Command and Scripting Interpreter, Technique T1059 - Enterprise

Archived: 2026-04-05 13:44:49 UTC

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]

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]
