Daily Ruleset Update Summary 2019/03/14

proofpoint.com/us/daily-ruleset-update-summary-20190314

March 18, 2019

Ransomware Hub

Stop ransomware in its tracks with the free research and resources in our Ransomware Hub.

Learn More

Daily Ruleset Update Summary

Daily Ruleset Update Summary 2019/03/14

[***] Summary: [***]

2 new Open, 56 new Pro (2 + 54). CageyChameleon, CVE-2019-0703, Various SSL/TLS, Various Phish.

[+++] Added rules: [+++]

Open:

2027083 - ET TROJAN Win32/Termite Agent Implant CnC Checkin (trojan.rules)
2027084 - ET TROJAN Win32/Termite Agent Implant Keep-Alive (trojan.rules)

Pro:

2835331 - ETPRO MOBILE_MALWARE Trojan-Dropper.AndroidOS.Wroba.g Reporting Infection via SMTP (mobile_malware.rules)
2835332 - ETPRO MOBILE_MALWARE Android/Wangniu Checkin (mobile_malware.rules)
2835333 - ETPRO MOBILE_MALWARE Android/Domob.G Checkin (mobile_malware.rules)
2835334 - ETPRO MOBILE_MALWARE Android.Monitor.SpyApp.D CnC Beacon (mobile_malware.rules)
2835335 - ETPRO TROJAN Possible BabyShark HTA Download (trojan.rules)
2835336 - ETPRO TROJAN Receiving BabyShark HTA (trojan.rules)
2835337 - ETPRO TROJAN VBS/CageyChameleon Retrieving In-Memory Implant (trojan.rules)
2835338 - ETPRO TROJAN VBS/CageyChameleon Receiving In-Memory Implant (trojan.rules)
2835339 - ETPRO TROJAN VBS/CageyChameleon CnC Beacon (trojan.rules)
2835340 - ETPRO TROJAN VBS/CageyChameleon CnC Beacon (Common Malicious Process List Construct) (trojan.rules)
2835341 - ETPRO TROJAN VBS/CageyChameleon Receiving Command (trojan.rules)
2835342 - ETPRO TROJAN VBS/CageyChameleon Retrieving Further Stage Payload (trojan.rules)
2835343 - ETPRO TROJAN PowerShell/PowerPike CnC Beacon (trojan.rules)
2835344 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 1) (trojan.rules)
2835345 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 2) (trojan.rules)
2835346 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 3) (trojan.rules)
2835347 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 4) (trojan.rules)
2835348 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 5) (trojan.rules)
2835349 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 6)

(trojan.rules)
2835350 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 7) (trojan.rules)
2835351 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 8) (trojan.rules)
2835352 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 9) (trojan.rules)
2835353 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2019-03-14 10) (trojan.rules)
2835354 - ETPRO EXPLOIT Possible CVE-2019-0703 Request SMBv1 (exploit.rules)
2835355 - ETPRO EXPLOIT Possible CVE-2019-0703 Response SMBv1 (exploit.rules)
2835356 - ETPRO EXPLOIT Possible CVE-2019-0703 Request SMBv2 (exploit.rules)
2835357 - ETPRO EXPLOIT Possible CVE-2019-0703 Response SMBv2 (exploit.rules)
2835358 - ETPRO TROJAN Unit13 Reporting Infection (trojan.rules)
2835359 - ETPRO TROJAN ELF/Tsunami.NCF IRC Checkin (trojan.rules)
2835360 - ETPRO CURRENT_EVENTS Observed EXE Request for Ursnif Payload 2018-03-14 (current_events.rules)
2835361 - ETPRO TROJAN Observed Malicious SSL Cert (Ursnif CnC) (trojan.rules)
2835363 - ETPRO TROJAN Observed Malicious SSL Cert (VBS Downloader/CnC) (trojan.rules)
2835364 - ETPRO TROJAN Observed Malicious SSL Cert (VBS Downloader/CnC 2) (trojan.rules)
2835365 - ETPRO CURRENT_EVENTS Successful Paypal Phish 2019-03-13 (current_events.rules)
2835366 - ETPRO CURRENT_EVENTS Successful CAF FR Phish 2019-03-14 (current_events.rules)
2835367 - ETPRO CURRENT_EVENTS Successful Apple Phish 2019-03-14 (current_events.rules)
2835368 - ETPRO CURRENT_EVENTS Successful BBVA Phish 2019-03-14 (current_events.rules)
2835369 - ETPRO CURRENT_EVENTS Successful Booking.com Phish 2019-03-14 (current_events.rules)
2835370 - ETPRO CURRENT_EVENTS Successful Smartsheet Phish 2019-03-14 (current_events.rules)
2835371 - ETPRO CURRENT_EVENTS Successful WeTransfer Phish 2019-03-14 (current_events.rules)
2835372 - ETPRO CURRENT_EVENTS Successful Paypal Phish 2019-03-14 (current_events.rules)
2835373 - ETPRO CURRENT_EVENTS Successful Paypal Credit Card Information Phish 2019-03-14 (current_events.rules)
2835374 - ETPRO CURRENT_EVENTS Successful Vodafone Credit Card Information Phish 2019-03-14 (current_events.rules)

2835375 - ETPRO CURRENT_EVENTS Successful Office 365 Phish 2019-03-14 (current_events.rules)
2835376 - ETPRO CURRENT_EVENTS Successful Microsoft Account Phish 2019-03-14 (current_events.rules)
2835377 - ETPRO CURRENT_EVENTS Successful Outlook Phish 2019-03-14 (current_events.rules)
2835378 - ETPRO CURRENT_EVENTS Successful Citrix Sharefile Phish 2019-03-14 (current_events.rules)
2835379 - ETPRO CURRENT_EVENTS Successful Dropbox Phish 2019-03-14 (current_events.rules)
2835380 - ETPRO CURRENT_EVENTS Successful Luno Phish 2019-03-14 (current_events.rules)
2835381 - ETPRO CURRENT_EVENTS Successful Deutsche Bank Phish 2019-03-14 (current_events.rules)
2835382 - ETPRO CURRENT_EVENTS Successful Paxful Phish 2019-03-14 (current_events.rules)
2835383 - ETPRO CURRENT_EVENTS Successful Paxful Phish 2019-03-14 (current_events.rules)
2835384 - ETPRO CURRENT_EVENTS Successful Paypal Phish 2019-03-14 (current_events.rules)
2835385 - ETPRO CURRENT_EVENTS Successful RedButton Phish 2019-03-14 (current_events.rules)

[///] Modified active rules: [///]

2831259 - ETPRO MOBILE_MALWARE Trojan-Banker.AndroidOS.Asacub.bo CnC Beacon (mobile_malware.rules)
2832759 - ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24 (current_events.rules)

Date:

Wednesday, March 13, 2019
Summary title:

2 new Open, 56 new Pro (2 + 54). CageyChameleon, CVE-2019-0703, Various SSL/TLS, Various Phish.