Unit42-timely-threat-intel/2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt at main · PaloAltoNetworks/Unit42-timely-threat-intel

By brad-duncan

Archived: 2026-04-05 17:41:49 UTC

- 2020-08-20-IOCs-for-Emotet-infection-with-Qakbot.txt
- 2020-08-24-IOCs-for-Trickbot-gtag-ono66.txt
- 2020-08-25-IOCs-for-Emotet-with-Trickbot.txt
- 2020-09-01-IOCs-for-Raccoon-Stealer.txt
- 2020-09-07-IOCs-for-Dridex-infection.txt
- 2020-09-21-IOCs-for-Dridex-infection.txt
- 2020-09-28-IOCs-for-Qakbot-activity.txt
- 2020-10-01-IOCs-for-Formbook-infection.txt
- 2020-10-05-IOCs-from-AZORult-infection.txt
- 2020-10-26-IOCs-for-Emotet-epoch-2-with-Trickbot-gtag-mor137.txt
- 2020-11-05-IOCs-for-Hancitor-activity.txt
- 2020-11-16-IOCs-for-Cobalt-Strike-activity.txt
- 2020-11-23-IOCs-for-SmokeLoader-Dridex-and-Webshell.txt
- 2020-12-02-IOCs-for-Astaroth-activity.txt
- 2020-12-10-IOCs-from-Ursnif-infection-with-Delf-variant.txt
- 2020-12-11-Zepplin-ransomware-note.txt
- 2020-12-14-IOCs-from-Qakbot-activity.txt
- 2021-01-05-IOCs-for-Emotet-with-Trickbot.txt
- 2021-01-06-SystemBC-domain-list.txt
- 2021-01-08-IOCs-from-Ave-Maria-RAT.txt

- 2021-01-11-IOCs-for-Dridex-traffic-with-webshell.txt
- 2021-01-20-IOCs-from-Emotet-epoch1-infection.txt
- 2021-02-01-IOCs-for-TA551-Qakbot.txt
- 2021-02-22-IOCs-from-Guildma-infection.txt
- 2021-03-01-IOCs-from-IcedID-with-Cobalt-Strike.txt
- 2021-03-08-IOCs-from-Banload-infection.txt
- 2021-03-15-IOCs-from-IcedID-infection.txt
- 2021-03-19-Mirai-variant-update.txt
- 2021-03-22-IOCs-from-Dridex-infection.txt
- 2021-03-24-IOCs-for-IcedID-infection-with-Cobalt-Strike.txt
- 2021-04-12-IOCs-for-IcedID-infection.txt
- 2021-04-15-IOCs-for-AsyncRAT-activity.txt
- 2021-04-26-IOCs-for-IcedID-with-Cobalt-Strike.txt
- 2021-05-10-IOCs-for-TA551-pushing-IcedID.txt
- 2021-05-17-IOCs-for-TA551-IcedID.txt
- 2021-06-07-IOCs-update-for-Mirai.txt
- 2021-06-21-TA551-IOCs-for-Ursnif.txt
- 2021-06-28-TA551-IOCs-for-Trickbot.txt
- 2021-07-12-IOCs-from-Hancitor-activity.txt
- 2021-07-20-IOCs-for-BazarLoader-and-Trickbot.txt
- 2021-07-26-IOCs-for-Trickbot-gtag-rob112.txt
- 2021-07-29-IOCs-for-BazarLoader-CobaltStrike-PrintNightmare.txt
- 2021-08-09-BazarLoader-and-Cobalt-Strike-IOCs.txt
- 2021-08-16-updated-IOCs-for-Mirai.txt
- 2021-08-18-IOCs-from-phishing-email.txt
- 2021-08-26-IOCs-for-BazarLoader-infection.txt

