# TTP Detail – T1049

## TTP Information

Name: System Network Connections Discovery

Description: Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. <code>show ip sockets</code>, <code>show tcp brief</code>).(Citation: US-CERT-TA18-106A) On ESXi servers, the command `esxi network ip connection list` can be used to list active network connections.(Citation: Sygnia ESXi Ransomware 2025)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Aria-body
* BADHATCH
* Babuk
* BlackEnergy
* Carbon
* CharmPower
* Cobalt Strike
* Comnie
* Conti
* Cuba
* Dtrack
* Duqu
* Egregor
* Epic
* Flagpro
* GravityRAT
* KONNI
* KOPILUWAK
* Kwampirs
* Lizar
* Lucifer
* LunarWeb
* MESSAGETAP
* Machete
* Mafalda
* Maze
* NETWIRE
* OSInfo
* Okrum
* POWRUNER
* PlugX
* PyDCrypt
* QakBot
* RATANKBA
* Ramsay
* RedLeaves
* Remsec
* SHOTPUT
* SLOTHFULMEDIA
* Sardonic
* Sibot
* SpeakUp
* Sykipot
* Torisma
* Trojan.Karagany
* USBferry
* Volgmer
* Waterbear
* Zebrocy
* jRAT

## Tools

* CrackMapExec
* Empire
* FRP
* Net
* Pacu
* PoshC2
* Pupy
* ShimRatReporter
* Sliver
* nbtstat
* netstat

## APTs (Intrusion Sets)

* APT1
* APT3
* APT32
* APT38
* APT41
* APT5
* Andariel
* BackdoorDiplomacy
* Chimera
* Earth Lusca
* FIN13
* GALLIUM
* HEXANE
* INC Ransom
* Ke3chang
* Lazarus Group
* Lotus Blossom
* Magic Hound
* MuddyWater
* Mustang Panda
* OilRig
* Poseidon Group
* Sandworm Team
* TeamTNT
* Threat Group-3390
* ToddyCat
* Tropic Trooper
* Turla
* Velvet Ant
* Volt Typhoon
* admin@338
* menuPass