

APT18, TG-0416, Dynamite Panda, Threat Group-0416, Group G0026

Archived: 2026-04-05 14:10:20 UTC

Domain	ID	Name	Use
Enterprise	T1071	Application Layer Protocol: Web Protocols	APT18 uses HTTP for C2 communications. ^[4]
		Application Layer Protocol: DNS	APT18 uses DNS for C2 communications. ^[4]
Enterprise	T1547	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT18 establishes persistence via the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key. ^{[3][4]}
Enterprise	T1059	Command and Scripting Interpreter: Windows Command Shell	APT18 uses cmd.exe to execute commands on the victim's machine. ^{[4][3]}
Enterprise	T1133	External Remote Services	APT18 actors leverage legitimate credentials to log into external remote services. ^[5]
Enterprise	T1083	File and Directory Discovery	APT18 can list files information for specific directories. ^[4]
Enterprise	T1070	Indicator Removal: File Deletion	APT18 actors deleted tools and batch files from victim systems. ^[1]
Enterprise	T1105	Ingress Tool Transfer	APT18 can upload a file to the victim's machine. ^[4]

Domain	ID	Name	Use
Enterprise	T1027	.013 Obfuscated Files or Information: Encrypted/Encoded File	APT18 obfuscates strings in the payload. ^[4]
Enterprise	T1053	.002 Scheduled Task/Job: At	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network. ^[1]
Enterprise	T1082	System Information Discovery	APT18 can collect system information from the victim's machine. ^[4]
Enterprise	T1078	Valid Accounts	APT18 actors leverage legitimate credentials to log into external remote services. ^[5]

Source: <https://attack.mitre.org/groups/G0026/>