# TTP Detail – T1021.001

## TTP Information

Name: Remote Desktop Protocol

Description: Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* Carbanak
* Cobalt Strike
* DarkComet
* Pysa
* Revenge RAT
* SDBbot
* ServHelper
* WarzoneRAT
* ZxShell
* jRAT
* njRAT
* reGeorg
* zwShell

## Tools

* Imminent Monitor
* Koadic
* Pupy
* QuasarRAT

## APTs (Intrusion Sets)

* APT1
* APT3
* APT39
* APT41
* APT5
* Agrius
* Akira
* Aquatic Panda
* Axiom
* BlackByte
* Blue Mockingbird
* Chimera
* Cobalt Group
* Dragonfly
* FIN10
* FIN13
* FIN6
* FIN7
* FIN8
* Fox Kitten
* HEXANE
* INC Ransom
* Indrik Spider
* Kimsuky
* Lazarus Group
* Leviathan
* Magic Hound
* OilRig
* Patchwork
* Silence
* Volt Typhoon
* Wizard Spider
* menuPass