AYI NEDJIMI Consultants

Silver Ticket : Attaque Kerberos Service Active

10 mai 2026 • Mis à jour le 17 mai 2026 • 31 min de lecture • 6132 mots •

Le Silver Ticket (MITRE T1558.002) est une attaque post-exploitation sur A
Directory consistant a forger localement un TGS Kerberos a partir du hash
des cles AES d'un compte de service compromis, afin d'acceder a ce serv
solliciter le KDC. Devoile en 2014 par Benjamin Delpy via Mimikatz, il cible
les SPN CIFS, MSSQLSvc, HOST, LDAP ou HTTP. Sa furtivite redoutable pr
l'absence totale de contact avec le DC : aucun Event 4768 ou 4769 n'est g
guide entity-first detaille le principe cryptographique, les pre-requis (Kerbe
DCSync, Pass-the-Hash), la fabrication avec Mimikatz, Rubeus et Impacke
services typiques, la detection (Event 4624, PAC validation, Defender for I
les mitigations (gMSA, AES-only, rotation hashes, PAC signature stricte).

Le **Silver Ticket** est une attaque post-exploitation sur Active Directory qui consiste **localement un ticket de service Kerberos (TGS)** à partir du hash NTLM ou des clé compte de service compromis, afin d'accéder à ce s olliciter le c domaine. Référencée sous l'identifiant **T1558.002** da ITRE ATT&

Steal or Forge Kerberos Tickets), la technique a été dévoilée publiquement en 201
Delpy, créateur de Mimikatz, en complément de son Golden Ticket. Là où le Golde
un TGT signé par `krbtgt` et ouvre tout le domaine, le Silver Ticket forge un **TGS**
avec le hash du compte de service hébergeant la ressource (CIFS, MSSQLSvc, HO
LDAP). Sa redoutable furtivité provient d'un détail protocolaire majeur : **aucun con
KDC n'est nécessaire pour l'exploitation, le serveur applicatif validant lui-même la
sa propre clé. Aucun Event 4768 (TGT request) ni 4769 (TGS request) n'est généré
contrôleurs de domaine, rendant la détection particulièrement difficile sans télémé
avancée. Cette page entity-first détaille le principe cryptographique, les pré-requi
(compromission du hash machine ou du compte de service via Kerberoasting, DCS
the-Hash), la fabrication du ticket avec Mimikatz, Rubeus et Impacket ticketer, les
typiquement ciblés, les stratégies de détection (Event 4624 LogonType 3, PAC val
Defender for Identity) et les contre-mesures de mitigation (gMSA, AES-only, rotati
Que vous soyez analyste SOC, pentester certifié OSCP/OSEP, architecte AD ou RS
le Silver Ticket est essentiel pour défendre votre infrastructure Microsoft en 2026.

À RETENIR

L'essentiel à retenir sur le Silver Ticket

Identifiant MITRE : T1558.002 — Steal or Forge Kerberos Tickets: Silver Tic

Type de ticket forgé : TGS (Ticket Granting Service), pas un TGT.

Clé de signature : hash NTLM ou clé AES du compte hébergeant le service

Pré-requis : compromission du hash machine ($) ou du compte de service
owner).

Furtivité majeure : aucun appel au DC, donc 769 côté KD

Réponse sous 24h

Devis gratuit →