- 2021-09-08-IOCs-for-Hancitor-with-Cobalt-Strike.txt
- 2021-09-13-IOCs-for-TA551-Trickbot-with-Cobalt-Strike-and-DarkVNC.txt
- 2021-09-20-IOCs-for-Squirrelwaffle-Loader-with-Cobalt-Strike.txt
- 2021-09-29-IOCs-for-TA551-BazarLoader-with-Cobalt-Strike.txt
- 2021-10-07-IOCs-for-Qakbot-obama111-and-Cobalt-Strike.txt
- 2021-10-18-IOCs-for-TR-based-Qakbot-with-Cobalt-Strike.txt
- 2021-11-03-IOCs-for-TA551-BazarLoader.txt
- 2021-11-04-IOCs-for-TR-Qakbot-with-Cobalt-Strike.txt
- 2021-11-05-IOCs-for-TA551-activity.txt
- 2021-11-15-IOCs-for-Matanbuchus-Qakbot-CobaltStrike-and-spambot-activity.txt
- 2021-11-22-IOCs-for-Contact-Forms-campaign-activity.txt
- 2021-12-07-IOCs-for-Qakbot-and-Matanbuchus-activity.txt
- 2021-12-10-IOCs-for-TA551-IcedID-infection-with-Cobalt-Strike-and-DarkVNC.txt
- 2022-01-04-IOCs-from-Remcos-RAT-infection.txt
- 2022-01-05-IOCs-for-TA551-IcedID-with-Cobalt-Strike.txt
- 2022-01-12-IOCs-for-IcedID-with-Cobalt-Strike-and-DarkVNC.txt
- 2022-01-17-IOCs-for-Astaroth-Guildma-infection.txt
- 2022-01-27-IOCs-for-Contact-Forms-IcedID-with-Cobalt-Strike.txt
- 2022-02-07-IOCs-for-BazarLoader-with-Cobalt-Strike.txt
- 2022-02-10-IOCs-for-Emotet-epoch5-infection-with-Cobalt-Strike.txt
- 2022-02-17-IOCs-for-Bazil-targeted-malware-infection.txt
- 2022-02-22-IOCs-for-Emotet-epoch4-activity.txt
- 2022-02-22-IOCs-for-Emotet-epoch5-activity.txt
- 2022-03-01-IOCs-for-Emotet-epoch4-with-Cobalt-Strike.txt
- 2022-03-03-IOCs-for-Bazil-targeted-malware-infection.txt
- 2022-03-03-IOCs-for-Emotet-epoch4-with-Cobalt-Strike.txt

- 2022-03-14-IOCs-from-Emotet-epoch5-with-Cobalt-Strike.txt
- 2022-03-21-IOCs-for-Cobalt-Strike-from-IcedID-infection.txt
- 2022-03-29-IOCs-for-Emotet-and-Cobalt-Strike.txt
- 2022-04-05-IOCs-for-Bumblebee-and-Cobalt-Strike.txt
- 2022-04-12-IOCs-for-SpringShell-exploitation-by-Enemybot.txt
- 2022-04-14-IOCs-for-aa-Qakbot-with-Cobalt-Strike.txt
- 2022-04-19-IOCS-for-infection-from-Brazil-malspam.txt
- 2022-04-25-IOCs-for-Emotet-epoch4.txt
- 2022-05-03-IOCs-for-Contact-Forms-Bumblebee-and-Cobalt-Strike.txt
- 2022-05-10-IOCs-for-Contact-Forms-IcedID-with-Cobalt-Strike.txt
- 2022-05-15-IOCs-for-Deadbolt-Ransomware.md
- 2022-05-17-IOCS-for-aa-distribution-Qakbot-with-Cobalt-Strike.txt
- 2022-05-23-IOCs-for-IcedID-and-DarkVNC.txt
- 2022-06-07-IOCs-for-Emotet-with-Cobalt-Strike.txt
- 2022-06-09-IOCs-from-TA578-Bumblebee-with-Cobalt-Strike.txt
- 2022-06-14-IOCs-from-TA578-Bumblebee-with-Cobalt-Strike.txt
- 2022-06-17-IOCs-for-Matanbuchus-with-Cobalt-Strike.txt
- 2022-06-21-IOCs-for-AA-distribution-Qakbot-with-DarkVNC-and-Cobalt-Strike.txt
- 2022-06-28-IOCs-for-TA578-IcedID-Cobalt-Strike-and-DarkVNC.txt
- 2022-07-06-IOCs-for-TA578-contact-forms-IcedID-with-DarkVNC-and-Cobalt-Strike.txt
- 2022-07-21-IOCs-for-IcedID-with-DarkVNC-and-Cobalt-Strike.txt
- 2022-07-25-IOCs-for-IcedID-with-Cobalt-Strike.txt
- 2022-08-03-IOCs-for-IcedID-and-Cobalt-Strike.txt
- 2022-08-08-IOCs-for-IcedID-and-Cobalt-Strike.txt
- 2022-08-10-IOCs-for-IcedID-and-Cobalt-Strike.txt
- 2022-08-15-IOCs-for-Monster-Libra-SVCready.txt

