# TTP Detail – T1021.002

## TTP Information

Name: SMB/Windows Admin Shares

Description: Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.  
  
SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.  
  
Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over SMB,(Citation: Wikipedia Server Message Block) to interact with systems using remote procedure calls (RPCs),(Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) and certain configuration and patch levels.(Citation: Microsoft Admin Shares)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* Anchor
* BlackByte Ransomware
* BlackEnergy
* Cobalt Strike
* Conficker
* Conti
* Diavol
* Duqu
* Emotet
* HermeticWizard
* Kwampirs
* LockBit 2.0
* LockBit 3.0
* Lucifer
* Net Crawler
* NotPetya
* Olympic Destroyer
* RansomHub
* Regin
* Royal
* Ryuk
* Shamoon
* Stuxnet
* Zox
* reGeorg
* zwShell

## Tools

* Brute Ratel C4
* Net
* PsExec

## APTs (Intrusion Sets)

* APT28
* APT3
* APT32
* APT39
* APT41
* Aquatic Panda
* BlackByte
* Blue Mockingbird
* Chimera
* Cinnamon Tempest
* Deep Panda
* FIN13
* FIN8
* Fox Kitten
* Ke3chang
* Lazarus Group
* Moses Staff
* Orangeworm
* Play
* Sandworm Team
* Storm-1811
* Threat Group-1314
* ToddyCat
* Turla
* Velvet Ant
* Wizard Spider