HC3: Analyst Note

May 25, 2021 TLP: White Report: 202105251512

Overview of Conti Ransomware

Executive Summary

Conti ransomware has recently been brought back into the spotlight due to its attack on Ireland's national health system - the Health Service Executive (HSE). Conti leverages many of the tools and techniques common among major ransomware operators such as encryption, double-extortion via the use of a leak site, ransomware-as-a-service partnerships and many of the frequently-successful infection vectors such as phishing and remote desktop protocol (RDP) compromise, among others. One of several recommendations given by Sophos security researchers to protect networks from Conti is to keep regular backups of important and current data on an offline storage device.

Report

On May 14, 2021, Ireland's HSE shut down "all national and local IT systems" in response to a Conti ransomware attack detected on their networks. The shutdown was an effort to contain the ransomware and "to protect [the systems] from encryption by attackers." Additionally, all HSE employees were instructed to turn off their computers and not turn on computers that were already powered down.

Conti ransomware is ransomware-as-a-service malware that targets victims primarily in North America and Western Europe. According to Sophos, the industries most frequently targeted by Conti are retail, manufacturing, construction, and the public sector but, any sector/industry can be targeted. Conti was found to have one of the biggest market shares of all ransomware operators in the first quarter of 2021 by Coveware. Conti is generally considered a successor to the Ryuk ransomware; however, one significant distinction between the two malwares is Conti ransomware uses the double-extortion technique.

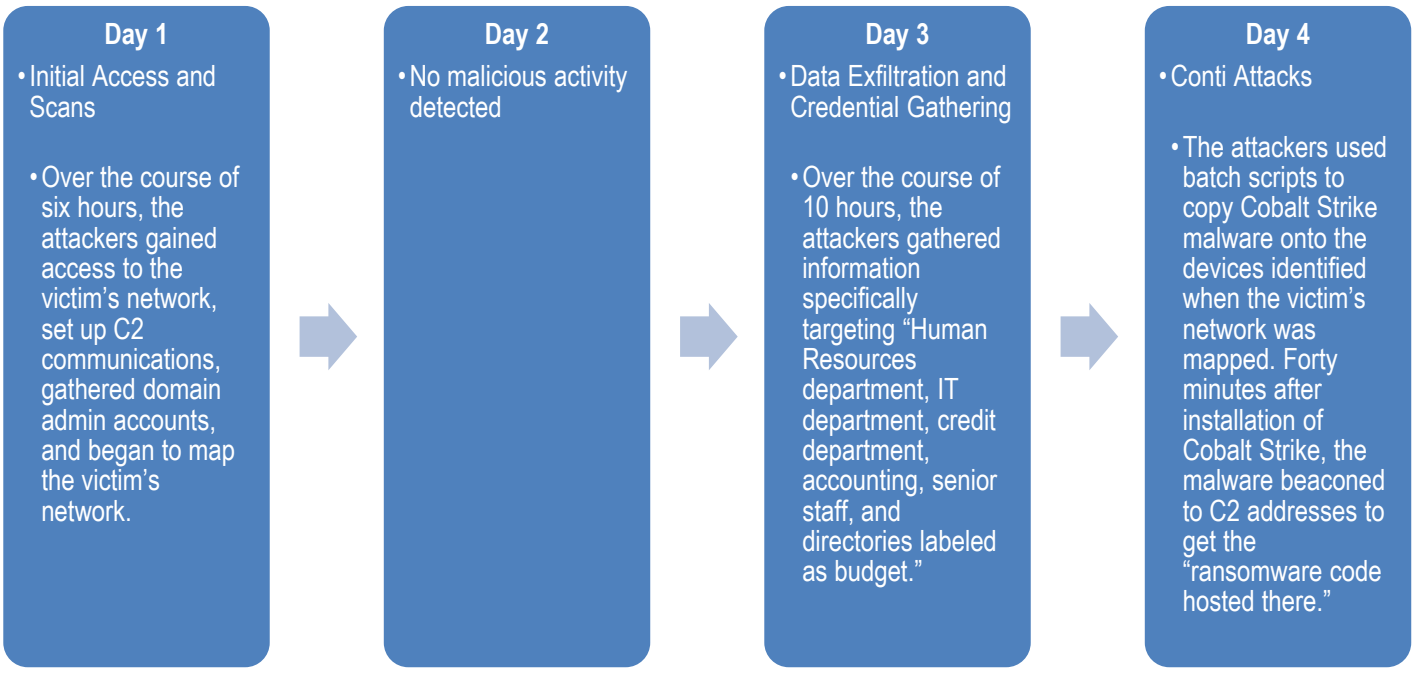
The double-extortion technique demands a ransom payment from the victim for the decryption key that will allow the victim to regain access to their encrypted files. If the ransom is not paid, the attackers will leak some or all of the victim's stolen information on the Conti leaks website—where anyone can download the information. In other instances, the attackers will sell the stolen data to other criminals for their use to further exploit the victim. Conti is known to use the cloud storage provider Mega to store victims' data.

Conti gains access to their victims' network through various means to include vulnerable firewalls, exposed remote desktop protocol (RDP) services, and phishing user credentials via spam emails. After initial access, Conti uses a two-stage process to infect the victim's network. The first stage uses a Cobalt Strike DLL "that allocates the memory space needed to decrypt and load meterpreter shellcode into system memory." After contacting the command-and-control (C2) the second stage occurs when "another Cobalt Strike shellcode loader that contains the reflective DLL loader instructions" is sent to the victim. Conti's manner of delivery makes it difficult for network defenders to identify it. As Sophos researchers explain, "[b]ecause the reflective loaders deliver the ransomware payload into memory, never writing the ransomware binary to the infected computer's file system. . ..[t]here is no artifact of the ransomware left behind for even a diligent malware analyst to discover and study."

After infection the ransomware can immediately begin to encrypt the victim's files (Conti uses a unique AES-256 encryption key per file, which is then encrypted with an RSA-4096 encryption key) while, "at the same time, sequentially attempting to connect to other computers on the same network subnet, in order to spread to nearby machines, using the SMB port." It can take attackers 15 minutes to move from server to server within a compromised network. Conti takes less than 20 minutes to setup communications with the C2 but even if those communications cannot be established, it can encrypt the victim's files without C2 instructions. According to

researchers at Sophos, because the encryption process can take hours "most targeted ransomware attacks are launched in the middle of the night, over a weekend or on a holiday, when fewer people are watching."

One attack observed by researchers at Sophos took place over approximately four days:



Tactics, techniques, and procedures associated with Conti ransomware identified by Sophos researchers include:

Tools used by Conti:

Tool Used by Conti Ransomware	Sophos Observed Conti Ransomware Use of Tool
Mimikatz	capture victim accounts of interest
Advanced Port Scanner	map victim network
Angry IP Scanner	map victim network
Remote administration tools like RDP	maintain access to victim network
AnyDesk	control victim machines
Cobalt Strike	control victim machines
RClone	exfiltrate victim data
Microsoft PsExec	distribute the Conti ransomware to victim devices

MITRE ATT&CK techniques associated with Conti:

MITRE ATT&CK Techniques	Sophos Observed Conti Ransomware Activity
T1190	Gains initial entry into victim environments by exploiting public facing applications.
T1212	Uses a compromised domain admin account to facilitate lateral movement.
T1016	Multiple batch scripts for system network configuration discovery.
T1018	Multiple batch scripts for system discovery.
T1046	Multiple batch scripts for network service scanning.
T1078.002	Following initial access, Conti searched to identify domain admin accounts.
T1021.002	Following initial access, Conti searched to identify network shares.
T1047	Deployment of Cobalt Strike beacons and loaders were performed using Windows Management Instrumentation commands.
T1567.002	Conti used RClone in order to exfiltrate data to file cloud storage service MEGA.
T1055.001	Cobalt Strike beacons loaded onto all target systems to perform a DLL reflective injection attack.
T1486	Where a DLL called to C2 addresses to get the Conti code, then load it and execute it directly in memory without writing the ransomware to disk before encrypting data for impact.

Vulnerabilities previously targeted by Conti:

Vulnerability Exploited by Conti Ransomware	Vulnerability Description
CVE-2018-13379	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.
CVE-2018-13374	An Improper Access Control in Fortinet FortiOS allows attacker to obtain the LDAP server login credentials configured in FortiGate via pointing a LDAP server connectivity test request to a rogue LDAP server instead of the configured one.

Patches, Mitigations, and Workarounds

Sophos security researchers recommend the following to protect networks from Conti ransomware:

- Monitor your network security 24/7 and be aware of early indicators an attacker is present to stop ransomware attacks before they launch
- Shut down internet-facing RDP to deny cybercriminals access to networks. If you need access to RDP, put it behind a VPN connection and enforce the use of Multi-Factor Authentication
- Educate employees on what to look out for in terms pf phishing and malicious spam and introduce robust security policies
- Keep regular backups of your most important and current data on an offline storage device. The standard recommendation for backups is to follow the 3-2-1 method: 3 copies of the data, using 2 different systems, 1 of which is offline
- Prevent attackers from getting access to and disabling your security: choose an advanced solution with a cloud-hosted management console with multi-factor authentication enabled and Role Based Administration to limit access rights
- Remember, there is no single silver bullet for protection, and a layered, defense-in-depth security model is essential – extend it to all endpoints and servers and ensure they can share security-related data
- Have an effective incident response plan in place and update it as needed.

References

Ní Aodha, Gráinne. "HSE confirms ransom has been sought over cyber attack but says it will not be paid," TheJournal.ie. May 14, 2021. https://www.thejournal.ie/hse-cyber-attack-5436981-May2021/.

Dwyer, Orla. "Explainer: What is a ransomware attack and why has the HSE been targeted?," TheJournal.ie. May 14, 2021. https://www.thejournal.ie/hse-it-system-ransomware-attack-explained-5437064-May2021/.

McDermott, Stephen. "HSE cyber attack: what services are affected and which ones are still working?," TheJournal.ie. May 14, 2021. https://www.thejournal.ie/hse-cyberattack-hospital-health-services-affected-5437328-May2021/.

Health Service Executive, "Who We Are, What We Do," Health Service Executive. May 14, 2021. https://www.hse.ie/eng/about/.

Brandt, Andrew and Ajjan, Anand. "Conti ransomware: Evasive by nature," Sophos. February 16, 2021. https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/.

Heller, Michael. "A Conti ransomware attack day-by-day," Sophos. February 16, 2021. https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/.

Mackenzie, Peter and Travers, Tilly. "What to expect when you've been hit with Conti ransomware," Sophos. February 16, 2021. https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/.

Lopp, Ashli. "Everything You Need to Know about the Conti Ransomware Gang," WAMS. March 4, 2021. https://wamsinc.com/2021/03/04/everything-you-need-to-know-about-the-conti-ransomware-gang/.

NIST. "CVE-2018-13379 Detail," National Vulnerability Database. November 19, 2020. https://nvd.nist.gov/vuln/detail/CVE-2018-13379.

NIST. "CVE-2018-13374 Detail," National Vulnerability Database. October 2, 2019. https://nvd.nist.gov/vuln/detail/CVE-2018-13374.

Olenick, Doug. "How Conti Ransomware Works," Bank Info Security. January 14, 2021. https://www.bankinfosecurity.com/how-conti-ransomware-works-a-15763.