- 2022-09-13-IOCs-for-Qakbot.txt
- 2022-09-29-IOCs-for-Obama207-Qakbot-and-Cobalt-Strike.txt
- 2022-10-04-IOCs-for-IcedID-infection-with-Cobalt-Strike.txt
- 2022-10-10-IOCs-for-Cobalt-Strike-from-Qakbot-infection.txt
- 2022-10-17-IOCs-for-IcedID-with-Cobalt-Strike.txt
- 2022-10-31-IOCs-for-IcedID-with-DarkVNC-and-Cobalt-Strike.txt
- 2022-11-03-IOCs-for-Emotet-with-IcedID.txt
- 2022-11-07-IOCs-for-Emotet-infection-with-IcedID-and-Bumblebee.txt
- 2022-11-28-IOCs-for-BB08-Qakbot-with-Cobalt-Strike.txt
- 2022-12-07-IOCs-for-Bumblebee-infection-with-Cobalt-Strike.txt
- 2022-12-09-IOCs-for-HTML-smuggling-to-ISO-files-for-Cobalt-Strike.txt
- 2022-12-20-IOCs-for-IcedID-infection-with-Cobalt-Strike.txt
- 2022-12-28-IOCs-for-NetSupport-RAT-infection.txt
- 2022-12-29-IOCs-for-malware-from-fake-Adobe-Reader-page.txt
- 2023-01-05-IOCs-from-Agent-Tesla-variant-infection.txt
- 2023-01-12-IOCs-from-IcedID-and-Cobalt-Strike-infection.txt
- 2023-01-16-IOCs-for-malware-from-fake-7zip-page.txt
- 2023-01-23-IOCs-for-Google-ad-for-possible-TA505-activity.txt
- 2023-01-31-IOCs-for-BB12-Qakbot-infection.txt
- 2023-02-07-IOCs-for-probable-Matanbuchus-activity.txt
- 2023-02-08-IOCs-for-Cobalt-Strike-from-IcedID.txt
- 2023-02-13-IOCs-for-IcedID-infection-from-fake-Microsoft-Teams-page.txt
- 2023-02-24-IOCs-for-IcedID-infection-with-BackConnect-and-Cobalt-Strike.txt
- 2023-03-06-IOCs-for-Gozi-infection.txt
- 2023-03-07-IOCs-for-Emotet-activity.txt
- 2023-03-10-IOCs-for-CloakedUrsa-APT29-Activity.txt

