June 2022

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

- Additional Threat Detections, on page 1

Additional Threat Detections

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

- AutoKMS HackTool
- Raspberry Robin
- UNC2447 Activity

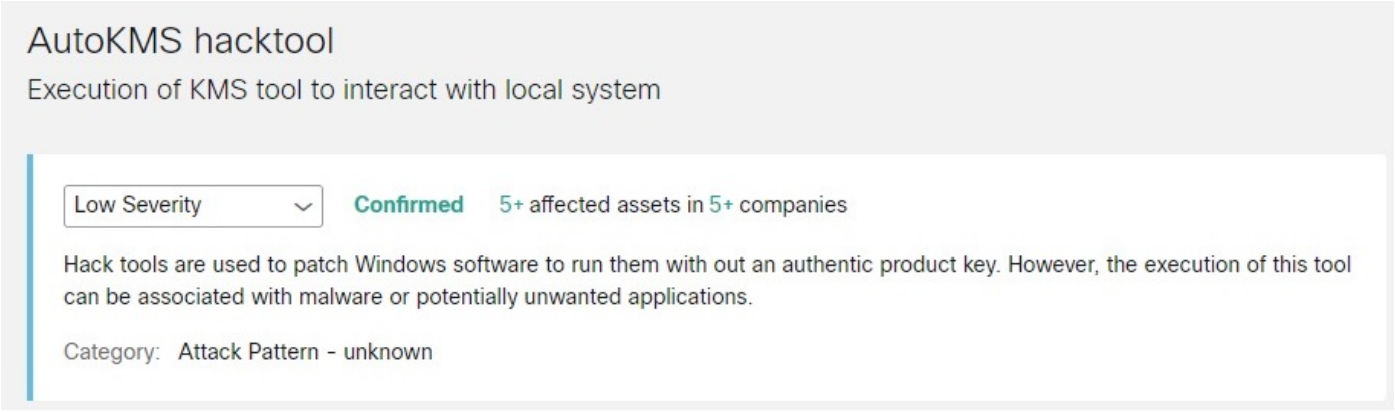
We've also updated indicators for our existing threat detections.

AutoKMS HackTool

Hack tools are used to patch Windows software and run them without an authentic product key. However, the execution of this tool can be associated with malware or potentially unwanted applications.

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

Figure 1:



Raspberry Robin

Raspberry Robin infects machines through a .lnk (T1204.002) file from an external drive, downloading actual payload through msiexec.exe (T1218.007), executing its code through rundll32.exe (T1218.011), and establishing its C2 through TOR connections (S0183). It's infrastructure is based on compromised QNAP devices.

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

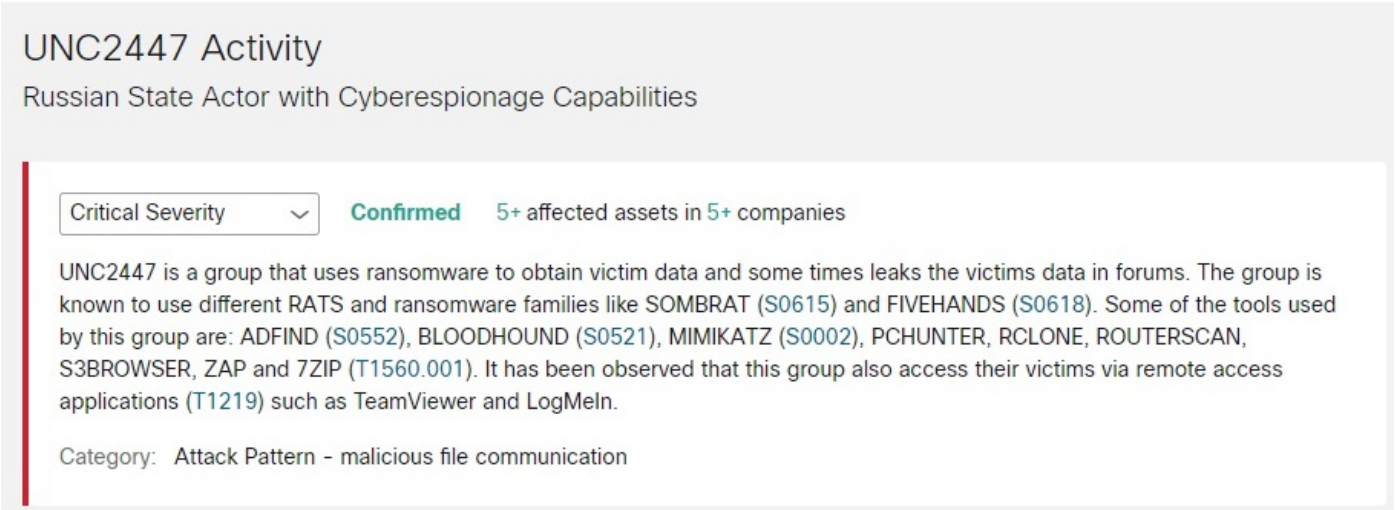
Figure 2:

UNC2447 Activity

UNC2447 is a group that uses ransomware to obtain data and may leak victim's data in forums. The group is known to use different RATS and ransomware families like SOMBRAT (S0615) and FIVEHANDS (S0618). Some of the tools used by this group include ADFIND (S0552), BLOODHOUND (S0521), MIMIKATZ (S0002), PCHUNTER, RCLONE, ROUTERSCAN, S3BROWSER, ZAP, and 7ZIP (T1560.001). This group also uses remote access applications (T1219) such as TeamViewer and LogMeIn.

To see if UNC2447 activity has been detected in your environment, click UNC2447 Activity Threat Detail to view its details in global threat alerts.

Figure 3:


UNC2447 Activity
Russian State Actor with Cyberespionage Capabilities
Critical Severity
Confirmed
5+ affected assets in 5+ companies
UNC2447 is a group that uses ransomware to obtain victim data and some times leaks the victims data in forums. The group is known to use different RATS and ransomware families like SOMBRAT (S0615) and FIVEHANDS (S0618). Some of the tools used by this group are: ADFIND (S0552), BLOODHOUND (S0521), MIMIKATZ (S0002), PCHUNTER, RCLONE, ROUTERSCAN, S3BROWSER, ZAP and 7ZIP (T1560.001). It has been observed that this group also access their victims via remote access applications (T1219) such as TeamViewer and LogMeIn.
Category: Attack Pattern - malicious file communication