# TTP Detail – T1027.013

## TTP Information

Name: Encrypted/Encoded File

Description: Adversaries may encrypt or encode files to obfuscate strings, bytes, and other specific patterns to impede detection. Encrypting and/or encoding file content aims to conceal malicious artifacts within a file used in an intrusion. Many other techniques, such as [Software Packing](https://attack.mitre.org/techniques/T1027/002), [Steganography](https://attack.mitre.org/techniques/T1027/003), and [Embedded Payloads](https://attack.mitre.org/techniques/T1027/009), share this same broad objective. Encrypting and/or encoding files could lead to a lapse in detection of static signatures, only for this malicious content to be revealed (i.e., [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140)) at the time of execution/use.

This type of file obfuscation can be applied to many file artifacts present on victim hosts, such as malware log/configuration and payload files.(Citation: File obfuscation) Files can be encrypted with a hardcoded or user-supplied key, as well as otherwise obfuscated using standard encoding schemes such as Base64.

The entire content of a file may be obfuscated, or just specific functions or values (such as C2 addresses). Encryption and encoding may also be applied in redundant layers for additional protection.

For example, adversaries may abuse password-protected Word documents or self-extracting (SFX) archives as a method of encrypting/encoding a file such as a [Phishing](https://attack.mitre.org/techniques/T1566) payload. These files typically function by attaching the intended archived content to a decompressor stub that is executed when the file is invoked (e.g., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: SFX - Encrypted/Encoded File)

Adversaries may also abuse file-specific as well as custom encoding schemes. For example, Byte Order Mark (BOM) headers in text files may be abused to manipulate and obfuscate file content until [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) execution.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Aria-body
* Astaroth
* Attor
* AuditCred
* Avenger
* BLINDINGCAN
* BLUELIGHT
* BOOSTWRITE
* Bazar
* BendyBear
* Bisonal
* BitPaymer
* BlackByte Ransomware
* CARROTBAT
* Carberp
* Cardinal RAT
* Chinoxy
* Chrommme
* CozyCar
* Cuckoo Stealer
* DCSrv
* DEADEYE
* DEADWOOD
* DOGCALL
* DUSTPAN
* DUSTTRAP
* Dacls
* DanBot
* DarkGate
* Elise
* Emissary
* Emotet
* EnvyScout
* Exaramel for Linux
* FELIXROOT
* FIVEHANDS
* FlawedGrace
* FoggyWeb
* FunnyDream
* Fysbis
* Gazer
* GoldMax
* GoldenSpy
* Grandoreiro
* GravityRAT
* GreyEnergy
* HAWKBALL
* HOMEFRY
* Helminth
* HermeticWizard
* Heyoka Backdoor
* Hi-Zor
* HiddenWasp
* Hildegard
* HotCroissant
* HyperBro
* IPsec Helper
* IcedID
* JHUHUGIT
* KEYPLUG
* KGH\_SPY
* KONNI
* Kapeka
* Kerrdown
* Kessel
* Kevin
* KeyBoy
* Kwampirs
* Latrodectus
* LightNeuron
* LightSpy
* LockBit 3.0
* LoudMiner
* Lumma Stealer
* LunarMail
* LunarWeb
* Mafalda
* MagicRAT
* Mango
* Metamorfo
* Micropsia
* Milan
* Mispadu
* More\_eggs
* Mosquito
* NanHaiShu
* Ninja
* OSX\_OCEANLOTUS.D
* PS1
* Penquin
* PipeMon
* Prikormka
* PyDCrypt
* RAPIDPULSE
* REvil
* ROADSWEEP
* Raccoon Stealer
* Raindrop
* RainyDay
* RansomHub
* Reaver
* RedLeaves
* Remexi
* Remsec
* Rifdoor
* Rising Sun
* STARWHALE
* SUPERNOVA
* Sagerunex
* Sakula
* SamSam
* Seasalt
* Shark
* Skidmap
* Smoke Loader
* SocGholish
* SpeakUp
* Squirrelwaffle
* StealBit
* StoneDrill
* StrelaStealer
* StrongPity
* Stuxnet
* SysUpdate
* TINYTYPHON
* TYPEFRAME
* Taidoor
* ThreatNeedle
* Torisma
* TrickBot
* UPSTYLE
* USBStealer
* Uroburos
* Ursnif
* VERMIN
* VersaMem
* Volgmer
* WastedLocker
* Waterbear
* WhisperGate
* WindTail
* Winnti for Linux
* Winnti for Windows
* Woody RAT
* XCSSET
* XLoader
* YAHOYAH
* ZeroT
* Zeus Panda
* Zox
* ZxxZ
* metaMain
* njRAT

## Tools

* Donut
* IronNetInjector
* PcShare
* Sliver

## APTs (Intrusion Sets)

* APT18
* APT19
* APT28
* APT32
* APT33
* APT39
* BITTER
* Blue Mockingbird
* Dark Caracal
* Darkhotel
* Elderwood
* Fox Kitten
* Group5
* Higaisa
* Inception
* Lazarus Group
* Leviathan
* Magic Hound
* Malteiro
* Metador
* Mofang
* Moonstone Sleet
* Moses Staff
* OilRig
* Putter Panda
* Saint Bear
* Sidewinder
* Storm-1811
* TA2541
* TA505
* TeamTNT
* Threat Group-3390
* Transparent Tribe
* Tropic Trooper
* Whitefly
* menuPass