# TTP Detail – T1083

## TTP Information

Name: File and Directory Discovery

Description: Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Many command shell utilities can be used to obtain this information. Examples include <code>dir</code>, <code>tree</code>, <code>ls</code>, <code>find</code>, and <code>locate</code>.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. <code>dir</code>, <code>show flash</code>, and/or <code>nvram</code>).(Citation: US-CERT-TA18-106A)

Some files and directories may require elevated or specific user permissions to access.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* 3PARA RAT
* 4H RAT
* ADVSTORESHELL
* AcidPour
* AcidRain
* Action RAT
* Akira
* Akira \_v2
* Amadey
* AppleSeed
* Aria-body
* Attor
* AuditCred
* AutoIt backdoor
* Avaddon
* Avenger
* AvosLocker
* Azorult
* BACKSPACE
* BADFLICK
* BADNEWS
* BBSRAT
* BLACKCOFFEE
* BLINDINGCAN
* BLUELIGHT
* BOLDMOVE
* Babuk
* BabyShark
* BackConfig
* Backdoor.Oldrea
* BadPatch
* Bandook
* Bankshot
* Bazar
* Bisonal
* Black Basta
* BlackCat
* BlackEnergy
* BlackMould
* BoomBox
* BoxCaon
* Brave Prince
* CHIMNEYSWEEP
* CHOPSTICK
* COATHANGER
* CORALDECK
* CaddyWiper
* Cannon
* Cardinal RAT
* Caterpillar WebShell
* ChChes
* CharmPower
* Cheerscrypt
* China Chopper
* Clambling
* Clop
* Cobalt Strike
* Conti
* CookieMiner
* CosmicDuke
* CreepyDrive
* Crimson
* CrossRAT
* Cryptoistic
* Cuba
* Cuckoo Stealer
* Cyclops Blink
* DDKONG
* DEATHRANSOM
* DUSTTRAP
* Dacls
* DarkGate
* DarkWatchman
* Denis
* Derusbi
* Diavol
* Doki
* DropBook
* Dtrack
* DustySky
* ELMER
* Elise
* Epic
* Exbyte
* FALLCHILL
* FIVEHANDS
* FLASHFLOOD
* FYAnti
* FatDuke
* FinFisher
* FoggyWeb
* FruitFly
* FunnyDream
* Fysbis
* Gelsemium
* GeminiDuke
* Gold Dragon
* GoldenSpy
* Gomir
* GravityRAT
* GrimAgent
* HOPLIGHT
* HTTPBrowser
* HermeticWiper
* Heyoka Backdoor
* HotCroissant
* Hydraq
* INC Ransomware
* IceApple
* Industroyer
* InnaputRAT
* InvisiMole
* Ixeshe
* JPIN
* KEYMARBLE
* KGH\_SPY
* KONNI
* Kasidet
* Kazuar
* KeyBoy
* KillDisk
* Kinsing
* Kivars
* Kwampirs
* LITTLELAMB.WOOLTEA
* Latrodectus
* LightSpy
* Linfo
* LoFiSe
* LockBit 2.0
* LockBit 3.0
* Lokibot
* LookBack
* LunarMail
* LunarWeb
* MESSAGETAP
* MacMa
* Machete
* Mafalda
* Mango
* Manjusaka
* MarkiRAT
* MegaCortex
* Megazord
* Metamorfo
* Micropsia
* MiniDuke
* Misdat
* Mispadu
* MobileOrder
* MoonWind
* MultiLayer Wiper
* NDiskMonitor
* NETEAGLE
* NETWIRE
* Nebulae
* NightClub
* Ninja
* NotPetya
* ODAgent
* OSX/Shlayer
* ObliqueRAT
* OceanSalt
* Octopus
* Okrum
* Orz
* OutSteel
* OwaAuth
* P.A.S. Webshell
* PACEMAKER
* PLEAD
* POORAIM
* POWRUNER
* Pasam
* Pcexter
* Penquin
* Peppy
* PinchDuke
* PingPull
* Pisloader
* Playcrypt
* PlugX
* PoetRAT
* PowerDuke
* Prestige
* Prikormka
* Proxysvc
* Psylo
* Pteranodon
* QakBot
* QuietSieve
* RARSTONE
* REvil
* ROADSWEEP
* ROKRAT
* RTM
* Raccoon Stealer
* RainyDay
* Ramsay
* RansomHub
* Raspberry Robin
* RedLeaves
* Remexi
* Remsec
* Rising Sun
* Rover
* Royal
* Ryuk
* SDBbot
* SHOTPUT
* SLOTHFULMEDIA
* SOUNDBITE
* SPACESHIP
* SUGARDUMP
* SUNBURST
* SUNSPOT
* Saint Bot
* Samurai
* Seasalt
* SharpDisco
* ShimRat
* SideTwist
* Siloscape
* Skidmap
* Smoke Loader
* SombRAT
* SoreFang
* Spica
* StealBit
* StreamEx
* StrifeWater
* StrongPity
* Stuxnet
* SynAck
* SysUpdate
* TAINTEDSCRIBE
* TINYTYPHON
* TSCookie
* TYPEFRAME
* Taidoor
* TajMahal
* ThreatNeedle
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UPPERCUT
* USBStealer
* USBferry
* Uroburos
* Volgmer
* WINERACK
* WannaCry
* WarzoneRAT
* WastedLocker
* WhisperGate
* WinMM
* WindTail
* Winnti for Windows
* Woody RAT
* XAgentOSX
* XCSSET
* ZIPLINE
* ZLib
* Zebrocy
* Zeus Panda
* Zox
* ZxShell
* ccf32
* down\_new
* jRAT
* metaMain
* njRAT
* yty
* zwShell

## Tools

* CrackMapExec
* Empire
* Forfiles
* Imminent Monitor
* Koadic
* PoshC2
* Pupy
* Rclone
* Remcos
* RemoteUtilities
* SILENTTRINITY
* Sliver
* cmd

## APTs (Intrusion Sets)

* APT18
* APT28
* APT3
* APT32
* APT38
* APT39
* APT41
* APT5
* Aoqin Dragon
* BRONZE BUTLER
* Chimera
* Confucius
* Dark Caracal
* Darkhotel
* Dragonfly
* FIN13
* Fox Kitten
* Gamaredon Group
* HAFNIUM
* Inception
* Ke3chang
* Kimsuky
* Lazarus Group
* Leafminer
* Lotus Blossom
* LuminousMoth
* Magic Hound
* MuddyWater
* Mustang Panda
* Patchwork
* Play
* RedCurl
* Sandworm Team
* Scattered Spider
* Sidewinder
* Sowbug
* TeamTNT
* ToddyCat
* Tropic Trooper
* Turla
* Velvet Ant
* Volt Typhoon
* Windigo
* Winnti Group
* Winter Vivern
* admin@338
* menuPass