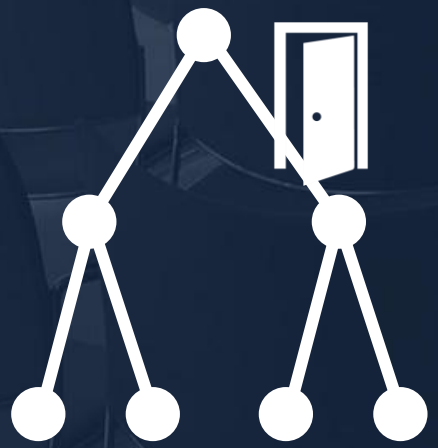
21 octobre 2025 - PARIS

Un grand merci à tous nos partenaires !

IDENTITY DAYS

21 octobre 2025 - PARIS

The funny story of Active Directory backdooring 💀 Season #2



Sylvain CORTES
VP of Strategy @ Hackuity

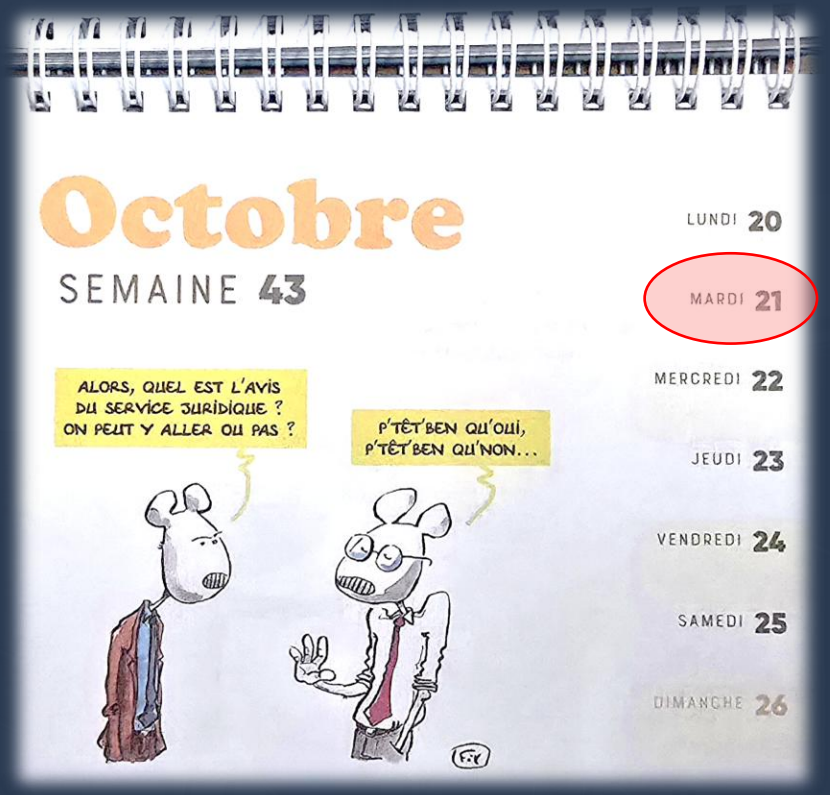
Microsoft MVP Most Valuable Professional

Hervé THIBAULT
Chief Strategy Officer @ Metsys

Microsoft REGIONAL DIRECTOR

Merci aux partenaires !

AGENDA DE LA CONFÉRENCE



Fix - Bullshit Calendrier 2025

- Introduction
- Comment les attaques Active Directory se produisent-elles dans la *vraie* vie ?
- Qu'est-ce qu'une Backdoor (porte dérobée) AD ?
- Techniques de backdooring AD
- Conclusion & Q&A

Introduction

If there's something strange In your Active Directory


Who ya
gonna
çall?


ECTO-1
NEW YORK


BACKDOOR
BUSTERS

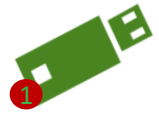
Comment les attaques Active Directory se produisent-elles dans la *vraie* vie ?

Comment se déroule une attaque par ransomware

Ransomware's classic sequence

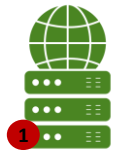
Mail infecté

Page Web infectée

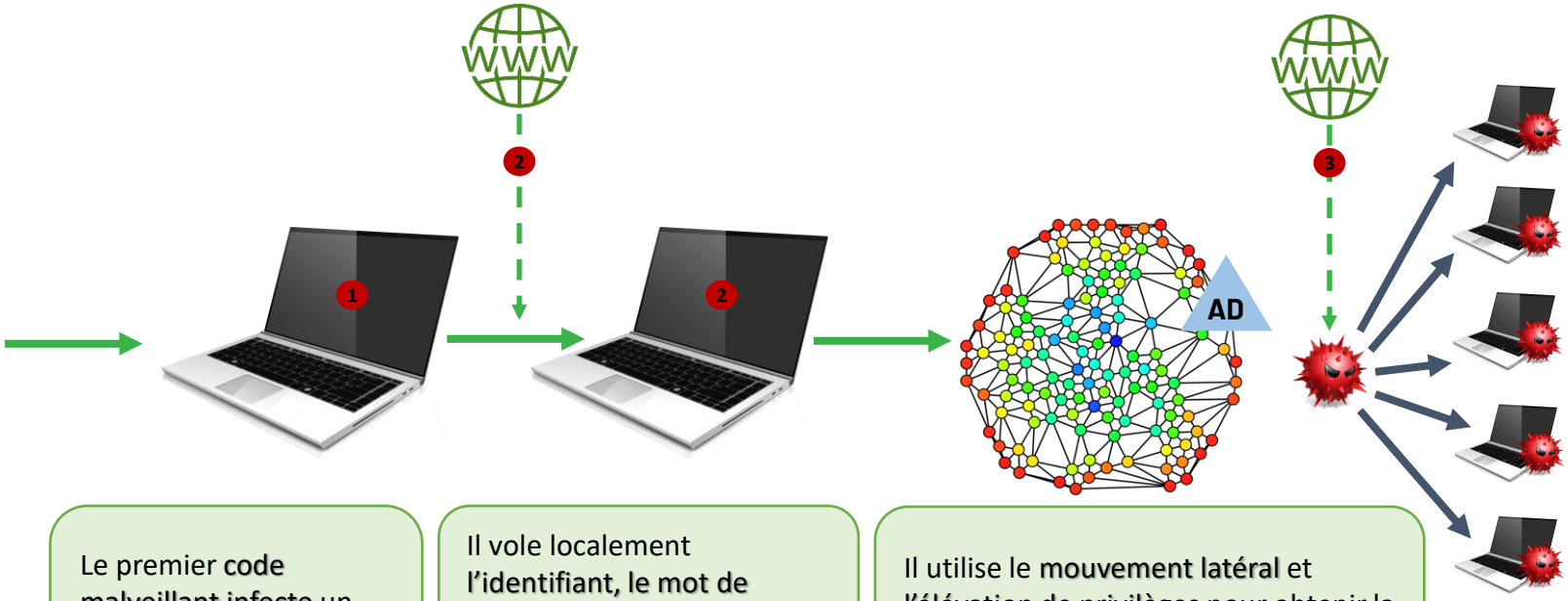


Clé USB infectée

Logiciel infecté



Access Gateway / RDP



Le premier code malveillant infecte un ordinateur

Il désactive l'AV/EDR local et créé de faux services AV/EDR et de faux journaux

Il télécharge le deuxième code malveillant

Il vole localement l'identifiant, le mot de passe, le hachage du mot de passe

Il effectue une reconnaissance Active Directory (AD)

Il Recherche les chemins d'attaque utilisant des CVE ou des erreurs de configuration AD

Il utilise le mouvement latéral et l'élévation de privilèges pour obtenir la maitrise complète du domaine AD

Un troisième code malveillant est téléchargé

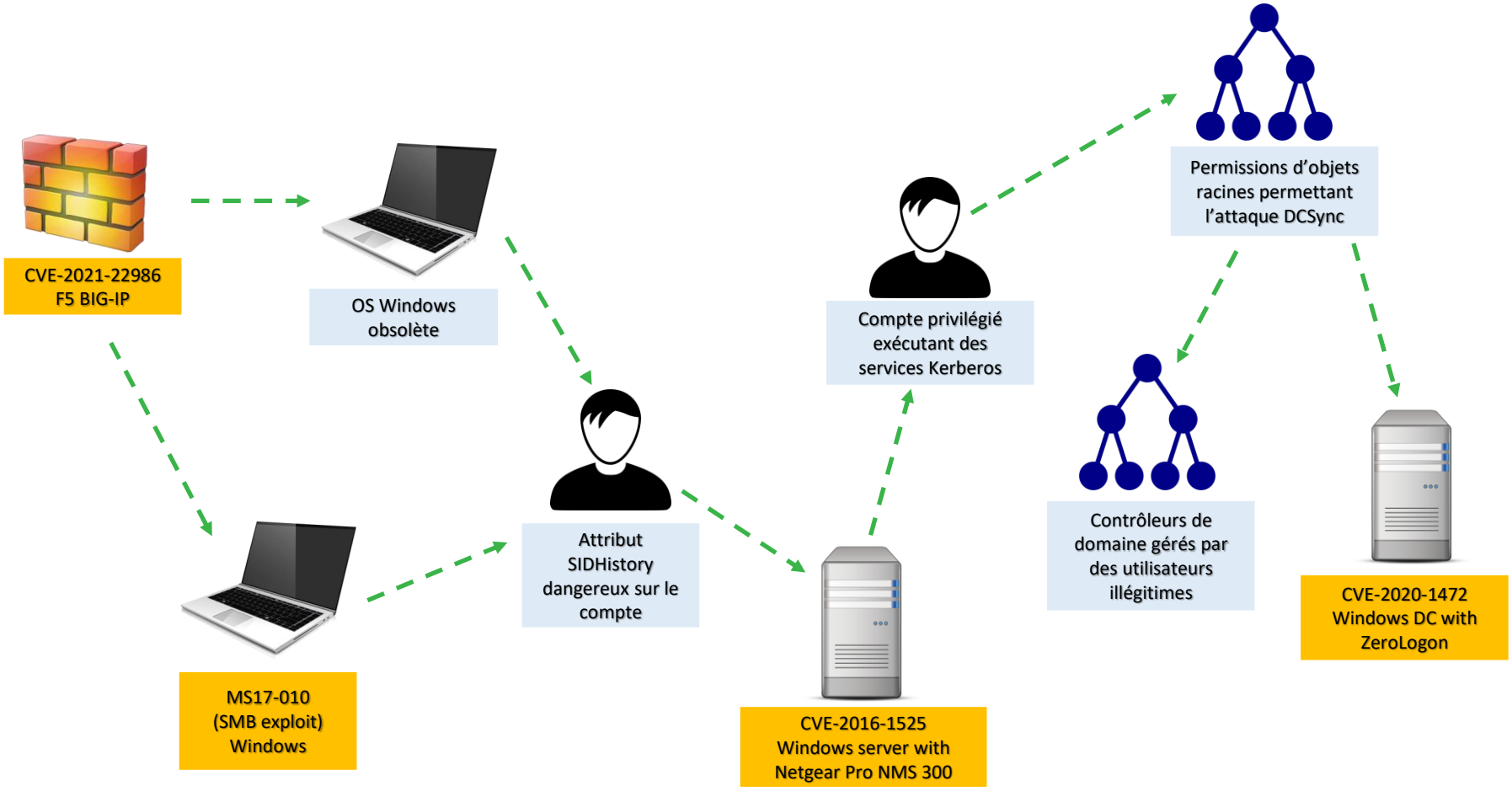
→Les sauvegardes sont détruites

→Des portes dérobées sont créées

→La charge utile de chiffrement est déployée sur toutes les machines

Comment les attaques Active Directory se produisent dans la vie réelle

Exemple de chemin d'attaque utilisant des CVE et des erreurs de configuration AD



Primo-infection | Mouvement latéral et élévation de privilèges | Prise de contrôle du domaine + AD Backdooring

Qu’est-ce qu’une Backdoor (porte dérobée) AD ?

Qu'est-ce qu'une Backdoor (porte dérobée) AD ?

Définition

A **backdoor** is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device (e.g. a home router), or its embodiment (e.g. part of a cryptosystem, algorithm, chipset, or even a "homunculus computer" —a tiny computer-within-a-computer such as that found in Intel's AMT technology).[1][2] Backdoors are most often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within autoschediastic networks.

