Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:11:06 UTC

Tool: CreepyDrive

Names	CreepyDrive
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(ESET) CreepyDrive is a PowerShell backdoor that reads and executes commands from a text file stored on OneDrive or Dropbox. It can upload or download files from attacker-controlled accounts in these cloud services, and execute supplied PowerShell code.
Information	<https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1023/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool CreepyDrive

Changed	Name	Country	Observed	
APT groups				
	Polonium		2022-Sep 2022	

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