- 2023-03-16-IOCs-for-Emotet-E5-activity.txt
- 2023-03-22-some-IOCs-for-Emotet-E4-activity.txt
- 2023-04-05-IOCs-for-STRRAT-activity.txt
- 2023-04-13-IOCs-for-MetaStealer-infection.txt
- 2023-05-02-IOCs-for-obama259-Qakbot.txt
- 2023-05-10-IOCs-for-IcedID-with-BackConnect-and-Keyhole-VNC-and-Cobalt-Strike.txt
- 2023-05-10-IOCs-for-obama262-Qakbot-with-DarkCat-VNC-and-Cobalt-Strike.txt
- 2023-05-17-IOCs-for-Pikabot-with-Cobalt-Strike.txt
- 2023-05-22-IOCs-for-Pikabot-infection-with-Cobalt-Strike.txt
- 2023-05-23-IOCs-for-Pikabot-with-Cobalt-Strike.txt
- 2023-06-28-IOCs-for-IcedID-activity.txt
- 2023-07-12-IOCs-from-Gozi-infection-with-Cobalt-Strike.txt
- 2023-08-03-IOCs-for-malicious-ad-to-Danabot.txt
- 2023-08-09-IOCs-from-IcedID-infection.txt
- 2023-08-29-IOCs-for-IcedID-activity.txt
- 2023-08-31-IOCs-for-IcedID-activity.txt
- 2023-09-21-thru-09-25-IOCs-for-AgentTesla-activity.txt
- 2023-09-28-IOCs-for-IcedID-with-KeyholeVNC-and-Cobalt-Strike.txt
- 2023-10-03-IOCs-for-Pikabot-infection-with-Cobalt-Strike.txt
- 2023-10-12-IOCs-for-DarkGate-from-Teams-chat.txt
- 2023-10-17-IOCs-for-Netscaler-CVE-2023-3519-activity.txt
- 2023-10-17-IOCs-for-TA577-Pikabot-infection.txt
- 2023-10-18-IOCs-from-IcedID-forked-variant-with-VNC-and-Cobalt-Strike.txt
- 2023-10-23-IOCs-from-404TDS-Async-RAT-infection.txt
- 2023-10-25-IOCs-from-DarkGate-activity.txt
- 2023-10-31-IOCs-for-IcedID-infection.txt

- 2023-11-02-IOCs-for-TA577-Pikabot-activity.txt
- 2023-11-20-IOCs-for-DarkGate-infection.txt
- 2023-11-27-IOCs-for-TA577-pushing-IcedID-variant.txt
- 2023-11-29-IOCs-for-JinxLoader-to-Formbook-XLoader.txt
- 2023-11-30-IOCs-for-DarkGate-activity.txt
- 2023-12-05-IOCs-from-loader-to-unidentified-malware.txt
- 2023-12-07-IOCs-for-DarkGate-infection.txt
- 2023-12-11-IOCs-for-Astaroth-Guildma-activity.txt
- 2023-12-15-IOCs-for-TA577-Pikabot-infection.txt
- 2023-12-18-IOCs-for-Pikabot-with-Cobalt-Strike.txt
- 2024-01-08-IOCs-for-GootLoader-infection.txt
- 2024-01-12-IOCs-from-StealC-activity.txt
- 2024-01-17-IOCs-for-WikiLoader-activity.txt
- 2024-01-19-IOCs-for-GootLoader-infection.txt
- 2024-01-23-IOCs-from-UltraVNC-infection.txt
- 2024-01-25-IOCs-for-DarkGate-activity.txt
- 2024-01-30-IOCs-for-DarkGate-activity.txt
- 2024-01-31-IOCs-from-Timely-Threat-Intel-post.txt
- 2024-02-08-IOCs-from-TA577-Pikabot-infection.txt
- 2024-02-14-IOCs-from-Danabot-infection.txt
- 2024-02-21-IOCs-from-SocGholish-AsyncRAT-infection.txt
- 2024-02-24-IOCs-for-possible-Lockbit-4.0-imposters.txt
- 2024-02-27-IOCs-for-Akira-Ransomware.txt
- 2024-03-06-IOCs-for-Pikabot-and-Meduza-Stealer-activity.txt
- 2024-03-07-IOCs-for-Latrodectus-and-Lumma-Stealer.txt
- 2024-03-13-IOCs-from-GootLoader-infection.txt

