Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:57:07 UTC

Tool: PowerShower

Names	PowerShower
Category	Malware
Type	Reconnaissance, Downloader
Description	(Palo Alto) POWERSHOWER acts as an initial reconnaissance foothold and is almost certainly used to download and execute a secondary payload with a more complete set of features. By only using this simple backdoor to establish a foothold, the attacker can hold back their most sophisticated and complex malware for later stages, making them less likely to be detected. In a nutshell, POWERSHOWER allows the attacker to: • Fingerprint the machine, and upload this information to the initial C&C. • Clean up a significant amount of forensic evidence from the dropper process, as we detail below. • Run a secondary payload, if the attacker decides the target machine is sufficiently interesting (based on analysis of the system data sent from the first beacon)
Information	<https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0441/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershower>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PowerShower

Changed	Name	Country	Observed

APT groups

	Inception Framework, Cloud Atlas		2012-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8f922508-3fd3-4018-997b-a7a9075af23e