LevelBlue - Open Threat Exchange

By scoreblue

Archived: 2026-04-02 10:48:55 UTC

PuffStealer

CIDR: 2 | **CVE:** 26 | **FileHash-MD5:** 1184 | **FileHash-SHA1:** 949 | **FileHash-SHA256:** 3712 | **URL:** 2925 | **Domain:** 627 | **Email:** 8 | **Hostname:** 1319

- 224 Subscribers

- 224 Subscribers

Ransom.Win64.PORNOASSET.SM1 | DeepScan:Generic.Ransom.GandCrab5

CIDR: 2 | **CVE:** 26 | **FileHash-MD5:** 1184 | **FileHash-SHA1:** 949 | **FileHash-SHA256:** 3712 | **URL:** 2925 | **Domain:** 627 | **Email:** 8 | **Hostname:** 1319

Ransom.Win64.PORNOASSET.SM1 DeepScan:Generic.Ransom.GandCrab5 BlackNET RAT $WebWatson Auto generated results from a variety of tools.

- 218 Subscribers

Lucky Mouse APT27 | Feodo Tracker | Malicious Tor Server | Apple iOS

CIDR: 2 | **CVE:** 26 | **FileHash-MD5:** 1184 | **FileHash-SHA1:** 949 | **FileHash-SHA256:** 3712 | **URL:** 2925 | **Domain:** 627 | **Email:** 8 | **Hostname:** 1319

Darkside 2020 Ecosystem .BEware Malicious Tor server. Link found in pulse created prior. Malvertizing target: Tsara Brashears Revenge Porn. There may me others. Malicious Apple activities, locating, CVE exploits, unlocking, hijacker, service transfer, spyware, malicious full auth, tracking, endless. Seems to originate from a law firm that goes to far to defend clients and silence alleged victims. Some State allow the same privileges and tools the federal government to insurance, workers compensation, investigators and insurance company law firms for investigations. Fear tactics they seem willing to back up. I was approached and asked about my cyber knowledge by strangers. I am followed now for using a tool properly. ALL terms auto populated from various tools from various tools used including, State, Brian Sabey, cyber stalking. Perhaps he's made contact with target. Danger!

- 218 Subscribers

Lucky Mouse APT27 | Feodo Tracker | Malicious Tor Server | Apple iOS

CIDR: 2 | **CVE:** 26 | **FileHash-MD5:** 1184 | **FileHash-SHA1:** 949 | **FileHash-SHA256:** 3712 | **URL:** 2925 | **Domain:** 627 | **Email:** 8 | **Hostname:** 1319

Darkside 2020 Ecosystem .BEware Malicious Tor server. Link found in pulse created prior. Malvertizing target: Tsara Brashears Revenge Porn. There may me others. Malicious Apple activities, locating, CVE exploits, unlocking, hijacker, service transfer, spyware, malicious full auth, tracking, endless. Seems to originate from a law firm that goes to far to defend clients and silence alleged victims. Some State allow the same privileges and tools the federal government to insurance, workers compensation, investigators and insurance company law firms for investigations. Fear tactics they seem willing to back up. I was approached and asked about my cyber knowledge by strangers. I am followed now for using a tool properly. ALL terms auto populated from various tools from various tools used including, State, Brian Sabey, cyber stalking. Perhaps he's made contact with target. Danger!

- 218 Subscribers

- 480 Subscribers

Feodo Tracker C&C Server| BotNet

FileHash-MD5: 6 | **FileHash-SHA1:** 6 | **FileHash-SHA256:** 6 | **URL:** 2

Command and Control Botnet Source: http://cloudbazaar.org/ researching DGA DGA Domain: PublicDomainRegistry.com Pattern Match: many if the vulnerabilities I've researched originate from Registrar. Not all, but enough to raise an eyebrow. Active: Feodo Tracker

- 218 Subscribers

Feodo Tracker C&C Server| BotNet

FileHash-MD5: 6 | **FileHash-SHA1:** 6 | **FileHash-SHA256:** 6 | **URL:** 2

Command and Control Botnet Source: http://cloudbazaar.org/ researching DGA DGA Domain: PublicDomainRegistry.com Pattern Match: many of the vulnerabilities I've researched originate from Registrar. Not all, but enough to raise an eyebrow. ActiveFeodo Tracker

- 218 Subscribers

Threat Actors Alter DGA Patterns to Improve C2 Communication

CVE: 1 | **FileHash-SHA256:** 2 | **URL:** 2 | **Domain:** 5

Malware is evolving to evade security measures and evade detection by changing the patterns of domain names used to communicate with C2 servers, according to security experts and a group of researchers in the UK.

- 480 Subscribers

- 171 Subscribers

Elastic Security Labs discovers the LOBSHOT malware | Elastic

FileHash-SHA256: 1 | **IPv4:** 1 | **URL:** 1

Elastic Security Labs is shedding light on an undiscovered hVNC malware that has been quietly collecting a large install base. This malware called LOBSHOT appears to be leveraged for financial purposes employing banking trojan and info-stealing capabilities. Adversaries continue to abuse and increase reach through malvertising such as Google Ads by impersonating legitimate software.

- 71 Subscribers

- 171 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

- 354 Subscribers

- 69 Subscribers

- 69 Subscribers

- 52 Subscribers

Email Malspam Campaign Infrastructure Analysis

Domain: 672

"From March to December 2020, we tracked segments of a dynamically generated email infrastructure that attackers used to send more than a million emails per month, distributing at least seven distinct malware families in dozens of campaigns using a variety of phishing lures and tactics. These campaigns aimed to deploy malware on target networks across the world, with notable concentration in the United States, Australia, and the United Kingdom. Attackers targeted the wholesale distribution, financial services, and healthcare industries."

- 373,184 Subscribers

Backdoor.Necurs

Backdoor.Necurs is a Trojan horse that opens a back door on the compromised computer. The Trojan may also disable antivirus products as well as download and install additional malware.

- 127 Subscribers

- 1,344 Subscribers

Indicators Search

Show expired indicators

We've found 535 indicators

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