# TTP Detail – T1057

## TTP Information

Name: Process Discovery

Description: Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or <code>Get-Process</code> via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as <code>CreateToolhelp32Snapshot</code>. In Mac and Linux, this is accomplished with the <code>ps</code> command. Adversaries may also opt to enumerate processes via `/proc`. ESXi also supports use of the `ps` command, as well as `esxcli system process list`.(Citation: Sygnia ESXi Ransomware 2025)(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show\_processes\_cisco\_cmd)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* 4H RAT
* ADVSTORESHELL
* Agent Tesla
* Akira
* Apostle
* AppleSeed
* Aria-body
* Astaroth
* Avaddon
* Avenger
* AvosLocker
* Azorult
* BACKSPACE
* BADHATCH
* BBSRAT
* BISCUIT
* BLACKCOFFEE
* BLUELIGHT
* Babuk
* BabyShark
* Backdoor.Oldrea
* Bad Rabbit
* Bankshot
* Bazar
* Bisonal
* BlackEnergy
* Bonadan
* Brave Prince
* Bumblebee
* Bundlore
* CHIMNEYSWEEP
* COATHANGER
* CaddyWiper
* Cannon
* Carbanak
* Carberp
* Carbon
* Cardinal RAT
* Caterpillar WebShell
* ChChes
* CharmPower
* Clambling
* Clop
* Cobalt Strike
* Comnie
* Conti
* Crimson
* Cuba
* Cuckoo Stealer
* Cyclops Blink
* DRATzarus
* DUSTTRAP
* Dacls
* DarkComet
* DarkGate
* DarkTortilla
* Derusbi
* Diavol
* Doki
* Dtrack
* Duqu
* DustySky
* EKANS
* ELMER
* Elise
* Emotet
* Epic
* EvilBunny
* FELIXROOT
* FatDuke
* FinFisher
* Final1stspy
* Flagpro
* FoggyWeb
* FrameworkPOS
* FruitFly
* FunnyDream
* Fysbis
* Gelsemium
* GeminiDuke
* Get2
* Gold Dragon
* Goopy
* Grandoreiro
* GravityRAT
* HALFBAKED
* HELLOKITTY
* Helminth
* Heyoka Backdoor
* HotCroissant
* Hydraq
* INC Ransomware
* IPsec Helper
* Industroyer2
* InvisiMole
* Ixeshe
* JHUHUGIT
* JPIN
* Javali
* KEYMARBLE
* KONNI
* KOPILUWAK
* Kasidet
* Kazuar
* KillDisk
* Kinsing
* Komplex
* Kwampirs
* Latrodectus
* LightSpy
* Linfo
* Lizar
* LockBit 2.0
* LockBit 3.0
* LookBack
* LoudMiner
* Lucifer
* LunarWeb
* MacMa
* Machete
* Mafalda
* MarkiRAT
* Maze
* Megazord
* Metamorfo
* Meteor
* MgBot
* Mispadu
* MobileOrder
* MoonWind
* Mosquito
* NETEAGLE
* NETWIRE
* NKAbuse
* NavRAT
* Nebulae
* NightClub
* Nightdoor
* Ninja
* ObliqueRAT
* OceanSalt
* Orz
* OutSteel
* P8RAT
* PLAINTEE
* PLEAD
* POORAIM
* POWERSTATS
* POWRUNER
* Pandora
* Pasam
* Pillowmint
* PipeMon
* PlugX
* PoetRAT
* PowerDuke
* PowerShower
* PowerStallion
* Proxysvc
* QakBot
* RATANKBA
* RCSession
* ROKRAT
* RTM
* RainyDay
* Ramsay
* RansomHub
* Raspberry Robin
* Remsec
* Rising Sun
* RogueRobin
* RotaJakiro
* Royal
* Ryuk
* SDBbot
* SHOTPUT
* SLOTHFULMEDIA
* SUNBURST
* SUNSPOT
* SVCReady
* SYSCON
* Sagerunex
* Saint Bot
* Sardonic
* Seasalt
* ShadowPad
* ShrinkLocker
* Skidmap
* SocGholish
* Socksbot
* SodaMaster
* SombRAT
* SoreFang
* StreamEx
* StrongPity
* Sykipot
* SynAck
* SysUpdate
* TAINTEDSCRIBE
* TSCookie
* Taidoor
* TajMahal
* ThiefQuest
* TrickBot
* Trojan.Karagany
* UBoatRAT
* UPSTYLE
* USBferry
* Uroburos
* Ursnif
* VERMIN
* Valak
* Volgmer
* WINERACK
* WarzoneRAT
* Waterbear
* WinMM
* Winnti for Windows
* Woody RAT
* XAgentOSX
* ZIPLINE
* Zebrocy
* Zeus Panda
* Zox
* ZxShell
* ZxxZ
* down\_new
* gh0st RAT
* iKitten
* jRAT
* macOS.OSAMiner
* metaMain
* njRAT
* yty

## Tools

* AsyncRAT
* Brute Ratel C4
* Donut
* Empire
* Imminent Monitor
* IronNetInjector
* PcShare
* PowerSploit
* Pupy
* SILENTTRINITY
* ShimRatReporter
* Tasklist

## APTs (Intrusion Sets)

* APT1
* APT28
* APT3
* APT37
* APT38
* APT5
* Andariel
* Chimera
* Darkhotel
* Deep Panda
* Earth Lusca
* Gamaredon Group
* HAFNIUM
* HEXANE
* Higaisa
* Inception
* Ke3chang
* Kimsuky
* Lazarus Group
* Magic Hound
* Molerats
* MuddyWater
* Mustang Panda
* OilRig
* Play
* Poseidon Group
* Rocke
* Sidewinder
* Stealth Falcon
* TeamTNT
* ToddyCat
* Tropic Trooper
* Turla
* Volt Typhoon
* Windshift
* Winnti Group