January 2023

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

Additional Threat Detections

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

- GootLoader
- Laplas Clipper
- Neoreklami
- Rhadamanthys

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

GootLoader

GootLoader is a dropper malware spreading through SEO poisoning (T1608.006). It tricks users into downloading benign-looking ZIP files containing a malicious JS file. It executes this initial payload using wscript and cscript (T1059.005). It gains persistence through scheduled tasks (T1053.005) and leverages Powershell (T1059.001) for its C2 traffic. It has been observed to drop CobaltStrike (S0154) on victim devices. Its command-and-control infrastructure consists of compromised WordPress websites (T1584.004).

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

Laplas Clipper

Laplas Clipper is a malware that steals cryptocurrencies. It is delivered by SmokeLoader (S0226) or phishing (T1566). For persistency, it creates a schedule task using schtasks (T1053.005). Laplas Clipper generates wallet addresses imitating the victim to hijack currency transactions. The malware steals from a variety of wallets, including Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and Dogecoin.

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

Neoreklami

Neoreklami is known to mimic AdBlockers in order to take control of the user's browser session (T1185). It schedules a task (T1053.005) to run WSF (T1059.005) and DLL (T1218.011) files for its persistence. To store these files, it creates a folder named with random alphanumerical characterss within ProgramData and Program Files (x86). After infecting the user's browser session, it downloads an obfuscated payload (T1027) to determine its next actions. The infected device may display random web page text turned into hyperlinks, advertising banners injected with legitimate web pages, popups recommending fake updates, and so on.

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

Rhadamanthys

Rhadamanthys is an information stealer that extracts and exfiltrates information from the infected device. The initial access is by fake software distribution (T1036) of applications such as AnyDesk, Zoom, and Notepad++. The domains distributing this malware have been observed to be promoted by Google ads and impersonates those applications. Rhadamanthys malware steals information related to crytocurrency wallets, along with device information such as operating system version, device name, and installed software. The malware exfiltrates data over command-and-control (T1041).

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