# TTP Detail – T1140

## TTP Information

Name: Deobfuscate/Decode Files or Information

Description: Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows <code>copy /b</code> or <code>type</code> command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016)(Citation: Sentinel One Tainted Love 2023)

Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ABK
* Action RAT
* Agent Tesla
* Amadey
* Apostle
* AppleJeus
* AppleSeed
* Aria-body
* Astaroth
* AuditCred
* Avaddon
* Avenger
* AvosLocker
* Azorult
* BADFLICK
* BBK
* BBSRAT
* BLINDINGCAN
* BOOSTWRITE
* BUSHWALK
* Babuk
* BabyShark
* BackConfig
* Bandook
* Bankshot
* Bazar
* BendyBear
* Bisonal
* BlackByte Ransomware
* BoomBox
* Bumblebee
* Bundlore
* CHIMNEYSWEEP
* COATHANGER
* Carbon
* Cardinal RAT
* Chaes
* CharmPower
* Chinoxy
* Chrommme
* Clambling
* Clop
* Cobalt Strike
* CoinTicker
* ComRAT
* Conti
* CookieMiner
* CostaBricks
* Crimson
* Cuckoo Stealer
* Cyclops Blink
* DDKONG
* DEADEYE
* DEADWOOD
* DUSTPAN
* DUSTTRAP
* DanBot
* DarkGate
* DarkTortilla
* DarkWatchman
* Denis
* DropBook
* Drovorub
* Dtrack
* Dyre
* Ebury
* Ecipekac
* Egregor
* Emotet
* EnvyScout
* Exaramel for Linux
* Exbyte
* FIVEHANDS
* FRAMESTING
* FYAnti
* FatDuke
* FinFisher
* Final1stspy
* FoggyWeb
* GLASSTOKEN
* Gelsemium
* GoldMax
* Goopy
* Gootloader
* Grandoreiro
* Green Lambert
* GrimAgent
* HUI Loader
* Hancitor
* HermeticWiper
* Heyoka Backdoor
* HiddenWasp
* Hildegard
* HyperBro
* INC Ransomware
* ISMInjector
* IceApple
* Industroyer
* InvisiMole
* KEYPLUG
* KGH\_SPY
* KOCTOPUS
* KONNI
* Kapeka
* Kerrdown
* Kessel
* Kobalos
* Kwampirs
* LIGHTWIRE
* Latrodectus
* LightNeuron
* Line Dancer
* LiteDuke
* Lizar
* LockBit 2.0
* LockBit 3.0
* Lokibot
* LookBack
* Lucifer
* Lumma Stealer
* LunarLoader
* LunarMail
* LunarWeb
* MESSAGETAP
* MacMa
* Machete
* Mafalda
* MagicRAT
* MegaCortex
* Metamorfo
* MirageFox
* Mispadu
* Mongall
* More\_eggs
* Mori
* NOKKI
* NativeZone
* Netwalker
* Nightdoor
* Ninja
* ODAgent
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* OilBooster
* Okrum
* OnionDuke
* OopsIE
* P.A.S. Webshell
* PITSTOP
* POWERSTATS
* PS1
* PUNCHBUGGY
* Pikabot
* Pillowmint
* PingPull
* PipeMon
* PlugX
* PoetRAT
* PolyglotDuke
* PowGoop
* PowerExchange
* PowerLess
* Proton
* Pteranodon
* PyDCrypt
* QUADAGENT
* QUIETCANARY
* QakBot
* RAPIDPULSE
* RDAT
* REvil
* RGDoor
* ROADSWEEP
* ROKRAT
* Raccoon Stealer
* Raindrop
* RainyDay
* Ramsay
* RansomHub
* Raspberry Robin
* RegDuke
* Remexi
* Rising Sun
* RogueRobin
* RotaJakiro
* SDBbot
* SLIGHTPULSE
* SQLRat
* STEADYPULSE
* SUNSPOT
* Sagerunex
* Saint Bot
* SampleCheck5000
* Sardonic
* ShadowPad
* Shamoon
* Shark
* SharpStage
* ShimRat
* Sibot
* SideTwist
* Siloscape
* Skidmap
* Smoke Loader
* Snip3
* SombRAT
* SoreFang
* Spark
* Spica
* Squirrelwaffle
* Starloader
* StealBit
* StrelaStealer
* Stuxnet
* SysUpdate
* TEARDROP
* TSCookie
* TYPEFRAME
* Taidoor
* ThreatNeedle
* Torisma
* TrickBot
* Turian
* UPSTYLE
* Uroburos
* Ursnif
* VERMIN
* Valak
* VaporRage
* Volgmer
* WIREFIRE
* WarzoneRAT
* WastedLocker
* Waterbear
* WellMail
* WellMess
* WhisperGate
* WindTail
* Winnti for Linux
* Winnti for Windows
* Woody RAT
* XLoader
* YAHOYAH
* Zebrocy
* ZeroT
* Zeus Panda
* ZxxZ
* gh0st RAT
* metaMain
* xCaon

## Tools

* Brute Ratel C4
* Expand
* Imminent Monitor
* IronNetInjector
* PcShare
* certutil

## APTs (Intrusion Sets)

* APT19
* APT28
* APT38
* APT39
* Agrius
* BRONZE BUTLER
* BlackByte
* Cinnamon Tempest
* Darkhotel
* Earth Lusca
* FIN13
* Gamaredon Group
* Gorgon Group
* Higaisa
* Ke3chang
* Kimsuky
* Lazarus Group
* Leviathan
* Malteiro
* Molerats
* Moonstone Sleet
* MuddyWater
* OilRig
* Rocke
* Sandworm Team
* Storm-1811
* TA505
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Turla
* WIRTE
* Winter Vivern
* ZIRCONIUM
* menuPass