Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:03:06 UTC

Tool: PowerPepper

Names	PowerPepper
Category	Malware
Type	Backdoor
Description	(Kaspersky) PowerPepper is a Windows in-memory PowerShell backdoor that can execute remotely sent shell commands. In strict accordance with DeathStalker's traditions, the implant will try to evade detection or sandboxes execution with various tricks such as detecting mouse movements, filtering the client's MAC addresses, and adapting its execution flow depending on detected antivirus products.
Information	<https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerpepper>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool PowerPepper

Changed	Name	Country	Observed	
APT groups				
	Deceptikons, DeathStalker	[Unknown]	2012-Jun 2020	

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