Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:42:53 UTC

Tool: PowerPunch

Names	PowerPunch
Category	Malware
Type	Downloader, Loader
Description	(Microsoft) PowerPunch is executed from within PowerShell as a one-line command, encoded using Base64. These binaries also exhibit features that rely on data from the compromised host to inform encryption of the next stage. PowerPunch also provides an excellent example of this. The VolumeSerialNumber of the host serves as the basis for a multibyte XOR key. The key is applied to an executable payload downloaded directly from adversary infrastructure, allowing for an encryption key unique to the target host. Ultimately, a next-stage executable is remotely retrieved and dropped to disk prior to execution.
Information	<https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0685/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PowerPunch

Changed	Name	Country	Observed	
APT groups				
	Gamaredon Group		2013-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2653faee-fcff-4add-8934-b0ae27606c61