- 2024-03-14-IOCs-from-malware-possibly-targeting-Spain.txt
- 2024-03-19-IOCs-from-DarkGate-infection.txt
- 2024-03-24-thru-26-IOCs-for-Fortnet-EMS-exploit-activity.txt
- 2024-03-25-Timeline-for-misake-by-Playful-Taurus.txt
- 2024-03-26-IOCs-for-Matanbuchus-infection-with-Danabot.txt
- 2024-03-27-IOCs-for-Google-ad-leading-to-Netsupport-RAT.txt
- 2024-04-04-IOCs-from-Koi-Loader-Stealer-activity.txt
- 2024-04-15-IOC-for-Contact-Forms-campaign-SSLoad-activity.txt
- 2024-04-18-IOCs-from-SSLoad-infection-with-Cobalt-Strike-DLL.txt
- 2024-04-30-examples-of-web-skimmers.txt
- 2024-05-09-IOCs-from-GootLoader-activity.txt
- 2024-05-14-IOCs-for-DarkGate-activity.txt
- 2024-05-16-IOCs-for-credit-card-scams.txt
- 2024-05-21-IOCs-for-Deepfake-scam-campaigns.txt
- 2024-06-11-CVE-2024-4577.txt
- 2024-06-12-IOCs-for-Koi-Loader-Stealer-infection.txt
- 2024-06-17-IOCs-from-Matanbuchus-infection-with-Danabot.txt
- 2024-06-24-IOCs-for-ClickFix-pushing-Lumma-Stealer.txt
- 2024-06-25-IOCs-from-Latrodectus-activity.txt
- 2024-06-27-deepfake-scams.txt
- 2024-07-15-IOCs-from-recent-phishing-campaign.txt
- 2024-07-20-squatting-and-improsonation-domains.txt
- 2024-07-24-new-Ransomhub-verson-or-variant.txt
- 2024-07-25-Paris-2024-Olympics-scams.txt
- 2024-07-30-Olympics-themed-investment-scam.txt
- 2024-07-31-increase-of-tech-support-scam-URLs.txt

- 2024-08-01-Cryptocurrency-Phishing-Scams.txt
- 2024-08-05-Google-drawings-and-slides-abuse-for-phishing.txt
- 2024-08-06-Xerxes-Android-Botnet-activity.txt
- 2024-08-07-domains-impersonating-postal-services.txt
- 2024-08-09-olympic-themed-domains-for-Chinese-gambling-sites.txt
- 2024-08-09-scam-impersonating-legit-crypto-exchange.txt
- 2024-08-12-Olympic-themed-domains-similar-infrastructure-2020-and-2024.txt
- 2024-08-14-crytpo-investment-scams-impersonating-Tesla.txt
- 2024-08-21-Kematian-Stealer-info.txt
- 2024-08-22-Black-Myth-Wukong-themed-phishing-and-scam-domains.txt
- 2024-08-26-GuLoader-for-Remcos-RAT-IOCs.txt
- 2024-08-28-IOCs-for-Lumman-Stealer-from-fake-human-captcha-copy-paste-script.txt
- 2024-09-04-IOCs-for-EtherHiding-popups.txt
- 2024-09-16-IOCs-for-Snake-KeyLogger.txt
- 2024-09-19-IOCs-for-file-downloader-to-Lumma-Stealer.txt
- 2024-09-20-IOCs-for-Revolver-Rabbit-RDGA.txt
- 2024-09-24-IOCs-for-Libra-themed-investment-scam.txt
- 2024-09-25-IOCs-for-domains-spoofing-Deribit.txt
- 2024-09-26-IOCs-for-Capybara-DNS-tunneling-campaign.txt
- 2024-10-01-IOCs-for-RMS-based-malware.txt
- 2024-10-03-IOCs-for-SmartLoader-to-Lumma-Stealer.txt
- 2024-10-08-IOCs-for-malware-from-fake-Clockify-site.txt
- 2024-10-09-IOCs-for-Lumma-Stealer-from-typosquatted-domain.txt
- 2024-10-10-crypto-investment-scams.txt
- 2024-10-11-IOCs-for-advanced-phishing-activity.txt
- 2024-10-14-IOCs-for-fake-shopping-scam-sites.txt

