Command and Scripting Interpreter

Sub-techniques (13)

ID	Name
T1059.001	PowerShell
T1059.002	AppleScript
T1059.003	Windows Command Shell
T1059.004	Unix Shell
T1059.005	Visual Basic
T1059.006	Python
T1059.007	JavaScript
T1059.008	Network Device CLI
T1059.009	Cloud API
T1059.010	AutoHotKey & AutoIT
T1059.011	Lua
T1059.012	Hypervisor CLI
T1059.013	Container CLI/API

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.[1][2][3]

ID: T1059

Sub-techniques: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008, T1059.009, T1059.010, T1059.011, T1059.012, T1059.013

ⓘ

Tactic: Execution

ⓘ

Platforms: ESXi, IaaS, Identity Provider, Linux, Network Devices, Office Suite, Windows, macOS

Version: 2.6

Created: 31 May 2017

Last Modified: 24 October 2025

Version Permalink

Procedure Examples

ID	Name	Description
G0073	APT19	APT19 downloaded and launched code within a SCT file.[4]
G0050	APT32	APT32 has used COM scriptlets to download Cobalt Strike beacons.[5]
G0067	APT37	APT37 has used Ruby scripts to execute payloads.[6]
G0087	APT39	APT39 has utilized custom scripts to perform internal reconnaissance.[7][8]
C0046	ArcaneDoor	ArcaneDoor included the adversary executing command line interface (CLI) commands.[9]
S0234	Bandook	Bandook can support commands to execute Java-based payloads.[10]
S0486	Bonadan	Bonadan can create bind and reverse shells on the infected system.[11]
S0023	CHOPSTICK	CHOPSTICK is capable of performing remote command execution.[12][13]
C0029	Cutting Edge	During Cutting Edge, threat actors used Perl scripts to enable the deployment of the THINSPOOL shell script dropper and for enumerating host data.[14][15]
S0334	DarkComet	DarkComet can execute various types of scripts on the victim's machine.[16]
S0695	Donut	Donut can generate shellcode outputs that execute via Ruby.[17]
G0035	Dragonfly	Dragonfly has used the command line for execution.[18]
S0363	Empire	Empire uses a command-line interface to interact with systems.[19]
G0053	FIN5	FIN5 scans processes on all victim systems in the environment and uses automated scripts to pull back the results.[20]
G0037	FIN6	FIN6 has used scripting to iterate through a list of compromised PoS systems, copy data to a log file, and remove the original data files.[21][22]
G0046	FIN7	FIN7 used SQL scripts to help perform tasks on the victim's machine.[23][24][23]
S0618	FIVEHANDS	FIVEHANDS can receive a command line argument to limit file encryption to specified directories.[25][26]
C0053	FLORAHOX Activity	FLORAHOX Activity has executed PHP and Shell scripts to identify and infect subsequent routers for the ORB network.[27]
G0117	Fox Kitten	Fox Kitten has used a Perl reverse shell to communicate with C2.[28]
S0460	Get2	Get2 has the ability to run executables with command-line arguments.[29]
S0032	gh0st RAT	gh0st RAT is able to open a remote shell to execute commands.[30][31]
S0434	Imminent Monitor	Imminent Monitor has a CommandPromptPacket and ScriptPacket module(s) for creating a remote shell and executing scripts.[32]
G0004	Ke3chang	Malware used by Ke3chang can run commands on the command-line interface.[33][34]
S0487	Kessel	Kessel can create a reverse shell between the infected host and a specified system.[11]
S0167	Matryoshka	Matryoshka is capable of providing Meterpreter shell access.[35]
G0129	Mustang Panda	Mustang Panda has utilized meterpreter shellcode.[36]

ID	Name	Description
S1192	NICECURL	NICECURL has provided an arbitrary command execution interface.[37]
G0049	OilRig	OilRig has used various types of scripting for execution.[38][39][40][41][42]
C0005	Operation Spalax	For Operation Spalax, the threat actors used Nullsoft Scriptable Install System (NSIS) scripts to install malware.[43]
S0598	P.A.S. Webshell	P.A.S. Webshell has the ability to create reverse shells with Perl scripts.[44]
S1130	Raspberry Robin	Raspberry Robin variants can be delivered via highly obfuscated Windows Script Files (WSF) for initial execution.[45]
G1031	Saint Bear	Saint Bear has used the Windows Script Host (wscript) to execute intermediate files written to victim machines.[46]
S1110	SLIGHTPULSE	SLIGHTPULSE contains functionality to execute arbitrary commands passed to it.[47]
S0374	SpeakUp	SpeakUp uses Perl scripts.[48]
S1227	StarProxy	StarProxy has used the command line for execution of commands.[49]
G0038	Stealth Falcon	Stealth Falcon malware uses WMI to script data collection and command execution on the victim.[50]
S1154	VersaMem	VersaMem was delivered as a Java Archive (JAR) that runs by attaching itself to the Apache Tomcat Java servlet and web server.[51]
G0107	Whitefly	Whitefly has used a simple remote shell tool that will call back to the C2 server and wait for commands.[52]
G0124	Windigo	Windigo has used a Perl script for information gathering.[11]
S0219	WINERACK	WINERACK can create a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands.[53]
G1035	Winter Vivern	Winter Vivern used XLM 4.0 macros for initial code execution for malicious document files.[54]
S1151	ZeroCleare	ZeroCleare can receive command line arguments from an operator to corrupt the file system using the RawDisk driver.[55]
S0330	Zeus Panda	Zeus Panda can launch remote scripts on the victim's machine.[56]

