MSRPC ATT&CK Mapping

red canary

Presenter

Jonny Johnson

Sr. Threat Researcher

RED CANARY

@jsecurity101

Previously: Detection Engineer @SpecterOps

Host on Detection: Challenging Paradigms Podcast

Publications:

- Blog: https://jsecurity101.medium.com/
- RPC Research Paper: https://specterops.io/assets/resources/RPC_for_Detection_Engineers.pdf

Projects: https://github.com/jsecurity101

Areas of Interest: Windows Internals, All Things Data, Reverse Engineering, Technique Abstraction, and IPC Mechanisms.

red canary

Overview

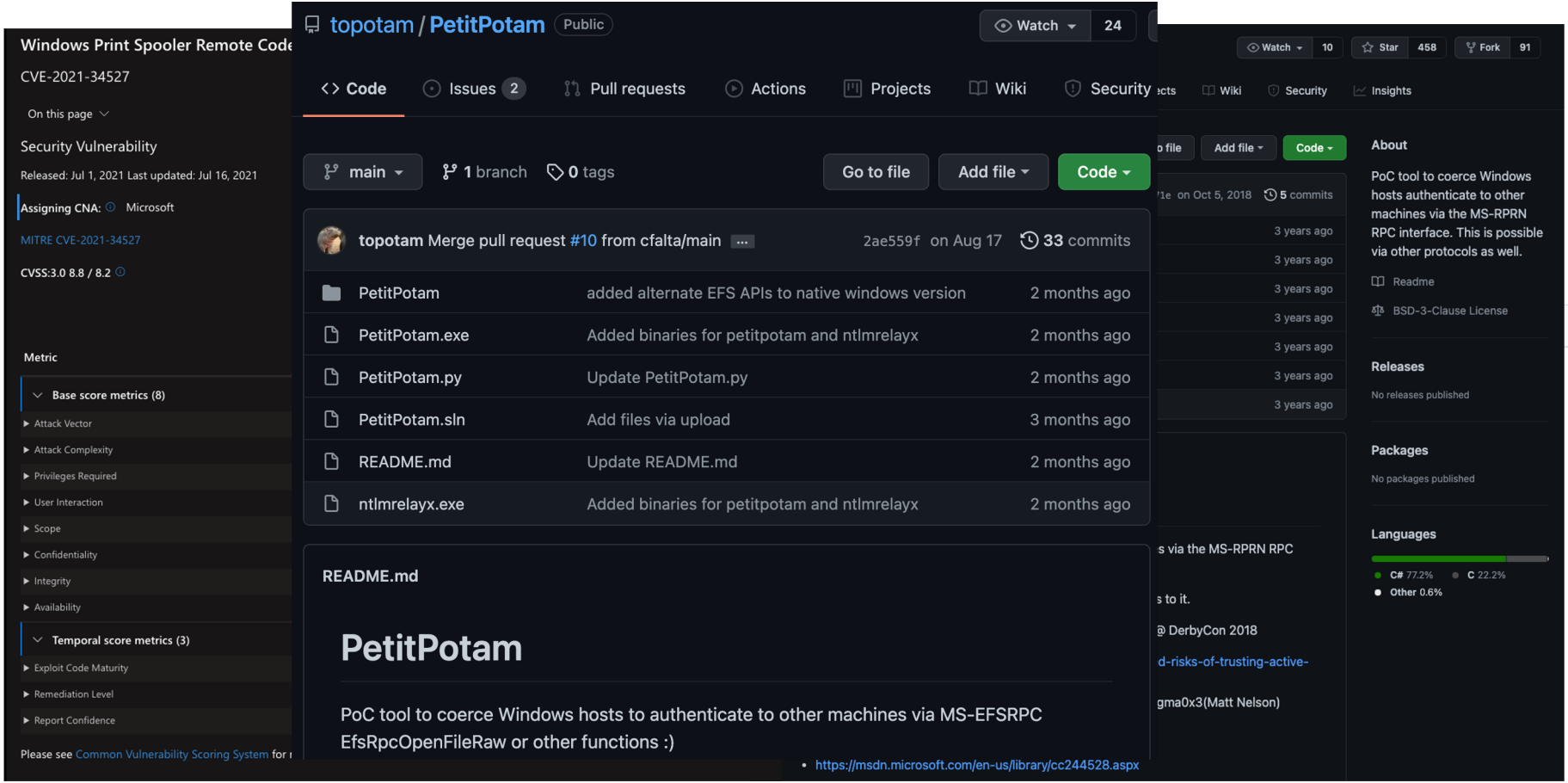
RPC Attack Volume

Explore a small set of attacks that leverage MSRPC
The significance of those attacks in 2021

