# Contexte

La clé secrète de Kerberos est utilisée pour autoriser l’accès d’un utilisateur à une ressource du domaine par l’intermédiaire de tickets. Si cette clé secrète est compromise cela peut permettre la création de tickets illégitimes, *Golden Tickets* en anglais. Il est donc recommandé, entre autres, de modifier cette clé secrète tous les 40 jours à 6 mois maximum.

Le compte Kerberos a un historique avec les deux clés secrètes les plus récentes, il est donc important de changer cette clé deux fois de suite de façon à supprimer l’ancienne clé de l’historique et ainsi d’invalider les éventuels tickets illégitimes. Cependant, il est important d’attendre la période maximale de validité d’un ticket Kerberos entre deux changements de clé. Par défaut la période maximale de validité d’un ticket Kerberos est de 10 heures.

Documentation :

* <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password>

# Conséquences

La compromission d’une clé secrète Kerberos peut avoir des impacts significatifs :

* **Déplacement latéral** : La compromission d’une clé secrète Kerberos permet aux attaquants d’obtenir un accès non autorisé à toutes les ressources du réseau cible.
* **Élévation de privilèges** : La compromission d’une clé secrète Kerberos permet aux attaquants de s'attribuer eux-mêmes n'importe quels privilèges qu'ils souhaitent au sein du réseau. Ils peuvent se donner accès à des comptes, systèmes ou services hautement privilégiés.
* **Persistance** : La compromission d’une clé secrète Kerberos permet de fournir un accès persistant au réseau. Même si l'organisation détecte et atténue la violation initiale, tant que les tickets illégitimes restent valides, l'attaquant peut continuer à accéder au réseau.

## Chaine de cyberattaques

La compromission d’une clé secrète Kerberos peut permettre l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Exploitation** : La création de tickets Kerberos illégitimes peut permettre de donner un accès à des services présentant une faille de sécurité et ainsi permettre d’exploiter des vulnérabilités.
* **Installation** : La création de tickets Kerberos illégitimes peut permettre la création d’accès permanent au systèmes compromis en offrant des droits administrateurs sur les systèmes de sécurité.
* **Commande** **et** **contrôle** : La création de tickets Kerberos illégitimes peut permettre le contrôle d’exécutables.
* **Actions** **sur** **objectif** : La création de tickets Kerberos illégitimes peut permettre la lecture ou l’écriture de données sur l’ensemble des systèmes compromis, rendant possible, par exemple, le vol de données.

Documentation :

* <https://attack.mitre.org/techniques/T1558/001/>

# Détection

Les commandes PowerShell suivantes permettent d’afficher la date de dernière mise-à-jour de la clé secrète Kerberos :

#

# Recherche la date de dernière mise-à-jour de la clé secrète Kerberos

#  
$Timestamp = Get-ADUser krbtgt -Properties "PasswordLastSet" | Select-Object -ExpandProperty PasswordLastSet | [datetime]::FromFileTime($\_)

Si la date de dernière mise-à-jour de la clé secrète Kerberos est supérieur à 6 mois, par rapport à la date du jour, alors celle-ci doit être mise à jour.

# Correction

## Prérequis

La dernière mise-à-jour du mot de passe Kerberos ne doit pas être plus récent que la durée maximale de validité des tickets Kerberos qui est, par défaut, de 10 heures. Par ailleurs, il est recommandé d’attendre trois jours pour être certain que la première mise-à-jour soit propagée sur les contrôleurs de domaine.

## Procédure

Les commandes PowerShell suivantes permettent de faire une mise à jour de la clé secrète Kerberos :

#  
# Liste les caractères utilisables pour le mot de passe :   
# - Minuscules (97..122)  
# - Majuscules (65..90)  
# - Chiffres (48..57)  
# - Caractères spéciaux (33..47), (58..64), (91..96), (123..126)  
#  
$CharactersSet = (97..122) + (65..90) + (48..57) + (33..47) + (58..64) + (91..96) + (123..126)  
  
#  
# Génère un mot de passe complexe de 256 charactères  
#  
$Password = ""  
  
ForEach ($Index in (0..255)) {  
 $Password += $CharactersSet | Get-Random | % {[char]$\_}  
}  
  
#

# Défini le nouveau mot de passe du compte utilisateur Kerberos

#   
Get-ADUser krbtgt -Server $Server | Set-ADAccountPassword -Reset -NewPassword -AsPlainText (ConvertTo-SecureString $Password) -Force

Documentation :

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

# Vérification

Pour vérifier la correction de l’anomalie, il est possible d’exécuter de nouveau la partie "Détection" et de s’assurer que la date de dernière mise-à-jour de la clé secrète Kerberos est inférieur à 6 mois.