March 2023

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

Additional Threat Detections

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

- Amadey
- BatLoader
- Retadup
- Stealc
- ViperSoftX

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

Amadey

Amadey is a Trojan bot known for stealing data and deploying additional malware. It is delivered through phishing (T1566) emails or deployed by other malware families. It maintains its persistence on the victim's device through registry entries (T1547.001) and scheduled tasks (T1053.005). Before communicating to its command-and-control server, it collects various data from the victim's device (T1005) such as domain name, user name, computer name, and OS version. After exfiltration of the collected data (T1041), it can download (T1105) and install malware such as exploit kits, information stealers, and ransomware.

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

BatLoader

BatLoader is a modular downloader that installs different malware in the victim's device, such as information stealers, banking Trojans, ransomware, and other loaders. BatLoader is distributed using cracked software (T1204.001); it has been observed to impersonate Adobe, AnyDesk, CCleaner, TeamViewer, and Zoom, among others. Once the victim downloads and executes the MSI file (T1204.002), it runs Powershell (T1059.001) payload through custom actions for further infection. Later, the victim's device contacts the command-and-control server (T1071.001) to download other payloads (T1105).

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

Retadup

Retadup is a Monero miner with self-replication capability. It copies LNK files to every available external drive of the victim's device (T1091). Later, it executes a malicious AutoIt-compiled script (T1204.002) and exports encoded host information (T1132.001) such as hostname and OS version to its command-and-control server. It can deploy additional malware (T1105) such as stealers and ransomware. Despite its takedown in 2019, it is still observed in networks, especially targeting devices in Latin America. Its payload names often mimic legitimate software or companies such as Google and Microsoft (T1036.005).

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

Stealc

Stealc is an information-stealer malware that is sold on darknet forums. It is distributed through phishing emails (T1566.001), malicious online advertisements, and fake software downloads (T1036). To communicate with the command-and-control server, Stealc can use application layer protocols such as HTTP or HTTPS (T1071.001). It is also capable of leveraging DNS requests (T1071.004) and capturing input actions (T1056) or screenshots (T1113) from the victim's device. Stealc uses web services (T1567) or alternative protocols (T1048) such as FTP or SMTP to exfiltrate stolen data to its command-and-control server.

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

ViperSoftX

ViperSoftX is a malware that deploys a Chrome browser extension called VenomSoftX. The malware is distributed using cracked software or torrent downloads (T1036). It can leverage encrypted binaries (T1027), Powershell payloads (T1059.001), and browser extensions (T1176) to achieve its tasks. It uses HTTP or HTTPS (T1071) to communicate with its command-and-control servers. The malware is capable of stealing cryptocurrency wallets (T1496), collecting clipboard data (T1115), executing commands (TA0002), and other tasks.

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