July 2023

Updates released in July of 2023 to Cisco cloud-based machine learning global threat alerts:

Additional Threat Detections

We've added new threat detections to our portfolio, including:

- Aurora
- GCleaner
- Kelihos
- Mystic
- RedDriver

We've also updated indicators for our existing threat detections.

Aurora

Aurora is an information stealer that targets browsers, passwords, cryptocurrency wallets, and RDP credentials (T1005). Starting from 2022, it gained popularity on Russian-speaking, hacking forums. It is delivered through SEO-poisoned, fake, cracked software in search engine results (T1189). Like many other stealers, it contains grabber and loader modules capable of collecting and exfiltrating files (T1041) and deploying additional payloads (T1105). It makes use of WMI (T1047) and PowerShell (T1059.001) while operating on the victim device. It is written in Golang.

To see if the Aurora stealer has been detected in your environment, click Aurora Stealer Threat Detail to view its details in global threat alerts.

GCleaner

GCleaner, also known as G-Cleaner or Garbage Cleaner, is an application that is promoted as a legitimate tool for speeding up and optimizing Windows devices. However, GCleaner is a malicious pay-per-install (PPI) loader that can deliver other malware such as Azorult, Stealc, and Vidar. It is distributed through websites (T1189) that share applications and pirated software. By disguising itself as a genuine optimization tool (T1036), GCleaner manages to infiltrate systems and execute its malicious payload. GCleaner utilizes a

geolocation-based command-and-control infrastructure, meaning that the behavior of the loader and subsequent malware downloads (T1105) depend on the location of the victim's IP address.

To see if GCleaner has been detected in your environment, click GCleaner Threat Detail to view its details in global threat alerts.

Kelihos

Kelihos, also known as Hlux, is a peer-to-peer botnet with a wide range of malicious activities, including spam email distribution, stealing sensitive information, conducting distributed denial-of-service (DDoS) (T1498), and mining bitcoins. Kelihos is distributed via malicious email campaigns containing attachments (T1566.001) or links that lead to the installation of its payload (T1566.002). It can also be distributed using the drive-by downloads when users visit compromised websites (T1189). Once the system is compromised, the malware contacts the command-and-control server to receive commands and download additional components (T1105).

To see if Kelihos has been detected in your environment, click Kelihos Threat Detail to view its details in global threat alerts.

Mystic

Mystic is an information stealer that also has loader capabilities (T1105). It's been advertised in the dark web since April 2023 and collects information such as system hostname, user name, and GUID (T1082). It can also identify user geolocation using the keyboard layout. The stealer targets various web browsers, browser extensions, cryptocurrency applications, MFA and password management programs, and Steam and Telegram credentials. It is capable of capturing browser history, auto-fill data, bookmarks, cookies, and other stored credentials from browsers (T1555.003). Mystic uses a custom binary protocol over TCP for command-and-control communication (T1095), used to exfiltrate data from the infected device (T1041). Mystic sends the information of the infected device on the fly, without storing it on the disk.

To see if the Mystic stealer has been detected in your environment, click Mystic Stealer Threat Detail to view its details in global threat alerts.

RedDriver

RedDriver is a driver-based browser hijacker (T1185) targeting Chinese users. It is distributed as an executable that mimics popular endpoint applications (T1036). It contains two DLLs that are used later for reflective code loading (T1620) into the browser session. The same executable is also used to download a malicious driver (T1105) in order to redirect browser traffic through a listening port on the victim system (T1557). It is capable of bypassing Windows driver-signing policies, due to its usage of the HookSignTool.

To see if RedDriver has been detected in your environment, click RedDriver Threat Detail to view its details in global threat alerts.