

MSRPC ATT&CK

Mapping



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.

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.

Windows Print Spooler Remote Code Execution

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 more information

Code

Issues 2

Pull requests

Actions

Projects

Wiki

Security

Events

Wiki

Security

Insights

main

1 branch

0 tags

Go to file

Add file

Code

file

Add file

Code

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



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>

s via the MS-RPRN RPC

s to it.

@ DerbyCon 2018

d-risks-of-trusting-active-

gma0x3(Matt Nelson)

Fact

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



Event 6, RPC (Microsoft-Windows-RPC)

[General](#) [Details](#)

Server RPC call started. InterfaceUuid: {c681d488-d850-11d0-8c52-00c04fd90f7e} OpNum: 0

[General](#) [Details](#)

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID: 4
Application Name: System

Network Information:

Direction: Inbound
Source Address: 192.168.1.167
Source Port: 62791
Destination Address: 192.168.1.165
Destination Port: 445
Protocol: 6

Filter Information:

Filter Run-Time ID: 0
Layer Name: Receive/Accept
Layer Run-Time ID: 44

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](#)

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:	\\\IPCS
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

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
Restricted Admin Mode:	-
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 Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Overview

MSRPC to ATT&CK

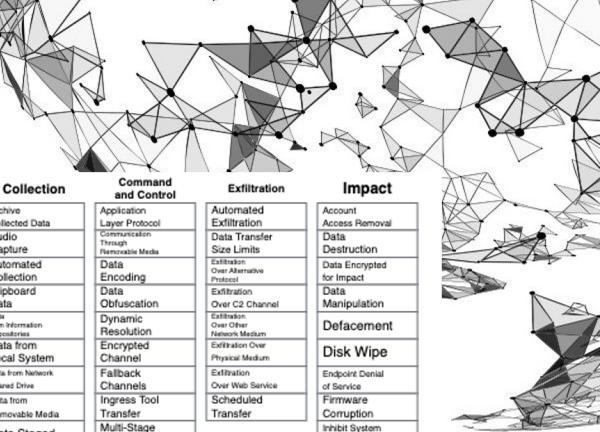
MSRPC-To-ATT&CK-Mapping

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 Protocols:

- 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

ATT&CK Mapping



MSRPC to ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise Exploit Public-Facing Applications External Remote Services Hardware Additions Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts	Command and Scripting Interpreters Deployment for Client Execution Inter-Process Communication Native API Scheduled Task Job At (Windows) Scheduled Task Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation	Account Manipulation BITS Jobs Boot or Login Autostart Execution File System Run Keys / Startup Folder Administrative Package Time Providers Winlogon Helper DLL Security Support Provider LSASS Driver ShowRun Modification Port Monitors Print Processors Active Setup Boot or Login Help File Scripts Browser Extensions Compromised Client Software Library Create Account Create or Modify System Process Windows Service Event Triggered Execution External Remote Services Hijack Execution Flow Modular Authentication Process Office Application Startup Pre-OS Boot Scheduled Task Job At (Windows) Scheduled Task Server Software Component TIPC Signaling Valid Accounts XSL Script Processing	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Login Autostart Execution File System Run Keys / Startup Folder Administrative Package Time Providers Winlogon Helper DLL Security Support Provider LSASS Driver ShowRun Modification Port Monitors Print Processors Active Setup Boot or Login Help File Scripts Create or Modify System Process Windows Service Event Triggered Execution External Remote Services Hijack Execution Flow Modular Authentication Process Office Application Startup Pre-OS Boot Scheduled Task Job At (Windows) Scheduled Task Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Deobfuscate/Decode Files or Information Direct File and Registry Access Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Manipulation Hide Artifacts Hijack Execution Flow Impair Defenses Indicator Removal on Host Indirect Command Execution Masquerading Domain Policy Modification Escape to Host Event Triggered Execution Exploitation for Privilege Escalation Hijack Execution Flow Process Injection Scheduled Task Job At (Windows) Scheduled Task Valid Accounts	Brute Force Credentialex from Password Stores Exploitation for Credential Access Forced Authentication Forge Web Credentials Input Capture	Account Discovery File and Registry Access Domain Account Email Account Man-in-the-Middle LLMNR/NBT-NS and SMB Relay ARP Cache Poisoning Modify Authentication Protocol Network Share Discovery Network Sniffing OS Credential Dumping LSASS Memory Security Assertion Manager NTDS DCSync Modify Registry Obfuscated Files or Information Pre-OS Boot Process Injection Rogue Domain Controller RootKit Signed Binary Proxy Execution Signed Script Proxy Execution Subvert Trust Controls Template Injection Traffic Signaling Trusted Developer Utilities Proxy Execution User Account Authentication Material Valid Accounts Virtual Machine/Device Emulation XSL Script Processing	Exploitation of Open Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Application Discovery Windows Discovery Browser Bookmark Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Interaction Discovery System Location Discovery System Network Configuration Discovery System Network Configuration Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization Sandbox	Archive Collected Data Audio Capture Automated Collection Clipboard Data Data Encoding Data Obfuscation Dynamic Resolution File from Information Repositories Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material Man in the Browser Man-in-the-Middle LLMNR/NBT-NS and SMB Relay ARP Cache Poisoning Process Discovery Query Registry Remote System Discovery Software Discovery System Interaction Discovery System Location Discovery System Network Configuration Discovery System Network Configuration Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization Sandbox	Application Layer Protocol Communication Through Removable Media Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Encrypted Channel Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot	

MSRPC to ATT&CK

Document Contents:

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

Indicator of Activity (IOA):

Prevention Opportunities:

Notes:

- Findings were made surrounding the domain joined compromise version of this attack, not the local privilege escalation implementation.

Useful Resources:

Technique References:

- <https://gist.github.com/tyranid/5527f5559041023714d67414271ca742>
- <https://www.bleepingcomputer.com/news/microsoft/windows-security-update-blocks-petitpotam-ntlm-relay-attacks/>

RPC Filter Example:

- EfsRpcRemoveUserFromFile
- EfsRpcAddUsersToFile

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 :)

— THIS IS A CALL TO ACTION

Get started with MSRPC to ATT&CK

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