Impact of mapping MSRPC to ATT&CK

What is involved within this project.
How can this information be used to help defenders.

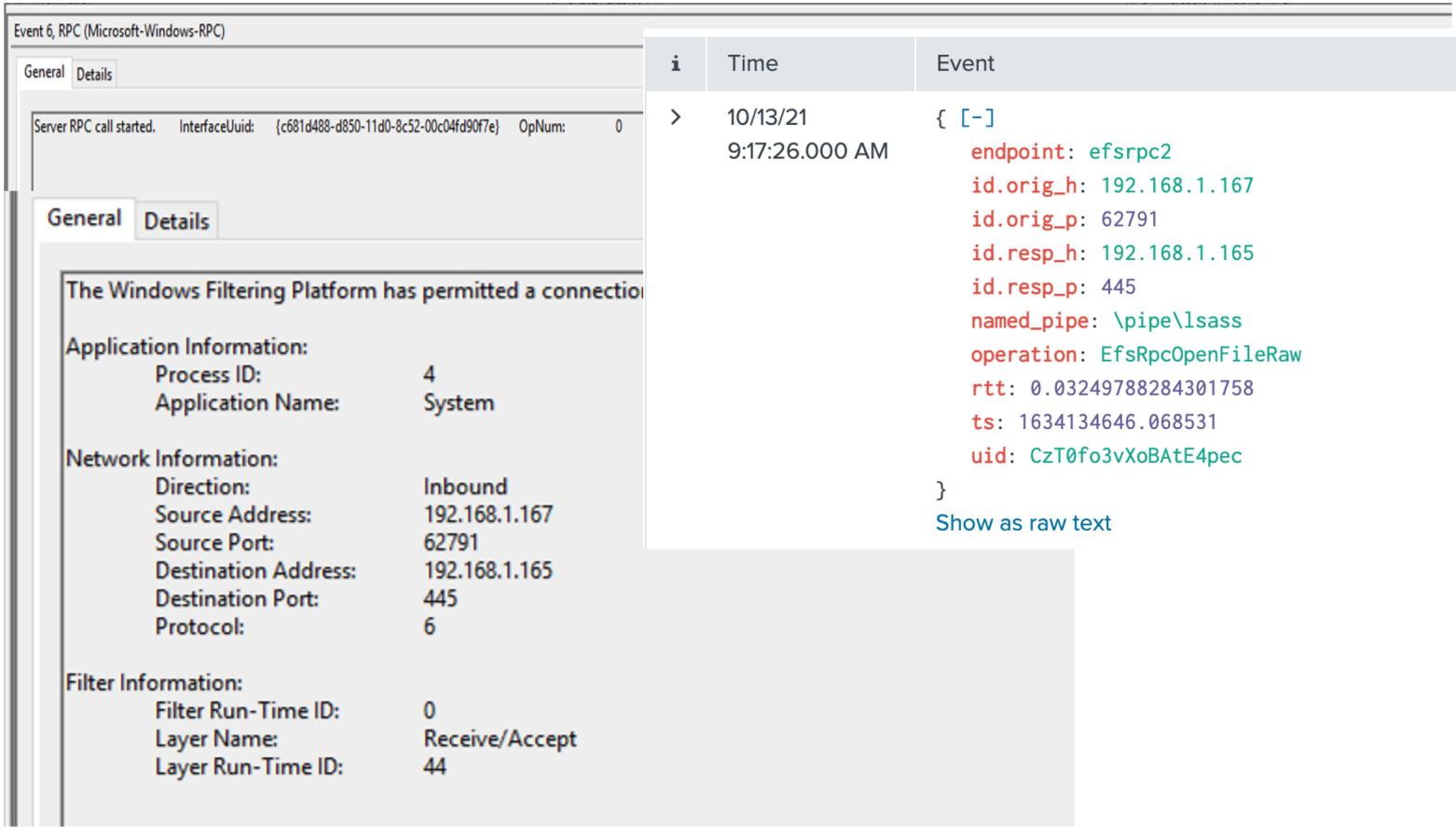
red canary


Windows Print Spooler Remote Code
CVE-2021-34527
On this page
Security Vulnerability
Released: Jul 1, 2021 Last updated: Jul 16, 2021
Assigning CNA: Microsoft
MITRE CVE-2021-34527
CVSS:3.0 8.8 / 8.2
Metric
Base score metrics (8)
Attack Vector
Attack Complexity
Privileges Required
User Interaction
Scope
Confidentiality
Integrity
Availability
Temporal score metrics (3)
Exploit Code Maturity
Remediation Level
Report Confidence
Please see Common Vulnerability Scoring System for
topotam / PetitPotam
Public
Watch 24
Code
Issues 2
Pull requests
Actions
Projects
Wiki
Security
main
1 branch
0 tags
Go to file
Add file
Code
topotam Merge pull request #10 from cfalta/main
2ae559f on Aug 17
33 commits
PetitPotam added alternate EFS APIs to native windows version 2 months ago
PetitPotam.exe Added binaries for petitpotam and ntlmrelayx 2 months ago
PetitPotam.py Update PetitPotam.py 2 months ago
PetitPotam.sln Add files via upload 3 months ago
README.md Update README.md 2 months ago
ntlmrelayx.exe Added binaries for petitpotam and ntlmrelayx 2 months ago
README.md
PetitPotam
PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions :)
https://msdn.microsoft.com/en-us/library/cc244528.aspx
Watch 10
Star 458
Fork 91
Wiki
Security
Insights
Add file
Code
on Oct 5, 2018
5 commits
3 years ago
3 years ago
3 years ago
3 years ago
3 years ago
3 years ago
s via the MS-RPRN RPC
s to it.
@ DerbyCon 2018
d-risks-of-trusting-active-
gma0x3(Matt Nelson)
About
PoC tool to coerce Windows hosts authenticate to other machines via the MS-RPRN RPC interface. This is possible via other protocols as well.
Readme
BSD-3-Clause License
Releases
No releases published
Packages
No packages published
Languages
C# 77.2%
C 22.2%
Other 0.6%

