Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:03:35 UTC

Tool: Conti

Names	Conti
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Carbon Black) Conti uses a large number of independent threads to perform encryption, allowing up to 32 simultaneous encryption efforts, resulting in faster encryption compared to many other families. Conti also utilizes command line options to allow for control over how it scans for data, suggesting that the malware may commonly be spread and directly controlled by an adversary. This control introduces the novel ability of skipping the encryption of local files and only targeting networked SMB shares, including those from IP addresses specifically provided by the adversary. This is a very rare ability that’s previously been seen with the Sodinokibi ransomware family. Another new technique, documented in very few ransomware families, is the use of the Windows Restart Manager to ensure that all files can be encrypted. Just as Windows will attempt to cleanly shut down open applications when the operating system is rebooted, the ransomware will utilize the same functionality to cleanly close the application that has a file locked. By doing so, the file is freed up for encryption.
Information	<https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/> <https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf> <https://www.zdnet.com/article/conti-ryuk-joins-the-ranks-of-ransomware-gangs-operating-data-leak-sites/> <https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware>

	<https://www.coveware.com/conti-ransomware> <https://thedfirreport.com/2021/05/12/conti-ransomware/> <https://www.bleepingcomputer.com/news/security/fbi-conti-ransomware-attacked-16-us-healthcare-first-responder-orgs/> <https://unit42.paloaltonetworks.com/conti-ransomware-gang/> <https://cycrafttechnology.medium.com/conti-ransomware-in-taiwan-45b44f1ab0d8> <https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/> <https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html> <https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/> <https://www.csoonline.com/article/3638056/conti-ransomware-explained-and-why-its-one-of-the-most-aggressive-criminal-groups.html> <https://www.bleepingcomputer.com/news/security/australian-govt-raises-alarm-over-conti-ransomware-attacks/> <https://www.cisa.gov/uscert/ncas/alerts/aa21-265a> <https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html> <https://www.malvuln.com/advisory/9eb9197cd58f4417a27621c4e1b25a71.txt> <https://www.trendmicro.com/en_us/research/22/f/conti-vs-lockbit-a-comparative-analysis-of-ransomware-groups.html> <https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0575/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.conti>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:conti>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=conti-ransomware> <https://usa.kaspersky.com/about/press-releases/2023_kaspersky-releases-tool-for-decrypting-conti-based-ransomware>

Last change to this tool card: 05 September 2023

Download this tool card in JSON format

All groups using tool Conti

Changed	Name	Country	Observed	
APT groups				
	Wizard Spider, Gold Blackburn		2014-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)
