December 2023

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

Additional Threat Detections

We've added new threat detections to our portfolio:

- Agniane Stealer
- Pikabot
- SectopRAT

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

Agniane Stealer

Agniane is a stealer targeting browsers, passwords, cryptocurrency wallets, and RDP credentials (T1005). Starting from 2023, it gained popularity through the Malware-as-a-Service model. Similar to 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), PowerShell (T1059.001), and .NET executables that are protected using the ConfuserEx obfuscator (T1027).

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

Pikabot

Pikabot is a modular malware consisting of loader and core payloads. It is written in C/C++ and is often used to deploy other malware on victim systems (T1105). It excludes members of CIS countries from its target list and is often delivered through phishing emails containing malicious attachments (T1566.001). Its core module is often deployed through multiple stages, such as file downloads and various payload executions (TA0002). Pikabot is highly evasive; it leverages anti-VM/debugging (T1622) techniques and obfuscated strings (T1027) to avoid detection. It exhibits similar behavior to malware such as Qakbot (S0650) and DarkGate.

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

SectopRAT

SectopRAT, also known as ArechClient2, is a .NET Remote Access Trojan that is distributed by malicious links (T1204.001) disguised as legitimate software. SectopRAT has multiple capabilities; it can extract detailed information from the infected device, such as the operating system and hardware information (T1082), steal stored credentials (T1552.001), or launch hidden browser sessions. It communicates with the command-and-control server using an application layer protocol (T1071) and uses a non-standard port (T1571) to download other payloads and exfiltrate information. SectopRAT has various capabilities to disable anti-malware solutions and to evade sandbox executions.

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