Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:09:34 UTC

Tool: MedusaLocker

Names	MedusaLocker AKO Doxware AKO Ransomware MedusaReborn
Category	Malware
Type	Ransomware, Big Game Hunting, Reconnaissance
Description	(Cybereason) The MedusaLocker ransomware first emerged in September 2019, infecting and encrypting Windows machines around the world. There have been reports of MedusaLocker attacks across multiple industries, especially the healthcare industry which suffered a great deal of ransomware attacks during the COVID-19 pandemic. In order to maximize the chances of successful encryption of the files on the compromised machine, MedusaLocker restarts the machine in safe mode before execution. This method is used to avoid security tools that might not run when the computer starts in safe mode. MedusaLocker avoids encrypting executable files, most likely to avoid rendering the targeted system unusable for paying the ransom. To make it even more dangerous, MedusaLocker uses a combination of AES and RSA-2048, making the procedure of brute forcing the encryption practically impossible.
Information	<https://www.cybereason.com/blog/medusalocker-ransomware> <https://www.bleepingcomputer.com/news/security/medusalocker-ransomware-wants-its-share-of-your-money/> <https://www.binarydefense.com/threat_watch/new-ransomware-medusalocker/> <https://www.sentinelone.com/blog/how-medusalocker-ransomware-aggressively-targets-remote-hosts/> <https://www.carbonblack.com/blog/tau-threat-analysis-medusa-locker-ransomware/> <https://cyware.com/news/uncovering-the-abilities-of-medusalocker-ransomware-3fb92eca> <https://blog.talosintelligence.com/2020/04/medusalocker.html> <https://www.cisa.gov/uscert/ncas/alerts/aa22-181a>

	<https://blog.talosintelligence.com/threat-actor-believed-to-be-spreading-new-medusalocker-variant-since-2022/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.medusalocker>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:medusalocker>

Last change to this tool card: 24 October 2024

Download this tool card in JSON format

All groups using tool MedusaLocker

Changed	Name	Country	Observed	
APT groups				
	EmpireMonkey, CobaltGoblin	[Unknown]	2018-Mar 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2680cd2f-0911-418c-8414-d01b475df8f2