A backdoor may take the form of a hidden part of a program,[3] a separate program (e.g. Back Orifice may subvert the system through a rootkit), code in the firmware of the hardware,[4] or parts of an operating system such as Windows.[5][6][7] Trojan horses can be used to create vulnerabilities in a device. A Trojan horse may appear to be an entirely legitimate program, but when executed, it triggers an activity that may install a backdoor.[8] Although some are secretly installed, other backdoors are deliberate and widely known. These kinds of backdoors have "legitimate" uses such as providing the manufacturer with a way to restore user passwords.

Many systems that store information within the cloud fail to create accurate security measures. If many systems are connected within the cloud, hackers can gain access to all other platforms through the most vulnerable system.[9]

Source: https://en.wikipedia.org/wiki/Backdoor_(computing)

Notre définition dans le contexte de l'Active Directory : « Après une prise de contrôle total d'un domaine, un moyen de revenir plus tard... »

AD est KO. D'accord, mais quelle est la prochaine étape ?

La question de la pilule rouge contre la pilule bleue

« Tu prends la pilule rouge… tu restes au pays des merveilles, et je te montre jusqu'où va le terrier du lapin "

> Réinstallation Active Directory

« Tu prends la pilule bleue… L'histoire se termine, tu te réveilles dans ton lit et croit ce que tu veux croire »

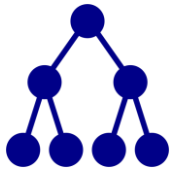
> La chasse aux portes dérobées AD

Techniques de backdooring AD

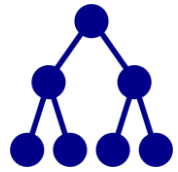
SIDhistory attribute manipulation

AD backdooring techniques - SIDhistory attribute manipulation

Understand the concept



Domain A



Domain B

ACE / S-1-5-21-971854990-4143533025-234257201-2078

User object migration

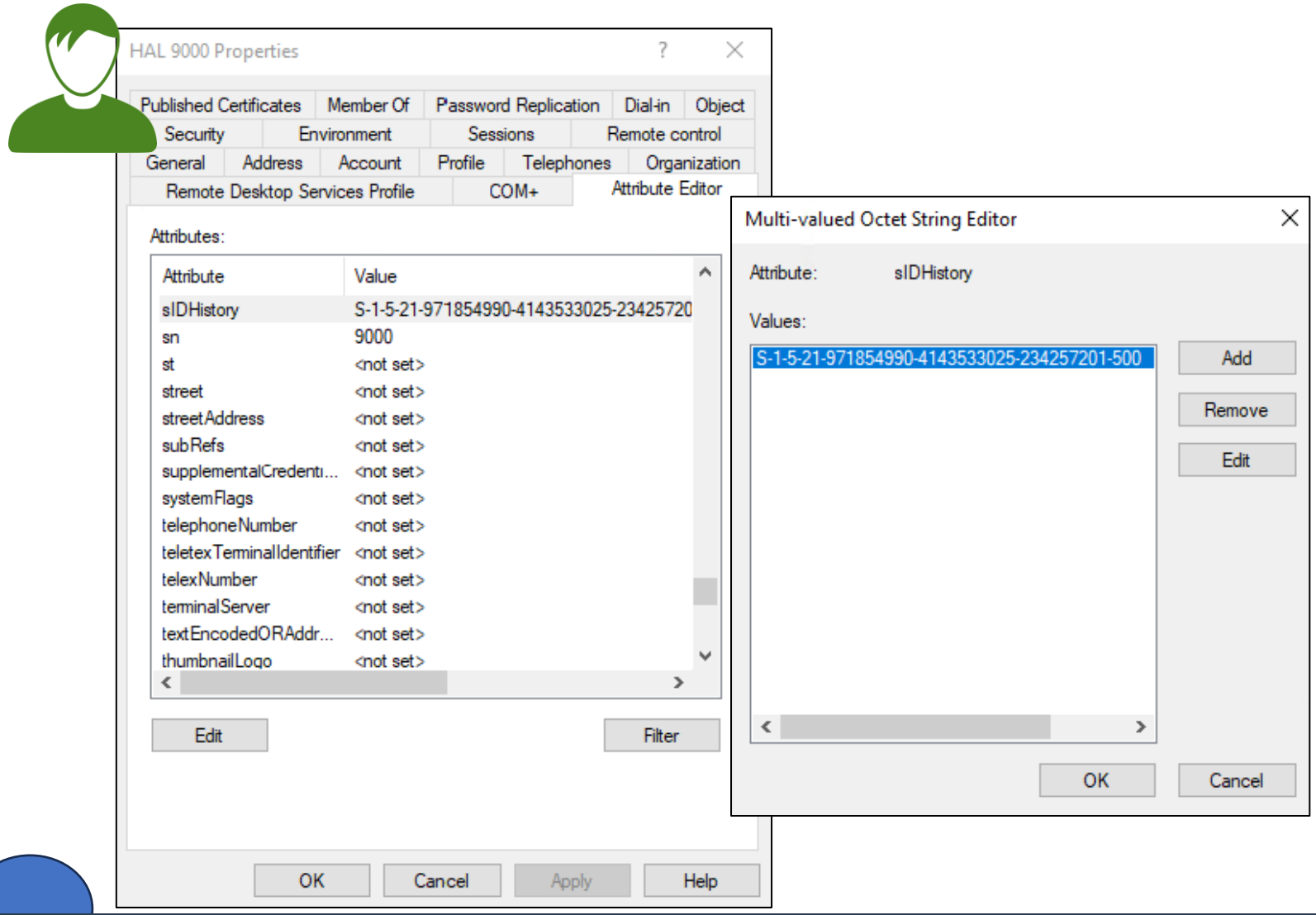
userPrincipalName	userx@domainA.priv
SID	S-1-5-21-971854990-4143533025-234257201-2078
SIDhistory	

userPrincipalName	userx@domainB.priv
SID	S-1-5-22-238747360-3847846620-347463388-1761
SIDhistory	S-1-5-21-971854990-4143533025-234257201-2078

SIDhistory attribute can host multiple values !

AD backdooring techniques - SIDhistory attribute manipulation

Understand the concept

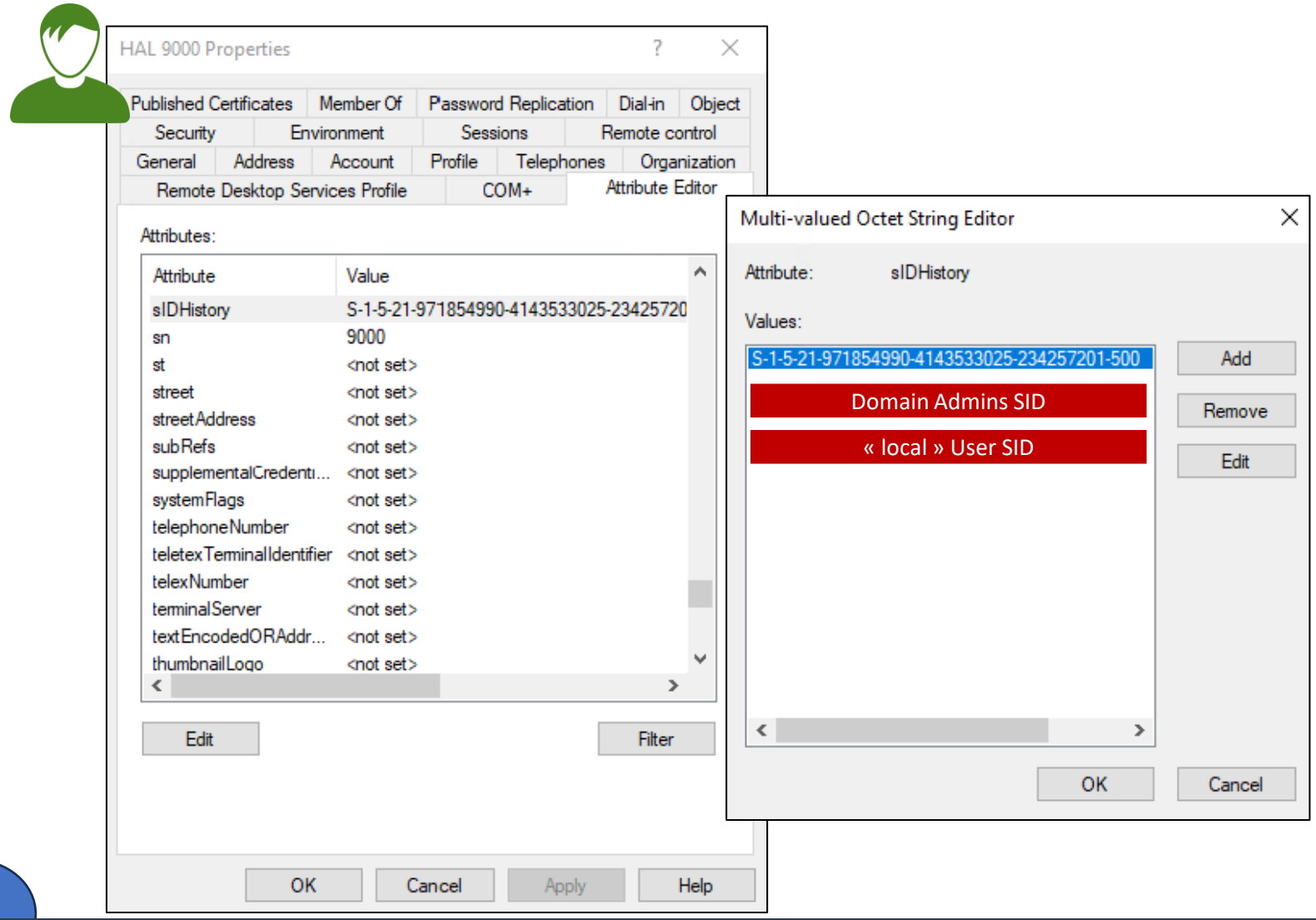


Comment le modifier ?

- Module VB.Net SidHist
- ADMT / All migration tools
- SIDCloner - https://github.com/GreyCorbel/SIDCloner
- DCShadow
- Etc.