Fact

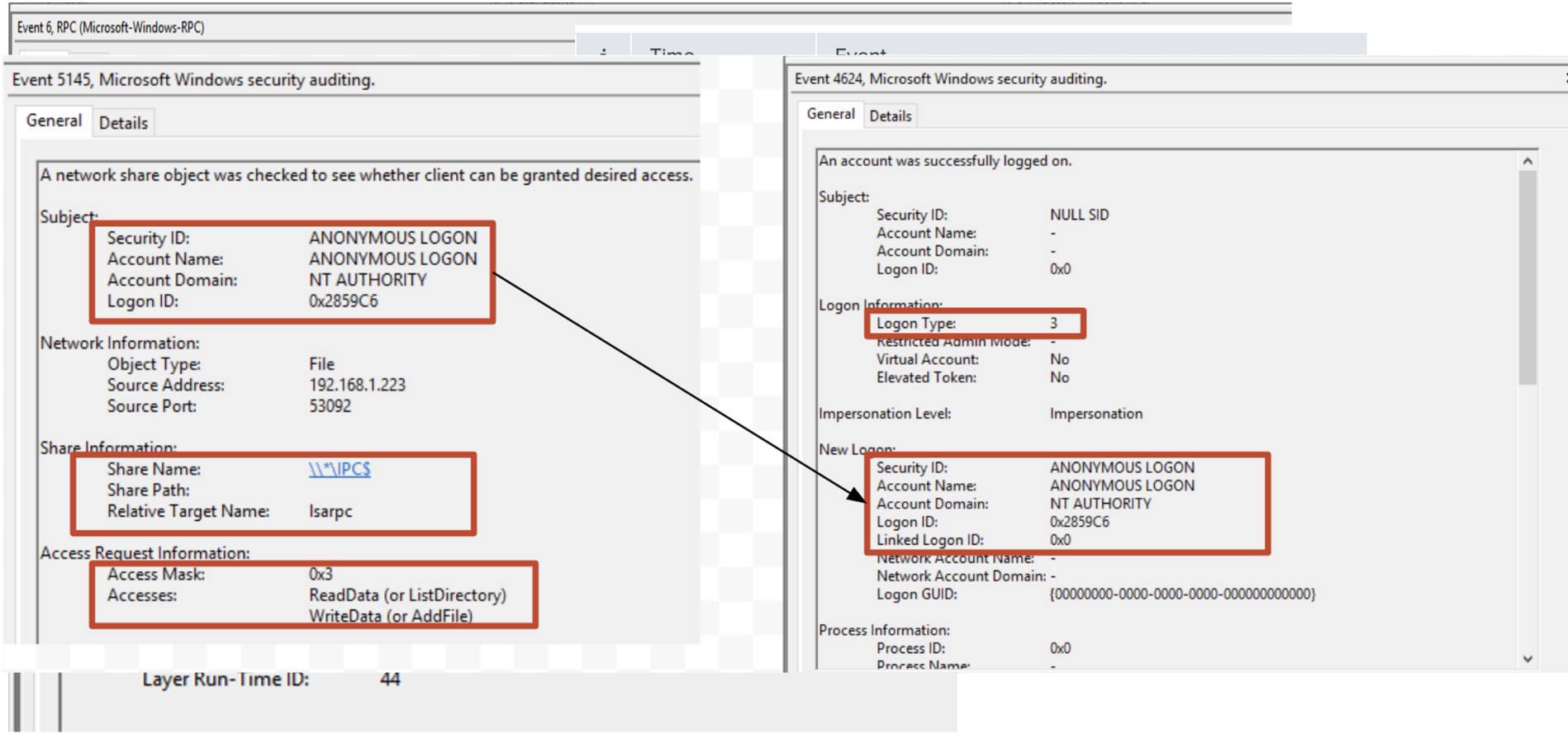
These aren’t the first attacks to leverage MSRPC, they won’t be the last.

red canary



i	Time	Event
>	10/13/21 9:17:26.000 AM	{ [-] endpoint: efsrpc2 id.orig_h: 192.168.1.167 id.orig_p: 62791 id.resp_h: 192.168.1.165 id.resp_p: 445 named_pipe: \pipe\lsass operation: EfsRpcOpenFileRaw rtt: 0.03249788284301758 ts: 1634134646.068531 uid: CzT0fo3vXoBAtE4pec } Show as raw text

red canary


Event 6, RPC (Microsoft-Windows-RPC)
Event 5145, Microsoft Windows security auditing.
General
Details
A network share object was checked to see whether client can be granted desired access.
Subject:
Security ID: ANONYMOUS LOGON
Account Name: ANONYMOUS LOGON
Account Domain: NT AUTHORITY
Logon ID: 0x2859C6
Network Information:
Object Type: File
Source Address: 192.168.1.223
Source Port: 53092
Share Information:
Share Name: *\IPC$
Share Path:
Relative Target Name: lsarpc
Access Request Information:
Access Mask: 0x3
Accesses: ReadData (or ListDirectory)
WriteData (or AddFile)
Layer Run-Time ID: 44
Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Information:
Logon Type: 3
Virtual Account: No
Elevated Token: No
Impersonation Level: Impersonation
New Logon:
Security ID: ANONYMOUS LOGON
Account Name: ANONYMOUS LOGON
Account Domain: NT AUTHORITY
Logon ID: 0x2859C6
Linked Logon ID: 0x0
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0x0

red canary

Overview

MSRPC to ATT&CK

MSRPC-To-ATT&CK-Mapping

A repository that maps commonly used MSRPC protocols to Mitre ATT&CK while providing context around potential indicators of activity, prevention opportunities, and related RPC information.

