PowerShower, Software S0441 | MITRE ATT&CK®

Archived: 2026-04-05 14:24:53 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	PowerShower has sent HTTP GET and POST requests to C2 servers to send information and receive instructions.[1]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	PowerShower has used 7Zip to compress .txt, .pdf, .xls or .doc files prior to exfiltration.[2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	PowerShower sets up persistence with a Registry run key.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	PowerShower is a backdoor written in PowerShell.[1]
		.005	Command and Scripting Interpreter: Visual Basic	PowerShower has the ability to save and execute VBScript.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	PowerShower has the ability to encode C2 communications with base64 encoding.[1][2]
Enterprise	T1041		Exfiltration Over C2 Channel	PowerShower has used a PowerShell document stealer module to pack and exfiltrate .txt, .pdf, .xls or .doc files smaller than 5MB that were modified during the past two days.[2]

Domain	ID		Name	Use
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	PowerShower has added a registry key so future powershell.exe instances are spawned with coordinates for a window position off-screen by default.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	PowerShower has the ability to remove all files created during the dropper process.[1]
Enterprise	T1112		Modify Registry	PowerShower has added a registry key so future powershell.exe instances are spawned off-screen by default, and has removed all registry entries that are left behind during the dropper process.[1]
Enterprise	T1057		Process Discovery	PowerShower has the ability to deploy a reconnaissance module to retrieve a list of the active processes.[2]
Enterprise	T1082		System Information Discovery	PowerShower has collected system information on the infected host.[1]
Enterprise	T1016		System Network Configuration Discovery	PowerShower has the ability to identify the current Windows domain of the infected host.[2]
Enterprise	T1033		System Owner/User Discovery	PowerShower has the ability to identify the current user on the infected host.[2]