Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:46:36 UTC

Tool: POWERTON

Names	POWERTON
Category	Malware
Type	Backdoor
Description	(FireEye) POWERTON is a backdoor written in PowerShell; FireEye has not yet identified any publicly available toolset with a similar code base, indicating that it is likely custom-built. POWERTON is designed to support multiple persistence mechanisms, including WMI and auto-run registry key. Communications with the C2 are over TCP/HTTP(S) and leverage AES encryption for communication traffic to and from the C2. POWERTON typically gets deployed as a later stage backdoor and is obfuscated several layers.
Information	<https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0371/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerton>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:powerton>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool POWERTON

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	

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