August 2023

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

Additional Threat Detections

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

- Spyder Backdoor
- AsyncRAT

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

Spyder Backdoor

Spyder is a backdoor, similar to WarHawk, that is mainly used by the threat actor SideWinder. The malware is an executable file disguised as a Word, Excel, PDF, or other document file. Once the backdoor is installed, it collects system information such as machine GUID, username, CPU, and antivirus information (T1082) and exfiltrates it by command-and-control using HTTP/HTTPS (T1071.001). Spyder is capable of creating scheduled tasks to execute itself the next day (T1053.005). It can also download additional payloads (T1105).

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

AsyncRAT

AsyncRAT was originally developed as an open-source remote administration tool by NYAN-x-CAT. Although it was originally written in C#, other developers have adapted it to Python and Java. Malware such as DcRAT, also known as DarkCrystal RAT, is a clone of AsyncRAT. Its popularity amongst adversaries is based on its versatile capabilities. AsyncRAT can record and view screens (T1113), run commands (T1059), upload and download files (T1105), and recover passwords (T1003) on victim devices. It has been observed to be injected into .NET framework binaries (T1055.002) and connected to dynamic DNS-based command-and-control servers (T1583.001).

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