AD backdooring techniques - SIDhistory attribute manipulation

Understand the concept

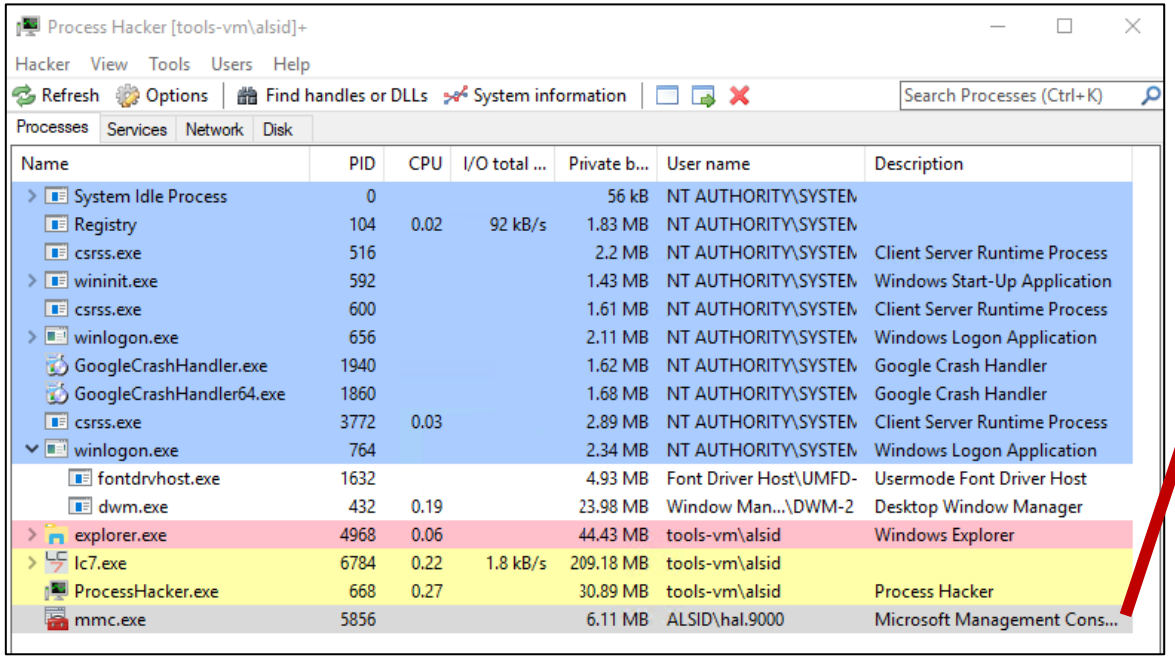


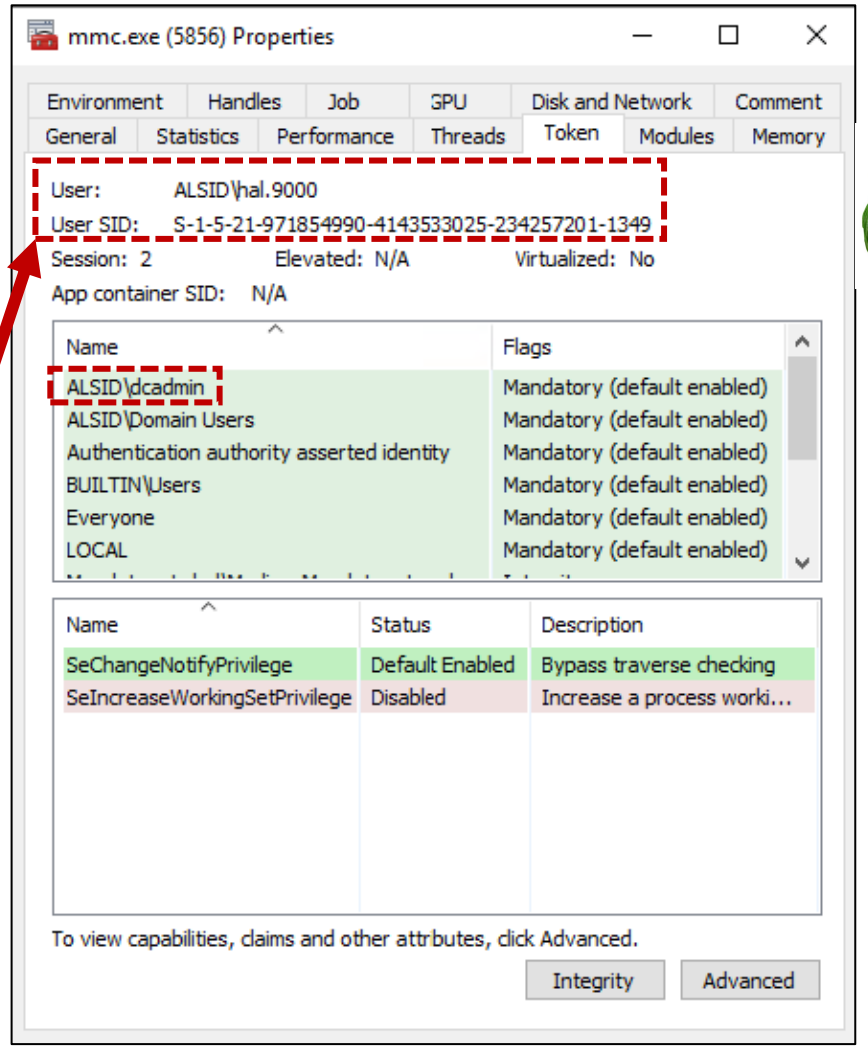
C’est dangereux ?

- Pas limité aux SID externes !
- Pas limité aux SID utilisateurs !
- En fait... Pas limité du tout !

AD backdooring techniques - SIDhistory attribute manipulation

Process example with DCadmin





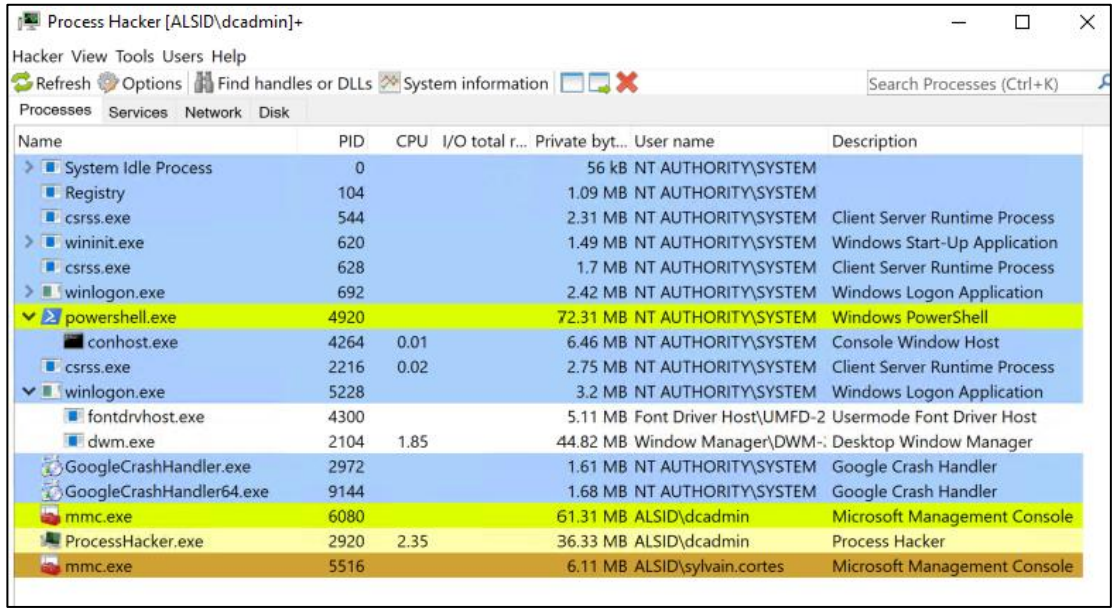
hal.9000 user

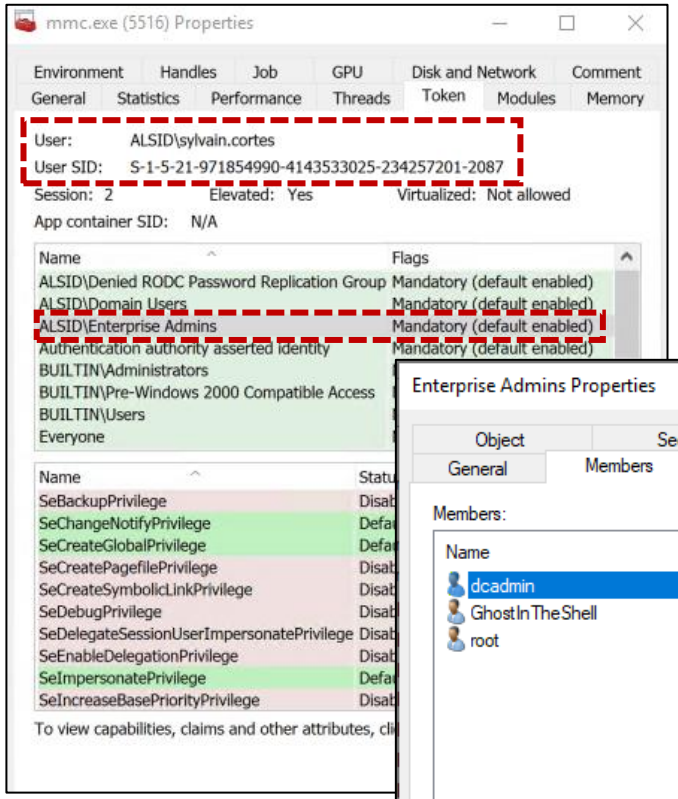
L'utilisateur hal.9000 héberge une valeur SID à partir d'un compte d'administrateur de domaine (alias dcadmin) dans l'attribut SIDhistory

→ Vous pouvez être Domain Admin sans être membre du groupe « Domain Admins »!

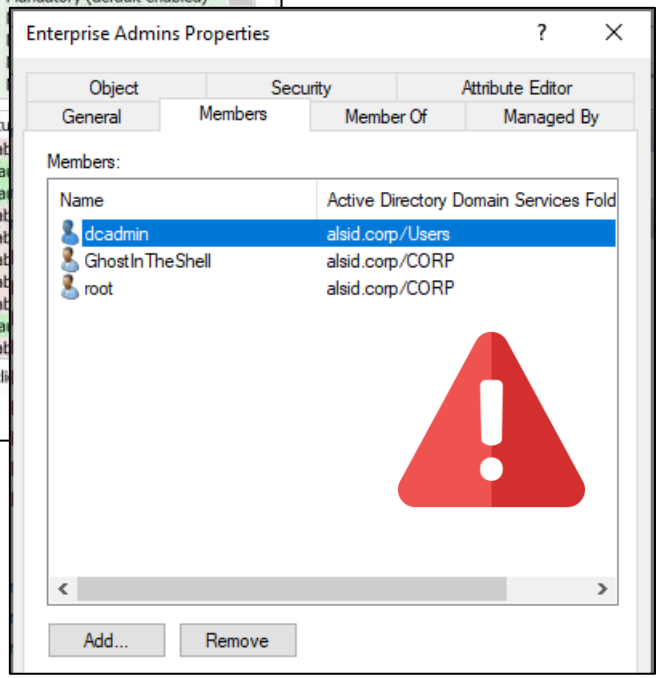
AD backdooring techniques - SIDhistory attribute manipulation

Process example with DCadmin





sylvain.cortes
user



Utilisateur Sylvain.Cortes avec valeur *S-1-5-21-971854990-4143533025-234257201-519* (**Enterprise Admins group**) dans l'attribut SIDhistory

Mais... Sylvain.Cortes n'est **pas** dans le groupe Enterprise Admins !

AD backdooring techniques - SIDhistory attribute manipulation

How to check

Comment verifier ?

- Search_SIDHistory PS script by Santhosh Sivarajan – https://santhoshsivarajan.wordpress.com/2010/12/12/powershell-script-search-active-directory-and-generate-sidhistory-report/
- LDAP query (LEX is the best!)
- AD security tools
- Etc.

https://www.ldapexplorer.com/index.htm

```powershell
$UserInfoFile = New-Item -type file -force "C:\_data\UserInfo.txt"
"SamAccountName`tSIDHistory" | Out-File $UserInfoFile -encoding ASCII
$ObjFilter = "(&(objectCategory=User)(sidHistory=*))"
$objSearch = New-Object System.DirectoryServices.DirectorySearcher
$objSearch.PageSize = 15000
$objSearch.Filter = $ObjFilter
$objSearch.SearchRoot = "LDAP://dc=alsid, dc=corp"
$AllObj = $objSearch.FindAll()
foreach ($Obj in $AllObj)
        {
            $objItemT = $Obj.Properties
            $tsam = $objItemT.samaccountname
            write-host $tsam
            $objpath = $obj.path
            $objpath1=[ADSI]"$objpath"
            $objectSID = [byte[]]$objpath1.sidhistory.value
            $sidHist = new-object System.Security.Principal.SecurityIdentifier $objectSID,0
            write-host $sidHist
            "$tsam`t$sidHist" | Out-File $UserInfoFile -encoding ASCII -append

        }
```

http://www.sivarajan.com/scripts/Search_SidHistory.txt

UserInfo.txt - Notepad

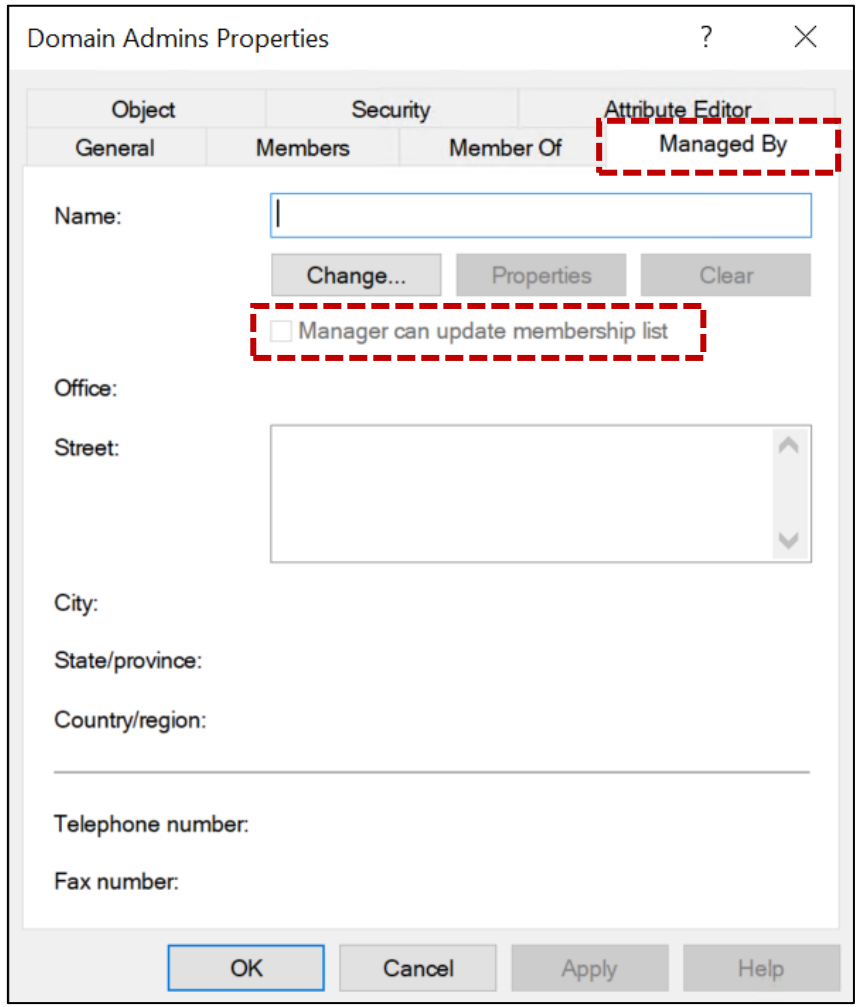
File Edit Format View Help

```
SamAccountName  SIDHistory
hal.9000        S-1-5-21-971854990-4143533025-234257201-500
```