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
M1047	Audit	Inventory systems for unauthorized command and scripting interpreter installations.
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content [57].
M1045	Code Signing	Where possible, only permit execution of signed scripts.
M1042	Disable or Remove Feature or Program	Disable or remove any unnecessary or unused shells or interpreters.
M1038	Execution Prevention	Use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[58]
M1033	Limit Software Installation	Prevent user installation of unrequired command and scripting interpreters.
M1026	Privileged Account Management	When PowerShell is necessary, consider restricting PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.[59] PowerShell JEA (Just Enough Administration) may also be used to sandbox administration and limit what commands admins/users can execute through remote PowerShell sessions.[60]
M1021	Restrict Web-Based Content	Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0516	Behavioral Detection of Command and Scripting Interpreter Abuse	AN1428	Detects the execution of scripting or command interpreters (e.g., powershell.exe, cmd.exe, wscript.exe) outside expected administrative time windows or from abnormal user contexts, often followed by encoded/obfuscated arguments or secondary execution events.
		AN1429	Detects use of shell interpreters (e.g., bash, sh, python, perl) initiated by users or processes not normally executing them, especially when chaining suspicious utilities like netcat, curl, or ssh.
		AN1430	Detects launch of command-line interpreters via Terminal, Automator, or hidden `osascript` , especially when parent process lineage deviates from user-initiated applications.
		AN1431	Detects use of 'esxcli system' or direct interpreter commands (e.g., busybox shell) invoked from SSH or host terminal unexpectedly.
		AN1432	Identifies CLI interpreter access (e.g., Cisco IOS, Juniper JUNOS) via `enable` mode or scripting-capable sessions used by uncommon accounts or from unknown IPs.

