November 2022

Updates released in November 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:

- ChromeLoader
- CryptBot
- Mispadu
- Pterodo

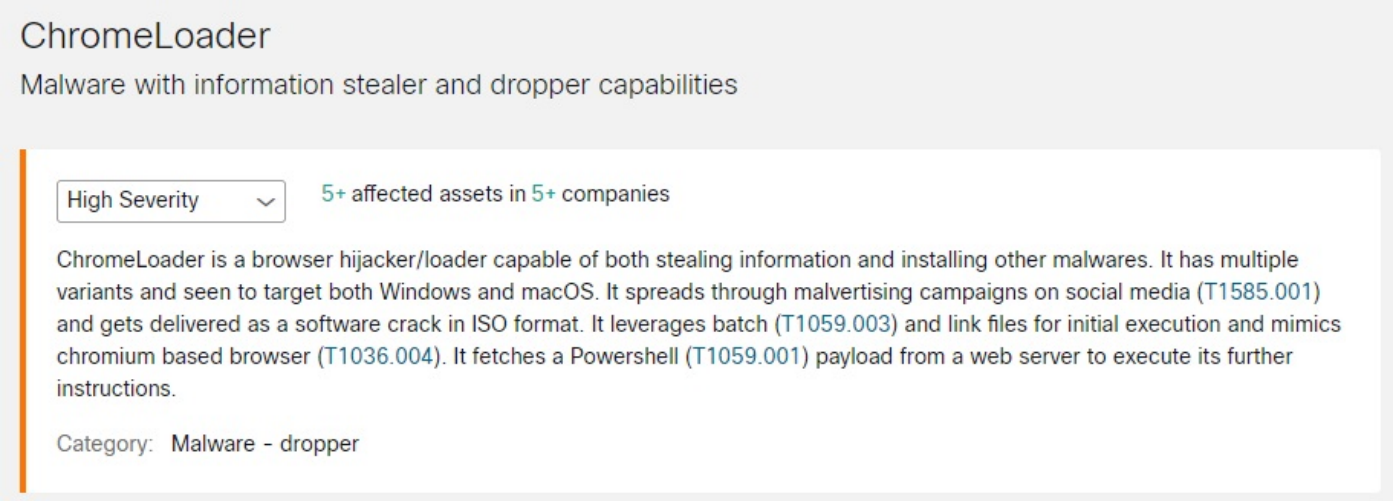
We've also updated indicators for our existing threat detections.

ChromeLoader

ChromeLoader is a browser hijacker/loader capable of both stealing information and installing other malware. It has multiple variants and targets both Windows and macOS. It spreads through malvertising campaigns on social media (T1585.001) and gets delivered as a software crack in ISO format. It leverages batch (T1059.003) and link files for initial execution and mimics Chromium-based browsers (T1036.004). It fetches a Powershell (T1059.001) payload from a web server to execute further instructions.

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

Figure 1:

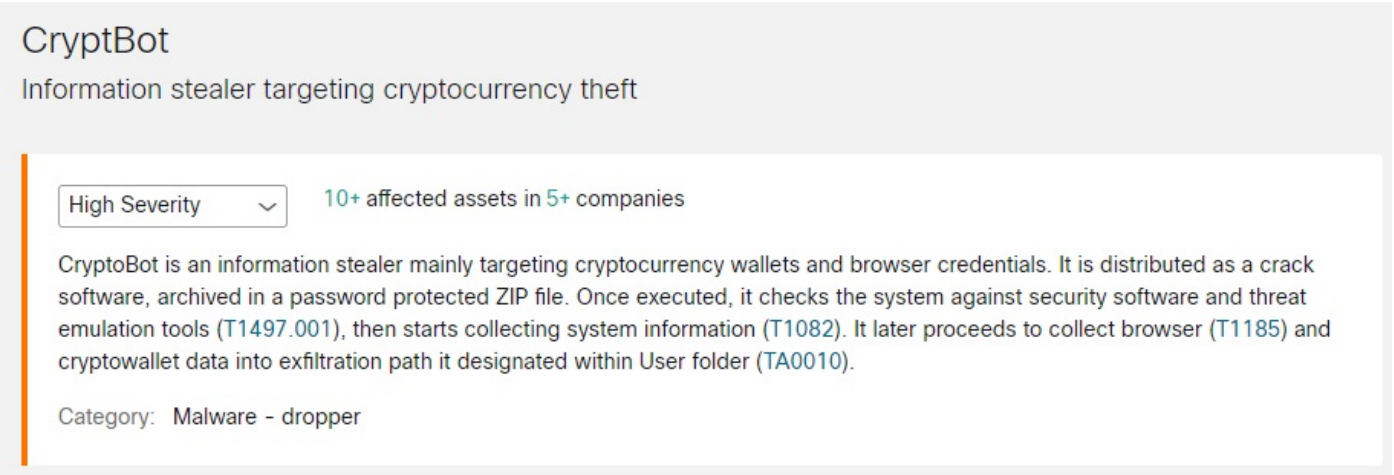


CryptBot

CryptBot is an information stealer that targets mainly cryptocurrency wallets and browser credentials. It is distributed as a crack software, archived in a password-protected ZIP file. Once executed, it checks the system against security software and threat-emulation tools (T1497.001), and then starts collecting system information (T1082). It later proceeds to collect browser (T1185) and crypto wallet data into an exfiltration path it designated within the User folder (TA0010).

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

Figure 2:



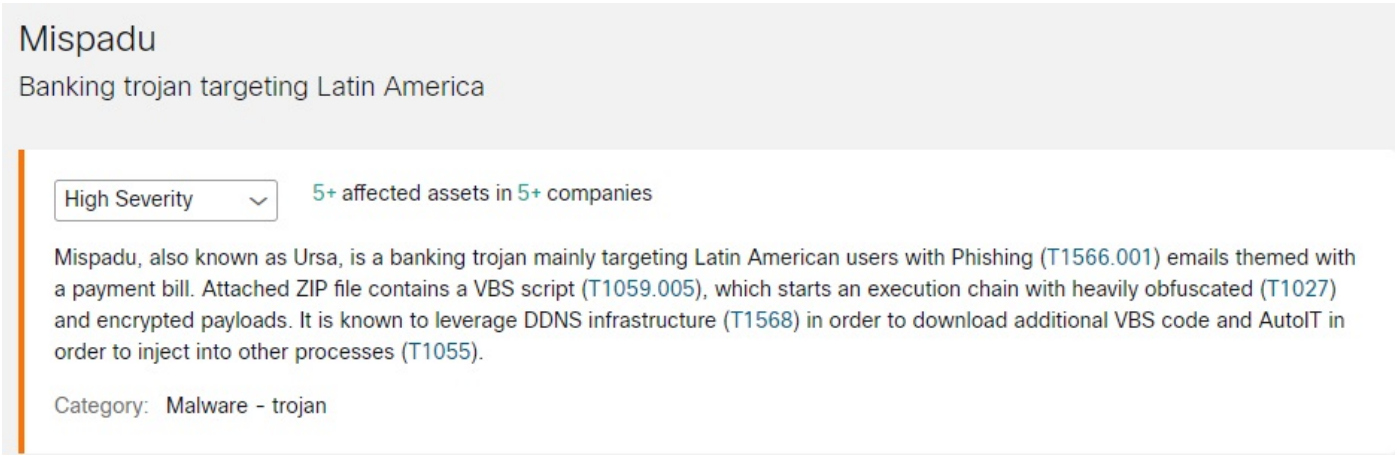
Mispadu

Mispadu, also known as Ursa, is a banking Trojan, mainly targeting Latin American users with phishing (T1566.001) emails themed with a payment bill. An attached ZIP file contains a VBS script (T1059.005) which starts an execution chain with heavily obfuscated (T1027) and encrypted payloads. It is known to

leverage DNS infrastructure (T1568) to download additional VBS code and AutoIT in order to inject into other processes (T1055).

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

Figure 3:



Pterodo

Pterodo, also known as Pteranodon (S0147), is a backdoor used by the Gamaredon group. It copies itself to the startup folder for persistency (T1547.001) and uses cmd.exe (T1059.003) and malicious VBS files for execution (T1059.005).

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

Figure 4: