Remote Services: Remote Desktop Protocol

Other sub-techniques of Remote Services (8)

Adversaries may use Valid Accounts 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).[1]

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 or Terminal Services DLL for Persistence.[2]

ID: T1021.001

Sub-technique of: T1021

ⓘ Tactic: Lateral Movement

ⓘ Platforms: Windows

ⓘ System Requirements: RDP service enabled, account in the Remote Desktop Users group

Contributors: Matthew Demaske, Adaptforward

Version: 1.2

Created: 11 February 2020

Last Modified: 07 August 2023

Version Permalink

Procedure Examples

ID	Name	Description
G1030	Agrius	Agrius tunnels RDP traffic through deployed web shells to access victim environments via compromised accounts.[3] Agrius used the Plink tool to tunnel RDP connections for remote access and lateral movement in victim environments.[4]
G0006	APT1	The APT1 group is known to have used RDP during operations.[5]
G0022	APT3	APT3 enables the Remote Desktop Protocol for persistence.[6] APT3 has also interacted with compromised systems to browse and copy files through RDP sessions.[7]
G0087	APT39	APT39 has been seen using RDP for lateral movement and persistence, in some cases employing the rdpwinst tool for mangement of multiple sessions.[8][9]
G0096	APT41	APT41 used RDP for lateral movement.[10][11] APT41 used NATBypass to expose local RDP ports on compromised systems to the Internet.[12]
G1023	APT5	APT5 has moved laterally throughout victim environments using RDP.[13]
G0143	Aquatic Panda	Aquatic Panda leveraged stolen credentials to move laterally via RDP in victim environments.[14]
G0001	Axiom	Axiom has used RDP during operations.[15]
G0108	Blue Mockingbird	Blue Mockingbird has used Remote Desktop to log on to servers interactively and manually copy files to remote hosts.[16]
C0015	C0015	During C0015, the threat actors used RDP to access specific network hosts of interest.[17]