# TTP Detail – T1059

## TTP Information

Name: Command and Scripting Interpreter

Description: 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](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).

There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) 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](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Bandook
* Bonadan
* CHOPSTICK
* DarkComet
* FIVEHANDS
* Get2
* Kessel
* Matryoshka
* NICECURL
* P.A.S. Webshell
* Raspberry Robin
* SLIGHTPULSE
* SpeakUp
* VersaMem
* WINERACK
* ZeroCleare
* Zeus Panda
* gh0st RAT

## Tools

* Donut
* Empire
* Imminent Monitor

## APTs (Intrusion Sets)

* APT19
* APT32
* APT37
* APT39
* Dragonfly
* FIN5
* FIN6
* FIN7
* Fox Kitten
* Ke3chang
* OilRig
* Saint Bear
* Stealth Falcon
* Whitefly
* Windigo
* Winter Vivern