Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:51:19 UTC

Tool: Apostle

Names	Apostle
Category	Malware
Type	Wiper, Ransomware
Description	(SentinelLabs) One of the wipers used in the attack, dubbed ‘Apostle’, was later turned into a fully functional ransomware, replacing its wiper functionalities. The message inside it suggests it was used to target a critical, nation-owned facility in the United Arab Emirates. The similarity to its wiper version, as well as the nature of the target in the context of regional disputes, leads us to believe that the operators behind it are utilizing ransomware for its disruptive capabilities.
Information	<https://assets.sentinelone.com/sentinellabs/evol-agrius> <https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/> <https://www.sentinelone.com/wp-content/uploads/2021/05/SentinelLabs_From-Wiper-to-Ransomware-The-Evolution-of-Agrius.pdf> <https://cyberpunkleigh.wordpress.com/2021/05/27/apostle-ransomware-analysis/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1133>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.apostle>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Apostle

Changed	Name	Country	Observed	
APT groups				
	Agrius		2020-May 2023	

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