

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-RRP.md

Jonathan Johnson and Jonathan Johnson

Pre Mitre EU update

01e9ddf · 3 years ago

History

Preview

Code

Blame

57 lines (45 loc) · 1.73 KB

Raw

Protocol:

Remote Registry (MS-RRP)

Interface UUID:

338CD001-2244-31F1-AAAA-900038001003

Server Binary:

regsvc.dll

 (loads into) 

svchost.exe

Endpoint:

ncacn\_np: \PIPE\winreg

ATT&CK Relation:

T1112 - Modify Registry

T1012 - Query Registry

Indicator of Activity (IOA):

Network:

Methods:

BaseRegCreateKey

BaseRegQueryInfoKey

BaseRegSetValue

Host:

Inbound network connection to: System over \pipe\winreg

Registry key modifications

Sysmon Event ID 12/13

Native windows binary to interact with registry remotely: reg.exe (look for ADD/QUERY parameters)

Process creation events

Remote Registry Service start type changed

Prevention Opportunities:

Turn off the remote registry service and disable it.

Modify permissions on sensitive registry keys

RPC Filter Example:

Page 1 of 2

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=338CD001-2244-31F1-AAAA
add condition field=remote_user_token matchtype=equal data=D:(A;;KA;;;DA
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32
add filter
quit
```



## Notes:

- By default local administrators can start the remote registry service and interact with the registry remotely.
- If remote registry is an operational need, create a group specific to this action. Apply changes to the registry/rpc filter.

## Useful Resources:

- <https://car.mitre.org/analytics/CAR-2014-11-005/>