (pwresetcisco .com)", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (netsecurity-essential .com)", "ET MOBILE_MALWARE Andr/com.sdwiurse", "ET USER_AGENTS Peppy/KeeOIL Google User-Agent (google/dance)", "ET MALWARE Upatre Common URI Struct July 15 2014", "ET MALWARE Pingback Upload Command Issued", "ET MALWARE Observed Malicious Filename in Outbound POST Request (Browsers/Cookies/Microsoft Edge_)", "ET MALWARE Possible CopyKittens DNS Lookup (windows-india.in)", "ET MALWARE HVNC USR Init Detected", "ET ATTACK_RESPONSE Muhstik Botnet Download Activity (GET)", "ET MALWARE [TGI] Py.Machete FTP Exfil 1", "ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to zupertech .com", "ET MOBILE_MALWARE Android/Locker.B Checkin 2", "ET MALWARE Observed Certificate Base64 Encoded Executable Inbound", "ET P2P p2p Related User-Agent (eChanblard)", "ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 11", "ET MALWARE Zeus User-Agent(z00sAgent)", "ET MALWARE Common Downloader Access Count Tracking URL", "ET MALWARE Zberp receiving config via image file - SET", "ET MALWARE MegalodonHTTP/LuciferHTTP/Gomorrah Client Action M2", "ET MOBILE_MALWARE Android Fancy Bear Checkin 5", "ET MALWARE Observed Ursnif Domain in TLS SNI (daydayvin .xyz)", "ET MALWARE OSX/WireLurker DNS Query Domain www.comeinbaby.com", "ET MALWARE Observed DNS Query to TA455 Domain (talent-recruitment .org)", "ET MALWARE ARM Binary Downloaded via WGET Containing GoAhead and Multiple Camera RCE 0Day Vulnerabilities", "ET MALWARE Zingo/GinzoStealer Downloading Additional Payloads", "ET MALWARE Win32/Nitol.A CnC Checkin M3", "ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B644W Oct 19 2017", "ET MALWARE Orca RAT URI Struct 1", "ET MALWARE W32/Bilakip.A Downloader Viruslist Download For Populating FakeAV", "ET MALWARE Godlua Backdoor Stage-3 Server Heartbeat Reply (Jun 2019 - Sep 2020)", "ET MALWARE Buran Ransomware Activity M2", "ET MALWARE MSIL/TrojanDownloader.Agent.JVN CnC Checkin", "ET MALWARE Xbagger Macro Encrypted DL", "ET MALWARE CN Based APT Related Activity (POST)", "ET MALWARE x0Proto File Info Request", "ET MALWARE Scarlet Mimic DNS Lookup 33", "ET MALWARE Win32/Vidar Variant/Mars Stealer Resources Download", "ET USER_AGENTS sysWeb User-Agent", "ET MALWARE Bitter APT Payload Request", "ET MALWARE LazyScripter Related Activity (GET)", "ET MALWARE Evilnum Activity (GET)", "ET MALWARE Dridex Post Check-in Activity", "ET MALWARE W32/Upatre.Downloader Encoded Binary Download Request", "ET MALWARE MyKings Bootloader Variant Requesting Payload M3", "ET MALWARE Banking Trojan HTTP Cookie", "ET MALWARE SolarBot Plugin Download MessageBox", "ET MALWARE WS/JS Downloader Mar 07 2017 M1", "ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (areadozemode .space in DNS Lookup)", "ET MALWARE Tonto_SPM Backdoor CnC Activity", "ET WEB_SERVER DNS Query for Suspicious 9507c4e8.com Domain - Anuna Checkin - Compromised PHP Site", "ET MALWARE VBS/Agent.6B29!tr CnC Checkin", "ET MALWARE Possible Covenant Framework Grunt MSBuild Stager HTTP Download", "ET MALWARE TA410 APT FlowCloud Dependency Download M4", "ET WEB_CLIENT Possible JS Credit Card Stealer Inbound", "ET MALWARE Lazarus APT Related VSingle Backdoor Activity (GET)", "ET MALWARE ATTACKER IRCBot - reg - PRIVMSG Command", "ET MALWARE Quant Loader Download Response", "ET MALWARE Possible Windows executable sent when remote host claims to send HTML/CSS Content", "ET MALWARE Win32/Pterodo Activity (POST)", "ET WEB_CLIENT Evil Redirect Compromised WP Feb 01 2016", "ET MALWARE Bebloh connectivity check", "ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M3", "ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (puppyandcats .online)", "ET CNC Feodo Tracker Reported CnC Server group 23", "ET MALWARE TA569 Fake Captcha Download", "ET MALWARE

	Win32/JSWORM Ransomware Style Geo IP Check M2", "ET MOBILE_MALWARE Android/Spy.Agent.AOX Checkin", "ET MALWARE Suspected Tunna Proxy M1", "ET MALWARE Unknown VBScript Loader with Encoded PowerShell Execution Inbound", "ET MALWARE NewPosThings POST with Fake UA and Accept Header", "ET POLICY Edwards Packed proxy.pac from 724sky", "ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Firefox.txt) M2", "ET MOBILE_MALWARE Android/Spy.Agent.ANA (mediadownload .space in DNS Lookup)", "ET MALWARE Observed AgentTesla Domain Request", "ET MALWARE Win32/Tobfy.S", "ET MALWARE Win32/HackTool.Agent.CS SMTP Scanner CnC Checkin", "ET MALWARE Observed DNS Query to TA455 Domain (funnychess .online)", "ET MALWARE Known Malicious Expires Header Seen In Malicious JavaScript Downloader Campaign", "ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (verble .software)", "ET MALWARE Win32.Riberow.A (mkdir)", "ET USER_AGENTS Si25f_302 User-Agent", "ET MALWARE FatDuke Domain Observed", "ET MALWARE GravityRAT CnC Domain (cvstyler .co .in in DNS Lookup)", "ET MALWARE Observed DNS Query to Budminer Domain (mpsdtupdsda .ezua .com)", "ET MALWARE Kimsuky Related Maldoc Retrieving Template (GET)", "ET MALWARE Cknife Shell Command Struct Inbound (PHP)", "ET WEB_CLIENT c3284d malware network iframe", "ET MALWARE 7ev3n Ransomware Related Activity (GET)", "ET MALWARE Cobalt Strike Related Domain in DNS Lookup (gawocag .com)", "ET MALWARE Observed DNS Query to TA444 Domain (team .msteam .biz)", "ET MALWARE Possible Backdoor.Linux.Tsunami Outbound HTTP request", "ET MALWARE SocGholish Domain in DNS Lookup (family .1ablecommunity .com)", "ET MALWARE Possible Rar'd Malware sent when remote host claims to send an Image", "ET MALWARE HTTPTool User-Agent", "ET MALWARE SmokeBot grab data plaintext", "ET MALWARE Possible TRAT proxy component user agent detected", "ET MALWARE Observed DNS Query to TA455 Domain (mastergatevpn .com)", "ET MALWARE CenterPOS Load Plugins", "ET USER_AGENTS Otwycal User-Agent (Downing)", "ET EXPLOIT DLSw Information Disclosure CVE-2014-7992", "ET MALWARE Critroni Variant .onion Proxy Domain", "ET MALWARE Observed TraderTraitor Domain (www .esilet .com) in TLS SNI", "ET MALWARE ReVBShell Command Response", "ET MALWARE Supercharge Component Download (ps1)"