CIRT.GY Guyana National Computer Incident Response Team

T2022_11 What you should know about Conti Ransomware (30th May 2022)

What is Conti Ransomware?

Conti Ransomware is a malicious program belonging to the Conti Cyber Threat group that steals information from organizations then demands a ransom to not release the information to the public. Conti acts on a ransomware-as-a-service (RaaS) model, with a vast network of affiliates and access brokers at its disposal to do its dirty work. The group also is known for targeting organizations for which attacks could have life-threatening consequences, such as hospitals, emergency number dispatch carriers, emergency medical services and law-enforcement agencies.

Technical Details

Conti is classified as a ransomware-as-a-service (RaaS) model ransomware variant; however, its structure differs from that of a traditional affiliate model. Conti developers are expected to pay ransomware deployers a wage rather than a percentage of the earnings used by affiliate cyber attackers and gain a share of the proceeds if the attack is successful.

Conti actors frequently acquire access to networks by:

- Spear phishing attacks involving customized emails containing harmful attachments or links;
  Malicious Word attachments frequently include embedded scripts that can be used to download or drop other malware, such as TrickBot and IcedID, and/or Cobalt Strike, to aid in lateral movement and later phases of the attack life cycle, with the goal of installing Conti ransomware.
- Remote Desktop Protocol (RDP) credentials that have been stolen or are insecure.
- Fake software promoted through search engine optimization.
- Other malware delivery networks (e.g., ZLoader); and external asset vulnerabilities.

Actors perform a getuid payload before employing a more aggressive payload in the execution phase to limit the risk of activating antivirus engines. Conti actors were seen scanning for and brute-forcing routers, webcams, and network-attached storage devices with web interfaces with Router Scan, a penetration testing tool. Actors also employ Kerberos assaults to try to obtain the admin hash to conduct brute force attacks.

Conti actors have been known to use legitimate remote monitoring and management software, as well as remote desktop software, as backdoors to stay on victim networks. To obtain users' hashes and clear-text credentials, the actors use tools already available on the victim network and, as needed, add additional tools such as Windows Sysinternals and Mimikatz, which enable the actors to escalate privileges within a domain and perform other post-exploitation and lateral movement tasks. Actors may also utilize TrickBot malware to do post-exploitation actions in specific instances.

A list of domains used by threat actors to deliver Conti ransomware can be found at the following URL:

https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

Mitigation

The following are some steps users and administrators can take to reduce the risk of infection by Conti ransomware:

Use multifactor authentication

- Require multifactor authentication to remotely access networks from external sources.

Implement network segmentation and filter traffic

- Implement and ensure robust network segmentation between networks and functions to reduce the spread of ransomware. Define a demilitarized zone that eliminates unregulated communication between networks.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files to prevent them from reaching end users.
- Implement a URL blocklist and/or allowlist to prevent users from accessing malicious websites.

Scan for vulnerabilities and keep software updated.

- Set antivirus/antimalware programs to conduct regular scans of network assets using up-to-date signatures.

- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner. Consider using a centralized patch management system.

Remove unnecessary applications and apply controls.

- Remove any application not deemed necessary for day-to-day operations. Conti threat actors leverage legitimate applications—such as remote monitoring and management software and remote desktop software applications—to aid in the malicious exploitation of an organization's enterprise.
- Investigate any unauthorized software, particularly remote desktop or remote monitoring and management software.
- Implement application allow listing, which only allows systems to execute programs known and permitted by the organization's security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.

Implement endpoint and detection response tools.

- Endpoint and detection response tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.

Limit access to resources over the network, especially by restricting RDP.

- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multifactor authentication.

Secure user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

Remediation

It is never advised to pay the attackers to decrypt your files, chances are they will take the ransom and vanish. If it is suspected that you have been infected by Conti ransomware the following steps are recommended for isolation and remediation:

STEP 1. Isolate the infected device(s):

i. If logged into any cloud storage, be sure to log out or disconnect from same.

ii. Disconnect the infected device from the network and the internet. You may even go as far as disabling all Network Interface Cards. You can follow the link below for instructions on disabling your Network Interface Card.

https://www.minitool.com/news/how-enable-disable-network-adapters-win10-003.html

iii. Disconnect all External Storage devices

STEP 2. Reimage the infected device(s). You can follow the link below for instructions on reimaging your device.

https://www.ubackup.com/articles/how-to-reimage-a-pc-4348.html

STEP 3. Restore a clean copy of files from backups. You can follow the link below for instructions on how to backup and restore your data.

https://www.pcmag.com/how-to/how-to-back-up-and-restore-an-image-file-of-windows-10

References

- Cyber Security & Infrastructure Security Agency. (22nd September 2021). Conti Ransomware. Retrieved from US-Cert. https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

- Federal Bureau of Investigation- Cyber Division. (20th May 2021). Conti Ransomware Attacks Impact Healthcare and First Responder Networks. Retrieved from FBI Flash. https://www.ic3.gov/Media/News/2021/210521.pdf

- Maskauskas, Tomas. (5th May 2022). How to eliminate Conti ransomware from the operating system. Retrieved from PC Risk. https://www.pcrisk.com/removal-guides/17011-conti-ransomware