APT18

attack.mitre.org/groups/G0026

APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. [1]

ID: G0026

ⓘ

Associated Groups: TG-0416, Dynamite Panda, Threat Group-0416

Version: 2.1

Created: 31 May 2017

Last Modified: 30 March 2020

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
TG-0416	[2][3]
Dynamite Panda	[2][3]
Threat Group-0416	[2]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT18 uses HTTP for C2 communications.[4]

Domain	ID	Name	Use	
		.004	Application Layer Protocol: DNS	APT18 uses DNS for C2 communications.[4]
Enterprise	T1547	.001	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	.003	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	.004	Indicator Removal on Host: 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]
Enterprise	T1027		Obfuscated Files or Information	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]

Domain	ID	Name	Use
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]

Software

ID	Name	References	Techniques
S0106	cmd	[1]	Command and Scripting Interpreter: Windows Command Shell, File and Directory Discovery, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Lateral Tool Transfer, System Information Discovery
S0032	gh0st RAT	[5]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter, Create or Modify System Process: Windows Service, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, Dynamic Resolution: Fast Flux DNS, Encrypted Channel: Symmetric Cryptography, Encrypted Channel, Hijack Execution Flow: DLL Side-Loading, Indicator Removal on Host: File Deletion, Indicator Removal on Host: Clear Windows Event Logs, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Native API, Non-Application Layer Protocol, Process Discovery, Process Injection, Query Registry, Screen Capture, Shared Modules, System Binary Proxy Execution: Rundll32, System Information Discovery, System Services: Service Execution
S0071	hcdLoader	[1][2]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service
S0070	HTTPBrowser	[5]	Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, File and Directory Discovery, Hijack Execution Flow: DLL Search Order Hijacking, Hijack Execution Flow: DLL Side-Loading, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information

ID	Name	References	Techniques
S0124	Pisloader	[6]	Application Layer Protocol: DNS, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, File and Directory Discovery, Ingress Tool Transfer, Obfuscated Files or Information, System Information Discovery, System Network Configuration Discovery

References

Carvey, H.. (2014, September 2). Where you AT?: Indicators of lateral movement using at.exe on Windows 7 systems. Retrieved January 25, 2016. Shelmire, A.. (2015, July 6). Evasive Maneuvers. Retrieved January 22, 2016. Shelmire, A. (2015, July 06). Evasive Maneuvers by the Wekby group with custom ROP-packing and DNS covert channels. Retrieved November 15, 2018. Grunzweig, J., et al. (2016, May 24). New Wekby Attacks Use DNS Requests As Command and Control Mechanism. Retrieved November 15, 2018. Adair, S. (2017, February 17). Detecting and Responding to Advanced Threats within Exchange Environments. Retrieved March 20, 2017. Grunzweig, J., et al. (2016, May 24). New Wekby Attacks Use DNS Requests As Command and Control Mechanism. Retrieved August 17, 2016.