Command and Scripting Interpreter: Unix Shell, Sub-technique T1059.004 - Enterprise

Archived: 2026-04-05 18:05:53 UTC

S0504 Anchor

Anchor can execute payloads via shell scripting.[3]

S0584 AppleJeus

AppleJeus has used shell scripts to execute commands after installation and set persistence mechanisms.[4][5]

G0096 APT41

APT41 used Linux shell commands for system survey and information gathering prior to exploitation of vulnerabilities such as CVE-2019-19871.[6]

G0143 Aquatic Panda

Aquatic Panda used malicious shell scripts in Linux environments following access via SSH to install Linux versions of Winnti malware.[7]

S1184 BOLDMOVE

BOLDMOVE is capable of spawning a remote command shell.[8]

S1161 BPFDoor

BPFDoor can create a reverse shell and supports vt100 emulator formatting.[9]

S0482 Bundlore

Bundlore has leveraged /bin/sh and /bin/bash to execute commands on the victim machine.[10]

S0077 CallMe

CallMe has the capability to create a reverse shell on victims.[11]

S1224 CASTLETAP

CASTLETAP has the ability to spawn BusyBox command shell in victim environments.[12]

S0220 Chaos

Chaos provides a reverse shell connection on 8338/TCP, encrypted via AES.[13]

S1105 COATHANGER

COATHANGER provides a BusyBox reverse shell for command and control.[14]

S0369 CoinTicker

CoinTicker executes a bash script to establish a reverse shell.[15]

G1052 Contagious Interview

Contagious Interview has targeted macOS victim hosts using a bash downloader coremedia.sh and a bash script cloud.sh.[16]

S0492 CookieMiner

CookieMiner has used a Unix shell script to run a series of commands targeting macOS.[17]

S1153 Cuckoo Stealer

Cuckoo Stealer can spawn a bash shell to enable execution on compromised hosts.[18]

S0021 Derusbi

Derusbi is capable of creating a remote Bash shell and executing commands.[19][20]

S0600 Doki

Doki has executed shell scripts with /bin/sh.[21]

S0502 Drovorub

Drovorub can execute arbitrary commands as root on a compromised system.[22]

S0377 Ebury

Ebury can use the commands `Xcsh` or `Xcls` to open a shell with Ebury level permissions and `Xxsh` to open a shell with root level.[23]

S0401 Exaramel for Linux

Exaramel for Linux has a command to execute a shell command on the system.[24][25]

C0053 FLORAHOX Activity

FLORAHOX Activity has executed multiple Bash controller scripts to provide command line inputs for FLORAHOX traversal configurations.[26]

S0410 Fysbis

Fysbis has the ability to create and execute commands in a remote shell for CLI.[27]

S1198 Gomir

Gomir reads command line arguments and parses them for functionality when executed from a Linux shell, and can execute arbitrary strings passed to it as shell commands.[28]

S0690 Green Lambert

Green Lambert can use shell scripts for execution, such as `/bin/sh -c`.[29][30]

S0601 Hildegard

Hildegard has used shell scripts for execution.[31]

S1203 J-magic

The J-magic agent is executed through a command line argument which specifies an interface and listening port.[32]

S0265 Kazuar

Kazuar uses /bin/bash to execute commands on the victim's machine.[33]

S0599 Kinsing

Kinsing has used Unix shell scripts to execute commands in the victim environment.[34]

S0641 Kobalos

Kobalos can spawn a new pseudo-terminal and execute arbitrary commands at the command prompt.[35]

C0035 KV Botnet Activity

KV Botnet Activity utilizes multiple Bash scripts during botnet installation stages, and the final botnet payload allows for running commands in the Bash shell.[36]

S0451 LoudMiner

LoudMiner used shell scripts to launch various services and to start/stop the QEMU virtualization.[37]

S1016 MacMa

MacMa can execute supplied shell commands and uses bash scripts to perform additional actions.[38][39]

S0198 NETWIRE

NETWIRE has the ability to use `/bin/bash` and `/bin/sh` to execute commands.[40][41]

S1107 NKAbuse

NKAbuse is initially installed and executed through an initial shell script.[42]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors piped output from stdout to bash for execution.[43][44]

S0402 OSX/Shlayer

OSX/Shlayer can use bash scripts to check the macOS version, download payloads, and extract bytes from files. OSX/Shlayer uses the command `sh -c tail -c +1381...` to extract bytes at an offset from a specified file. OSX/Shlayer uses the `curl -fsL "$url" >$tmp_path` command to download malicious payloads into a temporary directory.[45][46][47][48]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D uses a shell script as the main executable inside an app bundle and drops an embedded base64-encoded payload to the `/tmp` folder.[49][50]

S1109 PACEMAKER

PACEMAKER can use a simple bash script for execution.[51]

S0587 Penquin

Penquin can execute remote commands using bash scripts.[52]

S1123 PITSTOP

PITSTOP has the ability to receive shell commands over a Unix domain socket.[53]

S0279 Proton

Proton uses macOS' .command file type to script actions.[54]

S1108 PULSECHECK

PULSECHECK can use Unix shell script for command execution.[51]

C0055 Quad7 Activity

Quad7 Activity has enabled the creation of an access-controlled command shell `/bin/sh` on compromised routers.[55][56]

C0056 RedPenguin

During RedPenguin, UNC3886 used malware capable of launching an interactive shell.[57][58]

S1219 REPTILE

REPTILE can deploy components automatically with shell scripts.[59]

S1222 RIFLESPINE

RIFLESPINE can execute commands with `/bin/sh`.[59]

G0106 Rocke

Rocke used shell scripts to run commands which would obtain persistence and execute the cryptocurrency mining malware.[60]

G1015 Scattered Spider

Scattered Spider has used the command shell to upload and install the Teleport remote access tool to a compromised vCenter Server Appliance.[61]

G1041 Sea Turtle

Sea Turtle used shell scripts for post-exploitation execution in victim environments.[62][63]

S0468 Skidmap

Skidmap has used `pm.sh` to download and install its main payload.[64]

S1163 SnappyTCP

SnappyTCP creates the reverse shell using a pthread spawning a bash shell.[62]

G0139 TeamTNT

TeamTNT has used shell scripts for execution.[65][66]

S0647 Turian

Turian has the ability to use `/bin/sh` to execute commands.[67]

G1048 UNC3886

UNC3886 has used a bash script to install malicious vSphere Installation Bundles (VIBs).[68]

G1047 Velvet Ant

Velvet Ant used a custom tool, VELVETSTING, to parse encoded inbound commands to compromised F5 BIG-IP devices and then execute them via the Unix shell.[69]

S1217 VIRTUALPITA

VIRTUALPITA has the ability to spawn a bash shell for script execution.[68]

G1017 Volt Typhoon

Volt Typhoon has used Brightmetricagent.exe which contains a command- line interface (CLI) library that can leverage command shells including Z Shell (zsh).[70]

S0466 WindTail

WindTail can use the `open` command to execute an application.[71]

S0658 XCSSET

XCSSET uses a shell script to execute Mach-o files and `osacompile` commands such as, `osacompile -x -o xcode.app main.applescript` .[72]

S1114 ZIPLINE

ZIPLINE can use `/bin/sh` to create a reverse shell and execute commands.[73]