- 2024-10-17-IOCs-for-TLD-CyberSquatting.txt
- 2024-10-24-IOCs-for-crypto-investment-scam.txt
- 2024-10-28-IOCs-for-phising-campaign.txt
- 2024-10-29-IOCs-for-US-election-scams.txt
- 2024-10-30-IOCs-for-xAI-crypto-scam.txt
- 2024-11-04-IOCs-for-cash-and-loan-scam.txt
- 2024-11-05-Roblox-phishing-campaign.txt
- 2024-11-08-domains-for-Japan-targeted-phishing.txt
- 2024-11-13-phishing-domains-for-the-holidays.txt
- 2024-11-14-IOCs-for-Raspberry-Robin-activity.txt
- 2024-11-15-IOCs-for-redir_pup_apk_dist.txt
- 2024-11-19-IOC-updates-for-ApateWeb-campaign.txt
- 2024-11-25-IOCs-for-Christmas-themed-scam-sites.txt
- 2024-11-26-IOCs-for-tech-support-scams.txt
- 2024-Boggy-Serpens-use-of-AutodialDLL.txt
- 2025-01-06-changes-to-HeartCrypt-packed-malware.txt
- 2025-01-09-IOCs-for-stockpiled-domains-delivering-suspicious-android-app.txt
- 2025-01-10-IOCs-for-CVE-2017-0199-XLS-infection-chain.txt
- 2025-01-13-IOCs-for-Kongtuke-activity.txt
- 2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt
- 2025-01-22-IOCs-for-malware-from-fake-Microsoft-Teams-site.txt
- 2025-01-23-IOCs-for-wp3-xyz-activity.txt
- 2025-01-24-IOCs-for-phishing-campaign-impersonating-amazon.txt
- 2025-01-24-IOCs-for-phishing-pages-targeting-online-shoppers.txt
- 2025-01-29-IOCs-for-DeepSeek-themed-phishing-domains.txt
- 2025-02-03-IOCs-for-Netflix-themed-survey-phishing-campaign.txt

- 2025-02-04-IOCs-for-stockpiled-domains-for-gift-card-scam.txt
- 2025-02-06-IOCs-for-Crypto-investment-scam-phishing-campaign.txt
- 2025-02-10-IOCs-for-StrelaStealer-activity.txt
- 2025-02-11-IOCs-for-sports-themed-crypto-scams.txt
- 2025-02-18-IOCs-for-SmartApeSG-fake-browser-update-leads-to-NetSupport-RAT-and-StealC.txt
- 2025-02-21-IOCs-for-tunneling-platforms-for-phishing-sites.txt
- 2025-02-25-IOCs-Stately-Taurus-Pubload-activity.txt
- 2025-02-26-IOCs-for-XLoader-infection.txt
- 2025-03-04-group-likely-impersonating-BIanLian.md
- 2025-03-05-IOCs-for-Click-Fix-distribution-of-Lumma-Stealer.txt
- 2025-03-06-IOCs-for-smishing-activity.txt
- 2025-03-10-IOCs-for-Remcos-RAT-activity.txt
- 2025-03-12-IOCs-for-phishing-activity.txt
- 2025-03-14-Testing-CVE-2025-24813.md
- 2025-03-18-IOCs-for-APT-C-36-activity.txt
- 2025-03-19-IOCs-for-Chinese-Language-trojanized-installers.txt
- 2025-03-20-IOCs-for-strategically-aged-domain-activity.txt
- 2025-03-31-IOCs-for-evasive-campaign-pushing-Legion-Loader.txt
- 2025-04-04-IOCs-forKongTuke-web-inject-leading-to-fake-CAPTHA-page.txt
- 2025-04-10-phishing-campaign-impersonating-Nintendo.txt
- 2025-04-14-persistence-of-CVE-2024-27564-probes.txt
- 2025-04-15-IOCs-for-IRS-themed-domains-used-in-CAPTCHA-style-paste-hijacking.txt
- 2025-04-15-IOCs-for-tax-return-related-phishing-and-scams.txt
- 2025-04-16-IOCs-for-tunneling-based-scans-for-DNS-resolvers.txt
- 2025-04-17-IngressNightmare-Scans-and-Testing.md
- 2025-04-23-IOCs-for-domains-impersonating-OnChain.txt

