July 2022

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

- SSO Migrated to CCI, on page 1
- Additional Threat Detections, on page 1

SSO Migrated to CCI

To improve customer experience, single sign-on has been migrated to the Cisco Customer Identity (CCI) portal. Continue to click **Cisco SSO** and enter your email and password on **id.cisco.com** to log in.

Additional Threat Detections

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

- Conti
- REvil

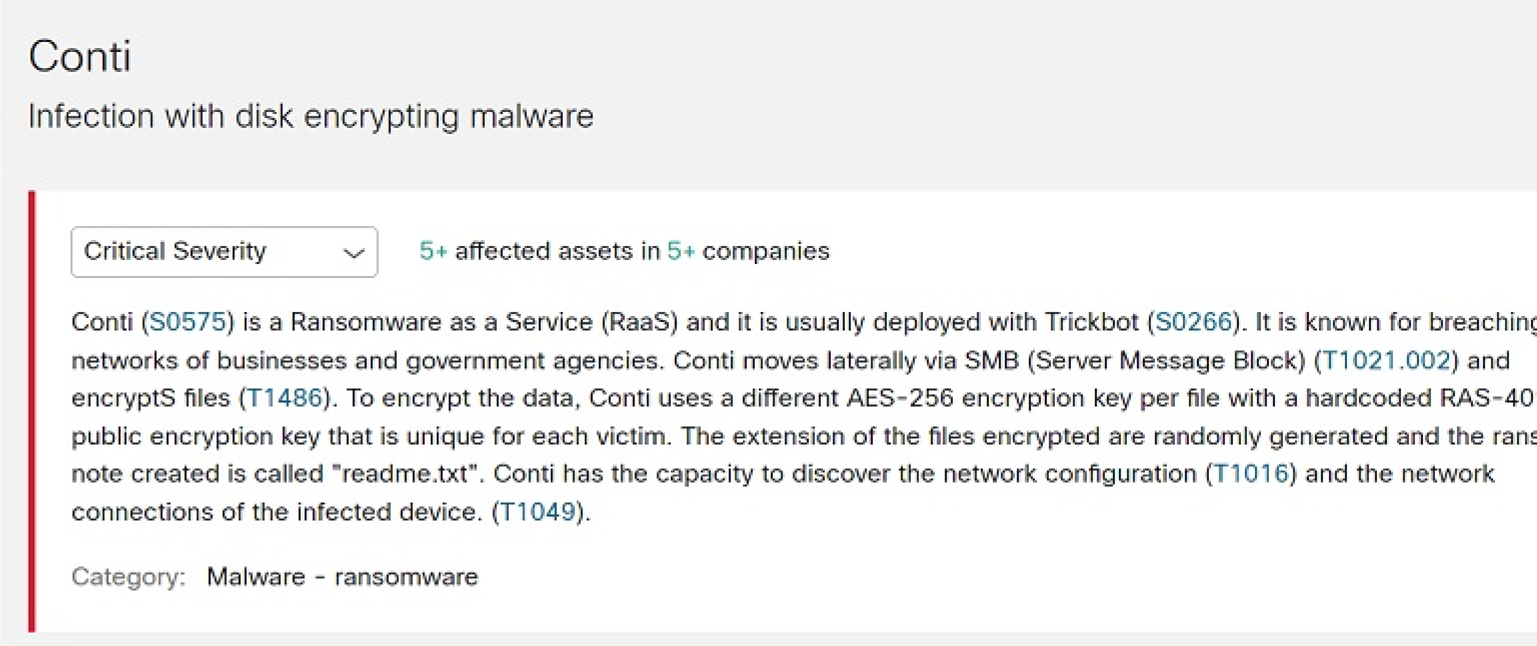
We've also updated indicators for our existing threat detections.

Conti

Conti (S0575) is a Ransomware as a Service (RaaS) usually deployed with Trickbot (S0266). It's known for breaching the networks of businesses and government agencies. Conti moves laterally using SMB (Server Message Block) (T1021.002) and encryptS files (T1486). To encrypt the data, Conti uses a different AES-256 encryption key per file with a hardcoded RAS-4096 public encryption key unique for each victim. The extension of the files encrypted are randomly generated, and the ransom note created is called "readme.txt." Conti has the capacity to discover the network configuration (T1016) and the network connections of the infected device (T1049).