“Managed By” attribute manipulation

AD backdooring techniques – "Managed by " attribute manipulation

Understand the concept

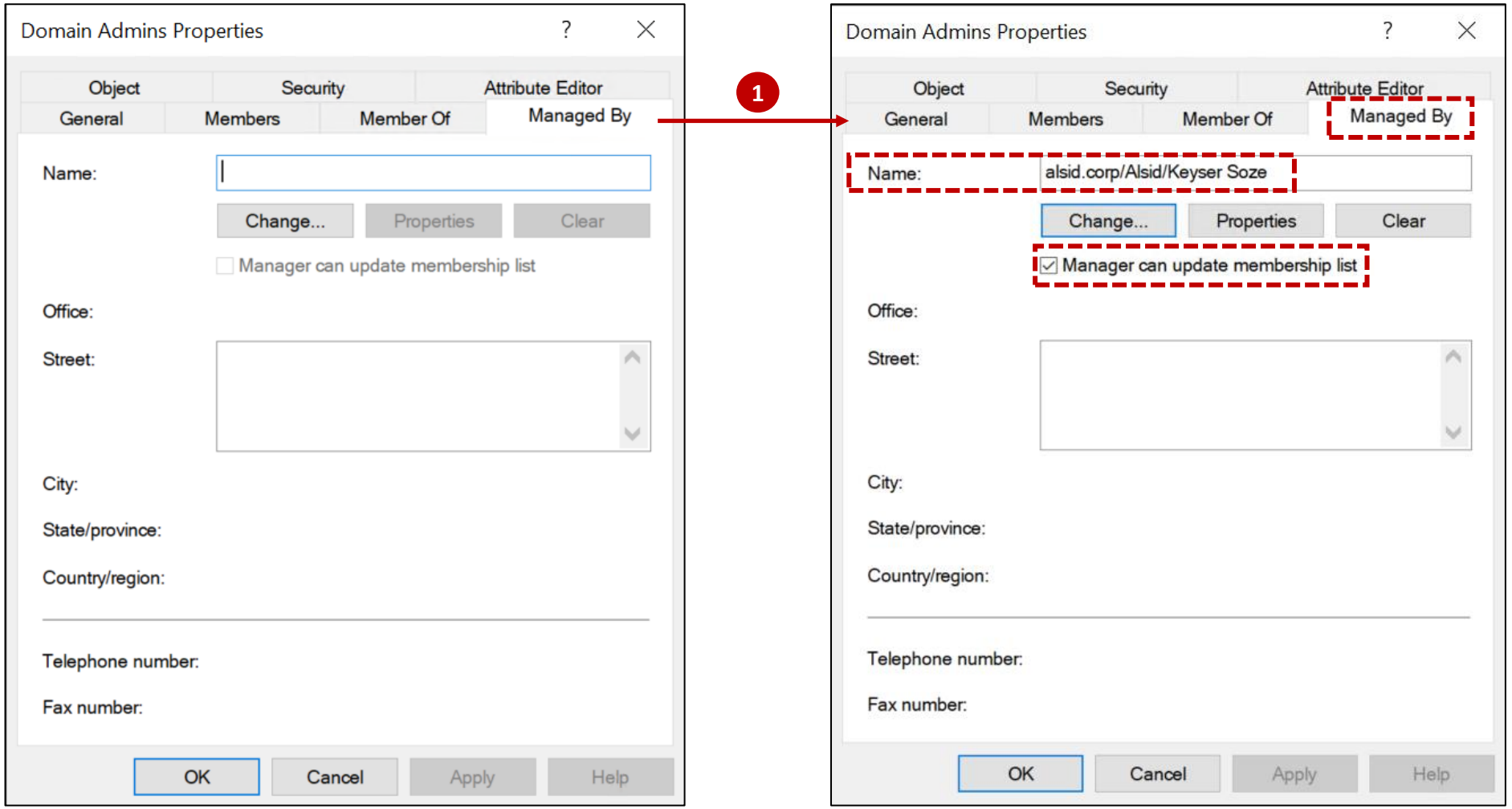


"Managed By" est un attribut « spécifique » conçu pour faciliter la délégation

Sur un objet de type groupe, cet attribut comporte des options « avancées » – Certaines de ces options « avancées » sont héritées de la première version d'Exchange Server, qui était (rappel) le premier véritable répertoire de l'histoire des produits Microsoft

AD backdooring techniques – "Managed by " attribute manipulation

Step-by-step example

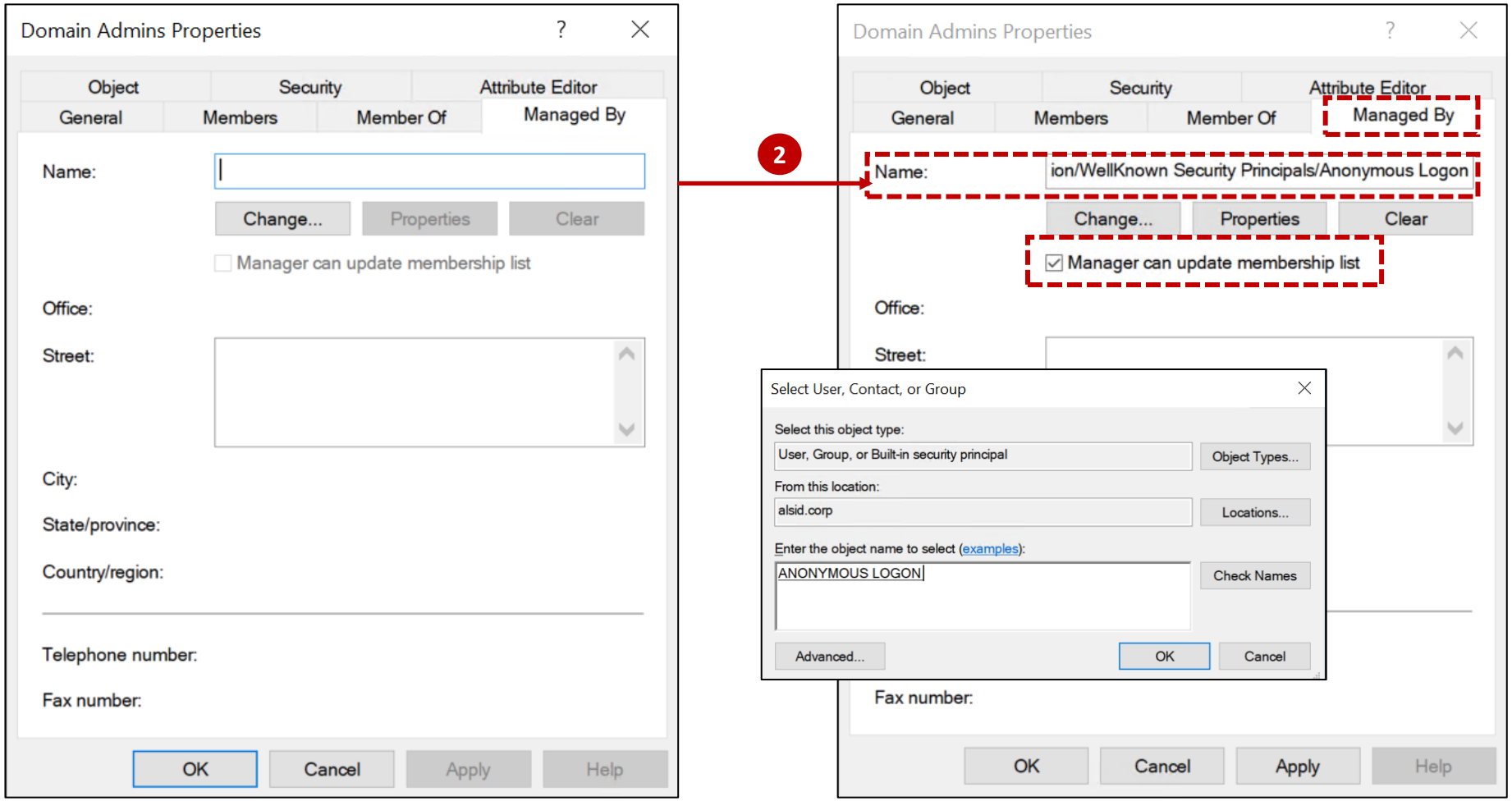


keyser.soze
user

Première option : créer un compte utilisateur (ici Keyser Soze) et cocher la case « Le gestionnaire peut mettre à jour la liste des membres »

AD backdooring techniques – "Managed by " attribute manipulation

Step-by-step example

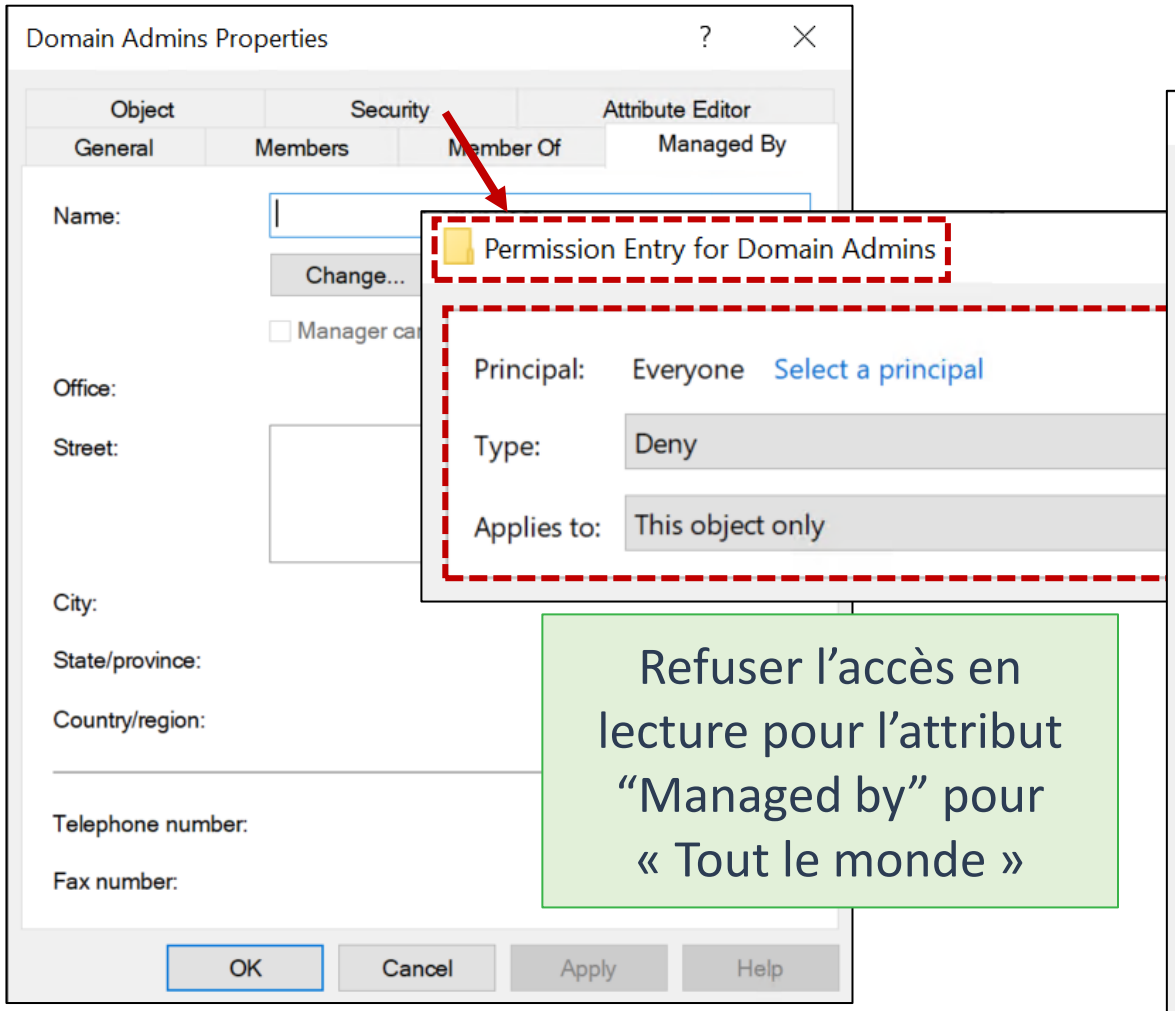


Deuxième option : Définir le compte utilisateur “Anonymous Logon” (*domain.priv/Configuration/WellKnown Security Principals/Anonymous Logon*) et cocher la case « Le manager peut mettre à jour la liste des membres »

