LevelBlue - Open Threat Exchange

By skocherhan

Archived: 2026-04-05 21:04:07 UTC

Author Url

Sality

FileHash-MD5: 200 | **FileHash-SHA1:** 200 | **FileHash-SHA256:** 1000

- 175 Subscribers

- 134 Subscribers

Mirai • Neurotox Institute

FileHash-MD5: 183 | **FileHash-SHA1:** 79 | **FileHash-SHA256:** 1442 | **SSLCertFingerprint:** 63 | **URL:** 511 | **Domain:** 471 | **Email:** 5 | **Hostname:** 198

Found in peripheral. Lazarus. Related tomOperation Endgame. Strangely related to the entertainment industry. Related to treatments facilities where a target I’ve been researching received ‘care’. Also links to Major Entertainment conglomerate : not surprisingly Hall Render and Foundry. Page was stated to expire 11/21 | expired after I was able to capture a live screenshot (not updated for years) [The Neurotoxin Institute (NTI) is a multidisciplinary organization created to serve as a comprehensive independent source of information related to the basic science and the clinical applications of neurotoxins. The Institute fosters the learning and teaching of both theory and practical techniques, and encourages further research in support of these goals. Experimental Biology (EB) www.aapmr.org]

- 134 Subscribers

dfirfanatic_IOC's

CVE: 11 | **FileHash-MD5:** 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 6 | **URL:** 20 | **Domain:** 39 | **Hostname:** 12

51.15.98.45 51.15.115.141 51.15.44.6 107.23.39.208 154.38.185.108 139.59.30.78 139.59.30.78 141.98.11.168 195.164.49.68 152.39.227.27 212.56.53.90 159.65.231.167 195.154.208.101 195.154.208.99 163.172.77.100 47.84.83.221 104.28.211.187 152.42.211.173 174.138.17.185 209.146.60.235 45.9.148.131 2a0e:fa00:0:25::1 178.128.208.31 157.66.55.50 178.128.208.31 104.28.211.187 13.76.244.181 201.46.112.135 118.41.203.50 51.75.126.7 188.166.163.12 195.242.212.198 93.123.109.246 152.32.129.236

- 1 Subscribers

九秀直播-高品质美女在线视频互动社区 - Malware packed | Botnet |Porn dumping affects Communities

CVE: 1 | **FileHash-MD5:** 671 | **FileHash-SHA1:** 641 | **FileHash-SHA256:** 1982 | **SSLCertFingerprint:** 17 | **URL:** 4063 | **Domain:** 596 | **Email:** 3 | **Hostname:** 1097

九秀直播-高品质美女在线视频互动社区 - Malware packed | Botnet | Porn dumping affects Communities | Packed. Russian linked YouTube channels that may none US or Canada, (unclear) Asian pornography dumping. Remotes phones. Spyware *can’t annotate #denver #mitm #advesaries #trojans #unix #linux #torrentinf #dumps #twiitter #listeners #spy || 2010382 Fake AV GET 2013149 RogueAntiSpyware.AntiVirusPro Checkin 2013178 Long Fake wget 3.0 User-Agent

- 134 Subscribers


Author Url

- 1,584 Subscribers


Author Url

2606:4700:3036::ac43:a8cb (2606:4700:3000::/42)

CIDR: 2 | **CVE:** 1 | **FileHash-MD5:** 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 471 | **URL:** 870 | **YARA:** 163 | **Domain:** 47 | **Email:** 4 | **Hostname:** 148

Here is a full set of words and phrases used by the BBC to describe the various types of ransomware that can be used to target victims of the Windows operating system, as well as the UK.

- 122 Subscribers


Author Url

PolymodXT.exe

FileHash-MD5: 414 | **FileHash-SHA1:** 410 | **FileHash-SHA256:** 1940 | **URL:** 171 | **YARA:** 759 | **Domain:** 134 | **Email:** 4 | **Hostname:** 56

- 122 Subscribers


Author Url

f83991c8-f2d9-5583-845a-d105034783ab

CVE: 1 | **FileHash-MD5:** 12 | **FileHash-SHA1:** 11 | **FileHash-SHA256:** 17 | **URL:** 55 | **YARA:** 53 | **Domain:** 4 | **Hostname:** 7

https://www.virustotal.com/gui/file/e79f57b603370d4cd4ab1d757833995b89c7d79c9071c75d72c6d082ba0a7ea4/detection A chronology of key events in the history of the United States:-1.1-2 January 2020.. and 1 February 2021.. (c.9/11):.

- 122 Subscribers

Threat Intel Report - W03-2025

CVE: 1 | **FileHash-MD5:** 12 | **FileHash-SHA1:** 12 | **FileHash-SHA256:** 13 | **URL:** 202 | **Domain:** 80 | **Hostname:** 85

This is a cyber-advisory document, presenting the compiled cyber threat intelligence sourced from various channels and tools. These are weekly base recommendations to all IT Administrators and CISOs to take corrective actions to upgrade their security infrastructure against newly identified threats and attacks in this week. Security is a continuous process, and it has to be reviewed and audited on a continuous manner through manual or automated tools. These details may be used as an additional layer to verify the current security posture of an organization against latest cyber trends

- 105 Subscribers

Threat Intel Report - W01-2025

FileHash-MD5: 14 | **FileHash-SHA1:** 14 | **FileHash-SHA256:** 14 | **URL:** 165 | **Domain:** 74 | **Hostname:** 83

This is a cyber-advisory document, presenting the compiled cyber threat intelligence sourced from various channels and tools. These are weekly base recommendations to all IT Administrators and CISOs to take corrective actions to upgrade their security infrastructure against newly identified threats and attacks in this week.

- 105 Subscribers

cobalt_loader_unpacked.exe

FileHash-MD5: 23 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 177 | **IPv4:** 38 | **URL:** 154 | **YARA:** 52 | **Domain:** 14 | **Email:** 7 | **Hostname:** 58

A guide to the Cobaltloader, a 32-bit executable for Windows, has been published by the University of Oxford.. and its website is published on the same day as the release.

- 122 Subscribers

Black Tech

CIDR: 1 | **CVE:** 37 | **FileHash-MD5:** 2449 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 3441 | **URL:** 2044 | **Domain:** 258 | **Email:** 4 | **Hostname:** 1100

Found in a malicious Apple iTunes link. Lists several independent artists. Music "producer" is potentially highly dependent on use of AI generated instrumentation and conception. Hacking seems to target a single target and associates.

- 224 Subscribers

- 224 Subscribers

- 224 Subscribers

- 1,584 Subscribers

- 224 Subscribers

Sality found in DGA unspecified phishing campaign. Immigration

FileHash-MD5: 339 | **FileHash-SHA1:** 329 | **FileHash-SHA256:** 1161 | **SSLCertFingerprint:** 2 | **URL:** 574 | **Domain:** 524 | **Email:** 9 | **Hostname:** 650

•A domain generation algorithm (DGA) is a subroutine adversaries implement to dynamically identify a destination domain for CnC traffic as opposed to usage of a list of static IP addresses or domains. Generates large numbers of new domain names. Cybercriminals and botnet operators use (DGA) evading detection, generated volumes of domains & IP addresses for malware CnC servers. •Sality is an appending polymorphic file infector virus that uses an Entry Point Obscuring (EPO) technique. Unlike other file infectors that modify the entry point of the host file to point to the virus code, Sality.

- 218 Subscribers

- 218 Subscribers

- 218 Subscribers

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