# TTP Detail – T1027

## TTP Information

Name: Obfuscated Files or Information

Description: Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.   
  
Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript.   
  
Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016)  
  
Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ADVSTORESHELL
* Action RAT
* Agent Tesla
* Amadey
* Anchor
* AppleJeus
* AppleSeed
* Avaddon
* AvosLocker
* BPFDoor
* BUSHWALK
* BoomBox
* BoxCaon
* Bumblebee
* Bundlore
* CHIMNEYSWEEP
* COATHANGER
* CORESHELL
* Carbanak
* Carbon
* Clambling
* Cobalt Strike
* CoinTicker
* ComRAT
* Comnie
* Conficker
* Conti
* Cuba
* DRATzarus
* DarkGate
* DarkTortilla
* Daserf
* Denis
* Diavol
* Dridex
* Drovorub
* DustySky
* ECCENTRICBANDWAGON
* EKANS
* Ebury
* Ecipekac
* Epic
* FatDuke
* FinFisher
* Final1stspy
* Flagpro
* Gootloader
* Green Lambert
* GrimAgent
* H1N1
* HTTPBrowser
* Hancitor
* Hydraq
* ISMInjector
* Industroyer
* InnaputRAT
* InvisiMole
* JPIN
* Kazuar
* KillDisk
* Kobalos
* Lokibot
* Lumma Stealer
* Matryoshka
* Maze
* MiniDuke
* NETWIRE
* NOKKI
* NanoCore
* NightClub
* OLDBAIT
* OopsIE
* Orz
* P.A.S. Webshell
* POSHSPY
* PUNCHBUGGY
* PUNCHTRACK
* Pillowmint
* Pisloader
* PlugX
* PoetRAT
* PoisonIvy
* PolyglotDuke
* PowerStallion
* QakBot
* ROKRAT
* RTM
* Ramsay
* Raspberry Robin
* RegDuke
* Ryuk
* SDBbot
* SHOTPUT
* SLOWPULSE
* SUNBURST
* SUNSPOT
* SVCReady
* Saint Bot
* Samurai
* Sardonic
* ShadowPad
* Shamoon
* Siloscape
* Small Sieve
* Snip3
* SodaMaster
* SombRAT
* SoreFang
* StreamEx
* StrelaStealer
* SynAck
* TEARDROP
* TajMahal
* TrickBot
* Trojan.Karagany
* Turian
* Valak
* XTunnel
* jRAT

## Tools

* Brute Ratel C4
* CARROTBALL
* Imminent Monitor
* MCMD
* Out1
* Remcos
* ShimRatReporter
* Sliver

## APTs (Intrusion Sets)

* APT-C-36
* APT3
* APT37
* APT41
* BackdoorDiplomacy
* BlackOasis
* Earth Lusca
* GALLIUM
* Gallmaker
* Gamaredon Group
* Ke3chang
* Kimsuky
* Moonstone Sleet
* Mustang Panda
* RedCurl
* Rocke
* Sandworm Team
* Windshift