References

1. Microsoft. (2020, August 21). Running Remote Commands. Retrieved July 26, 2021.
2. Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Command History. Retrieved October 21, 2020.
3. Abdou Rockikz. (2020, July). How to Execute Shell Commands in a Remote Machine in Python. Retrieved July 26, 2021.
4. Ahl, I. (2017, June 06). Privileges and Credentials: Phished at the Request of Counsel. Retrieved May 17, 2018.
5. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
6. Cash, D., Grunzweig, J., Adair, S., Lancaster, T. (2021, August 25). North Korean BLUELIGHT Special: InkySquid Deploys RokRAT. Retrieved October 1, 2021.
7. Hawley et al. (2019, January 29). APT39: An Iranian Cyber Espionage Group Focused on Personal Information. Retrieved February 19, 2019.
8. FBI. (2020, September 17). Indicators of Compromise Associated with Rana Intelligence Computing, also known as Advanced Persistent Threat 39, Chafer, Cadelspy, Remexi, and ITG07. Retrieved December 10, 2020.
9. Cisco Talos. (2024, April 24). ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices. Retrieved January 6, 2025.
10. Check Point. (2020, November 26). Bandook: Signed & Delivered. Retrieved May 31, 2021.
11. Dumont, R., M.Léveillé, M., Porcher, H. (2018, December 1). THE DARK SIDE OF THE FORSSHE A landscape of OpenSSH backdoors. Retrieved July 16, 2020.
12. Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.
13. ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.
14. Lin, M. et al. (2024, January 31). Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation. Retrieved February 27, 2024.
15. McLellan, T. et al. (2024, January 12). Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. Retrieved February 27, 2024.
16. Kujawa, A. (2018, March 27). You dirty RAT! Part 1: DarkComet. Retrieved November 6, 2018.
17. TheWover. (2019, May 9). donut. Retrieved March 25, 2022.
18. US-CERT. (2018, March 16). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved June 6, 2018.
19. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
20. Bromiley, M. and Lewis, P. (2016, October 7). Attacking the Hospitality and Gaming Industries: Tracking an Attacker Around the World in 7 Years. Retrieved October 6, 2017.
21. FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved November 17, 2024.
22. McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.
23. Pantazopoulos, N. (2018, April 17). Decoding network data from a Gh0st RAT variant. Retrieved November 2, 2018.
24. QiAnXin Threat Intelligence Center. (2019, February 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Retrieved May 5, 2020.
25. Villeneuve, N., Bennett, J. T., Moran, N., Haq, T., Scott, M., & Geers, K. (2014). OPERATION “KE3CHANG”: Targeted Attacks Against Ministries of Foreign Affairs. Retrieved November 12, 2014.
26. Smallridge, R. (2018, March 10). APT15 is alive and strong: An analysis of RoyalCli and RoyalDNS. Retrieved April 4, 2018.
27. ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.
28. Asheer Malhotra, Jungsoo An, Kendall Mc. (2022, May 5). Mustang Panda deploys a new wave of malware targeting Europe. Retrieved August 4, 2025.
29. Rozmann, O., et al. (2024, May 1). Uncharmed: Untangling Iran's APT42 Operations. Retrieved October 9, 2024.
30. Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit. Retrieved December 20, 2017.
31. Falcone, R. and Lee, B. (2017, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group. Retrieved January 8, 2018.
32. Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
33. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
34. Falcone, R., Wilhoit, K.. (2018, November 16). Analyzing OilRig’s Ops Tempo from Testing to Weaponization to Delivery. Retrieved April 23, 2019.
35. M. Porolli. (2021, January 21). Operation Spalax: Targeted malware attacks in Colombia. Retrieved September 16, 2022.
36. ANSSI. (2021, January 27). SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS. Retrieved March 30, 2021.
37. Patrick Schläpfer . (2024, April 10). Raspberry Robin Now Spreading Through Windows Script Files. Retrieved May 17, 2024.
38. Unit 42. (2022, February 25). Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot. Retrieved June 9, 2022.
39. Perez, D. et al. (2021, April 20). Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day. Retrieved February 5, 2024.
40. Check Point Research. (2019, February 4). SpeakUp: A New Undetected Backdoor Linux Trojan. Retrieved April 17, 2019.
41. Sudeep Singh. (2025, April 16). Latest Mustang Panda Arsenal: ToneShell and StarProxy | P1. Retrieved July 21, 2025.
42. Marczak, B. and Scott-Railton, J.. (2016, May 29). Keep Calm and (Don’t) Enable Macros: A New Threat Actor Targets UAE Dissidents. Retrieved June 8, 2016.
43. Black Lotus Labs. (2024, August 27). Taking The Crossroads: The Versa Director Zero-Day Exploitaiton. Retrieved August 27, 2024.

23. Carr, N., et al. (2018, August 01). On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation. Retrieved August 23, 2018.
24. Platt, J. and Reeves, J.. (2019, March). FIN7 Revisited: Inside Astra Panel and SQLRat Malware. Retrieved June 18, 2019.
25. McLellan, T. and Moore, J. et al. (2021, April 29). UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat. Retrieved June 2, 2021.
26. Matthews, M. and Backhouse, W. (2021, June 15). Handy guide to a new Fivehands ransomware variant. Retrieved June 24, 2021.
27. Raggi, Michael. (2024, May 22). IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders. Retrieved July 8, 2024.
28. ClearSky. (2020, December 17). Pay2Key Ransomware – A New Campaign by Fox Kitten. Retrieved December 21, 2020.
29. Schwarz, D. et al. (2019, October 16). TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader. Retrieved May 29, 2020.
30. FireEye Threat Intelligence. (2015, July 13). Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak. Retrieved January 25, 2016.
52. Symantec. (2019, March 6). Whitefly: Espionage Group has Singapore in Its Sights. Retrieved May 26, 2020.
53. FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved November 17, 2024.
54. Chad Anderson. (2021, April 27). Winter Vivern: A Look At Re-Crafted Government MalDocs Targeting Multiple Languages. Retrieved July 29, 2024.
55. Jenkins, L. at al. (2022, August 4). ROADSWEEP Ransomware - Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations. Retrieved August 6, 2024.
56. Ebach, L. (2017, June 22). Analysis Results of Zeus.Variant.Panda. Retrieved November 5, 2018.
57. Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.
58. PowerShell Team. (2017, November 2). PowerShell Constrained Language Mode. Retrieved March 27, 2023.
59. Sutherland, S. (2014, September 9). 15 Ways to Bypass the PowerShell Execution Policy. Retrieved September 12, 2024.
60. Microsoft. (2022, November 17). Just Enough Administration. Retrieved March 27, 2023.