Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:49:21 UTC

Tool: PowerTrick

Names	PowerTrick
Category	Malware
Type	Backdoor
Description	(SentinelLabs) SentinelLabs research into this PowerShell-based backdoor called “PowerTrick” traces back to the initial infection, we assess with high confidence at least some of the initial PowerTrick infections are being kicked off as a PowerShell task through normal TrickBot infections utilizing a repurposed backconnect module that can accept commands to execute called “NewBCtest”. After the initial stager for the “PowerTrick backdoor” is kicked off, then the actor issues the first command which is to download a larger backdoor. This process is similar to what you see in Powershell Empire with its stager component. PowerTrick is designed to execute commands and return the results in Base64 format, the system uses a generated UUID based on computer information as a “botID.”
Information	<https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/> <https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/>

Last change to this tool card: 24 June 2020

Download this tool card in JSON format

All groups using tool PowerTrick

Changed	Name	Country	Observed	
APT groups				
	Wizard Spider, Gold Blackburn		2014-May 2025	

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