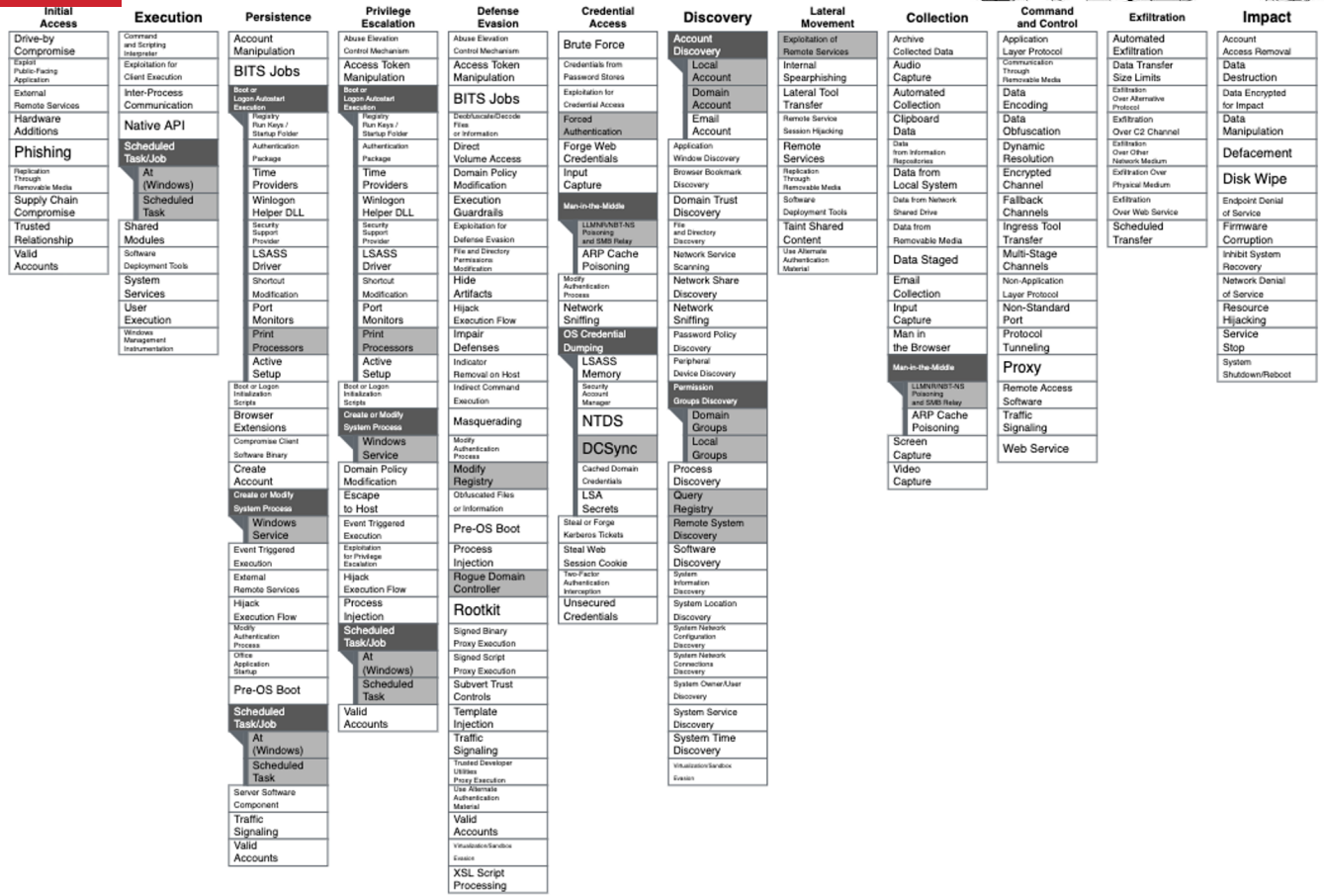
List of MSRPC Protcols:

