


Mphasis SOC – Information Security News

Date & Time Issued: 02-JUL-2024, 23:00 IST

Title	Monti Ransomware	
Summary	<ul style="list-style-type: none"> A new group, Monti, appears to have used leaked Conti code, TTPs, and infrastructure approaches to launch its own ransomware campaign. The Monti group emerged with a round of ransomware attacks over the Independence Day weekend, and was able to successfully exploit the Log4Shell vulnerability to encrypt 20 BlackBerry user hosts and 20 servers, BlackBerry's Research and Intelligence Team reported. After further analysis, researchers discovered that the indicators of compromise (IoCs) for the new ransomware attacks were the same as in previous Conti ransomware attacks, with one twist: Monti incorporates the Acron 1 Remote Monitoring and Maintenance (RMM) Agent. Researchers at Trend Micro analyzing the new encryption tool from Monti found that it has "significant deviations from its other Linux-based predecessors. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> After gaining initial system access, Monti downloads and installs two remote monitoring and maintenance (RMM) agents, AnyDesk and Action1, to establish persistence and provide additional remote access. Then, the threat actors use Windows built-in Remote Desktop Protocol (RDP) to connect to other servers, access stored data files, and deploy their ransomware strain that encrypts multiple network hosts, including Veeam-based backups. The ransomware appends the encrypted files with the .PUUUK extension and drops a ransom note (encrypted using the ChaCha8 algorithm) that is almost identical to the one used by Conti. Monti uses temporary file transfer websites to fetch tools into the compromised network and exfiltrate data (e.g. MEGASync and PuTTY). In addition, the group was observed using GMER to remove endpoint security products and Mimikatz to dump credentials stored in memory. The group was observed targeting organizations in the legal and government sectors using a novel Linux variant that is substantially different from its predecessors (which were based on the leaked Conti source code). This ransomware variant features improved security evasion methods, can encrypt smaller files, uses the AES-256-CTR encryption method rather than the usual Salsa20 algorithm, and appends the encrypted files with the .MONTI extension. In June 2024, Monti claimed to have breached the Wayne Memorial Hospital in Honesdale, PA. The threat actors added an entry for the hospital on their dedicated Tor leak site, where they threatened to leak data that was allegedly stolen from the victim if a ransom was not paid. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	Domain	<ul style="list-style-type: none"> Dropmefiles[.]com.ua mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvj33rycmzczpid[.]onion monti5o7lvyrpyk26lqofnfvajtyqrwatlfazgm3zskt3xiktudwid[.]onion
	Hashes	<ul style="list-style-type: none"> 13ab5762ff5023163b1ca7c7749112b3673cd3db 158dcb26239a5db7a0eb67826178f1eaa0852d9d86e59afb86f04e88096a19bc 2bde2bb7b02950999daba6df694a587d80ad9207 5036747c069c42a5e12c38d94db67fad 6345ac3f61b9f4ce64e82d3896baf1fa 65f71c07e76c2452022158537107490677629d51 702099b63cb2384e11f088d6bc33afbd43a4c91848f393581242a6a17f1b30a0 78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d 9325f2301ad9e5fb4cf5673fa64446ae 9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732 b45fe91d2e2340939781d39daf606622e6d0b9ddacd8425cb8e49c56124c1d56 c924c22fadbe9fa6ae67df401aa03d13 df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54
	URLs	<ul style="list-style-type: none"> http[:]//mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvj33rycmzczpid.onion http[:]//mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvj33rycmzczpid.onion/

Recommendations	<ul style="list-style-type: none">• Update your admin credentials.• Check for malicious administrators.• Block all threat indicators at your respective controls.• Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.• Never trust or open links and attachments received from unknown sources/senders.• Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. <p>NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.</p>
References	<ul style="list-style-type: none">• https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger• https://www.bleepingcomputer.com/news/security/monti-ransomware-targets-vmware-esxi-servers-with-new-linux-locker/
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2024. All rights reserved by Mphasis.</p>	