# TTP Detail – T1033

## TTP Information

Name: System Owner/User Discovery

Description: Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Various utilities and commands may acquire this information, including <code>whoami</code>. In macOS and Linux, the currently logged in user can be identified with <code>w</code> and <code>who</code>. On macOS the <code>dscl . list /Users | grep -v '\_'</code> command can also be used to enumerate user accounts. Environment variables, such as <code>%USERNAME%</code> and <code>$USER</code>, may also be used to access this information.

On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show\_ssh\_users\_cmd\_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Action RAT
* Agent Tesla
* Agent.btz
* Amadey
* Aria-body
* AuTo Stealer
* Azorult
* BADHATCH
* BISCUIT
* BLUELIGHT
* BabyShark
* Backdoor.Oldrea
* Bazar
* BlackCat
* Bonadan
* BoomBox
* Bumblebee
* CHIMNEYSWEEP
* Cannon
* Cardinal RAT
* Caterpillar WebShell
* Chaes
* Chrommme
* Clambling
* CreepySnail
* Crimson
* Cryptoistic
* Cuckoo Stealer
* DRATzarus
* DarkComet
* DarkWatchman
* Denis
* Derusbi
* Diavol
* DnsSystem
* DownPaper
* Dyre
* EVILNUM
* Egregor
* Emotet
* Epic
* Exaramel for Linux
* Explosive
* FELIXROOT
* Felismus
* Flagpro
* FlawedAmmyy
* FunnyDream
* Gazer
* Gelsemium
* Get2
* Gold Dragon
* Goopy
* Grandoreiro
* GravityRAT
* GrimAgent
* HAPPYWORK
* HAWKBALL
* HotCroissant
* InvisiMole
* Ixeshe
* JPIN
* KONNI
* KOPILUWAK
* Kazuar
* Komplex
* Kwampirs
* Latrodectus
* Linux Rabbit
* LiteDuke
* LitePower
* Lizar
* Lokibot
* Lucifer
* LunarWeb
* MacMa
* Mafalda
* Mango
* MarkiRAT
* MechaFlounder
* Metamorfo
* MgBot
* Micropsia
* Milan
* MirageFox
* Mis-Type
* MoonWind
* More\_eggs
* Mosquito
* NDiskMonitor
* NGLite
* NOKKI
* NanHaiShu
* Neoichor
* Nightdoor
* ObliqueRAT
* Octopus
* OilBooster
* Okrum
* POWERSTATS
* POWRUNER
* PoetRAT
* PowerDuke
* PowerShower
* Prikormka
* PyDCrypt
* QUADAGENT
* QakBot
* RATANKBA
* RCSession
* RGDoor
* ROKRAT
* RTM
* Raccoon Stealer
* Raspberry Robin
* Reaver
* RedLeaves
* Remsec
* Revenge RAT
* Rifdoor
* Rising Sun
* RogueRobin
* S-Type
* SDBbot
* SHARPSTATS
* SLOTHFULMEDIA
* SMOKEDHAM
* STARWHALE
* SUNBURST
* SVCReady
* Saint Bot
* ServHelper
* ShadowPad
* SideTwist
* Small Sieve
* SocGholish
* SodaMaster
* SombRAT
* Spark
* SpeakUp
* Squirrelwaffle
* SslMM
* StrifeWater
* SynAck
* Sys10
* SysUpdate
* T9000
* TrickBot
* Trojan.Karagany
* Turian
* UPPERCUT
* Unknown Logger
* VERMIN
* Valak
* WINDSHIELD
* WINERACK
* WellMail
* WellMess
* WinMM
* Woody RAT
* XAgentOSX
* XLoader
* Zebrocy
* ZxShell
* ZxxZ
* metaMain
* njRAT
* yty
* zwShell

## Tools

* AsyncRAT
* BloodHound
* Empire
* Koadic
* NBTscan
* Pupy
* QuasarRAT
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT19
* APT3
* APT32
* APT37
* APT38
* APT39
* APT41
* Aquatic Panda
* Chimera
* Dragonfly
* Earth Lusca
* FIN10
* FIN7
* FIN8
* GALLIUM
* Gamaredon Group
* HAFNIUM
* HEXANE
* Ke3chang
* Lazarus Group
* LuminousMoth
* Magic Hound
* Moonstone Sleet
* MuddyWater
* OilRig
* Patchwork
* Sandworm Team
* Sidewinder
* Stealth Falcon
* Storm-1811
* Threat Group-3390
* Tropic Trooper
* Volt Typhoon
* Windshift
* Winter Vivern
* Wizard Spider
* ZIRCONIUM