LevelBlue - Open Threat Exchange

By Q.Vashti

Archived: 2026-04-29 07:02:11 UTC

Show:

All

Sort:

Recently Modified

GoBrut Service Bruter CnC Activity • TAM Legal • Christopher P. Ahmann

CVE: 1 | **FileHash-MD5:** 441 | **FileHash-SHA1:** 432 | **FileHash-SHA256:** 1015 | **SSLCertFingerprint:** 9 | **URL:** 4792 | **Domain:** 3031 | **Email:** 8 | **Hostname:** 1840

Malicious attacks from Special Counsel criminal attorney defending Jeffrey Scott Reimer and Concentra against and on premises vicious SA. Caused grate bodily injury. Christopher P. Ahmann and Hall Render (down the street) Palantir has been harassing , working 24/7 at silencing one crime victim. I’m sure there are more because we thwarted an attempt in 2018. Hitman hired. You couldn’t believe manpower and cyber attacks one family has been through. They attack the Large Loss clients.

- 138 Subscribers

IOC Blocking

FileHash-MD5: 24 | **FileHash-SHA1:** 24 | **FileHash-SHA256:** 24 | **Domain:** 5

- 21 Subscribers

Lunar Spider Expands their Web via FakeCaptcha

CVE: 1 | **FileHash-MD5:** 22 | **FileHash-SHA1:** 22 | **FileHash-SHA256:** 54 | **URL:** 7 | **Domain:** 80 | **Hostname:** 6

Lunar Spider, a Russian-speaking cybercriminal group, has escalated its attack strategies by targeting vulnerable websites primarily in Europe, exploiting Cross-Origin Resource Sharing (CORS) vulnerabilities. Their approach involves injecting a FakeCaptcha framework into these sites through a JavaScript snippet that creates an iframe, effectively overlaying malicious content on legitimate sites. This technique allows them to track victim interactions and report clicks back to a Telegram channel. The infection process begins with an MSI downloader that embeds a legitimate Intel executable alongside a malicious DLL dubbed Latrodectus. This downloader registers the Intel EXE in the Windows Run registry key for persistence and then sideloads the Latrodectus DLL by exploiting the DLL search order hijacking mechanism.

- 172 Subscribers

sdfzsdf.ele fac1ec40eea5a4fc05f17e019328e287

FileHash-MD5: 28 | **FileHash-SHA1:** 27 | **FileHash-SHA256:** 1077 | **URL:** 1092 | **YARA:** 535 | **Domain:** 282 | **Email:** 4 | **Hostname:** 316

SHA1- 33008f85428a83996083c3da92a8f00595071403 SHA256 cdab1c3196887d4f749d82f014786a966c87f35a7189f0f3d078558b957847bf
https://sandbox.ti.qianxin.com/sandbox/page/detail?type=file&id=7b6726e20c513baebf7fd387a3dd1b7d67a4c7c4
https://ti.qianxin.com/v2/search?type=file&value=fac1ec40eea5a4fc05f17e019328e287
https://www.virustotal.com/gui/file/cdab1c3196887d4f749d82f014786a966c87f35a7189f0f3d078558b957847bf/relations

- 121 Subscribers

PolymodXT.exe

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

- 121 Subscribers

Svchost id: 16c37b52-b141-42a5-a3ea-bbe098444397

FileHash-MD5: 39 | **FileHash-SHA1:** 28 | **FileHash-SHA256:** 1065 | **URL:** 984 | **YARA:** 535 | **Domain:** 262 | **Email:** 4 | **Hostname:** 316

The following rules for the Windows.Trojan.Tofsee malware have been revealed by the BBC's Panorama programme and are subject to a review by BBC Newsnight and BBC Radio 5 live.

- 121 Subscribers

Android - BankBot

CVE: 2 | **FileHash-MD5:** 31 | **FileHash-SHA1:** 28 | **FileHash-SHA256:** 28 | **URL:** 10 | **Domain:** 11

BankBot is a free guide to how to access the bank's online banking services, which can be accessed via your mobile phone or tablet, and is available to download on the BBC app and website.

- 24 Subscribers

DarkGate: Opening Gates for Financially Motivated Threat Actors

FileHash-MD5: 4 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 14 | **URL:** 6 | **Domain:** 4 | **Hostname:** 1

EclecticIQ's Threat Intelligence Platform is a collection of analyst-centric threat intelligence products and services designed to improve the security posture of your company and its global partner networks, and to enhance the ability of its partners to deliver world-class cybersecurity solutions.

- 848 Subscribers

- 65 Subscribers

DarkGate: Opening Gates for Financially Motivated Threat Actors

FileHash-MD5: 4 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 14 | **URL:** 4 | **Domain:** 4 | **Hostname:** 1

EclecticIQ's Threat Intelligence Platform is a collection of analyst-centric threat intelligence products and services designed to improve the security posture of your company and its global partner networks, and to enhance the ability of its partners to deliver world-class cybersecurity solutions.

- 58 Subscribers

- 848 Subscribers

- 267 Subscribers

- 183 Subscribers

- 568 Subscribers

- 487 Subscribers

New XWorm Variant

FileHash-MD5: 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 22 | **Hostname:** 1

- 487 Subscribers

- 267 Subscribers

- 183 Subscribers

Bumblebee Loader Resurfaces in New Campaign | Intel471

URL: 1 | **Domain:** 4

Intel 471 Malware Intelligence systems have uncovered new techniques for distributing Bumblebee, a type of malware used by organized cybercriminal gangs, as well as a new campaign to disseminate malware.

- 71 Subscribers

- 44 Subscribers

Sort:

Most Pulses

Sort:

Most Members

Indicators Search

Filter by:

Reset Filters

All Time

Show expired indicators

Indicator Type

All (835)

CIDR (0)

CVE (0)

Domain (293)

Email (0)

FileHash-IMPHASH (0)

FileHash-MD5 (0)

FileHash-PEHASH (0)

FileHash-SHA1 (0)

FileHash-SHA256 (12)

FilePath (0)

Hostname (0)

IPv4 (516)

IPv6 (0)

Mutex (0)

NIDS (0)

URI (0)

URL (9)

YARA (5)

Ja3 (0)

Osquery (0)

Sslcertfingerprint (0)

Bitcoinaddress (0)

Role

Adware

Backdoor

Bruteforce

Command & Control

Delivery Email

Document Exploit

Domain Owner

Exploit Kit

Exploit Source

File Scanning

Hacking Tools

Hunting

Macro Malware

Malvertising

Malware Hosting

Memory Scanning

PCAP Scanning

Phishing

RAT

Ransomware

Scanning Host

Trojan

Unknown

Web Attack

Worm

We've found 835 indicators

Sort:

Recently Modified

Sort:

Name Ascending

Sort:

Ascending

Sort:

Ascending
