

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Search

Sign in

Sign up

jsecurity101 / MSRPC-to-ATTACK

Public

Notifications

Fork

40

Star

308

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

Files

ddd4608

Go to file

> .github

▼ documents

MS-DFSNM.md

MS-DRSR.md

MS-EFSR.md

MS-FSRVP.md

MS-LSAD-LSAT.md

MS-NRPC.md

MS-RPRN-PAR.md

MS-RRP.md

MS-SAMR.md

MS-SCMR.md

**MS-SRVS.md**

MS-TSCH.md

MS-WKST.md

template.md

> images

README.md

MSRPC-to-ATTACK / documents / MS-SRVS.md

Jonathan Johnson and Jonathan Johnson

Pre Mitre EU update

01e9ddf · 3 years ago

History

Preview

Code

Blame

78 lines (58 loc) · 3.07 KB

Raw

Protocol:

[Server Service Remote Protocol \(MS-SRVS\)](#)

Interface UUID:

- 4b324fc8-1670-01d3-1278-5a47bf6ee188

Server Binary:

srvsvc.dll

 (loads into) 

svchost.exe

Endpoint:

- ncacn\_np: \PIPE\srvsvc

ATT&CK Relation:

- [T1018 - Remote System Discovery](#)
- System Enumeration

Indicator of Activity (IOA):

- Network:
  - Inbound network connections to System over port 445
  - Network connection to pipe - \pipe\srvsvc
  - Methods:
    - NetSessionEnum
- Host:
  - Window Security Event 5145 (Detailed Network File Share):
    - Share Name: IPC\$
    - Relative Target Name: \pipe\srvsvc
    - Look at the user who made the connection
    - Access Request Information: Access Mask (0x3 or higher) ( ReadData or ListDirectory + WriteData or AddFile )

Note::

 BH has been seen to have the hardcoded rights: 0x12019f (READ\_CONTROL, SYNCHRONIZE, ReadData (or ListDirectory), WriteData (or AddFile), AppendData (or AddSubdirectory or CreatePipeInstance), ReadEA, WriteEA , ReadAttributes, WriteAttributes)

- Ransomware has been known to shut off the Lanman Server Service

## Prevention Opportunities:

- Prevent relay attacks by enabling SMB signing:
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature = 1`
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature = 1`
- MSFT link for guidance: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing>
- [NetCease](#): Changes  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\SrvsvcInfo` binary value
- RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=4b324fc8-1670-01d3-1278
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;BA
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=4b324fc8-1670-01d3-1278
add filter
quit
```

- RPC filter to only allow Administrators

## Notes:

- Adding `NT AUTHORITY\BATCH, NT AUTHORITY\INTERACTIVE, NT AUTHORITY\SERVICE` to filter might help with compatibility/functionality issues.
- Lanman Server
  - System Enumeration:
    - User Session Enumuration ( `NetSessionEnum/NetrSessionEnum` )
    - Share Enumeration ( `NetShareEnum/NetrShareEnum` )
    - Connection Enumeration ( `NetConnectionEnum/NetrConnectionEnum` )
    - File Enumeration ( `NetFileEnum/NetrFileEnum` )
- Often seen with BH activity
- Look for connection to named pipe (both client and server)

## Useful Resources:

- <https://www.darktrace.com/en/blog/making-the-red-team-wave-the-white-flag-with-darktrace-ai/> <https://www.sentinelone.com/blog/deep-dive-exploring-an-ntlm-brute-force-attack-with-bloodhound/> <https://en.hackndo.com/ntlm-relay/>
- <https://github.com/p0w3rsh3ll/NetCease>