Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:05:54 UTC

Tool: PowerSploit

Names	PowerSploit
Category	Tools
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	PowerSploit is an open source, offensive security framework comprised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration.
Information	<https://github.com/PowerShellMafia/PowerSploit>
MITRE ATT&CK	<https://attack.mitre.org/software/S0194/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:powersploit>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool PowerSploit

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	CostaRicto	[Unknown]	2017	
	Dark Pink	[Unknown]	2022-Feb 2023	
	FIN13	[Unknown]	2016	

	Indrik Spider		2007-Oct 2024	●
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	●
	Patchwork, Dropping Elephant		2013-Jun 2025	
	PowerPool	[Unknown]	2018	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	Wizard Spider, Gold Blackburn		2014-May 2025	●

11 groups listed (11 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7bd2fb19-68b5-4e20-984e-4f807fe45636