# TTP Detail – T1016

## TTP Information

Name: System Network Configuration Discovery

Description: Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103).  
  
Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. <code>show ip route</code>, <code>show ip interface</code>).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion ) On ESXi, adversaries may leverage esxcli to gather network configuration information. For example, the command `esxcli network nic list` will retrieve the MAC address, while `esxcli network ip interface ipv4 get` will retrieve the local IPv4 address.(Citation: Trellix Rnasomhouse 2024)  
  
Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Action RAT
* Agent Tesla
* Agent.btz
* Amadey
* Anchor
* AppleSeed
* Aria-body
* Astaroth
* Avaddon
* Avenger
* Azorult
* BADCALL
* BADFLICK
* BLINDINGCAN
* BLUELIGHT
* BOLDMOVE
* BabyShark
* Backdoor.Oldrea
* Bandook
* Bazar
* Bisonal
* BlackEnergy
* Bonadan
* BoxCaon
* Brave Prince
* Calisto
* Carbon
* Catchamas
* Caterpillar WebShell
* CharmPower
* Chrommme
* Clambling
* Cobalt Strike
* Comnie
* Conti
* CreepySnail
* Crimson
* Cuba
* Cyclops Blink
* DEADEYE
* DUSTTRAP
* Denis
* Diavol
* Dtrack
* Duqu
* Dyre
* EKANS
* Elise
* Emissary
* Epic
* Explosive
* FALLCHILL
* FELIXROOT
* FatDuke
* Felismus
* Flagpro
* FunnyDream
* GeminiDuke
* GoldMax
* Gomir
* Gootloader
* Grandoreiro
* GravityRAT
* Green Lambert
* GrimAgent
* HotCroissant
* Hydraq
* IceApple
* IcedID
* Industroyer
* InvisiMole
* Ixeshe
* J-magic
* JHUHUGIT
* JPIN
* KEYMARBLE
* KONNI
* KOPILUWAK
* Kazuar
* Kessel
* Kevin
* KeyBoy
* Kobalos
* Kwampirs
* Latrodectus
* LightNeuron
* LiteDuke
* Lizar
* Lokibot
* LoudMiner
* Lucifer
* LunarLoader
* LunarWeb
* MacMa
* Machete
* Mafalda
* MagicRAT
* Manjusaka
* Milan
* Mis-Type
* MoonWind
* More\_eggs
* Mosquito
* NETWIRE
* NGLite
* NOKKI
* Naid
* NanHaiShu
* NanoCore
* Neoichor
* Nightdoor
* Ninja
* OSInfo
* OSX\_OCEANLOTUS.D
* OceanSalt
* Octopus
* Okrum
* Olympic Destroyer
* Orz
* PLAINTEE
* POWERSTATS
* POWRUNER
* Pay2Key
* Penquin
* Pikabot
* PingPull
* PipeMon
* Pisloader
* PowerDuke
* PowerShower
* Prikormka
* Proxysvc
* Pysa
* QUADAGENT
* QUIETCANARY
* QakBot
* RATANKBA
* Ramsay
* Reaver
* RedLeaves
* Remsec
* Revenge RAT
* Rifdoor
* Rising Sun
* RogueRobin
* Royal
* Ryuk
* S-Type
* SDBbot
* SHARPSTATS
* STARWHALE
* SUNBURST
* Sagerunex
* Saint Bot
* Sardonic
* ShadowPad
* Shamoon
* ShrinkLocker
* Sibot
* SideTwist
* Small Sieve
* SocGholish
* SoreFang
* SpeakUp
* SpicyOmelette
* Squirrelwaffle
* StrongPity
* Stuxnet
* Sykipot
* Sys10
* SysUpdate
* T9000
* TSCookie
* Taidoor
* TajMahal
* Torisma
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UPPERCUT
* USBferry
* Unknown Logger
* VERMIN
* Valak
* Volgmer
* WannaCry
* WellMail
* WellMess
* Woody RAT
* Xbash
* Zebrocy
* ZeroT
* cd00r
* down\_new
* iKitten
* jRAT
* xCaon
* yty
* zwShell

## Tools

* AdFind
* Arp
* CrackMapExec
* Empire
* Koadic
* NBTscan
* Nltest
* PcShare
* PoshC2
* Pupy
* QuasarRAT
* ShimRatReporter
* Sliver
* ifconfig
* ipconfig
* nbtstat
* route

## APTs (Intrusion Sets)

* APT1
* APT19
* APT3
* APT32
* APT41
* APT42
* BlackByte
* Chimera
* Darkhotel
* Dragonfly
* Earth Lusca
* FIN13
* GALLIUM
* HAFNIUM
* HEXANE
* Higaisa
* Ke3chang
* Kimsuky
* Lazarus Group
* Lotus Blossom
* Magic Hound
* Moonstone Sleet
* Moses Staff
* MuddyWater
* Mustang Panda
* Naikon
* OilRig
* Play
* SideCopy
* Sidewinder
* Stealth Falcon
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Turla
* Volt Typhoon
* Wizard Spider
* ZIRCONIUM
* admin@338
* menuPass