POSHSPY, Software S0150 | MITRE ATT&CK®

Archived: 2026-04-02 12:43:49 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	POSHSPY uses PowerShell to execute various commands, one to execute its payload.[1]
Enterprise	T1030		Data Transfer Size Limits	POSHSPY uploads data in 2048-byte chunks.[1]
Enterprise	T1568	.002	Dynamic Resolution: Domain Generation Algorithms	POSHSPY uses a DGA to derive command and control URLs from a word list.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	POSHSPY encrypts C2 traffic with AES and RSA.[1]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	POSHSPY uses a WMI event subscription to establish persistence.[1]
Enterprise	T1070	.006	Indicator Removal: Timestomp	POSHSPY modifies timestamps of all downloaded executables to match a randomly selected file created prior to 2013.[1]
Enterprise	T1105		Ingress Tool Transfer	POSHSPY downloads and executes additional PowerShell code and Windows binaries.[1]

Domain	ID	Name	Use
Enterprise	T1027	Obfuscated Files or Information	POSHSPY appends a file signature header (randomly selected from six file types) to encrypted data prior to upload or download.[1]

Source: https://attack.mitre.org/software/S0150