Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:47:47 UTC

Tool: IPsec Helper

Names	IPsec Helper
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(SentinelLabs) The backdoor malware requires installation as a service. It is registered as 'IPsec Helper'. Upon execution, it sleeps for a random number of seconds (iterating 200 times over sleeps between 1 to 3 seconds). It then checks for an internet connection by connecting to a predefined list of Microsoft servers.
Information	<https://assets.sentinelone.com/sentinellabs/evol-agrius>
MITRE ATT&CK	<https://attack.mitre.org/software/S1132>

Last change to this tool card: 29 December 2024

Download this tool card in JSON format

All groups using tool IPsec Helper

Changed	Name	Country	Observed	
APT groups				
	Agrius		2020-May 2023	

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