# TTP Detail – T1059.004

## TTP Information

Name: Unix Shell

Description: Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux, macOS, and ESXi systems, though many variations of the Unix shell exist (e.g. sh, ash, bash, zsh, etc.) depending on the specific OS or distribution.(Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges.

Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

Some systems, such as embedded devices, lightweight Linux distributions, and ESXi servers, may leverage stripped-down Unix shells via Busybox, a small executable that contains a variety of tools, including a simple shell.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Anchor
* AppleJeus
* BOLDMOVE
* BPFDoor
* Bundlore
* COATHANGER
* CallMe
* Chaos
* CoinTicker
* CookieMiner
* Cuckoo Stealer
* Derusbi
* Doki
* Drovorub
* Ebury
* Exaramel for Linux
* Fysbis
* Gomir
* Green Lambert
* Hildegard
* J-magic
* Kazuar
* Kinsing
* Kobalos
* LoudMiner
* MacMa
* NETWIRE
* NKAbuse
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* PACEMAKER
* PITSTOP
* PULSECHECK
* Penquin
* Proton
* Skidmap
* SnappyTCP
* Turian
* WindTail
* XCSSET
* ZIPLINE

## APTs (Intrusion Sets)

* APT41
* Aquatic Panda
* Rocke
* Sea Turtle
* TeamTNT
* Velvet Ant
* Volt Typhoon