AYI NEDJIMI Consultants

Mimikatz : Extraction Credentials Active Directory

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3661 mots • 68 vues •

Mimikatz, l'outil de Benjamin Delpy (gentilkiwi) qui a redéfini les attaques Active Directory : Pass-the-Hash, Golden Ticket, DCSync, LSASS dump, forks (Pypykatz, Lsassy, NanoDump), détection EDR et mitigations Microsoft (Credential Guard, LSA Protection, Tier model).

Mimikatz est l'outil d'extraction de credentials Windows le plus emblématique de l'histoire de la cybersécurité offensive, créé en 2007 par le chercheur français **Benjamin Delpy** alias *gentilkiwi*. Distribué en open source sous licence CC BY 4.0 sur GitHub, ce logiciel écrit en C exploite les mécanismes internes du sous-système d'authentification Windows (LSASS, SAM, LSA Secr
Manager) pour extraire mots de passe en clair, hash

Kerberos et clés cryptographiques directement depuis la mémoire vive ou les bases de données système. Initialement conçu comme un proof-of-concept pédagogique pour démontrer les faiblesses du stockage des credentials sous Windows, Mimikatz est devenu en quinze ans la pierre angulaire de la quasi-totalité des compromissions Active Directory documentées : attaques APT (APT28, APT29, Lazarus), ransomwares (Conti, LockBit, BlackCat, Ryuk), opérations red team et exercices de pentest interne. Ses techniques signature — **Pass-the-Hash**, **Pass-the-Ticket**, **Golden Ticket**, **Silver Ticket**, **DCSync**, **Overpass-the-Hash** — ont durablement transformé la doctrine de défense des environnements Windows et imposé l'adoption de contre-mesures spécifiques (Credential Guard, LSA Protection, modèle Tier 0/1/2, Protected Users group). Cette page entity-first synthétise l'architecture modulaire de Mimikatz, ses modules emblématiques (sekurlsa, lsadump, kerberos), ses dérivés modernes (PyKatz, Lsassy, NanoDump, SharpKatz) et les stratégies de détection EDR/AV applicables en 2026. Que vous soyez analyste SOC, pentester certifié OSCP/OSEP, architecte AD ou RSSI, comprendre Mimikatz reste un prérequis incontournable pour défendre efficacement votre infrastructure Microsoft.

À RETENIR

L'essentiel à retenir sur Mimikatz

Auteur : Benjamin Delpy (gentilkiwi), chercheur français
premier release interne 2007, publication Gith

Réponse sous 24h

Devis gratuit →