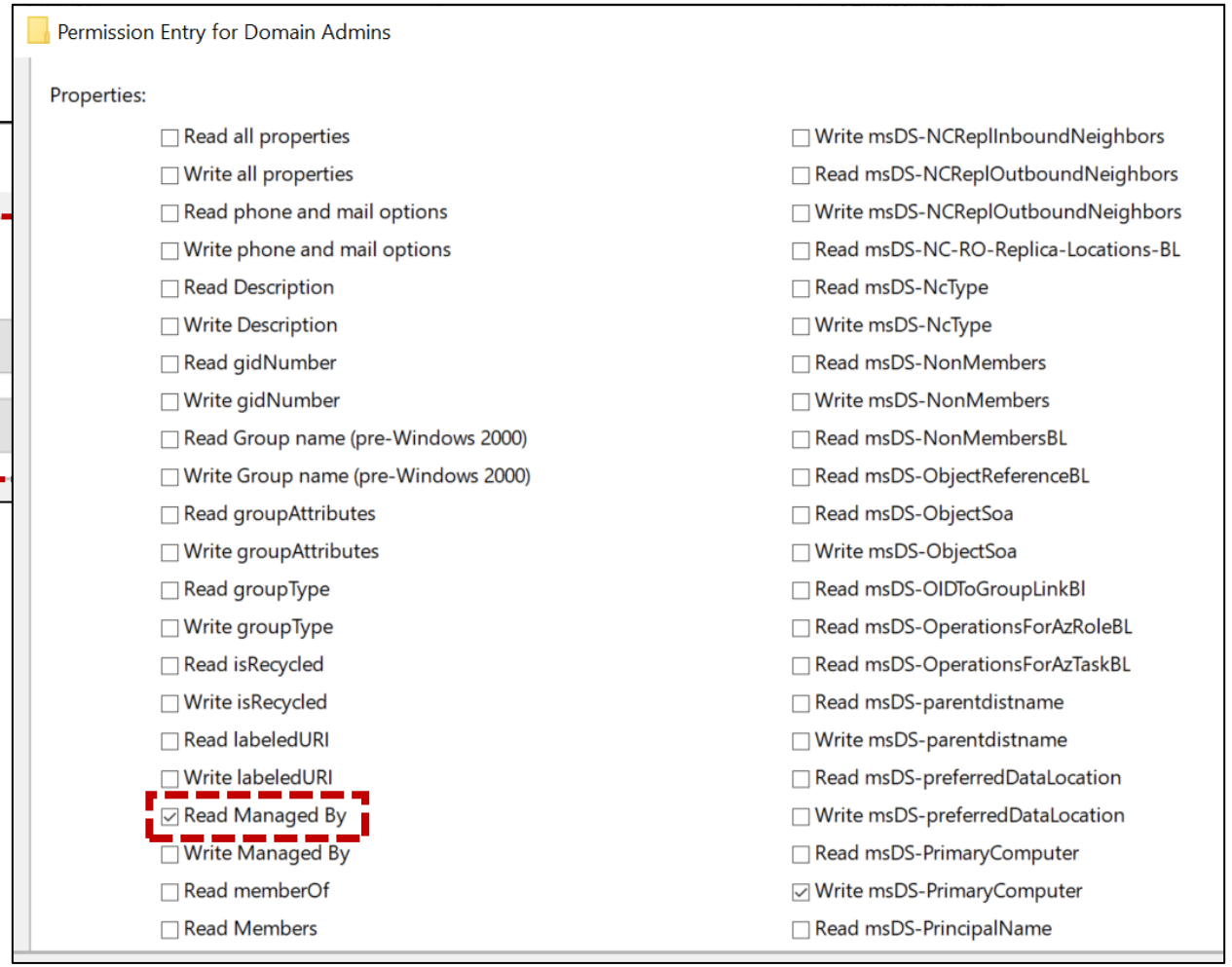
Rappel : L’ouverture de session anonyme dans Active Directory fait référence à un utilisateur ou à un ordinateur accédant à des ressources sans fournir d’informations d’identification d’authentification

AD backdooring techniques – "Managed by " attribute manipulation

Step-by-step example



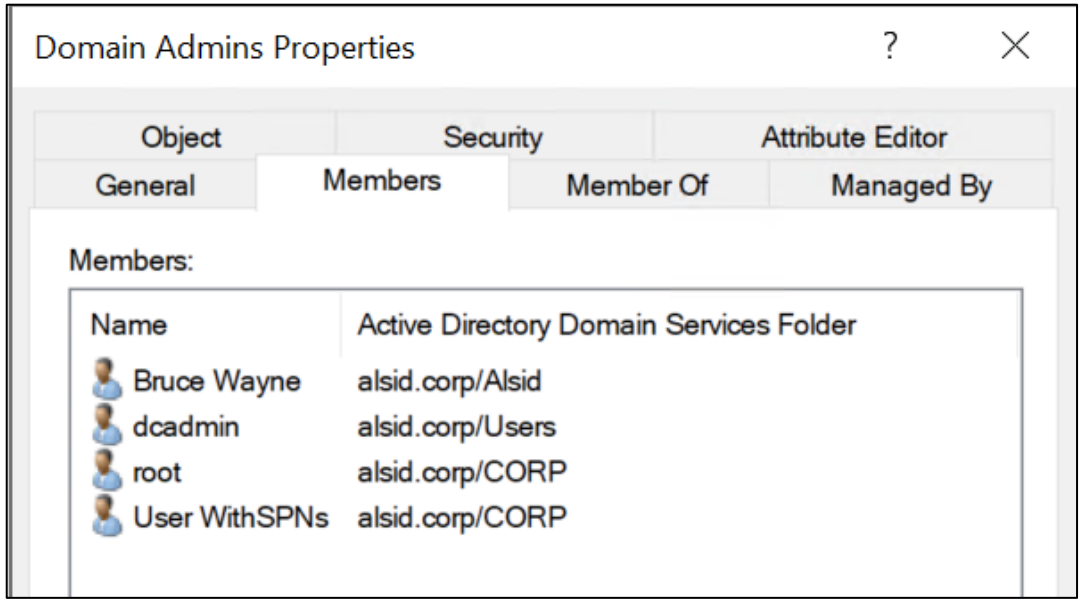
Refuser l'accès en lecture pour l'attribut "Managed by" pour « Tout le monde »

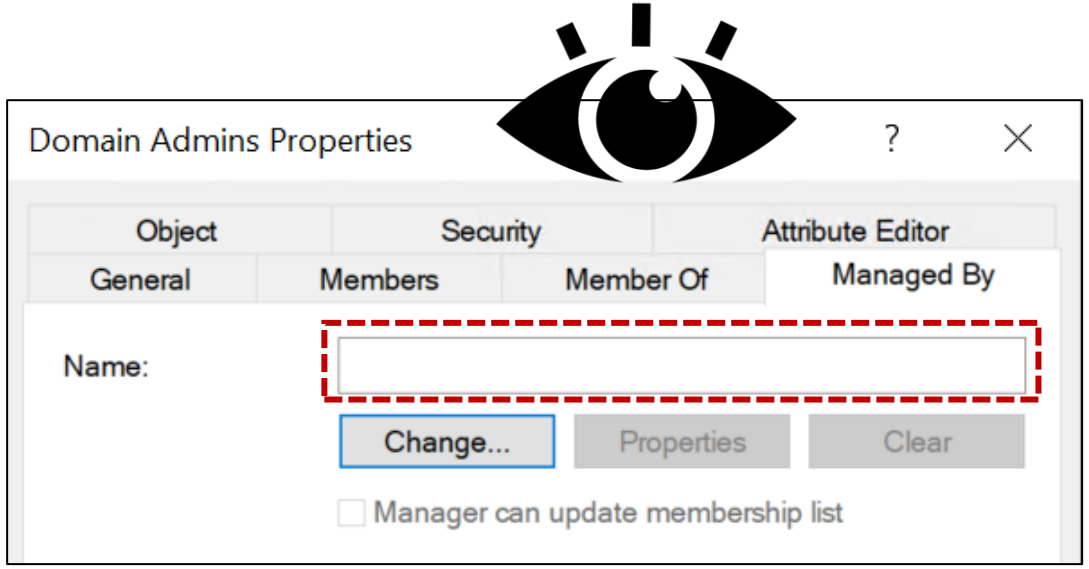


AD backdooring techniques – "Managed by " attribute manipulation

Step-by-step example

Retirer ensuite le compte ‘Keyser Soze” du groupe ‘Domain Admins’





Désormais, parce que nous avions défini l’accès « Refuser la lecture » sur l’attribut « Managed by » pour « Tout le monde », les administrateurs système ou même les administrateurs de domaine ne peuvent plus lire cet attribut et ne peuvent donc pas en vérifier la valeur !

→ Le compte ‘Keyser Soze’ est cependant toujours en mesure de modifier la liste des membres ‘Domain Admins’ !

AD backdooring techniques – "Managed by " attribute manipulation

How to check

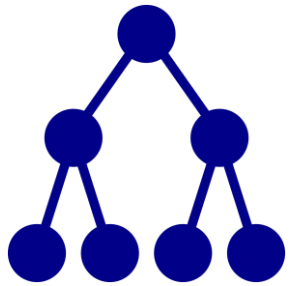
Comment verifier ?

- ‘Deny’ ACE hunting is the way
- Etc.

gPLink attribute to perform Domain Controllers future dominance

AD backdooring techniques - gPLink attribute to perform Domain Controllers future dominance

Understand the concept



NEW DOMAIN

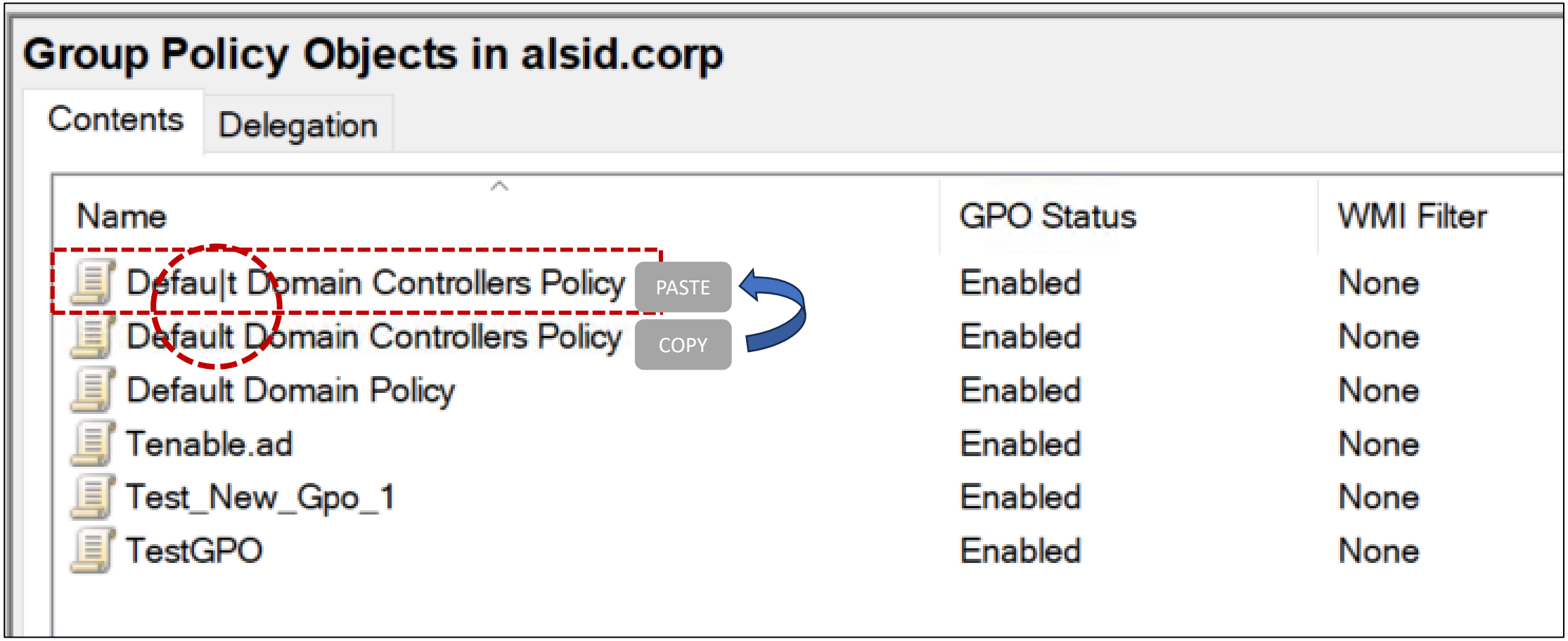
Default Domain Controllers Policy

Default Domain Policy

« Celui qui est maître de la stratégie est maître du monde »

