# TTP Detail – T1082

## TTP Information

Name: System Information Discovery

Description: An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.  
  
Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the <code>systemsetup</code> configuration tool on macOS. As an example, adversaries with user-level access can execute the <code>df -aH</code> command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. <code>show version</code>).(Citation: US-CERT-TA18-106A) On ESXi servers, threat actors may gather system information from various esxcli utilities, such as `system hostname get`, `system version get`, and `storage filesystem list` (to list storage volumes).(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)(Citation: Varonis)  
  
Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)  
  
[System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* 4H RAT
* ADVSTORESHELL
* AcidPour
* Action RAT
* Agent Tesla
* Akira
* Amadey
* Anchor
* AppleJeus
* AppleSeed
* Aria-body
* Astaroth
* Attor
* AuTo Stealer
* Avenger
* Azorult
* BACKSPACE
* BADCALL
* BADFLICK
* BADHATCH
* BISCUIT
* BLINDINGCAN
* BLUELIGHT
* BOLDMOVE
* BUBBLEWRAP
* Babuk
* BabyShark
* BackConfig
* Backdoor.Oldrea
* BadPatch
* Bandook
* Bankshot
* Bazar
* Bisonal
* Black Basta
* BlackByte Ransomware
* BlackCat
* BlackEnergy
* BlackMould
* Bonadan
* BoomBox
* Brave Prince
* Bumblebee
* Bundlore
* CARROTBAT
* CORESHELL
* CaddyWiper
* Cadelspy
* Cannon
* Carberp
* Cardinal RAT
* Caterpillar WebShell
* ChChes
* Chaes
* CharmPower
* Chrommme
* Clambling
* Comnie
* CozyCar
* Crimson
* Cuba
* Cuckoo Stealer
* Cyclops Blink
* DEADEYE
* DEATHRANSOM
* DUSTTRAP
* DarkComet
* DarkGate
* DarkTortilla
* DarkWatchman
* Denis
* Derusbi
* Diavol
* DownPaper
* Dridex
* DropBook
* Dtrack
* DustySky
* Dyre
* EVILNUM
* Egregor
* Elise
* Emissary
* EnvyScout
* Epic
* Explosive
* FALLCHILL
* FELIXROOT
* FatDuke
* Felismus
* Ferocious
* FinFisher
* Final1stspy
* FlawedAmmyy
* FunnyDream
* Fysbis
* GRIFFON
* Gelsemium
* Get2
* Gold Dragon
* GoldenSpy
* Gomir
* Gootloader
* Grandoreiro
* GravityRAT
* Green Lambert
* GrimAgent
* HALFBAKED
* HAPPYWORK
* HAWKBALL
* HELLOKITTY
* HOPLIGHT
* HermeticWiper
* Heyoka Backdoor
* Hildegard
* HotCroissant
* Hydraq
* IMAPLoader
* INC Ransomware
* IceApple
* IcedID
* Industroyer
* InnaputRAT
* InvisiMole
* Ixeshe
* JHUHUGIT
* JPIN
* KARAE
* KEYMARBLE
* KGH\_SPY
* KOCTOPUS
* KOMPROGO
* KONNI
* KOPILUWAK
* Kapeka
* Kasidet
* Kazuar
* Kerrdown
* Kessel
* Kevin
* KeyBoy
* KillDisk
* Kobalos
* Kwampirs
* LITTLELAMB.WOOLTEA
* Latrodectus
* LightNeuron
* LightSpy
* Line Dancer
* Linfo
* LiteDuke
* LitePower
* Lizar
* LockBit 2.0
* LockBit 3.0
* Lokibot
* LoudMiner
* Lucifer
* Lumma Stealer
* LunarMail
* LunarWeb
* MURKYTOP
* MacMa
* Machete
* Mafalda
* MagicRAT
