Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:25:42 UTC

Tool: Egregor

Names	Egregor
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Malwarebytes) Egregor ransomware is a relatively new ransomware (first spotted in September 2020) that seems intent on making its way to the top right now. Egregor is considered a variant of Ransom.Sekhmet based on similarities in obfuscation, API-calls, and the ransom note. As we've reported in the past, affiliates that were using Maze ransomware started moving over to Egregor even before the Maze gang officially announced they were calling it quits.
Information	<https://blog.malwarebytes.com/ransomware/2020/12/threat-profile-egregor-ransomware-is-making-a-name-for-itself/> <https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware> <https://securelist.com/targeted-ransomware-encrypting-data/99255/> <https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis> <https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html> <https://www.ic3.gov/Media/News/2021/210108.pdf> <https://assets.sentinelone.com/labs/Egregor> <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-007.pdf> <https://www.csoonline.com/article/3602148/egregor-ransomware-group-explained-and-how-to-defend-against-it.html> <https://www.group-ib.com/whitepapers/egregor-ransomware.html> <https://securityintelligence.com/posts/egregor-ransomware-negotiations-uncovered/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0554/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.egregor>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:egregor>

Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=egregor-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 Egregor

Changed	Name	Country	Observed	
APT groups				
	Mallard Spider	[Unknown]	2008-Dec 2020	
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4e65ee26-1493-4c96-a38d-441224e8f833