- 2025-04-23-IOCs-for-smishing-activity-update.txt
- 2025-04-25-IOCs-for-Blitz-malware.txt
- 2025-04-30-IOCs-for-suspciouis-search-pages.txt
- 2025-05-02-IOCs-for-Unknown-Loader.txt
- 2025-05-07-IOCs-from-Teams-phishing-for-MadMxShell.txt
- 2025-05-16-IOCs-on-recent-ClickFix-activity.txt
- 2025-05-19-IOCs-for-CypherIT-and-AutoIt-used-in-distribution-of-Lumma-Stealer.txt
- 2025-05-20-IOCs-for-AdaptixC2-activity.txt
- 2025-05-20-IOCs-for-TDS-leading-to-UP-X-gambling-platform.txt
- 2025-05-21-IOCs-for-BTMOB-RAT-activity.txt
- 2025-05-22-campaign-switches-from-Lumma-to-StealC-v2.txt
- 2025-05-30-IOCs-for-Chinese-language-campaign-impersonating-legitimate-applications.txt
- 2025-06-09-IOCs-for-Agent-Serpens-activity.txt
- 2025-06-10-IOCs-for-cryptocurrency-scam-impersonating-WWDC25.txt
- 2025-06-11-IOCs-for-Neptune-RAT-version-5.3.txt
- 2025-06-12-Iron-Taurus-remains-an-active-threat.txt
- 2025-06-20-IOCs-for-malware-disgused-as-cracked-software.txt
- 2025-06-24-IOCs-for-01flip-ransomware.txt
- 2025-06-25-IOCs-for-phishing-campaign-impersonating-Telegram.txt
- 2025-06-26-IOCs-for-phishing-campaing-impersonating-Microsoft-login-pages.txt
- 2025-06-30-IOCs-for-Labubu-scam-domains.txt
- 2025-07-17-IOCs-for-Soul-Stealer-2025-update.txt
- 2025-07-19-Microsoft-SharePoint-vulnerabilities-CVE-2025-49704-and-49706.txt
- 2025-07-24-IOCs-for-Vidar-activity.txt
- 2025-07-29-IOCs-for-Replit-activity.txt
- 2025-07-31-4L4MD4R-ransomware-from-ToolShell-exploit-activity.txt

