tweets/2020-09-07-Dridex-IOCs.txt at master · pan-unit42/tweets

By brad-duncan

Files

- 2020-08-20-Emotet-infection-with-Qakbot.pcap.zip
- 2020-08-20-IOCs-for-Emotet-infection-with-Qakbot.txt
- 2020-08-24-Trickbot-gtag-ono66-IOCs.txt
- 2020-08-25-IOCs-for-Emotet-with-Trickbot.txt
- 2020-09-01-raccoon-stealer-IOCs.txt
- 2020-09-07-Dridex-IOCs.txt
- 2020-09-21-Dridex-IOCs.txt
- 2020-09-28-Qakbot-IOCs.txt
- 2020-10-01-Formbook-IOCs.txt
- 2020-10-05-AZORult-IOCs.txt
- 2020-10-26-Emotet-epoch-2-with-Trickbot-gtag-mor137-IOCs.txt
- 2020-11-05-Hancitor-IOCs.txt

- 2020-11-16-Cobalt-Strike-IOCs.txt
- 2020-11-23-SmokeLoader-Dridex-and-webshell-IOCs.txt
- 2020-11-23-SmokeLoader-and-Dridex-infection-with-webshell.pcap.zip
- 2020-12-02-Astaroth-IOCs.txt
- 2020-12-02-Astaroth-email-and-malware.zip
- 2020-12-10-IOCs-from-Ursnif-infection-with-Delf-variant.txt
- 2020-12-10-Ursnif-infection-with-Delf-variant.pcap.zip
- 2020-12-11-Zepplin-ransomware-note.txt
- 2020-12-14-IOCs-from-Qakbot-activity.txt
- 2021-01-05-Emotet-and-Trickbot-IOCs.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-TA551-IOCs-for-Qakbot.txt
- 2021-02-08-tech-zupport-scam-audio.mp3
- 2021-02-22-IOCs-from-Guildma-infection.txt
- 2021-03-01-IcedID-IOCs.txt
- 2021-03-08-IOCs-from-Banload-infection.txt
- 2021-03-15-IcedID-IOCs.txt
- 2021-03-15-IcedID-infection-traffic.pcap.zip
- 2021-03-15-IcedID-malware-and-artifacts.zip
- 2021-03-15-malspam-pushing-IcedID.eml.zip
- 2021-03-22-Dridex-malspam-10-examples.zip
- 2021-03-22-Dridex-malware-and-artifacts.zip
- 2021-03-22-IOCs-from-Dridex-infection.txt

- 2021-03-24-IOCs-for-IcedID-infection-with-Cobalt-Strike.txt
- 2021-03-24-IcedID-malware-and-artifacts.zip
- 2021-04-12-IcedID-IOCs.txt
- 2021-04-12-IcedID-malware-and-artifacts.zip
- 2021-04-15-IOCs-for-AsyncRAT-activity.txt
- 2021-04-26-IcedID-with-Cobalt-Strike-IOCs.txt
- 2021-04-26-IcedID-with-Cobalt-Strike-malware-and-artifacts.zip
- 2021-04-26-IcedID-with-Cobalt-Strike-traffic.pcap.zip
- 2021-05-10-IOCs-for-TA551-pushing-IcedID.txt
- 2021-05-10-TA551-IcedID-malware-and-artifacts.zip
- 2021-05-17-TA551-IOCs-for-IcedID.txt
- 2021-05-17-TA551-IcedID-malware-and-artifacts.zip
-
- 2021-06-21-TA551-IOCs-for-Ursnif.txt
- 2021-06-28-TA551-IOCs-for-Trickbot.txt
- 2021-07-12-Hancitor-IOCs.txt
- 2021-07-20-IOCs-for-BazarLoader-and-Trickbot.txt
- 2021-07-26-Trickbot-gtag-rob112.txt
- 2021-07-29-IOCs-for-BazarLoader-CobaltStrike-PrintNightmare.txt
- 2021-08-09-BazarLoader-and-Cobalt-Strike-IOCs.txt
-
- 2021-08-18-phishing-example.txt
- 2021-08-26-IOCs-for-DDoS-themed-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-TA551-BazarLoader-with-Cobalt-Strike-IOCs.txt
- 2021-10-07-Qakbot-obama111-and-Cobalt-Strike-IOCs.txt
- 2021-10-07-Qakbot-obama111-and-Cobalt-Strike-malware-and-artifacts.zip
- 2021-10-18-IOCs-for-TR-based-Qakbot-with-Cobalt-Strike.txt
- 2021-11-03-TA551-BazarLoader-info.txt
- 2021-11-04-IOCs-for-TR-Qakbot-with-Cobalt-Strike.txt
- 2021-11-05-TA551-IOCs.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-Emotet-epoch4-IOCs.txt
- 2022-02-22-Emotet-epoch5-IOCs.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-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
- 2022-08-29-IOCs-for-Monster-Libra-TA551-IcedID-with-Cobalt-Stike.txt
- 2022-09-13-IOCs-for-Qakbot.txt

- 2022-09-21-IOCs-for-Astaroth-Guildma-infection.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-BB12-Qakbot-infection-IOCs.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
- 2023-08-10-moved-to-new-Github-repository.txt
-
-

Latest commit

135 lines (113 loc) · 6.54 KB

Breadcrumbs

1. tweets

2020-09-07-Dridex-IOCs.txt

File metadata and controls

-
-

135 lines (113 loc) · 6.54 KB

Source: https://github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt