Conti Ransomware Gang: An Overview

By Richard Hickman

Published: 2021-06-18 · Archived: 2026-04-05 14:08:12 UTC

Executive Summary

Conti ransomware stands out as one of the most ruthless of the dozens of ransomware gangs that we follow. The group has spent more than a year attacking organizations where IT outages can have life-threatening consequences: hospitals, 911 dispatch carriers, emergency medical services and law enforcement agencies. Ireland has yet to recover from an attack in mid-May that prompted the shutdown of the entire information technology network of the nation's healthcare system – prompting cancellation of appointments, the shutdown of X-ray systems and delays in COVID testing.

Conti also stands out as unreliable. We've seen the group stiff victims who pay ransoms, expecting to be able to recover their data.

The FBI has connected Conti to more than 400 cyberattacks against organizations worldwide, three-quarters of which are based in the U.S., with demands as high as $25 million. This makes Conti one of the greediest groups out there.

If you think you may have been impacted, please email unit42-investigations@paloaltonetworks.com or call (866) 4-UNIT42 to get in touch with the Unit 42 Incident Response team.

Conti Ransomware Overview

We've followed Conti for more than a year through our work helping organizations respond to ransomware attacks. It appears to be one of many private cybercrime groups that have set up their operations by leveraging the booming ransomware-as-a-service (RaaS) ecosystem. Such gangs obtain their foothold in the networks of their victims by purchasing access from other threat actors, who sell it as a commodity. They can also procure infrastructure, malware, communications tools and money laundering from other RaaS providers. Most of these actors use the same methods of access found in many ransomware attacks, such as phishing emails and exploiting unprotected internet-facing applications, the lack of multi-factor authentication (MFA), as well as the typical avenues used to preserve and enhance access once it's achieved, such as through the use of Cobalt Strike or PowerShell.

These approaches are not particularly clever or sophisticated, but often they are effective. Conti's methodology often follows the "double extortion" approach that many leading ransomware groups are presently using. When using double extortion, attackers will not only lock up a victim's files and demand ransom, but they will also steal files and threaten to publish them on a website or otherwise leak them if their initial ransom demand is not met.

But Conti's methods do have atypical elements.

Usually, the more successful ransomware operators put a lot of effort into establishing and maintaining some semblance of “integrity” as a way of facilitating ransom payments from victims. They want to establish stellar reputations for “customer service” and for delivering on what they promise – that if you pay a ransom, your files will be decrypted (and they will not appear on a leak website). Yet in our experience helping clients remediate attacks, Conti has not demonstrated any signs that it cares about its reputation with would-be victims.

In one recent case, Conti did not return a client’s files who had paid the ransom. This client got only a small fraction of the file restorations that were promised before the Conti ransomware representatives disappeared back into the dark web. In another case, our client needed an inventory of all files accessed, so that they could notify parties whose data was affected. Conti agreed to share that information if a payment was made, then changed their minds, saying, “We do not own that data anymore. It was deleted and there is no chance to restore it.” Like many ransomware gangs, Conti is constantly adapting to changes, including recent heightened scrutiny by law enforcement and policy makers following high-profile disruptive attacks on the Colonial pipeline and healthcare organizations. When Ireland's healthcare system refused to pay any ransom, Conti provided the agency with what it said was a free decryption key. But there was a twist: The group maintained that it would still make good on its "double extortion" threat to publish stolen data on its leak site.

Conclusion

Unfortunately, keeping Conti out of your network often isn’t simple. A primary means of infection appears to be through phishing scams, and attackers are constantly upping their game in this area. While phishing emails used to be pretty easy for almost anyone to spot, particularly after some awareness training, we are seeing increasingly sophisticated attacks in which the threat actors have done plenty of homework on their intended victims. Sometimes they’ll send a blitz of scam emails to employees throughout an organization, and it takes only one to open the attachment and release the malware into the network.

Ransomware attacks are getting easier to unleash, and the rewards to the attackers are still growing by leaps and bounds. Accordingly, it continues to be a growth industry that will attract multitudes of new practitioners, and it is likely that high-profile targets will continue to fall.

Palo Alto Networks detects and prevents Conti ransomware in the following ways:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
    - Indicators for Conti ransomware.
    - Anti-Ransomware Module to detect Conti ransomware encryption behaviors.
    - Local Analysis detection for Conti binaries.
- Next-Generation Firewalls: DNS Signatures detect the known Conti ransomware command and control (C2) domains, which are also categorized as malware in Advanced URL Filtering.
- AutoFocus: Tracking related activity using the Conti tag.
- Unit 42 Security Consulting: The Ransomware Readiness Assessment detects any hidden threats, tests for preparedness and provides remediation recommendations.

Additionally, Indicators of Compromise (IoCs) associated with Conti are available on GitHub, and have been published to the Unit 42 TAXII feed.

Courses of Action

Product / Service	Course of Action
Initial Access	
The below courses of action mitigate the following techniques: Exploit Public-Facing Application [T1190], Spearphishing Attachment [T1566.001]	
Threat Prevention†	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic
	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low and informational vulnerabilities
	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure a secure antivirus profile is applied to all relevant security policies
Wildfire†	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure that WildFire file size upload limits are maximized
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
Cortex XSOAR	Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint
	Deploy XSOAR Playbook - Endpoint Malware Investigation
	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
Execution	

The below courses of action mitigate the following techniques: Windows Command Shell [T1059.003], Native API [T1106]	
Cortex XDR	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection
Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques: Deobfuscate/Decode Files or Information [T1140], Obfuscated Files or Information [T1027], Dynamic-link Library Injection [T1055.001]	
Wildfire †	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure that WildFire file size upload limits are maximized
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
Cortex XDR	Enable Anti-Malware Protection
	Enable Anti-Exploit Protection
Discovery	
The below courses of action mitigate the following techniques: File and Directory Discovery [T1083], Network Share Discovery [T1135], Process Discovery [T1057], System Network Configuration Discovery [T1016], System Network Connections Discovery [T1049]	
Cortex XDR	XDR monitors for behavioral events via BIOCs along a causality chain to identify discovery behaviors*
Lateral Movement	

The below courses of action mitigate the following techniques: SMB/Windows Admin Shares [T1021.002], Taint Shared Content [T1080]	
Threat Prevention †	Ensure a secure antivirus profile is applied to all relevant security policies
Cortex XDR	Enable Anti-Malware Protection
	Enable Anti-Exploit Protection
Impact	
The below courses of action mitigate the following techniques: Data Encrypted for Impact [T1486], Inhibit System Recovery [T1490], Service Stop [T1489]	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.
	Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation
Cortex XDR	Enable Anti-Malware Protection
	Look for the following BIOCs alerts to detect activity*: Manipulation of Volume Shadow Copy configuration

Table 1. Courses of Action for Conti ransomware.

†These capabilities are part of the NGFW security subscriptions service.

* These analytic detectors will trigger automatically for Cortex XDR Pro customers.

Enlarged Image

Source: https://unit42.paloaltonetworks.com/conti-ransomware-gang/