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

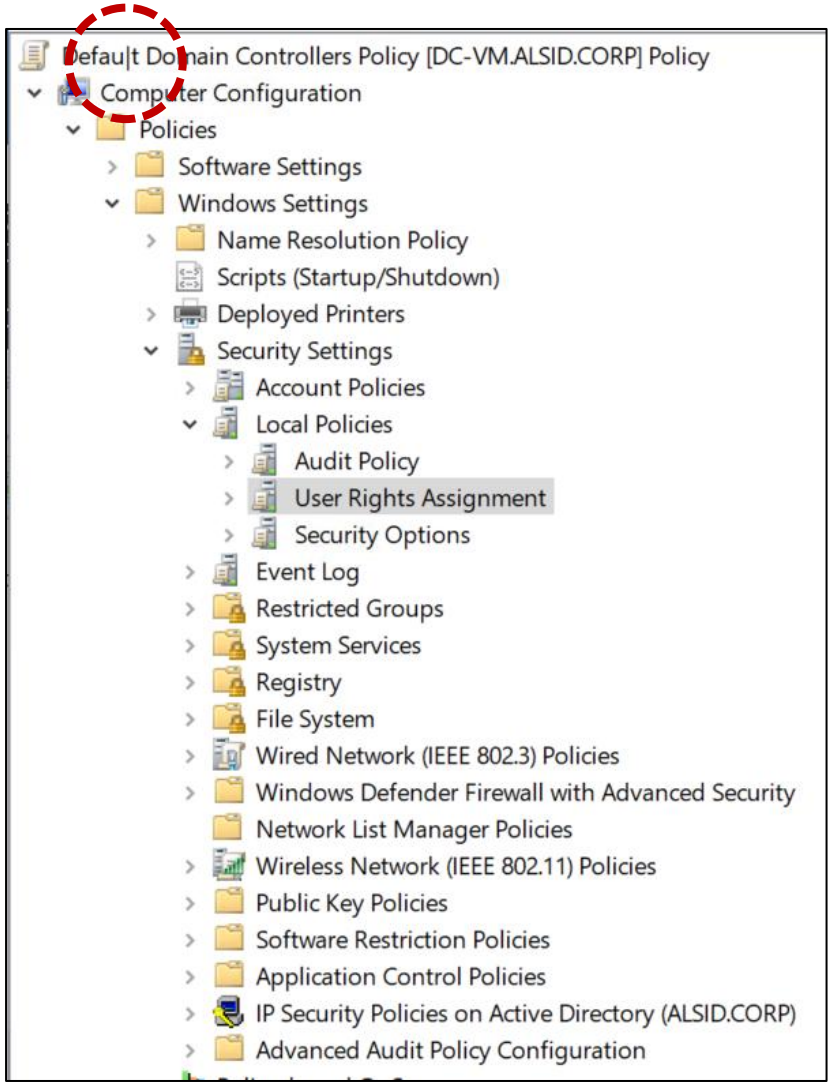
Step-by-step example

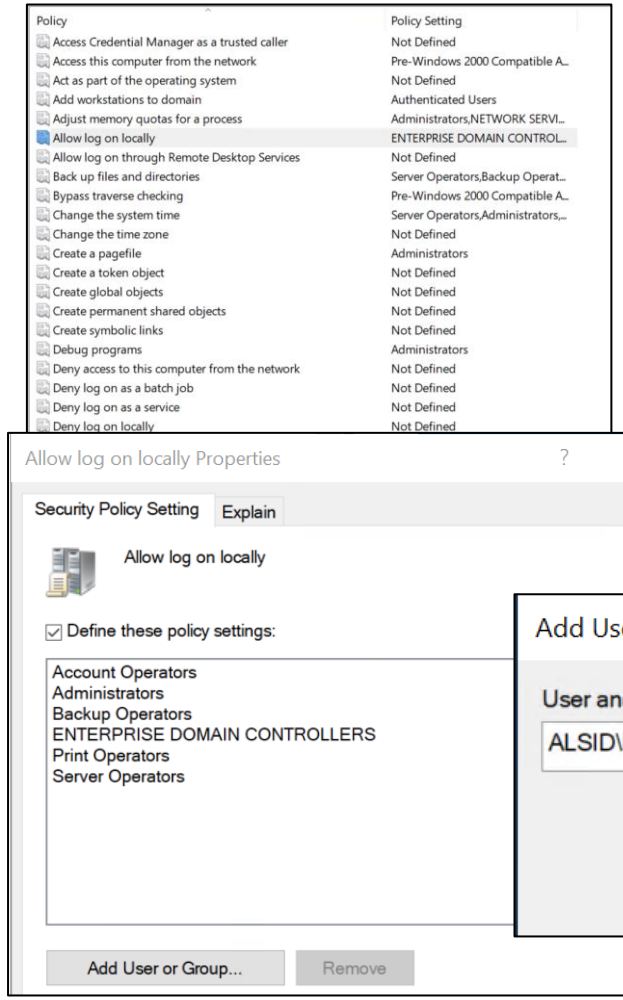


Copier/coller "*Default Domain Controllers Policy*" et renommer le nouvel objet de stratégie de groupe: "*Defau|t Domain Controllers Policy*" (changer le "l" par "|")

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

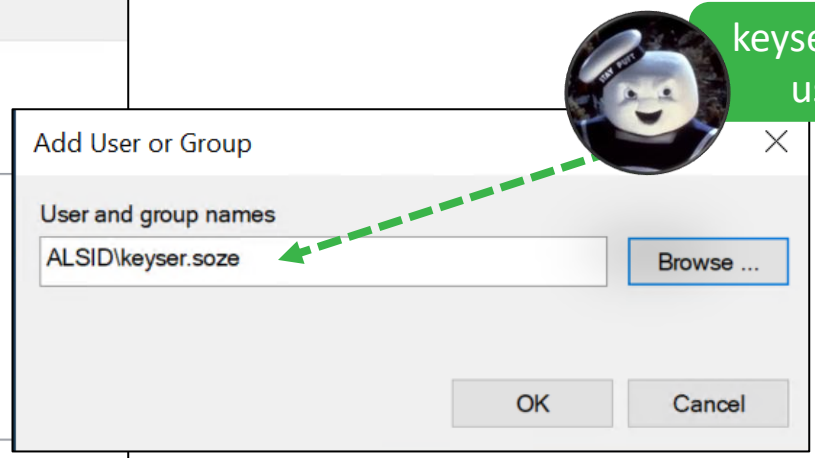
Step-by-step example





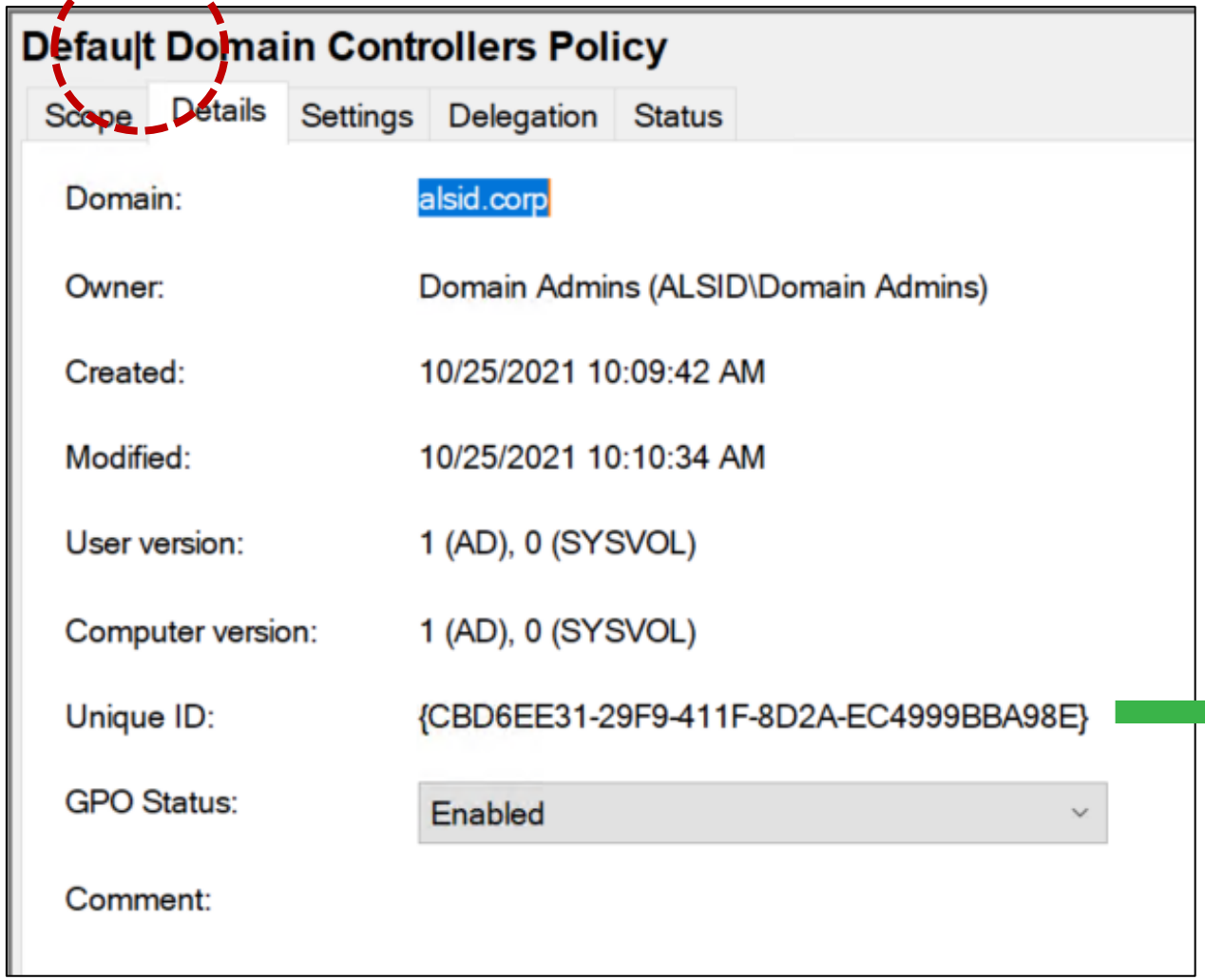
Modifier la stratégie *User Rights Assignment* pour keyser.soze et activer:

- *Allow log on locally*
- *Allow log on through Remote Desktop Services*
- *Debug programs*
- *Log on as a batch job*
- *Log on as a service*



AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Step-by-step example



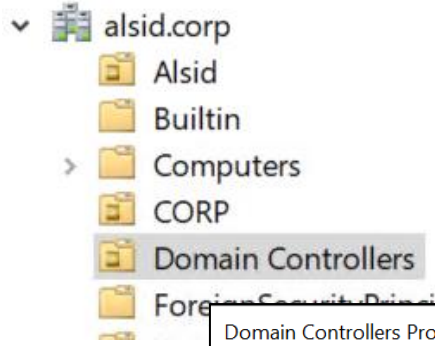
Vérifier et copier/coller l'identifiant unique de "Defau|t Domain Controllers Policy" :

