Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:46:27 UTC

Tool: PowerBrace

Names	PowerBrace
Category	Malware
Type	Backdoor, Exfiltration
Description	(IBM) PowerBrace is a PowerShell backdoor that supports multiple commands such as command execution, uploading/downloading files, etc. Most of the function names and variable names in PowerBrace have been replaced with MD5 hashes to make the analysis more difficult. Furthermore, many commands are Based64 encoded. It generates a random string as a session key, which is used in communication.
Information	<https://exchange.xforce.ibmcloud.com/malware-analysis/guid:7ce62d3322cecbb29e55b27cd393b729>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerbrace>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PowerBrace>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool PowerBrace

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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