PowerShell RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:08:35 UTC

Tool: PowerShell RAT

Names	PowerShell RAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Group-IB) PowerShell RAT functions: • Update configuration • Collect and send information about the infected PC and running processes with ability to ruminate them • Collect and send files to a remote server • Change properties and attributes of files • Supports operations with Registry • Supports operations for working with ZIP-archives • Download and run PowerShell scripts • Uploading files to an infected PC • Execute commands from a remote server in the command line interpreter
Information	<https://www.aptld.org/meeting/20190910/7B%20Lazarus%20attacks%20on%20banks%20in%20the%20APAC%20RegGroup%20IB.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool PowerShell RAT

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	Operation Silent Skimmer	[Unknown]	2022	

2 groups listed (2 APT, 0 other, 0 unknown)