{CBD6EE31-29F9-411F-8D2A-EC4999BBA98E}

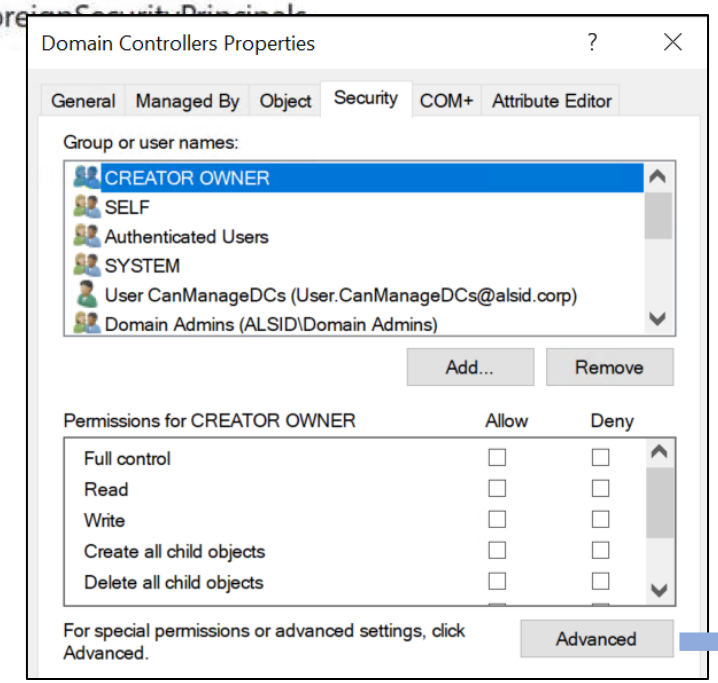
Conservez cette valeur quelque part

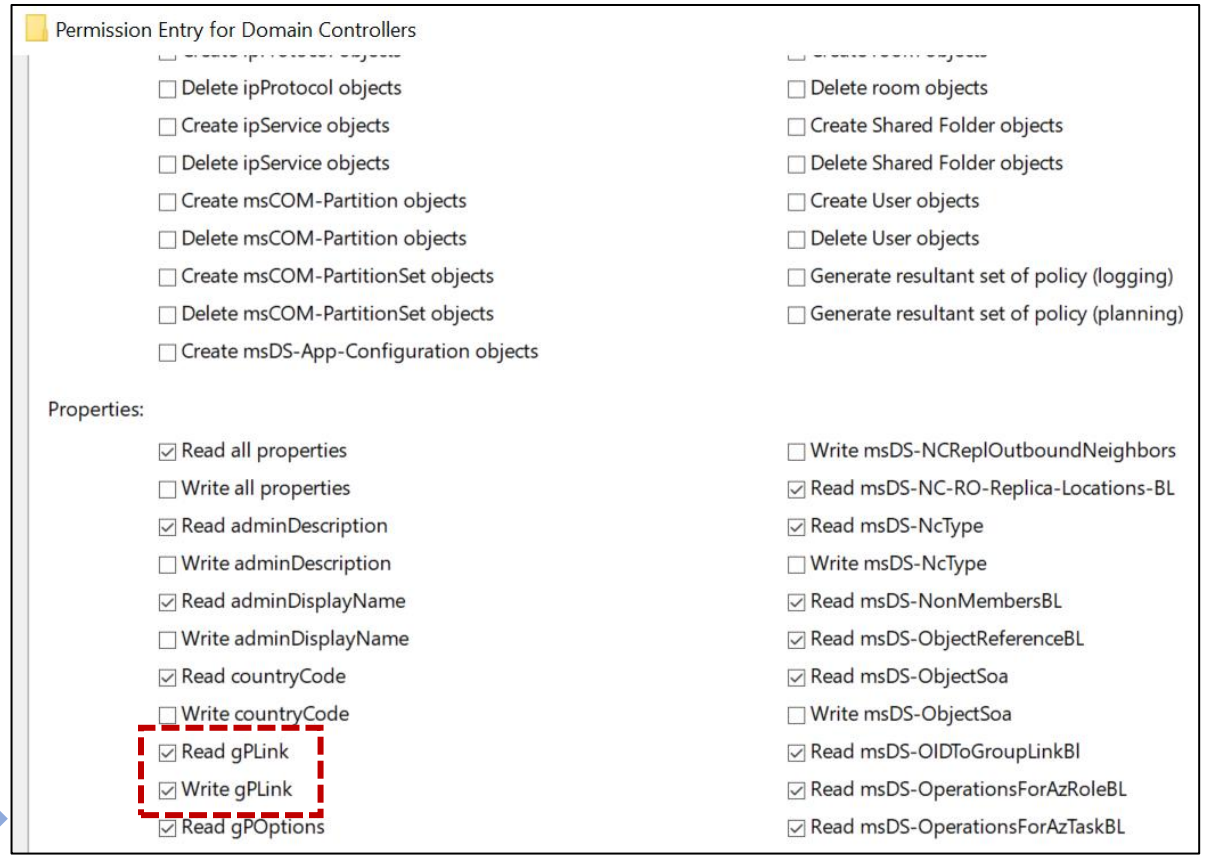
AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Step-by-step example



Modifier la Domain Controllers ACL et ajouter la permission “Write gPLink” au compte d’utilisateur « hacker » *keyser.soze*



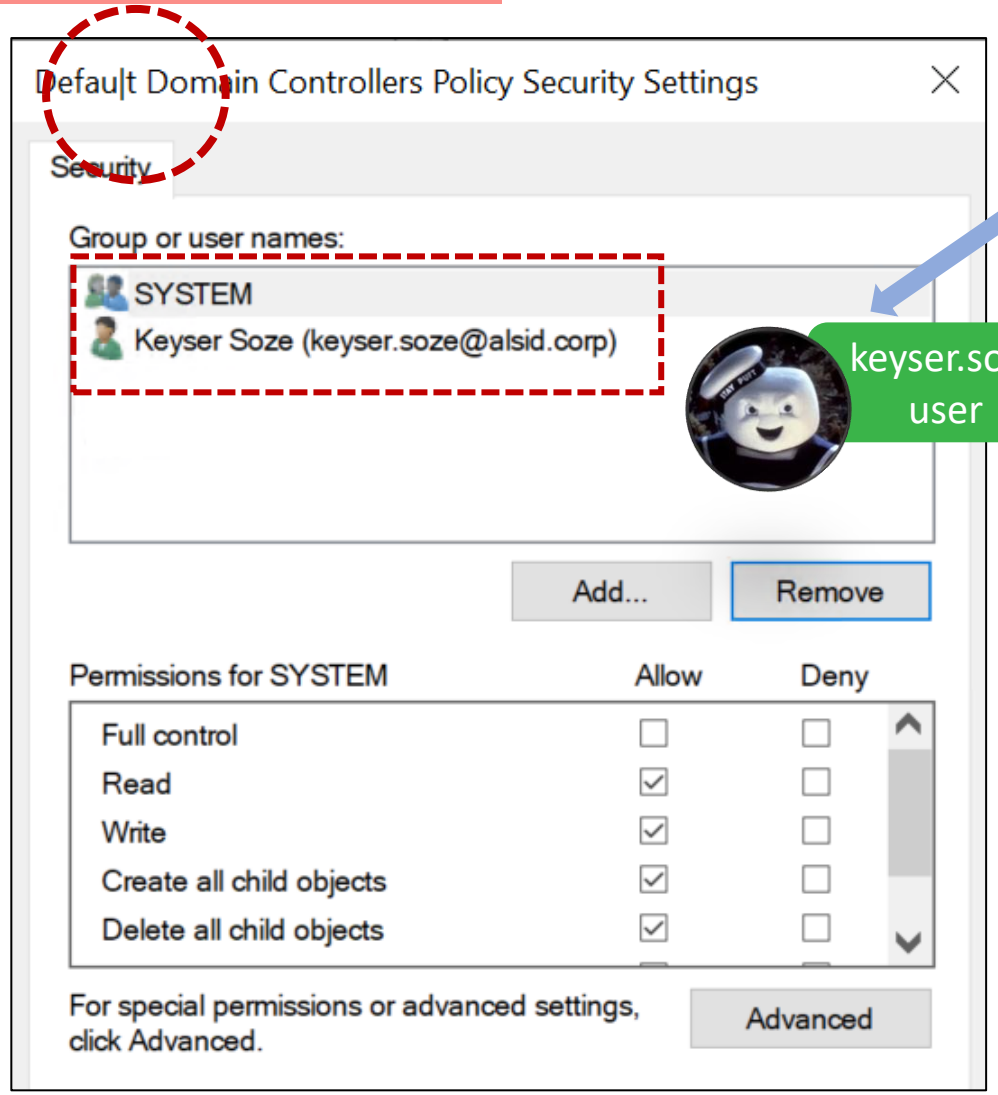


?

{ Ou accorder l’autorisation à un groupe et utiliser la technique ‘managed by’ pour le rendre impossible à détecter ! }

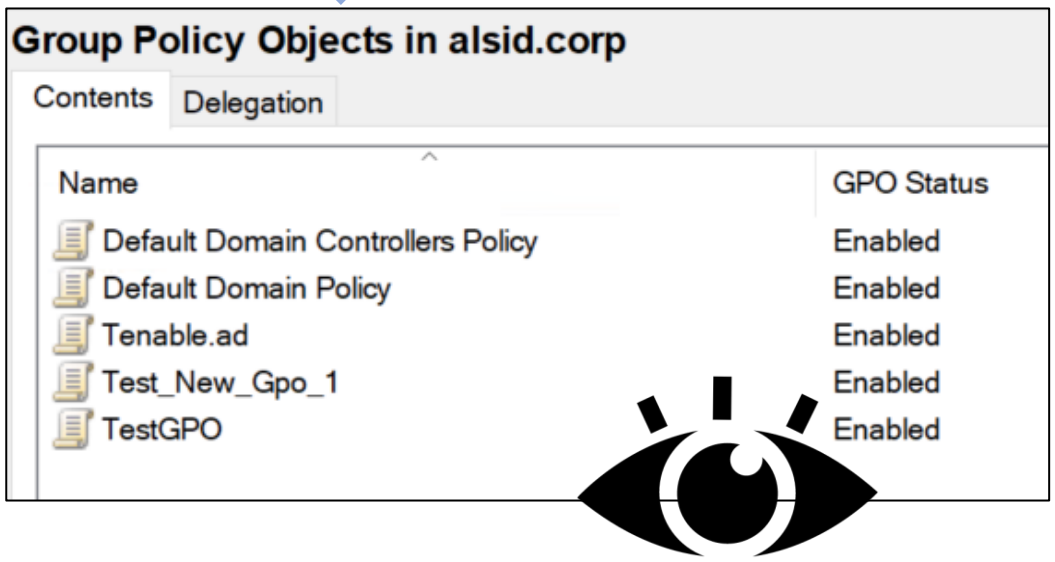
AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Step-by-step example



Masquer le nouvel objet de stratégie de groupe :
Modifier la sécurité sur “Defau|t Domain Controllers Policy” et supprimer tout accès à l’exception de SYSTEM et le compte utilisateur hacker

→ Désormais, l’objet de stratégie de groupe n’est plus répertorié dans l’interface graphique, même pour les administrateurs de domaine !



?

