Daily Ruleset Update Summary 2021/09/24

proofpoint.com/us/daily-ruleset-update-summary-20210924

September 24, 2021

Daily Ruleset Update Summary
Daily Ruleset Update Summary 2021/09/24

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

13 new OPEN, 25 new PRO (13 + 12). MirrorBlast, Jupyter Stealer, PerSwaysion Phishkit.

Thanks @ffforward, @pr0xylife, @James_inthe_box, @LNadav, @h2jazi
and @ShadowChasing1

We are hiring!
https://proofpoint.wd5.myworkdayjobs.com/ProofpointCareers/job/Sunnyval…

Please share issues, feedback, and requests at
https://feedback.emergingthreats.net/feedback

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

Open:

2033996 - ET INFO Possible Outdated Browser Landing Page M1 (info.rules)
2033997 - ET INFO Outdated Browser Landing Page M2 (info.rules)
2033998 - ET INFO Outdated Browser Landing Page M3 (info.rules)
2034021 - ET USER_AGENTS Suspicious User-Agent (REBOL) (user_agents.rules)
2034022 - ET TROJAN MirrorBlast CnC Activity M2 (trojan.rules)
2034023 - ET TROJAN MirrorBlast CnC Activity M3 (trojan.rules)
2034024 - ET TROJAN Jupyter Stealer CnC Checkin (trojan.rules)
2034025 - ET INFO Microsoft Netconnection Domain in DNS Lookup (info.rules)
2034026 - ET CURRENT_EVENTS PerSwaysion Phishkit Javascript Variable (current_events.rules)
2034027 - ET CURRENT_EVENTS PerSwaysion Phishkit Landing Page (current_events.rules)
2034028 - ET CURRENT_EVENTS PerSwaysion Phishkit Message Variables (current_events.rules)
2034029 - ET TROJAN Maldoc CnC Domain in DNS Lookup (r .significantbyte .com) (trojan.rules)
2034030 - ET TROJAN Maldoc Domain in DNS Lookup (aljazeera .cc) (trojan.rules)

Pro:

2850040 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2021-09-23 7) (trojan.rules)
2850041 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2021-09-23 1) (trojan.rules)
2850042 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2021-09-23 2) (trojan.rules)
2850043 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2021-09-23 3) (trojan.rules)
2850044 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2021-09-23 4) (trojan.rules)
2850045 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline

(2021-09-23 5) (trojan.rules)
2850046 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline
(2021-09-23 6) (trojan.rules)
2850047 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline
(2021-09-23 8) (trojan.rules)
2850048 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline
(2021-09-23 9) (trojan.rules)
2850049 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline
(2021-09-23 10) (trojan.rules)
2850050 - ETPRO TROJAN CoinMiner Known Malicious Stratum Authline
(2021-09-23 11) (trojan.rules)
2850051 - ETPRO TROJAN MSIL/Spy.Agent.AES CnC Exfil (trojan.rules)

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

2034001 - ET CURRENT_EVENTS PerSwaysion Phishkit Javascript -
Observed Repetitive Custom CSS Components (current_events.rules)
2034002 - ET CURRENT_EVENTS PerSwaysion Phishkit Javascript -
Observed Repetitive Custom JS Components (current_events.rules)
2034012 - ET TROJAN MirrorBlast Checkin (trojan.rules)
2810655 - ETPRO TROJAN Trojan.Win32.SchwarzeSonne CnC Beacon (trojan.rules)
2850018 - ETPRO CURRENT_EVENTS ET INFO Observed HTTP GET to
outdatedbrowser .com (current_events.rules)

[---] Removed rules: [---]

2033996 - ET CURRENT_EVENTS Outdated Browser Lure Landing Page M1
(current_events.rules)
2033997 - ET CURRENT_EVENTS Outdated Browser Lure Landing Page M2
(current_events.rules)
2033998 - ET CURRENT_EVENTS Outdated Browser Lure Landing Page M3
(current_events.rules)

Date:

Friday, September 24, 2021
Summary title:

13 new OPEN, 25 new PRO (13 + 12). MirrorBlast, Jupyter Stealer, PerSwaysion Phishkit.