Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:59:25 UTC

Tool: POSHSPY

Names	POSHSPY
Category	Malware
Type	Backdoor
Description	(FireEye) POSHSPY makes the most of using built-in Windows features – so-called "Living off the Land" – to make an especially stealthy backdoor. POSHSPY's use of WMI to both store and persist the backdoor code makes it nearly invisible to anyone not familiar with the intricacies of WMI. Its use of a PowerShell payload means that only legitimate system processes are utilized and that the malicious code execution can only be identified through enhanced logging or in memory. The backdoor's infrequent beaconing, traffic obfuscation, extensive encryption and use of geographically local, legitimate websites for command and control (C2) make identification of its network traffic difficult. Every aspect of POSHSPY is efficient and covert. Mandiant initially identified an early variant of the POSHSPY backdoor deployed as PowerShell scripts during an incident response engagement in 2015. Later in that same engagement, the attacker updated the deployment of the backdoor to use WMI for storage and persistence. Mandiant has since identified POSHSPY in several other environments compromised by APT29 over the past two years.
Information	<https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html> <https://github.com/matthewdunwoody/POSHSPY>
MITRE ATT&CK	<https://attack.mitre.org/software/S0150/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.poshspy>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool POSHSPY

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=28eff50b-ad42-43e6-b5ee-2bbabd58d9b6