May 2023

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

Additional Threat Detections

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

- DarkCrystal RAT
- Fabookie
- Nemesis Project
- TrueBot

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

DarkCrystal RAT

DarkCrystal RAT, also known as DCRAT, is a remote-access Trojan that can gain control of and steal information from the victim's device. It is distributed through phishing (T1566), other loaders (like PrivateLoader), or fake software cracks and updates (T1036). Being a modular malware, it is capable of keylogging (T1056.001) and stealing cookies, credentials, and other information from the infected device. Once the information is collected, it is exfiltrated via command-and-control communication (T1041).

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

Fabookie

Fabookie is an information stealer that aims to steal credentials from infected devices, particularly Facebook credentials. Fabookie is typically distributed by other malware, such as SmokeLoader, PrivateLoader, or Nullmixer. Once Fabookie is installed on the device, it searches for stored credentials (T1552) and gathers information about the software installed in the system (T1518). Once it obtains the credentials, it interacts with the Facebook API and communicates with the command-and-control server (T1071).

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

Nemesis Project

Nemesis Project is an information stealer that is sold on darknet forums. It is distributed through phishing emails (T1566.001), malicious online ads, and fake software downloads (T1036). It can also be distributed with other malware, such as Dave or Minodo Loader. In order to communicate with the command-and-control server, Nemesis Project uses application layer protocols such as HTTP or HTTPS (T1071.001) and is capable of leveraging DNS requests (T1071.004). The information stealer targets VPNs and browsers and is capable of capturing input actions (T1056) and screenshots (T1113) from victim systems. Nemesis Project malware 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 Nemesis Projecthas been detected in your environment, click Nemesis Project Threat Detail to view its details in global threat alerts.

TrueBot

TrueBot, also known as Silence, is a downloader malware that can fetch and execute additional payloads on victim devices. It can be deployed through prior infections (T1105) and by exploiting a public-facing application (T1190). TrueBot is known to deploy malware and tools such as Grace (S0383), Clop (S0611), and CobaltStrike (S0154). TrueBot infections consist of two modules, a loader and a downloader. Once the loader decrypts (T1140), it drops the downloader for fetching additional payloads. TrueBot maintains persistence through scheduled tasks (T1053.005) and the registry run key (T1547.001). It is assumed to be part of TA505's (G0092) arsenal due to relevant malware usage later in the infection chain.

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