# Contexte

L’historique d’identificateurs de sécurité (SID History) peut être utilisé lors d’une migration entre deux domaines ou forêts. La présence de cet attribut dans un compte utilisateur indique une migration en cours. Dans ce cas, les identifiants de domaines contenus dans les SID de cet historique devraient pouvoir être résolu. Dans le cas contraire, cela indique que la migration est terminée et que l’ancien domaine a été supprimé. Donc l’historique d’identificateurs de sécurité devrait être supprimé également.

# Conséquences

La présence d’un historique d’identificateurs de sécurité peut participer à l’introduction des risques suivants :

* **Déplacement latéral** : Si un attaquant obtient l'accès à un compte utilisateur avec l'historique d’identificateurs de sécurité activé, il pourrait exploiter cette fonctionnalité pour se déplacer latéralement dans le réseau. En se faisant passer pour un utilisateur d'un autre domaine ou d'une autre forêt avec des privilèges élevés, l'attaquant pourrait accéder à des ressources dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations.
* **Élévation de privilèges** : Si un attaquant compromet un compte utilisateur avec l'historique d’identificateurs de sécurité activé et parvient à élever ses privilèges dans son propre domaine, il pourrait exploiter l'historique d’identificateurs de sécurité pour escalader davantage les privilèges dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations historiques. Cela pourrait conduire à l'obtention d'un accès administratif à des systèmes critiques ou à des données sensibles.
* **Persistance** : Un attaquant qui obtient l'accès à un environnement peut tenter d'établir une présence persistante en modifiant l'historique d’identificateurs de sécurité des comptes utilisateur compromis. En ajoutant leur propre identificateur de sécurité à l'historique d'un compte à privilèges élevés, l'attaquant pourrait maintenir l'accès aux ressources même si leur accès initial est détecté et corrigé.

## Chaine de cyberattaques

La présence d’un historique d’identificateurs de sécurité peut participer à l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Reconnaissance** : L’activation du filtrage des identificateurs de sécurité rend plus difficile pour les attaquants de tirer parti des autorisations historiques lors des activités de reconnaissance.
* **Exploitation** : L’activation du filtrage des identificateurs de sécurité peut rendre plus difficile pour les attaquants d'exploiter les relations de confiance entre les domaines ou les forêts, limitant leur capacité à escalader les privilèges et à se déplacer latéralement dans le réseau.
* **Installation** : L’activation du filtrage des identificateurs de sécurité peut aider à empêcher les attaquants d'utiliser des identifiants compromis avec des autorisations historiques pour maintenir la persistance dans l'environnement.
* **Commande et contrôle** : L’activation du filtrage des identificateurs de sécurité peut perturber la capacité des attaquants à se faire passer pour des utilisateurs avec des autorisations historiques, rendant plus difficile pour eux d'éviter la détection et de contrôler les systèmes compromis.

Documentation :

* <https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html>

# Détection

Les commandes PowerShell suivantes permettent de lister les identificateurs de sécurité non résolus des historiques d’identificateurs de sécurité des utilisateurs du domaine :

#

# Installer le module Active Directory  
#

# Install-Module ActiveDirectory

#

# Importer le module Active Directory

#

Import-Module ActiveDirectory

#

# Rechercher tous les utilisateurs du domaine avec un historique d’identificateurs de sécurité

#

$Users = Get-ADUser -Filter {sidhistory -like "\*"} -Properties sidHistory  
  
#  
# Pour chaque utilisateur du domaine  
#

ForEach ($User in $Users) {  
 #

# Pour chaque identificateur de sécurité

#

ForEach ($SID in $User.sidHistory) {

#

# Créer un objet .NET identificateur de sécurité

#

$SIDObject = New-Object System.Security.Principal.SecurityIdentifier($SID)

#

# Rechercher le domaine correspondant à l’identificateur de sécurité

#

$Domain = Get-ADDomain -Filter {Sid -eq $ SIDObject.AccountDomainSid}

#  
 # Si le domaine n’existe pas  
 #

if (-not $Domain) {

Write-Host $SIDObject.AccountDomainSid

}

}  
}

Les commandes PowerShell suivantes permettent de lister les identificateurs de sécurité non résolus des historiques d’identificateurs de sécurité des groupes d’utilisateurs du domaine :

#

# Installer le module Active Directory  
#

# Install-Module ActiveDirectory

#

# Importer le module Active Directory

#

Import-Module ActiveDirectory

#  
# Rechercher tous les groupes d’utilisateurs du domaine avec un historique d’identificateurs de sécurité

#

$Groups = Get-ADGroup -Filter {sidhistory -like "\*"} -Properties sidHistory  
  
#  
# Pour chaque groupe d’utilisateurs du domaine  
#

ForEach ($Group in $Groups) {  
 #

# Pour chaque identificateur de sécurité

#

ForEach ($SID in $Group.sidHistory) {

#

# Créer un objet .NET identificateur de sécurité

#

$SIDObject = New-Object System.Security.Principal.SecurityIdentifier($SID)

#

# Rechercher le domaine correspondant à l’identificateur de sécurité

#

$Domain = Get-ADDomain -Filter {Sid -eq $ SIDObject.AccountDomainSid}

#  
 # Si le domaine n’existe pas  
 #

if (-not $Domain) {

Write-Host $SIDObject.AccountDomainSid

}

}  
}

# Correction

## Prérequis

Il faut s’assurer qu’aucune migration de forêt légitime ne soit en cours, car la suppression de l’historique d’identificateurs de sécurité sur une forêt en cours de migration pourrait compromettre le bon fonctionnement des comptes dont l’ancien identificateur de sécurité est encore utilisé dans des listes de contrôle d’accès (ACL) sur le nouveau domaine. Si une migration est en cours, celle-ci doit être terminée au plus vite et les anciens identificateurs de sécurité ne doivent plus être utilisés.

## Procédure

Il est recommandé de supprimer les historiques d’identificateurs de sécurité des comptes et groupes d’utilisateurs du domaine.

Les commandes PowerShell suivantes permettent de supprimer l’historique d’identificateurs de sécurité de tous les utilisateurs du domaine :

#

# Installer le module Active Directory  
#

# Install-Module ActiveDirectory

#

# Importer le module Active Directory

#

Import-Module ActiveDirectory

#

# Rechercher tous les utilisateurs du domaine avec un historique d’identificateurs de sécurité et le supprimer

#

$Users = Get-ADUser -Filter {sidhistory -like "\*"} -Properties sidHistory | ForEach {Set-ADUser $\_ -Remove @{sidhistory=$\_.sidhistory.value}}

Les commandes PowerShell suivantes permettent de supprimer l’historique d’identificateurs de sécurité de tous les groupes d’utilisateurs du domaine

#

# Installer le module Active Directory  
#

# Install-Module ActiveDirectory

#

# Importer le module Active Directory

#

Import-Module ActiveDirectory  
  
#  
# Rechercher tous les groupes d’utilisateurs du domaine avec un historique d’identificateurs de sécurité et le supprimer

#

$Users = Get-ADGroup -Filter {sidhistory -like "\*"} -Properties sidHistory | ForEach {Set-ADGroup $\_ -Remove @{sidhistory=$\_.sidhistory.value}}

Documentation :

* <https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-adobject?view=windowsserver2022-ps>

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater qu’aucun identificateur de sécurité n’est listé.