Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:18:59 UTC

Tool: PoshC2

Names	PoshC2
Category	Tools
Type	Backdoor
Description	PoshC2 is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in PowerShell. Although PoshC2 is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS.
Information	<https://github.com/nettitude/PoshC2/> <https://www.prodefence.org/poshc2-red-teaming-post-exploitation-tool/> <https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0378/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.poshc2>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:poshc2>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool PoshC2

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

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