CopyKittens, Group G0052 | MITRE ATT&CK®

Archived: 2026-04-05 16:04:20 UTC

Domain	ID		Name	Use
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	CopyKittens uses ZPP, a .NET console program, to compress files with ZIP.[2]
		.003	Archive Collected Data: Archive via Custom Method	CopyKittens encrypts data with a substitute cipher prior to exfiltration.[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	CopyKittens has used PowerShell Empire.[2]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	CopyKittens has used `-w hidden` and `-windowstyle hidden` to conceal PowerShell windows. [2]
Enterprise	T1588	.002	Obtain Capabilities: Tool	CopyKittens has used Metasploit, Empire, and AirVPN for post-exploitation activities.[4][5]
Enterprise	T1090		Proxy	CopyKittens has used the AirVPN service for operational activity.[5]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	CopyKittens digitally signed an executable with a stolen certificate from legitimate company AI Squared.[2]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	CopyKittens uses rundll32 to load various tools on victims, including a lateral movement tool named Vminst, Cobalt Strike, and shellcode.[2]

Source: https://attack.mitre.org/groups/G0052/