

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-DRSR.md

Jonathan Johnson and Jonathan Johnson Pre Mitre EU update 01e9ddf · 3 years ago History

Preview

Code

Blame

82 lines (59 loc) · 3.08 KB

Raw

Protocol:

Directory Replication Service (MS-DRSR)

Interface UUID:

e3514235-4b06-11d1-ab04-00c04fc2dcd2

Server Binary:

ntdsai.dll (loads into) lsass.exe on DCs.

Endpoint:

ncacn\_ip\_tcp

ATT&CK Relation:

T1003.006 - DCSync

T1207 - Rogue Domain Controller

Indicator of Activity (IOA):

Network:

Methods:

DCSync:

IDL\_DRSCrackNames

IDL\_DRSGetNCChanges

DCShadow:

IDL\_DRAddEntry

IDL\_DRUpdateRefs

IDL\_DRReplicaAdd

Host:

Inbound network connection to LSASS on domain controllers over TCP\_IP Port.

Access to the Domain-DNS Class object {19195a5b-6da0-11d0-afd3-00c04fd930c9} with extended rights:

{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} -DS-Replication-Get-Change

Page 1 of 2

- {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} - DS-Replication-Get-Changes-All
  - Window Security Event 4662
- DCSshadow specific:
  - Seeing hosts be promoted to a global category server (GC)

## Prevention Opportunities:

- Remove the replication based extended rights from DA's.
- For force replication - create a new group and apply extended rights. Only use this group on a case by case basis.
- Remove traffic ability between workstation <-> domain controllers (DC <-> DC is normal traffic) (firewall or rpc filter)

RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=e3514235-4b06-11d1-ab04
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DD
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=e3514235-4b06-11d1-ab04
add filter
quit
```

- Filter forces the interface e3514235-4b06-11d1-ab04-00c04fc2dcd2 to only accept calls coming from other DCs (the DD in the SDDL string).

## Notes:

- RPC filter hasn't been tested in production. Things to keep in mind if pushed out:
  - gpupdate.exe will fail on workstations. Use Invoke-GPUUpdate on DC's.
  - Functionality issues may arise as a good amount of services/actions leverage replication within their process. Name conversions allow clients to map the different names used to identify directory service objects through DsCrackNames under the hood which is apart of this RPC interface.
    - Example - Splunk Universal Forwarder can use DsCrackNames to help with name resolution.
  - Force replication by a user on a domain controller will fail.
  - Normal replication will occur as needed by the DC.
  - Andrew Robbins suggests restricting domain admins interactive logons on DCs. Aka - don't allow DA's to login to hosts within the organization, but create groups for specific use cases.

## Useful Resources:

- <https://adsecurity.org/?p=1729>
- <https://attack.mitre.org/techniques/T1003/006/>
- <https://medium.com/@jsecurity101/syncing-into-the-shadows-bbd656dd14c8>