- 2025-08-11-AI-summary-browser-extensions.txt
- 2025-08-13-IOCs-for-Smishing-activity.txt
- 2025-08-15-IOCs-for-Lumma-Stealer-infection-with-Sectop-RAT.txt
- 2025-08-18-IOCs-for-Chrome-extensions-leading-to-thank-you-pages-for-unwanted-content.txt
- 2025-08-19-IOCs-for-Chrome-extensions-leading-to-adware-or-PUP.txt
- 2025-08-28-Vishing-activity.txt
- 2025-08-29-IOCs-for-luxury-shop-fraud.txt
- 2025-09-05-IOCs-for-Smishing-impersonating-CA-francise-tax-board.txt
- 2025-09-09-scam-domains-related-to-2026-FIFA-World-Cup.txt
- 2025-09-11-dangling-commits-used-in-GitHub-malvertising.txt
- 2025-09-19-phishing-activity-targeting-Japanese-speakers.txt
- 2025-09-23-IOCs-for-phishing-campaign-using-BitM-pages.txt
- 2025-09-24-IOCs-for-AI-prompt-hijacker-extensions.txt
- 2025-09-25-IOCs-for-NFC-relay-Android-malware.txt
- 2025-10-01-IOCs-for-possible-Rhadamanthys.txt
- 2025-10-02-IOCs-for-phishing-pages-using-blob-URLs.txt
- 2025-10-02-IOCs-for-updated-smishing-URL-tactics.txt
- 2025-10-09-White-Lynx-Activity.txt
- 2025-10-10-domains-impersonating-Sora-2-sites.txt
- 2025-10-15-C2-sock-phishing-campaign.txt
- 2025-10-16-Multi-Stage-Android-Malware-Campaign.md
- 2025-10-17-IOCs-for-phishing-abusing-web-form-services.txt
- 2025-10-23-OAuth-flow-phishing.txt
- 2025-10-30-IOCs-for-cryptocurrency-scams-using-fake-chatbots.txt
- 2025-11-07-IOCs-for-phishing-activity-spoofing-spam-filters.txt
- 2025-11-10-IOCs-from-Stately-Taurus-activity.txt

- 2025-11-11-IOCs-for-TDS-pushing-PUP.txt
- 2025-11-13-IOCs-for-Squeamish-Libra-activity.txt
- 2025-11-21-IOCs-for-ShinySp1d3r-ransomware.txt
- 2025-11-24-ongoing-testing-of-malicious-Chrome-extension-samples.txt
- 2025-11-25-Domains-for-Black-Friday-scams.txt
- 2025-12-03-recent-surge-in-ClickFix-activity.txt
- 2025-12-08-White-Lynx-uses-CAPTCHA-macros.txt
- 2025-12-15-real-world-case-of-malicious-indirect-prompt-injection.md
- 2025-12-18-phishing-for-authentication-tokens.txt
- 2026-01-07-scams-using-calendar-invites.txt
- 2026-01-16-W-8BEN-themed-phishing-activity.txt
- 2026-01-22-Attack-chain-targeting-users-looking-for-legitimate-tools.txt
- 2026-01-30-IOCs-for-traffic-ticket-search-portal-themed-phishing.txt
- 2026-02-03-IOCs-from-KongTuke-ClickFix-activity.txt
- 2026-02-04-IOCs-for-December-2025-Contagious-Interview-activity.txt
- 2026-02-05-IOCs-for-phishing-and-scams.txt
- 2026-02-06-IOCs-for-Super-Bowl-LX-scams.txt
- 2026-02-10-IOCs-for-smishing-impersonating-US-wireless-carriers.txt
- 2026-02-11-IOCs-for-RAT-disguinsed-as-AI-based-browser-extension.txt
- 2026-02-13-IOCs-for-tactics-by-browser-extensions-to-avoid-bans.txt
- 2026-02-20- AI-Accelerated Malicious Chrome Extension Campaigns.txt
- 2026-02-20-IOCs-for-tech-support-scam-activity.txt
- 2026-02-27-IOCs-for-Alloy-Taurus-infrastructure
- 2026-03-09-Threat-Alert-30K-domains-distributing-malicious-AI-related-browser-extension.txt
- 2026-03-10-IOCs-for-VoidLink-activity.txt
- 2026-03-12-Vishing-Campaigns-Lead-to-Data-Theft-and-Extortion.txt

- 2026-03-19-THE-GHOST-IN-CAMPAIGN.txt
- 2026-03-23- Device-Code-based-OAuth-Phishing.txt
- 2026-03-30-KIMWOLF-V7-IoT.txt
- 2026-03-31-SHub-Stealer-Activity.txt
- 2026-04-02-Threat-Actor-Targets-Military-Entities.txt
-
-
-

Source: https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt