AYI NEDJIMI Consultants

DCSync : Attaque de Réplication Active Directory 2026

10 mai 2026 • Mis à jour le 17 mai 2026 • 21 min de lecture • 4478 mots • 72 vues •

DCSync est une attaque de credential dumping (MITRE T1003.006) qui exploite le protocole legitime MS-DRSR de replication Active Directory pour extraire a distance les hashes NTLM de n'importe quel compte du domaine, y compris krbtgt. Formalisee en 2015 par Benjamin Delpy et Vincent Le Toux dans Mimikatz, elle ne necessite aucune execution de code sur le DC cible et abuse une fonctionnalite documentee de Microsoft, sans CVE associe. Ce guide entity-first detaille le fonctionnement protocolaire, les outils (Mimikatz, Impacket secretsdump, Invoke-DCSync), la detection (Event 4662, Defender for Identity, Splunk ES) et les contre-mesures (audit ACL DRS, rotation krbtgt biannuelle, modele Tier 0).

DCSync est une attaque de credential dumping qui exploite le protocole légitime de réplication des contrôleurs de domaine Active Directory, le **MS-DRSR** (Directory Replication Service Remote Protocol), pour extraire à distance les hashes NTLM de n'importe quel compte du domaine, y compris le compte hautement privilégié `krbtgt`. Référencée sous l'identifiant **T1003.006** dans le framework MITRE ATT&CK (catégorie *OS Credential Dumping*), cette technique a été formalisée et opérationnalisée en 2015 par **Benjamin Delpy** et **Vincent Le Toux** via le module `lsadump::dcsync` de Mimikatz. Sa puissance redoutable provient de trois caractéristiqu
ne nécessite *aucune exécution de code* sur le contrô

Réponse sous 24h

Devis gratuit →