Remote Services: Remote Desktop Protocol, Sub-technique T1021.001 - Enterprise

Archived: 2026-04-05 18:39:38 UTC

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]

G1024 Akira

Akira has used RDP for lateral movement.[5]

G0006 APT1

The APT1 group is known to have used RDP during operations.[6]

C0051 APT28 Nearest Neighbor Campaign

During APT28 Nearest Neighbor Campaign, APT28 used RDP for lateral movement.[7]

G0022 APT3

APT3 enables the Remote Desktop Protocol for persistence.[8] APT3 has also interacted with compromised systems to browse and copy files through RDP sessions.[9]

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.[10][11]

G0096 APT41

APT41 used RDP for lateral movement.[12][13] APT41 used NATBypass to expose local RDP ports on compromised systems to the Internet.[14]

G1023 APT5

APT5 has moved laterally throughout victim environments using RDP.[15]

G0143 Aquatic Panda

Aquatic Panda leveraged stolen credentials to move laterally via RDP in victim environments.[16]

G0001 Axiom

Axiom has used RDP during operations.[17]

G1043 BlackByte

BlackByte has used RDP to access other hosts within victim networks.[18][19]

G0108 Blue Mockingbird

Blue Mockingbird has used Remote Desktop to log on to servers interactively and manually copy files to remote hosts.[20]

C0015 C0015

During C0015, the threat actors used RDP to access specific network hosts of interest.[21]

C0018 C0018

During C0018, the threat actors opened a variety of ports to establish RDP connections, including ports 28035, 32467, 41578, and 46892.[22]

C0032 C0032

During the C0032 campaign, TEMP.Veles utilized RDP throughout an operation.[23]

S0030 Carbanak

Carbanak enables concurrent Remote Desktop Protocol (RDP) sessions.[24]

G0114 Chimera

Chimera has used RDP to access targeted systems.[25]

G0080 Cobalt Group

Cobalt Group has used Remote Desktop Protocol to conduct lateral movement.[26]

S0154 Cobalt Strike

Cobalt Strike can start a VNC-based remote desktop server and tunnel the connection through the already established C2 channel.[27][28]

C0029 Cutting Edge

During Cutting Edge, threat actors used RDP with compromised credentials for lateral movement.[29]

S0334 DarkComet

DarkComet can open an active screen of the victim's machine and take control of the mouse and keyboard.[30]

G0035 Dragonfly

Dragonfly has moved laterally via RDP.[31]

G0051 FIN10

FIN10 has used RDP to move laterally to systems in the victim environment.[32]

G1016 FIN13

FIN13 has remotely accessed compromised environments via Remote Desktop Services (RDS) for lateral movement.[33]

G0037 FIN6

FIN6 used RDP to move laterally in victim networks.[34][35]

G0046 FIN7

FIN7 has used RDP to move laterally in victim environments.[36]

G0061 FIN8

FIN8 has used RDP for lateral movement.[37]

G0117 Fox Kitten

Fox Kitten has used RDP to log in and move laterally in the target environment.[38][39]

G1001 HEXANE

HEXANE has used remote desktop sessions for lateral movement.[40]

C0038 HomeLand Justice

During HomeLand Justice, threat actors primarily used RDP for lateral movement in the victim environment.[41][42]

S0434 Imminent Monitor

Imminent Monitor has a module for performing remote desktop access.[43]

G1032 INC Ransom

INC Ransom has used RDP to move laterally.[44][45][46][47]

G0119 Indrik Spider

Indrik Spider has used RDP for lateral movement.[48]

S0283 jRAT

jRAT can support RDP control.[49]

G0094 Kimsuky

Kimsuky has used RDP for direct remote point-and-click access.[50]

S0250 Koadic

Koadic can enable remote desktop on the victim's machine.[51]

G0032 Lazarus Group

Lazarus Group malware SierraCharlie uses RDP for propagation.[52][53]

G0065 Leviathan

Leviathan has targeted RDP credentials and used it to move through the victim environment.[54]

G0059 Magic Hound

Magic Hound has used Remote Desktop Services to copy tools on targeted systems.[55][56]

G1051 Medusa Group

Medusa Group has used RDP to conduct lateral movement and exfiltrate data.[57] Medusa Group has also utilized the Windows executable `mstsc.exe` for RDP activities through the command `mstsc.exe /v:{hostname/ip}`.[57]

G0045 menuPass

menuPass has used RDP connections to move across the victim network.[58][59]

S0385 njRAT

njRAT has a module for performing remote desktop access.[60]

G0049 OilRig

OilRig has used Remote Desktop Protocol for lateral movement. The group has also used tunneling tools to tunnel RDP into the environment.[61][62][13][63][63]

G0040 Patchwork

Patchwork attempted to use RDP to move laterally.[64]

S0192 Pupy

Pupy can enable/disable RDP connection and can start a remote desktop session using a browser web socket client.[65]

S0583 Pysa

Pysa has laterally moved using RDP connections.[66]

S0262 QuasarRAT

QuasarRAT has a module for performing remote desktop access.[67][68]

S1187 reGeorg

reGeorg can be used to tunnel RDP connections.[69]

S0379 Revenge RAT

Revenge RAT has a plugin to perform RDP access.[70]

G1015 Scattered Spider

Scattered Spider has used RDP to enable lateral movement.[71]

S0461 SDBbot

SDBbot has the ability to use RDP to connect to victim's machines.[72]

S0382 ServHelper

ServHelper has commands for adding a remote desktop user and sending RDP traffic to the attacker through a reverse SSH tunnel.[73]

G0091 Silence

Silence has used RDP for lateral movement.[74]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used RDP sessions from public-facing systems to internal servers.[75]

G1017 Volt Typhoon

Volt Typhoon has moved laterally to the Domain Controller via RDP using a compromised account with domain administrator privileges.[76]

S0670 WarzoneRAT

WarzoneRAT has the ability to control an infected PC using RDP.[77]

G0102 Wizard Spider

Wizard Spider has used RDP for lateral movement and to deploy ransomware interactively.[78][79][80][81]

S0350 zwShell

zwShell has used RDP for lateral movement.[82]

S0412 ZxShell

ZxShell has remote desktop functionality.[83]