- MS-SCMR: Service Control Manager Remote Protocol
  - MS-SCMR.md
- MS-DRSR: Directory Replication Service Remote Protocol
  - MS-DRSR.md
- MS-RRP: Windows Remote Registry Remote Protocol
  - MS-RRP.md
- MS-TSCH: Task Scheduler Service Remoting Protocol
  - MS-TSCH.md
- MS-WKST: Workstation Service Remote Protocol
  - MS-WKST.md
- MS-SRVS: Server Service Remote Protocol
  - MS-SRVS.md
- MS-RPRN: Print System Remote Protocol
  - MS-RPRN.md
- MS-PAR: Print System Asynchronous Remote Protocol
  - MS-PAR.md
- MS-SAMR: Security Account Manager Remote Protocol
  - MS-SAMR.md
- MS-LSAD: Local Security Authority (Domain Policy) Remote Protocol
  - MS-LSAD.md
- MS-LSAT: Local Security Authority (Translation Methods) Remote Protocol
  - MS-LSAT.md
- MS-EFSR: Encrypting File System Remote (EFSRPC) Protocol
  - MS-EFSR.md
- MS-NRPC: Netlogon Remote Protocol
  - MS-NRPC.md

red canary

ATT&CK Mapping

MSRPC to ATT&CK

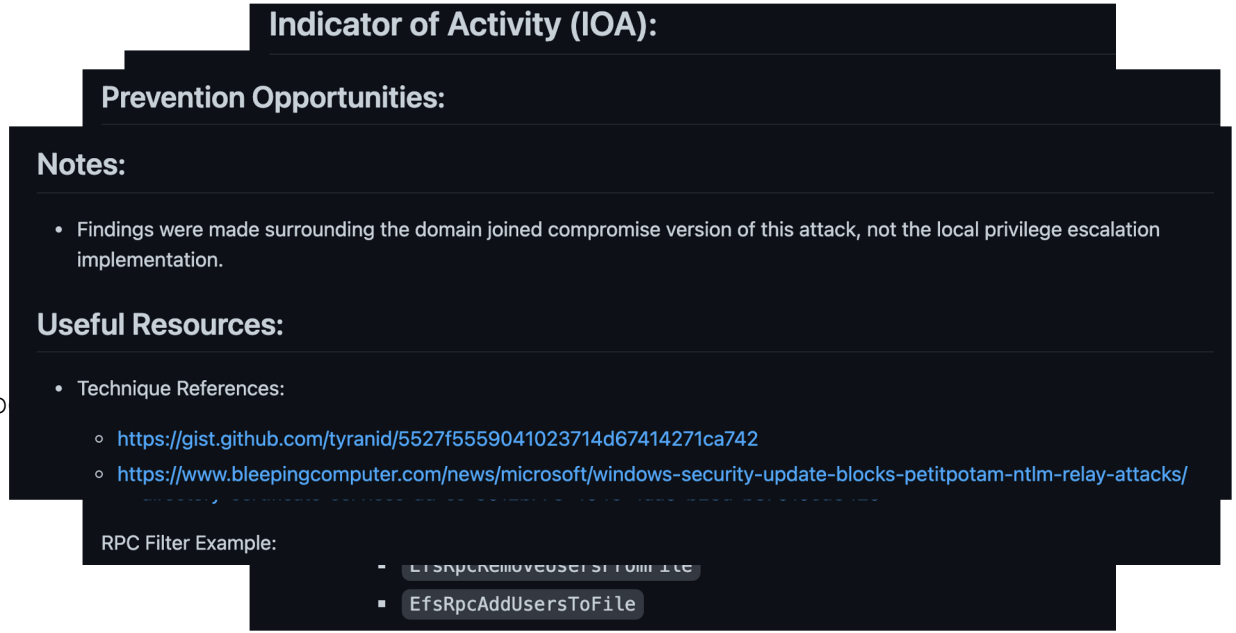


red canary

MSRPC to ATT&CK

Document Contents:

- Protocol Name
- Interface UUID
- Server Binary
- Interface's Transport Proto
- ATT&CK Relation
- Indicator of Activity (IOA)
- Prevention Opportunities
- Notes
- Useful Resources



MSRPC to ATT&CK

How can this be used?:

- As a reference:
  - General information regarding a MSRPC protocol
  - Attack understanding
  - Detection strategies
  - Data gaps
  - Preventive strategies

The goal is to add more to this project as time goes on :)

red canary

THIS IS A CALL TO ACTION

Get started with MSRPC to ATT&CK

https://github.com/jsecurity101/MSRPC-to-ATTACK

red canary