# TTP Detail – T1070.004

## TTP Information

Name: File Deletion

Description: Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.  
  
There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) functions include <code>del</code> on Windows, <code>rm</code> or <code>unlink</code> on Linux and macOS, and `rm` on ESXi.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ADVSTORESHELL
* AcidPour
* Anchor
* Apostle
* AppleJeus
* AppleSeed
* Aria-body
* Attor
* AuditCred
* Azorult
* BADHATCH
* BBSRAT
* BLACKCOFFEE
* BLINDINGCAN
* BLUELIGHT
* BOLDMOVE
* BPFDoor
* BabyShark
* BackConfig
* Backdoor.Oldrea
* Bandook
* Bankshot
* Bazar
* Bisonal
* BlackByte 2.0 Ransomware
* Bumblebee
* CARROTBAT
* COATHANGER
* Calisto
* Carbanak
* Cardinal RAT
* CharmPower
* Cherry Picker
* Crimson
* Cryptoistic
* Cuba
* DanBot
* DarkGate
* DarkWatchman
* Denis
* Derusbi
* Drovorub
* Dtrack
* DustySky
* ECCENTRICBANDWAGON
* Elise
* Epic
* EvilBunny
* Exaramel for Linux
* Exbyte
* FALLCHILL
* FELIXROOT
* FatDuke
* Ferocious
* FlawedAmmyy
* FruitFly
* FunnyDream
* Fysbis
* Gazer
* Gelsemium
* Gold Dragon
* GoldenSpy
* Gomir
* Grandoreiro
* Green Lambert
* GreyEnergy
* GrimAgent
* GuLoader
* HALFBAKED
* HAWKBALL
* HTTPBrowser
* Hancitor
* HermeticWiper
* Heyoka Backdoor
* Hi-Zor
* Hildegard
* HotCroissant
* Hydraq
* HyperBro
* IPsec Helper
* IceApple
* InnaputRAT
* InvisiMole
* Ixeshe
* JHUHUGIT
* JPIN
* KEYMARBLE
* KONNI
* Kazuar
* Kevin
* KillDisk
* Kivars
* Komplex
* Latrodectus
* LightNeuron
* Line Runner
* Linfo
* LiteDuke
* LockBit 2.0
* LockBit 3.0
* LockerGoga
* Lokibot
* LookBack
* LoudMiner
* LunarMail
* LunarWeb
* MESSAGETAP
* MURKYTOP
* MacMa
* MacSpy
* Machete
* MagicRAT
* Metamorfo
* Meteor
* Milan
* Misdat
* MoonWind
* More\_eggs
* Mori
* Mosquito
* MultiLayer Wiper
* NICECURL
* NOKKI
* NanHaiShu
* Nebulae
* Nightdoor
* ODAgent
* OSX\_OCEANLOTUS.D
* OceanSalt
* Okrum
* OopsIE
* OutSteel
* P.A.S. Webshell
* PLEAD
* POWERSTATS
* PUNCHBUGGY
* Pasam
* Pay2Key
* Penquin
* Pillowmint
* PoetRAT
* Pony
* PowerDuke
* PowerShower
* Prikormka
* ProLock
* Proton
* Proxysvc
* Pteranodon
* PyDCrypt
* Pysa
* QUADAGENT
* QakBot
* RCSession
* RDAT
* RDFSNIFFER
* REvil
* ROADSWEEP
* ROKRAT
* RTM
* Raccoon Stealer
* RainyDay
* RansomHub
* Raspberry Robin
* Reaver
* RedLeaves
* Remsec
* Rising Sun
* RunningRAT
* S-Type
* SDBbot
* SLOTHFULMEDIA
* SQLRat
* SUNBURST
* SUNSPOT
* Saint Bot
* Sakula
* SamSam
* SeaDuke
* Seasalt
* ServHelper
* Shark
* ShimRat
* ShrinkLocker
* Sibot
* Solar
* SombRAT
* SpeakUp
* StealBit
* StoneDrill
* StrifeWater
* StrongPity
* Stuxnet
* SysUpdate
* TAINTEDSCRIBE
* TDTESS
* TYPEFRAME
* Taidoor
* Trojan.Karagany
* Troll Stealer
* UPSTYLE
* USBStealer
* Uroburos
* Ursnif
* VBShower
* VERMIN
* VersaMem
* Volgmer
* WINDSHIELD
* WhisperGate
* WindTail
* Wingbird
* Winnti for Windows
* Woody RAT
* XAgentOSX
* XLoader
* Zebrocy
* ZeroCleare
* Zeus Panda
* ZxShell
* ccf32
* gh0st RAT
* jRAT
* metaMain
* njRAT
* pngdowner
* zwShell

## Tools

* CSPY Downloader
* Imminent Monitor
* PcShare
* SDelete
* SILENTTRINITY
* cmd

## APTs (Intrusion Sets)

* APT18
* APT28
* APT29
* APT3
* APT32
* APT38
* APT39
* APT41
* APT5
* Aquatic Panda
* BRONZE BUTLER
* BlackByte
* Chimera
* Cobalt Group
* Dragonfly
* Ember Bear
* Evilnum
* FIN10
* FIN5
* FIN6
* FIN8
* Gamaredon Group
* Group5
* INC Ransom
* Kimsuky
* Lazarus Group
* Magic Hound
* Metador
* Mustang Panda
* OilRig
* Patchwork
* Play
* RedCurl
* Rocke
* Sandworm Team
* Silence
* TeamTNT
* The White Company
* Threat Group-3390
* Tropic Trooper
* Volt Typhoon
* Wizard Spider
* menuPass