Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:31:53 UTC

Tool: Maze

Names	Maze ChaCha
Category	Malware
Type	Ransomware, Big Game Hunting
Description	Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated. Actors are known to exfiltrate the data from the network for further extortion. It spreads mainly using email spam and various exploit kits (Spelevo, Fallout). The code of Maze ransomware is highly complicated and obfuscated, which helps to evade security solutions using signature-based detections.
Information	<https://www.bleepingcomputer.com/news/security/fbi-warns-of-maze-ransomware-focusing-on-us-companies/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze> <https://www.kroll.com/en/insights/publications/cyber/latest-maze-ransomware-ttps> <https://www.tripwire.com/state-of-security/healthcare/maze-ransomware-targets-hospitals-labs-fighting-coronavirus/> <https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html> <https://unit42.paloaltonetworks.com/threat-brief-maze-ransomware-activities/> <https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/> <https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/> <https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/> <https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/>

	<https://nakedsecurity.sophos.com/2020/09/18/a-real-life-maze-ransomware-attack-if-at-first-you-dont-succeed/> <https://securelist.com/maze-ransomware/99137/> <https://www.webroot.com/blog/2021/01/13/maze-ransomware-is-dead-or-is-it/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0449/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.maze>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=maze-ransomware> <https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/> <https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Maze

Changed	Name	Country	Observed	
APT groups				
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6b19a42e-91bb-4261-a38f-06cd033e2781