December 2022

Updates released in December of 2022 to Cisco cloud-based machine learning global threat alerts:

- Additional Threat Detections, on page 1

Additional Threat Detections

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

- Private Loader
- PlugX

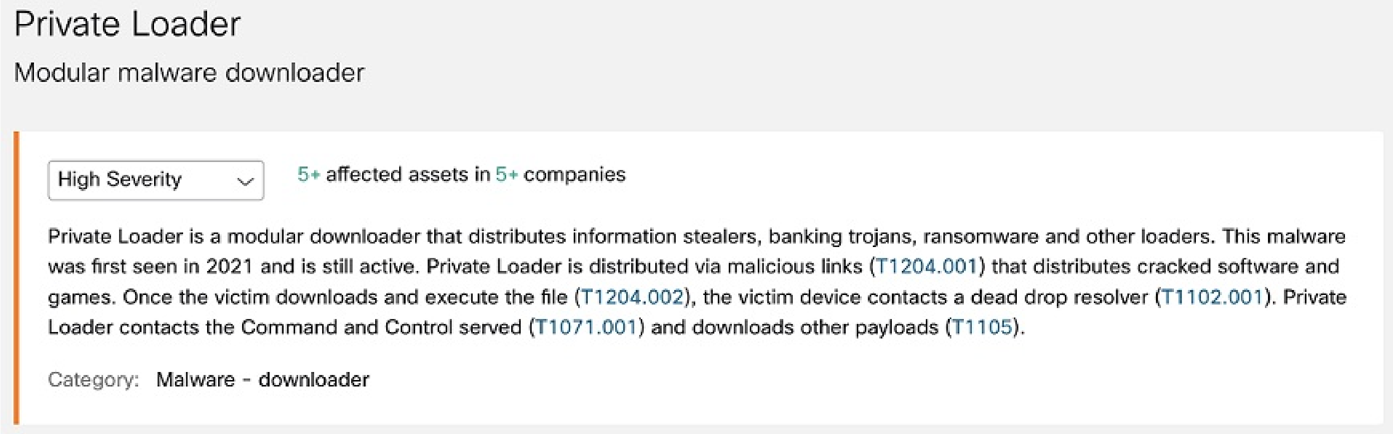
We’ve also updated indicators for our existing threat detections.

Private Loader

Private Loader is a modular downloader that distributes information stealers, banking Trojans, ransomware, and other loaders. This malware was first seen in 2021 and is still active. Private Loader is distributed using malicious links (T1204.001) that distribute cracked software and games. Once the victim downloads and executes the file (T1204.002), the victim's device contacts a dead drop resolver (T1102.001). Private Loader contacts the command-and-control server (T1071.001) and downloads other payloads (T1105).

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

Figure 1:



Private Loader

Modular malware downloader

5+ affected assets in 5+ companies

Private Loader is a modular downloader that distributes information stealers, banking trojans, ransomware and other loaders. This malware was first seen in 2021 and is still active. Private Loader is distributed via malicious links (T1204.001) that distributes cracked software and games. Once the victim downloads and execute the file (T1204.002), the victim device contacts a dead drop resolver (T1102.001). Private Loader contacts the Command and Control served (T1071.001) and downloads other payloads (T1105).

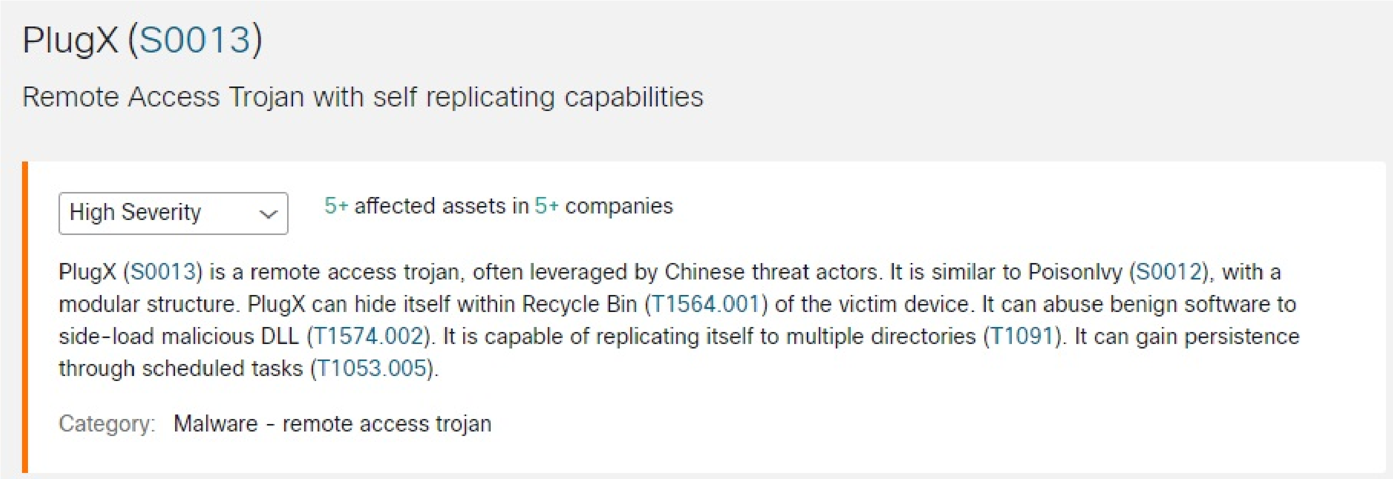
Category: Malware - downloader

PlugX

PlugX (S0013) is a remote access Trojan, often leveraged by Chinese threat actors. It is similar to PoisonIvy (S0012), with a modular structure. PlugX can hide itself within the recycle bin (T1564.001) of the victim's device. It can also abuse benign software to side-load malicious DLLs (T1574.002). It is capable of replicating itself to multiple directories (T1091) and can gain persistence through scheduled tasks (T1053.005).

To see if PlugX has been detected in your environment, click [PlugX Threat Detail]() to view its details in global threat alerts.

Figure 2:



PlugX (S0013)

Remote Access Trojan with self replicating capabilities

5+ affected assets in 5+ companies

PlugX (S0013) is a remote access trojan, often leveraged by Chinese threat actors. It is similar to Poisonlvy (S0012), with a modular structure. PlugX can hide itself within Recycle Bin (T1564.001) of the victim device. It can abuse benign software to side-load malicious DLL (T1574.002). It is capable of replicating itself to multiple directories (T1091). It can gain persistence through scheduled tasks (T1053.005).

Category: Malware - remote access trojan