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

Figure 1:



Conti

Infection with disk encrypting malware

Critical Severity

5+ affected assets in 5+ companies

Conti (S0575) is a Ransomware as a Service (RaaS) and it is usually deployed with Trickbot (S0266). It is known for breaching networks of businesses and government agencies. Conti moves laterally via SMB (Server Message Block) (T1021.002) and encryptS files (T1486). To encrypt the data, Conti uses a different AES-256 encryption key per file with a hardcoded RAS-40 public encryption key that is unique for each victim. The extension of the files encrypted are randomly generated and the rans note created is called "readme.txt". Conti has the capacity to discover the network configuration (T1016) and the network connections of the infected device. (T1049).

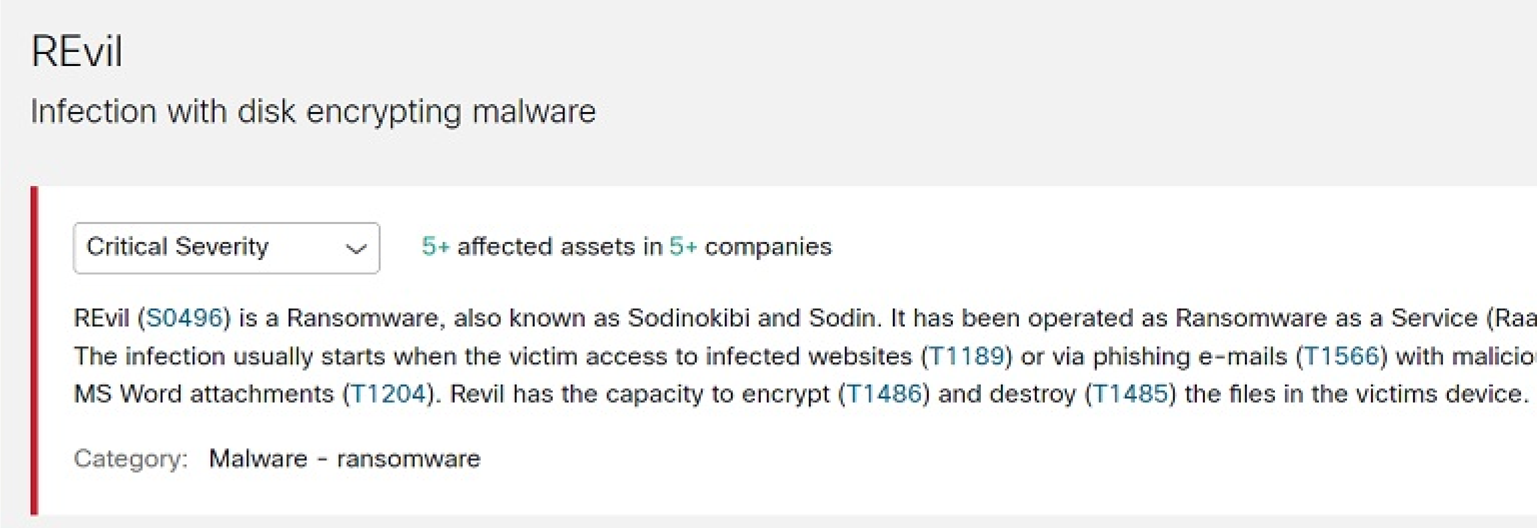
Category: Malware - ransomware

REvil

REvil (S0496) is a Ransomware as a Service (RaaS) also known as Sodinokibi and Sodin. The infection usually starts when the victim accesses infected websites (T1189) or phishing e-mails (T1566) with malicious MS Word attachments (T1204). REvil has the capacity to encrypt (T1486) and destroy (T1485) files on the victims device.

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

Figure 2:



REvil

Infection with disk encrypting malware

Critical Severity

5+ affected assets in 5+ companies

REvil (S0496) is a Ransomware, also known as Sodinokibi and Sodin. It has been operated as Ransomware as a Service (Raa The infection usually starts when the victim access to infected websites (T1189) or via phishing e-mails (T1566) with malicio MS Word attachments (T1204). Revil has the capacity to encrypt (T1486) and destroy (T1485) the files in the victims device.

Category: Malware - ransomware