CSPY Downloader - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:58:49 UTC

Tool: CSPY Downloader

Names	CSPY Downloader
Category	Malware
Type	Downloader
Description	(Cybereason) Upon analysis, the Nocturnus determined that winload.exe is a new type of a downloader, dubbed “CSPY” by Cybereason, that is packed with robust evasion techniques meant to ensure that the “coast is clear” and that the malware does not run in a context of a virtual machine or analysis tools before it continues to download secondary payloads.
Information	<https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite>
MITRE ATT&CK	<https://attack.mitre.org/software/S0527/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool CSPY Downloader

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

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