Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:38:55 UTC

Tool: EmpireProject

Names	EmpireProject Empire EmPyre PowerShell Empire
Category	Tools
Type	Backdoor
Description	Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. PowerShell Empire premiered at BSidesLV in 2015 and Python EmPyre premeiered at HackMiami 2016.
Information	<https://github.com/EmpireProject>
MITRE ATT&CK	<https://attack.mitre.org/software/S0363/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool EmpireProject

Changed	Name	Country	Observed	
APT groups				
	APT 19, Deep Panda, C0d0so0		2013-Mar 2022	

	APT 33, Elfin, Magnallium		2013-Apr 2024	
	CopyKittens, Slayer Kitten		2013-Jan 2017	
	FIN10	[Unknown]	2016	
	Indrik Spider		2007-Oct 2024	
	LazyScripter	[Unknown]	2018	
	LockBit Gang	[Unknown]	2019-May 2025	
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	
	Turla, Waterbug, Venomous Bear		1996-2024	
	WIRTE Group	[Middle East]	2018-Feb 2024	

10 groups listed (10 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cc8ad066-31e0-47a0-b5b3-20b9950ed7c0