April 2023

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

Additional Threat Detections

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

- Lumma
- PYbot

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

Lumma

The malicious information stealer Lumma has many capabilities, including getting information about the victim's computer (T1005), grabbing messages from messenger applications, and collecting browser history, cookies, and stored credentials (T1185). Lumma is distributed by phishing (T1566), exfiltrates data through command-and-control (T1071), and uses an automated exfiltration technique (T1020).

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

PYbot

PYbot is a DDoS bot (T1498) written in Python (T1059.006) and compiled using PyInstaller. This enables the malware to be executed (T1204.002) in hosts that do not have Python installed. It is distributed through fake and cracked software (T1189) that contain the .NET based downloader. Later, the downloader fetches a PYbot payload from the internet (T1105). PYbot is capable of targeting victims through Layer 4 and Layer 7 flooding attacks (T1498.001).

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