LevelBlue - Open Threat Exchange

By msudosos

Archived: 2026-04-29 07:02:54 UTC

- 48 Subscribers

- 121 Subscribers

WarzoneRAT impacts Social Media of users with compromised systems

CVE: 1 | **FileHash-MD5:** 274 | **FileHash-SHA1:** 226 | **FileHash-SHA256:** 2494 | **URL:** 4194 | **Domain:** 624 | **Email:** 1 | **Hostname:** 1563

Injection affects compromised user/s social media accounts including YouTube. Uploads to social media accounts from infected systems divert to adversary’s alt YouTube media center labeled ‘watch’ instead of YouTube . Remote access observed. Threat actor has full access , cnc , devices, personal information, images, contacts, network, private information including all financial information. Alt / adversarial Pinterest, Tumblr, YouTube, Facebook, Twitter / X, Instagram , LinkedIn

- 138 Subscribers

- 487 Subscribers

- 267 Subscribers

- 183 Subscribers

Howling at the Inbox: Sticky Werewolf's Latest Malicious Aviation Attacks

FileHash-MD5: 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 10 | **Domain:** 1

Morphisec Labs has been monitoring increased activity associated with Sticky Werewolf, a suspected geopolitical or hacktivist group. While their origin remains unclear, recent techniques suggest espionage and data exfiltration intent. Sticky Werewolf has targeted the aviation industry, employing phishing emails with archive attachments containing LNK files pointing to malicious payloads on WebDAV servers. The infection chain involves executing these LNK files, triggering a process that ultimately injects commodity malware like RATs or stealers to facilitate data theft.

- 379,483 Subscribers

IOCS202312212258

CVE: 3 | **FileHash-MD5:** 112 | **FileHash-SHA1:** 98 | **FileHash-SHA256:** 425 | **URL:** 170 | **Domain:** 104 | **Hostname:** 201

The following is the full text of the text and images that can be accessed via the internet. Â£1.3bn, $2.4bn and £2bn.. and

- 418 Subscribers

IOCS202312171728

CVE: 3 | **FileHash-MD5:** 117 | **FileHash-SHA1:** 97 | **FileHash-SHA256:** 424 | **URL:** 181 | **Domain:** 96 | **Hostname:** 208

Hashes, which are subject to change, have been published by the Office for National Statistics (ONS) and the Royal Mail (RPS) in a bid to track down the most common addresses on the internet.

- 418 Subscribers

- 1,607 Subscribers

https://myaccount.uscis.gov/

CVE: 19 | **FileHash-MD5:** 204 | **FileHash-SHA1:** 182 | **FileHash-SHA256:** 6268 | **URL:** 13989 | **Domain:** 3229 | **Email:** 3 | **Hostname:** 4412

- 218 Subscribers

- 218 Subscribers

https://myaccount.uscis.gov/

CVE: 19 | **FileHash-MD5:** 204 | **FileHash-SHA1:** 182 | **FileHash-SHA256:** 6268 | **URL:** 13989 | **Domain:** 3229 | **Email:** 3 | **Hostname:** 4412

After Mark Montano Md reported alleged acts by Jeffrey Scott Reimer after receiving 'multiple' reports of him aggressively pursuing Brashears, she was contacted, told she violated the Patriot Act by Big O Tires?!! Received letters from the above and harassed for years. Colorado Workers compensation is so corrupt this may be my last post. She was immediately framed , blamed, porn smeared and stalked. Denied medical care , when received died on surgery table, revised and disabled. Even the mafia would tackle only the associates bringing undue negative attention to their own organization.

- 218 Subscribers

https://myaccount.uscis.gov/

CVE: 19 | **FileHash-MD5:** 204 | **FileHash-SHA1:** 182 | **FileHash-SHA256:** 6268 | **URL:** 13989 | **Domain:** 3229 | **Email:** 3 | **Hostname:** 4412

- 224 Subscribers

https://myaccount.uscis.gov/

CVE: 19 | **FileHash-MD5:** 204 | **FileHash-SHA1:** 182 | **FileHash-SHA256:** 6268 | **URL:** 13989 | **Domain:** 3229 | **Email:** 3 | **Hostname:** 4412

- 224 Subscribers

- 224 Subscribers

https://myaccount.uscis.gov/

CVE: 19 | **FileHash-MD5:** 204 | **FileHash-SHA1:** 182 | **FileHash-SHA256:** 6268 | **URL:** 13989 | **Domain:** 3229 | **Email:** 3 | **Hostname:** 4412

HOW!?!? My device was remotely logged into this account somehow. This is egregious. Silence Threats. I have no connection to this but was contacted by a while ago. I don't know how or why a part of the government would attack a person with a TBI and C1 - S1 Spinal cord injury allegedly caused by Colorado physical therapist and protect him. Why is victim, tracked and unsafe, receiving death threats, monitored, denied medical care, stalked EVERYWHERE. Even felons aren't monitored for life. STOP. Will this get us killed. Do the right thing. God bless America, purge the government. The truth should set you fee not get you harmed.

- 218 Subscribers

IOCS202311072259

CVE: 3 | **FileHash-MD5:** 113 | **FileHash-SHA1:** 100 | **FileHash-SHA256:** 401 | **URL:** 154 | **Domain:** 53 | **Hostname:** 181

Hosts, web addresses and addresses are all listed on the official list of the world's most popular web address providers. and they all appear to have the same name and address.. the.

- 418 Subscribers

Remote & other attacks. Dapato I Detplock I Emotet I

CVE: 13 | **FileHash-MD5:** 2522 | **FileHash-SHA1:** 862 | **FileHash-SHA256:** 2855 | **URL:** 7963 | **Domain:** 1168 | **Email:** 2 | **Hostname:** 3181

http://bpdb.portal.gov.bd:3128/sites/default/files/files/bpdb.portal.gov.bd/npfblock/2021-34bc869d2906198362a4346373ce5b94.jpg Purports to be based in Bangladesh, bounces to USA. Tor exit, relay router. Many proxies. Malicious. Very malicious targeting involved. Apple iOS hacking, device unlocking, CNC. Legal mischief.

- 218 Subscribers

Kraddare • Agent Tesla • CVE Jar

CVE: 13 | **FileHash-MD5:** 2522 | **FileHash-SHA1:** 862 | **FileHash-SHA256:** 2855 | **URL:** 7963 | **Domain:** 1168 | **Email:** 2 | **Hostname:** 3181

http://bpdb.portal.gov.bd:3128/sites/default/files/files/bpdb.portal.gov.bd/npfblock/2021-34bc869d2906198362a4346373ce5b94.jpg Purports to be based in Bangladesh, bounces to USA. Tor exit, relay router. Many proxies. Malicious. Very malicious targeting involved. Apple iOS hacking, device unlocking, CNC. Legal mischief? CVE CVE-2017-0147 CVE CVE-2015-1650 CVE CVE-2014-6352 CVE CVE-2014-3153 CVE CVE-2017-8570 CVE CVE-2015-6585 CVE CVE-2012-0158 CVE CVE-2010-3333 CVE CVE-2017-17215 http://1.116.132.182/weblogic_CVE_2020_2551.jar

- 218 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:Netwire