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Step-by-step example

Domain admin user

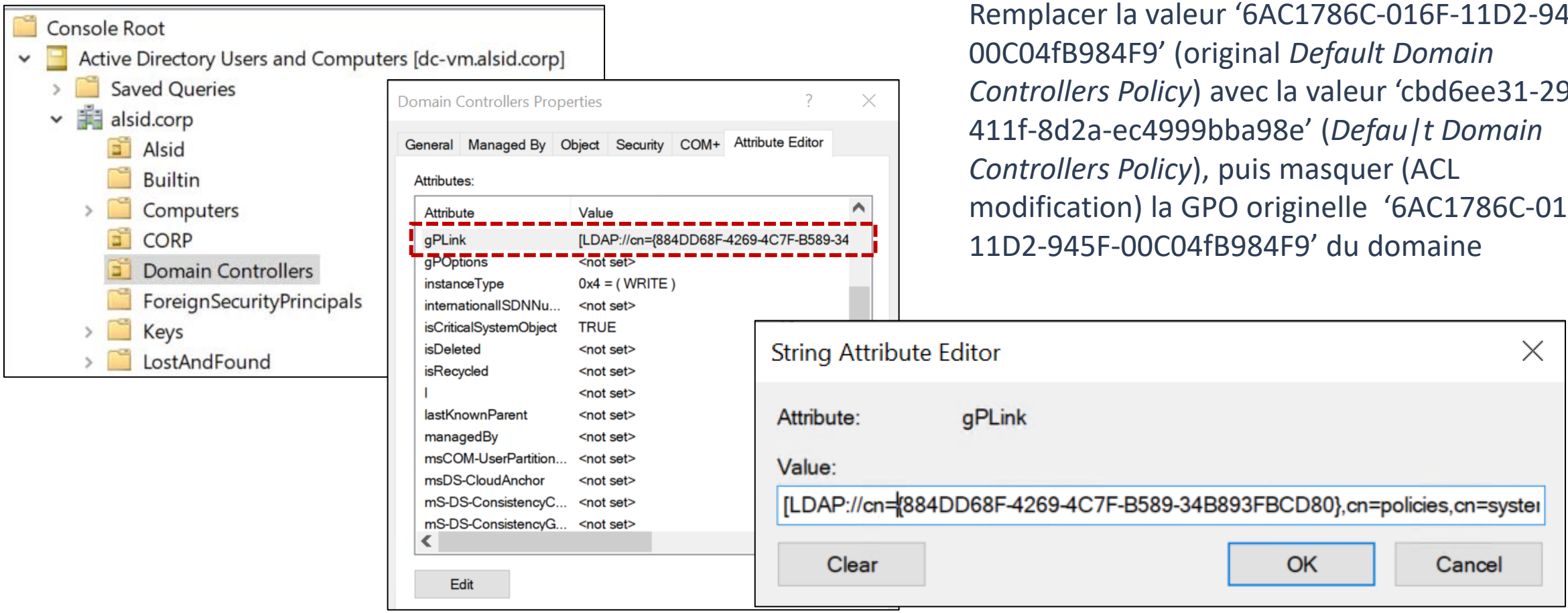
```
PS C:\Users\dcadmin> whoami
alsid\dcadmin
PS C:\Users\dcadmin> get-gpo -all

DisplayName      : Default Domain Policy
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/29/2021 12:17:39 AM
ModificationTime : 8/24/2021 2:39:02 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 11, SysVol Version: 11
WmiFilter        :

DisplayName      : Test_New_Gpo_1
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 3e7fa477-e34e-4d64-aa92-d58d9d939537
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 10/12/2021 7:33:54 AM
ModificationTime : 10/12/2021 7:36:28 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : TestGPO
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 431bfee5-fd5d-4af2-bf3e-5ab1c925fc10
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 8/24/2021 2:00:25 PM
ModificationTime : 8/24/2021 2:00:24 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

DisplayName      : Default Domain Controllers Policy
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 6ac1786c-016f-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/29/2021 12:17:39 AM
ModificationTime : 8/24/2021 8:08:04 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : Tenable.ad
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 884dd68f-4269-4c7f-b589-34b893fbcd80
GpoStatus        : AllSettingsEnabled
Description      : This GPO has been created as part of the deployment of Tenable.ad
CreationTime     : 8/24/2021 2:23:59 PM
ModificationTime : 8/24/2021 2:24:08 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

keyser.soze user

```
Windows PowerShell
PS C:\Users\dcadmin> whoami
alsid\keyser.soze
PS C:\Users\dcadmin> get-gpo -all

DisplayName      : Default Domain Policy
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/29/2021 12:17:39 AM
ModificationTime : 8/24/2021 2:39:02 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 11, SysVol Version: 11
WmiFilter        :

DisplayName      : Test_New_Gpo_1
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 3e7fa477-e34e-4d64-aa92-d58d9d939537
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 10/12/2021 7:33:54 AM
ModificationTime : 10/12/2021 7:36:28 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : TestGPO
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 431bfee5-fd5d-4af2-bf3e-5ab1c925fc10
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 8/24/2021 2:00:25 PM
ModificationTime : 8/24/2021 2:00:24 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

DisplayName      : Default Domain Controllers Policy
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 6ac1786c-016f-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 7/29/2021 12:17:39 AM
ModificationTime : 8/24/2021 8:08:04 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : Tenable.ad
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : 884dd68f-4269-4c7f-b589-34b893fbcd80
GpoStatus        : AllSettingsEnabled
Description      : This GPO has been created as part of the deployment of Tenable.ad
CreationTime     : 8/24/2021 2:23:59 PM
ModificationTime : 8/24/2021 2:24:08 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : Defau|t Domain Controllers Policy
DomainName       : alsid.corp
Owner            : ALSID\Domain Admins
Id               : cbd6ee31-29f9-11f-8d2a-ec4999bba98e
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 10/25/2021 10:09:42 AM
ModificationTime : 10/25/2021 10:41:08 AM
UserVersion      : AD Version: 1, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 0
WmiFilter        :
```

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Step-by-step example



Pour activer la porte dérobée :
Remplacer la valeur '6AC1786C-016F-11D2-945F-00C04fB984F9' (original *Default Domain Controllers Policy*) avec la valeur 'cbd6ee31-29f9-411f-8d2a-ec4999bba98e' (*Defau|t Domain Controllers Policy*), puis masquer (ACL modification) la GPO originelle '6AC1786C-016F-11D2-945F-00C04fB984F9' du domaine

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

How to check

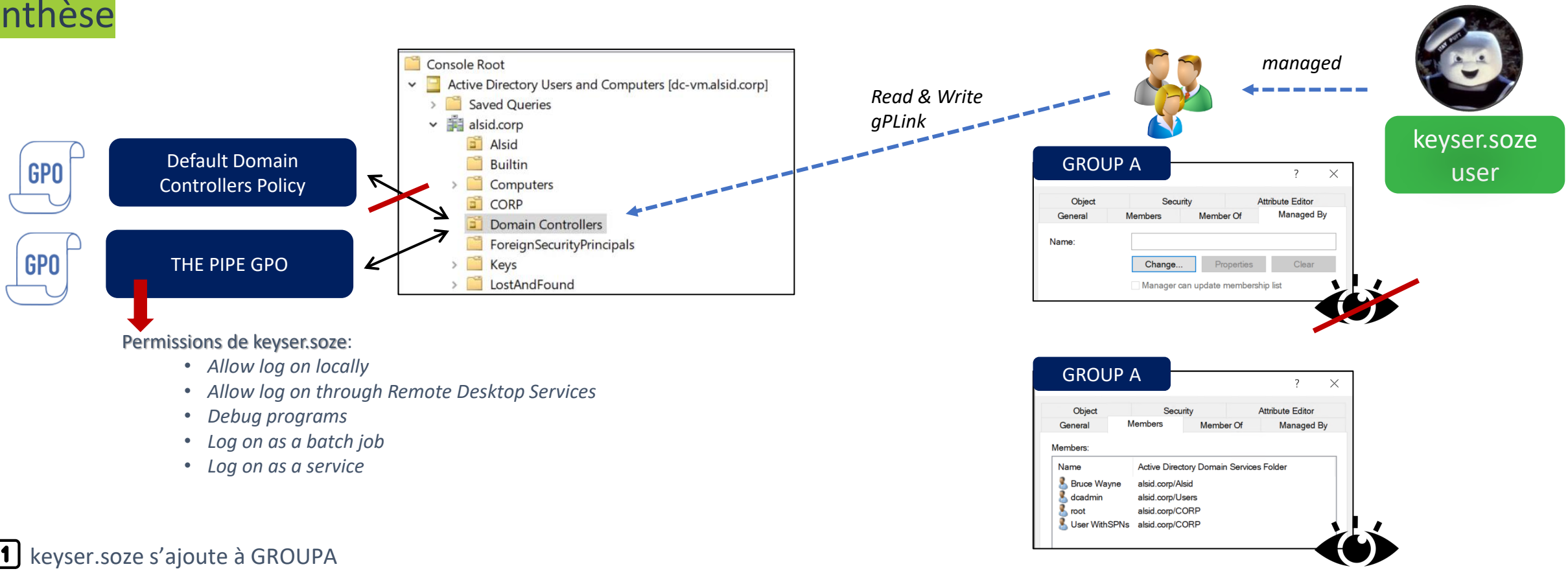
Comment verifier ?

- Check the “well-known” Group Policies values

Default Domain Controllers Policy	{6AC1786C-016F-11D2-945F-00C04FB984F9}
Default Domain Policy	{31B2F340-016D-11D2-945F-00C04FB984F9}

AD backdooring techniques – gPLink attribute to perform Domain Controllers future dominance

Synthèse



Permissions de keyser.soze:

- *Allow log on locally*
- *Allow log on through Remote Desktop Services*
- *Debug programs*
- *Log on as a batch job*
- *Log on as a service*

1 keyser.soze s'ajoute à GROUPA
2 GROUPA peut modifier le gPLink attribute au niveau de l'unité d'organisation– keyser.soze remplace le « default domain controllers policy » ID par le « PIPE GPO » ID
3 « THE PIPE GPO » autorise l'accès global à keyser.soze à tous les contrôleurs de domaine
4 keyser.soze masque la stratégie originelle « default domain controllers policy »
5 keyser.soze peut tout faire sur les DCs sans être membre des groupes « Domain admins » ou « Enterprise admins »

Conclusion & Q&A

A retenir

Faire la chasse aux portes dérobées AD, c’est FUN !

Souvenez-vous de la pilule bleue et de la pilule rouge

En fait, vous ne pouvez pas compter sur vos sauvegardes

Astuce : Surveillez les nouvelles entrées Deny ACEs dans votre répertoire

Très souvent ce n’est pas bon signe du tout...

Y’a rien à gagner cette année ???? 😭

Je suis …

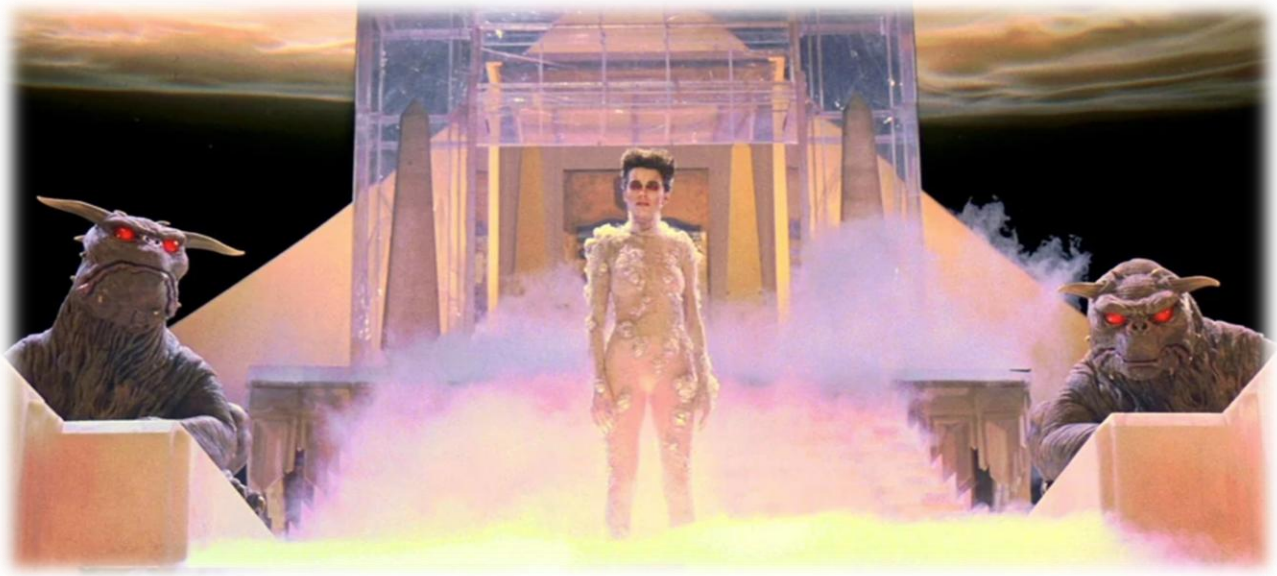
Je suis un monstre du film originel « Ghostbusters » qui n’a pas été cité / représenté jusque là

Je suis une entité ancienne et malveillante, considérée comme une divinité extra-dimensionnelle et qui possède des pouvoirs quasi illimités (manipuler la réalité, invoquer des serviteurs, provoquer des catastrophes massives)

J’apparais tout d’abord sous une forme humanoïde, avec un look très étrange et franchement kitsch.
Ensuite, les Ghostbusters choisissent mon apparence finale en tant que Bibendum.

Je suis … Je suis …

GOZER le Gozerien



IDENTITY DAYS

21 octobre 2025 - PARIS

Un grand merci à tous nos partenaires !

21 octobre 2025 - PARIS

IDENTITY DAYS

@IdentityDays
#identitydays2025