# TTP Detail – T1018

## TTP Information

Name: Remote System Discovery

Description: Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097), <code>net view</code> using [Net](https://attack.mitre.org/software/S0039), or, on ESXi servers, `esxcli network diag ping`.

Adversaries may also analyze data from local host files (ex: <code>C:\Windows\System32\Drivers\etc\hosts</code> or <code>/etc/hosts</code>) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment.

Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. <code>show cdp neighbors</code>, <code>show arp</code>).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* BADHATCH
* Backdoor.Oldrea
* Bazar
* BitPaymer
* Black Basta
* BlackCat
* Carbon
* Cobalt Strike
* Comnie
* Conti
* DRATzarus
* DUSTTRAP
* Diavol
* Epic
* Flagpro
* FunnyDream
* Gomir
* HermeticWizard
* Industroyer
* Kinsing
* Kwampirs
* MURKYTOP
* MgBot
* OSInfo
* Olympic Destroyer
* PoetRAT
* QakBot
* RATANKBA
* RansomHub
* Remsec
* SHOTPUT
* Shamoon
* SpicyOmelette
* Sykipot
* TAINTEDSCRIBE
* TrickBot
* USBferry
* WannaCry
* njRAT
* yty

## Tools

* AdFind
* Arp
* BloodHound
* CrackMapExec
* NBTscan
* Net
* Nltest
* Ping
* ROADTools
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT3
* APT32
* APT39
* APT41
* Agrius
* Akira
* BRONZE BUTLER
* BlackByte
* Chimera
* Deep Panda
* Dragonfly
* Earth Lusca
* Ember Bear
* FIN5
* FIN6
* FIN8
* Fox Kitten
* GALLIUM
* HAFNIUM
* HEXANE
* Indrik Spider
* Ke3chang
* Leafminer
* Lotus Blossom
* Magic Hound
* Naikon
* Play
* Rocke
* Sandworm Team
* Scattered Spider
* Silence
* Threat Group-3390
* ToddyCat
* Turla
* Volt Typhoon
* Wizard Spider
* menuPass