* Mango
* Manjusaka
* MarkiRAT
* Maze
* Metamorfo
* Meteor
* Micropsia
* Milan
* MiniDuke
* MirageFox
* Mis-Type
* Misdat
* Mispadu
* MobileOrder
* MoleNet
* Mongall
* MoonWind
* More\_eggs
* NDiskMonitor
* NETWIRE
* NKAbuse
* NOKKI
* Naid
* NanHaiShu
* NavRAT
* Nebulae
* Neoichor
* Netwalker
* Nightdoor
* Ninja
* OSInfo
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* ObliqueRAT
* OceanSalt
* Octopus
* OilBooster
* Okrum
* OopsIE
* Orz
* PLAINTEE
* POORAIM
* POWERSTATS
* POWRUNER
* PUNCHBUGGY
* Pasam
* Pay2Key
* Penquin
* Pikabot
* PinchDuke
* PingPull
* PipeMon
* Pisloader
* PoetRAT
* Pony
* PowerDuke
* PowerShower
* Prikormka
* Proxysvc
* QakBot
* RATANKBA
* RCSession
* REvil
* ROADSWEEP
* ROKRAT
* RTM
* Raccoon Stealer
* Ramsay
* RansomHub
* Raspberry Robin
* Reaver
* RedLeaves
* Remsec
* Revenge RAT
* Rifdoor
* Rising Sun
* RogueRobin
* RotaJakiro
* Royal
* RunningRAT
* Ryuk
* S-Type
* SDBbot
* SHARPSTATS
* SHUTTERSPEED
* SLOTHFULMEDIA
* SLOWDRIFT
* SMOKEDHAM
* SOUNDBITE
* STARWHALE
* SUNBURST
* SVCReady
* SYSCON
* Sagerunex
* Saint Bot
* SampleCheck5000
* Sardonic
* ServHelper
* ShadowPad
* Shamoon
* Shark
* SharpDisco
* SharpStage
* ShrinkLocker
* SideTwist
* Skidmap
* Snip3
* SocGholish
* SodaMaster
* Solar
* SombRAT
* SoreFang
* Spark
* SpeakUp
* SpicyOmelette
* Squirrelwaffle
* SslMM
* StealBit
* StoneDrill
* StreamEx
* StrelaStealer
* StrifeWater
* StrongPity
* Stuxnet
* SynAck
* Sys10
* SysUpdate
* T9000
* TAINTEDSCRIBE
* TURNEDUP
* TYPEFRAME
* TajMahal
* ThreatNeedle
* Torisma
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UPPERCUT
* Unknown Logger
* Uroburos
* Ursnif
* VERMIN
* Valak
* Volgmer
* WINDSHIELD
* WINERACK
* WarzoneRAT
* WellMess
* WhisperGate
* WinMM
* Wingbird
* Winnti for Windows
* Woody RAT
* XAgentOSX
* XCSSET
* XLoader
* YAHOYAH
* ZLib
* Zebrocy
* ZeroCleare
* ZeroT
* Zeus Panda
* Zox
* ZxShell
* ZxxZ
* build\_downer
* down\_new
* gh0st RAT
* jRAT
* macOS.OSAMiner
* metaMain
* njRAT
* yty
* zwShell

## Tools

* AsyncRAT
* Covenant
* CrackMapExec
* Empire
* Koadic
* PoshC2
* Pupy
* QuasarRAT
* SILENTTRINITY
* ShimRatReporter
* Systeminfo
* cmd
* dsquery

## APTs (Intrusion Sets)

* APT18
* APT19
* APT3
* APT32
* APT37
* APT38
* APT41
* APT42
* Aquatic Panda
* BlackByte
* Blue Mockingbird
* CURIUM
* Chimera
* Confucius
* Daggerfly
* Darkhotel
* FIN13
* FIN8
* Gamaredon Group
* HEXANE
* Higaisa
* Inception
* Ke3chang
* Kimsuky
* Lazarus Group
* Magic Hound
* Malteiro
* Moonstone Sleet
* Moses Staff
* MuddyWater
* Mustang Panda
* Mustard Tempest
* OilRig
* Patchwork
* Play
* RedCurl
* Rocke
* Sandworm Team
* SideCopy
* Sidewinder
* Sowbug
* Stealth Falcon
* TA2541
* TeamTNT
* ToddyCat
* Tropic Trooper
* Turla
* Volt Typhoon
* Windigo
* Windshift
* Winter Vivern
* Wizard Spider
* ZIRCONIUM
* admin@338