# TTP Detail – T1046

## TTP Information

Name: Network Service Discovery

Description: Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port, vulnerability, and/or wordlist scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021)

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host’s registered services on the network. For example, adversaries can use a mDNS query (such as <code>dns-sd -B \_ssh.\_tcp .</code>) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* BADHATCH
* Backdoor.Oldrea
* BlackByte Ransomware
* BlackEnergy
* Caterpillar WebShell
* China Chopper
* Cobalt Strike
* Conficker
* HDoor
* HermeticWizard
* Hildegard
* Industroyer
* InvisiMole
* LightSpy
* Lucifer
* MURKYTOP
* MgBot
* P.A.S. Webshell
* Pysa
* Ramsay
* Remsec
* Royal
* SpeakUp
* XTunnel
* Xbash
* ZxShell

## Tools

* Brute Ratel C4
* Empire
* FRP
* Koadic
* NBTscan
* Peirates
* PoshC2
* Pupy
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT32
* APT39
* APT41
* Agrius
* BackdoorDiplomacy
* BlackByte
* BlackTech
* Chimera
* Cobalt Group
* DarkVishnya
* Ember Bear
* FIN13
* FIN6
* Fox Kitten
* INC Ransom
* Lazarus Group
* Leafminer
* Lotus Blossom
* Magic Hound
* Naikon
* OilRig
* RedCurl
* Rocke
* Suckfly
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Volt Typhoon
* menuPass