SecurityRisk ADVISORS

CTI Threat Bulletin

Conti Ransomware

Executive Summary

On May 20, 2021, the Federal Bureau of Investigation (FBI) Cyber Division released a Flash Alert, #CP-000147-MW, regarding Conti ransomware attacks over the past year.

- More than 400 organizations worldwide have been victim to Conti ransomware attacks
- Over 290 of those attacks were located in the United States
- At least 16 attacks targeted healthcare and first responder networks
- Ransomware amounts vary and are believed to be tailored to each victim
- Ransom demands have been as high as 25 million dollars

Two common methods Conti threat actors use to gain unauthorized access to victim networks are phishing attacks which include links or malicious Word document attachments, as well as stolen Remote Desktop Protocol (RDP) credentials.

On May 12, 2021, The DFIR Report posted an in-depth write-up detailing a Conti intrusion. They assess with moderate confidence that Conti threat actors have been seen using IcedID, also known as BokBot, to gain initial access to victim networks before deploying Conti ransomware.

The transition of initial access to IcedID may have been influenced by the takedown of Emotet in January 2021. The takedown dismantled foundational components of Emotet's infrastructure. Threat actors using Emotet were temporarily shut down, forcing them to find new methods to deliver their payloads.

Bleeping computer reported that thirty-four ransomware gangs threaten to leak data on the dark web. The top five active operations are Conti (338 leaks), Sodinokibi/REvil (222 leaks), DoppelPaymer (200 leaks), Avaddon (123 leaks), and Pysa (103 leaks).

Organizations can be proactive and prepare themselves for defending against ransomware attacks by performing table-top exercises and reviewing ransomware incident response plans. Additional info can be found here: https://sra.io/blog/getting-specific-with-ransomware-preparedness/.

Conti Threat Actor Techniques

Conti threat actors have been seen implementing the following tactics:

- Delivered using Emotet, and more recently, IcedID
- Use of remote access tools that beacon over ports 80, 443, 8080, and 8443
- Identified persistence mechanisms communicating over port 53
- Large HTTPS transfers to cloud-based storage providers MegaNZ and pCloud servers
- Appearance of new accounts
- Use of Sysinternals tools that were not present before the attack
- Disabled endpoint detection software

Historical Conti reports aggregated on malpedia.

References

https://therecord.media/fbi-conti-ransomware-gang-attacked-more-than-400-orgs-including-911-centers/

https://thedfirreport.com/2021/05/12/conti-ransomware/

https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://www.bleepingcomputer.com/news/security/ransomware-gangs-have-leaked-the-stolen-data-of-2-100-companies-so-far/

https://therecord.media/irish-health-system-hit-by-ransomware-gang/

https://malpedia.caad.fkie.fraunhofer.de/details/win.conti

https://sra.io/table-top-excercises/

https://sra.io/cyberdefense/

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io