# TTP Detail – T1135

## TTP Information

Name: Network Share Discovery

Description: Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the <code>net view \\\\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>. For macOS, the <code>sharing -l</code> command lists all shared points used for smb services.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Akira
* Avaddon
* AvosLocker
* BADHATCH
* Babuk
* Bad Rabbit
* Bazar
* BitPaymer
* BlackByte 2.0 Ransomware
* BlackByte Ransomware
* BlackCat
* Clambling
* Clop
* Cobalt Strike
* Conti
* Cuba
* DEATHRANSOM
* DUSTTRAP
* Diavol
* Emotet
* FIVEHANDS
* Flagpro
* HELLOKITTY
* INC Ransomware
* IcedID
* InvisiMole
* KOPILUWAK
* Kwampirs
* Latrodectus
* LockBit 2.0
* LockBit 3.0
* LunarWeb
* MURKYTOP
* OSInfo
* Olympic Destroyer
* PlugX
* QakBot
* QuietSieve
* Ramsay
* RansomHub
* Royal
* Sardonic
* ShimRat
* Stuxnet
* TrickBot
* WastedLocker
* WhisperGate
* Zebrocy

## Tools

* CrackMapExec
* Empire
* Koadic
* Net
* Pupy
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT1
* APT32
* APT38
* APT39
* APT41
* BlackByte
* Chimera
* DarkVishnya
* Dragonfly
* FIN13
* INC Ransom
* Sowbug
* Tonto Team
* Tropic Trooper
* Wizard Spider