# TTP Detail – T1027.010

## TTP Information

Name: Command Obfuscation

Description: Adversaries may obfuscate content during command execution to impede detection. Command-line obfuscation is a method of making strings and patterns within commands and scripts more difficult to signature and analyze. This type of obfuscation can be included within commands executed by delivered payloads (e.g., [Phishing](https://attack.mitre.org/techniques/T1566) and [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)) or interactively via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059).(Citation: Akamai JS)(Citation: Malware Monday VBE)

For example, adversaries may abuse syntax that utilizes various symbols and escape characters (such as spacing, `^`, `+`. `$`, and `%`) to make commands difficult to analyze while maintaining the same intended functionality.(Citation: RC PowerShell) Many languages support built-in obfuscation in the form of base64 or URL encoding.(Citation: Microsoft PowerShellB64) Adversaries may also manually implement command obfuscation via string splitting (`“Wor”+“d.Application”`), order and casing of characters (`rev <<<'dwssap/cte/ tac'`), globing (`mkdir -p '/tmp/:&$NiA'`), as well as various tricks involving passing strings through tokens/environment variables/input streams.(Citation: Bashfuscator Command Obfuscators)(Citation: FireEye Obfuscation June 2017)

Adversaries may also use tricks such as directory traversals to obfuscate references to the binary being invoked by a command (`C:\voi\pcw\..\..\Windows\tei\qs\k\..\..\..\system32\erool\..\wbem\wg\je\..\..\wmic.exe shadowcopy delete`).(Citation: Twitter Richard WMIC)

Tools such as <code>Invoke-Obfuscation</code> and <code>Invoke-DOSfucation</code> have also been used to obfuscate commands.(Citation: Invoke-DOSfuscation)(Citation: Invoke-Obfuscation)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Astaroth
* BADHATCH
* BackConfig
* CARROTBAT
* ComRAT
* CookieMiner
* DarkWatchman
* Denis
* Emotet
* FruitFly
* IceApple
* KOCTOPUS
* LoudMiner
* Machete
* Netwalker
* POWERSTATS
* PoetRAT
* PowerPunch
* QUADAGENT
* QakBot
* RogueRobin
* SHARPSTATS
* SQLRat
* Sardonic
* Sibot
* Ursnif
* Zeus Panda

## Tools

* Empire
* PowerSploit

## APTs (Intrusion Sets)

* APT19
* APT32
* Aquatic Panda
* Chimera
* Cobalt Group
* FIN6
* FIN7
* FIN8
* Fox Kitten
* GOLD SOUTHFIELD
* Gamaredon Group
* HEXANE
* LazyScripter
* Leafminer
* Magic Hound
* MuddyWater
* Patchwork
* Play
* Sandworm Team
* Sidewinder
* Silence
* TA505
* TA551
* Turla
* Wizard Spider