Active Directory en 2026 : la cible éternelle

> Analyse terrain : pourquoi Active Directory reste la cible n°1 des attaquants en 2026 malgré 30 ans d'existence. ZeroLogon, CVE-2026-41089, Kerberoasting,...

Chaque semaine, une nouvelle vulnérabilité critique dans Active Directory ou dans un composant satellite. Chaque année, les rapports d'incidents des grandes entreprises de threat intelligence placent AD en tête des vecteurs de compromission. CVE-2026-41089 dans Netlogon, ZeroLogon en 2020, PrintNightmare en 2021, NTLM relay en permanence, Kerberoasting industrialisé. Le même film depuis trente ans, avec des acteurs de plus en plus capables et des défenseurs qui accumulent des outils sans résoudre le problème structurel. Voici ce que les audits terrain révèlent vraiment.

Points clés à retenir

• La cybersécurité proactive prévaut sur la réaction post-incident pour limiter l'impact

• La documentation et les procédures formalisées sont essentielles lors des audits et certifications

• La veille continue et la mise à jour régulière des compétences sont indispensables face à l'évolution des menaces

Trente ans et toujours n°1 des vecteurs de compromission

Active Directory a été introduit avec Windows 2000 Server, en l'an 2000. Nous sommes en 2026. Vingt-six ans plus tard, il est présent dans la quasi-totalité des entreprises de plus de 50 salariés, il gère les identités de centaines de millions d'utilisateurs dans le monde, et il reste — de très loin — la cible la plus exploitée dans les incidents de sécurité que j'instruis ou que j'analyse.

> ⚡ **Retour terrain**
>
> Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

Selon le DBIR 2025 de Verizon, les attaques par compromission d'identifiants représentent le vecteur d'attaque initial le plus fréquent dans les incidents d'entreprise. Une grande majorité de ces compromissions aboutit à une escalade de privilèges dans Active Directory, que ce soit via des techniques de Kerberoasting, d'AS-REP Roasting, de DCSync, ou de Path-of-Least-Privilege (exploitation des chemins d'attaque dans BloodHound). Mandiant, dans ses M-Trends récents, note que le temps médian entre la compromission initiale et l'atteinte de Domain Admin continue de diminuer — non parce que les vulnérabilités AD sont plus nombreuses, mais parce que les attaquants les maîtrisent mieux et les outillent davantage.

CVE-2026-41089 dans Netlogon, avec son CVSS 9.8 et son exploitation active confirmée dès fin mai 2026, n'est pas une anomalie. C'est le dernier exemple d'un schéma récurrent : une composante fondamentale d'Active Directory, dont le code remonte à plusieurs décennies et dont la surface d'attaque est structurellement difficile à réduire, est affectée par une vulnérabilité critique exploitable sans authentification. ZeroLogon en 2020 suivait le même schéma. PrintNightmare en 2021 idem. Les vulnérabilités NTLM relay qui se renouvellent chaque année depuis quinze ans, idem.

Ce n'est pas une question de compétence des équipes Microsoft. C'est une question d'architecture héritée. Active Directory a été conçu pour un monde où le réseau interne était un espace de confiance totale, où les postes clients n'étaient jamais compromis, et où la priorité absolue était l'interopérabilité et la rétrocompatibilité. Ces trois hypothèses sont fausses depuis au moins quinze ans. L'écart entre l'architecture du protocole et le contexte de menace actuel ne se comble pas avec des patches — il nécessite une réécriture fondamentale que les contraintes de compatibilité et les intérêts commerciaux de l'écosystème rendent politiquement impossible.

Le résultat : on patch, on surveille, on détecte — mais on ne résout pas. Et les attaquants le savent parfaitement.

Les chemins d'attaque classiques qui fonctionnent toujours en 2026

Je réalise des audits de sécurité en conditions réelles depuis plusieurs années. La constante la plus frappante : les mêmes techniques de compromission Active Directory fonctionnent d'une

organisation à l'autre, année après année, quelle que soit la taille ou le secteur de l'entreprise. Voici les principales, avec leur niveau de maturité offensif actuel.

Kerberoasting. Technique documentée depuis 2014 par Tim Medin, encore pleinement opérationnelle en 2026. Elle consiste à demander des tickets Kerberos de service (TGS) pour des comptes de service ayant un SPN (Service Principal Name) enregistré, puis à les craquer hors ligne pour récupérer le mot de passe du compte. Dans la quasi-totalité des organisations que j'audite, je trouve au minimum 5 à 10 comptes de service Kerberoastables avec des mots de passe faibles ou non rotés depuis plusieurs années. Ces comptes ont souvent des privilèges élevés — délégation, accès à des bases de données, droits d'administration locale sur des serveurs critiques. Le chemin de Domain Admin est souvent direct. La défense existe (comptes gMSA, mots de passe longs et complexes, tiering) mais n'est que rarement déployée de manière cohérente.

AS-REP Roasting. Variante du Kerberoasting ciblant les comptes dont le pré-authentification Kerberos est désactivée. Ces comptes permettent à n'importe quel utilisateur de requêter un TGT (Ticket Granting Ticket) chiffré avec le hash du compte cible, récupérable et crackable hors ligne. Ce paramètre est parfois désactivé pour des raisons de compatibilité avec des applications legacy ou par erreur de configuration. Dans mes audits, je le trouve dans 60 à 70% des environnements testés, sur au moins un compte à privilèges.

DCSync. Technique qui exploite les droits de réplication d'AD (Replication Directory Changes, Replication Directory Changes All) pour extraire les hash NTLM de n'importe quel compte, y compris les Domain Admins et le compte krbtgt, sans accès physique au DC. DCSync est l'outil de référence post-exploitation dans tous les frameworks offensifs modernes (Mimikatz, Impacket, CrackMapExec, BloodHound + Certipy). Dans les audits, trouver un compte avec ces droits de réplication hors des Domain Admins légitimes est la règle plus que l'exception — délégations oubliées, comptes de backup logiciel, connecteurs d'applications tierces.

NTLM Relay. Famille de techniques exploitant le protocole d'authentification NTLM pour capturer et relayer des authentifications vers d'autres services. Documentée depuis les années 2000, toujours exploitable en 2026 dans la grande majorité des réseaux d'entreprise. Les variantes les plus récentes — PetitPotam, DFSCoerce, PrinterBug, ShadowCoerce — exploitent des fonctionnalités légitimes de Windows pour forcer des authentifications NTLM automatiques depuis des comptes système, y compris les comptes machines des contrôleurs de domaine eux-mêmes. Résultat : dans un réseau non durci, un attaquant sans aucune authentification initiale

peut récupérer le hash NTLMv2 d'un DC et l'utiliser pour prendre le contrôle du domaine via des attaques de type relay vers LDAP ou SMB.

Active Directory Certificate Services (ADCS). Les misconfigurations dans les templates de certificats AD CS constituent depuis 2021 (publication de l'article SpecterOps sur ESC1-ESC8) un vecteur d'attaque particulièrement productif. Dans les organisations ayant déployé ADCS (une majorité des grandes entreprises), des templates de certificats mal configurés permettent souvent d'obtenir un certificat pour n'importe quel compte du domaine — y compris Domain Admin — et de l'utiliser pour s'authentifier via PKINIT Kerberos. L'outil Certipy automatise entièrement la reconnaissance et l'exploitation de ces configurations en quelques minutes.

Ces cinq vecteurs ne nécessitent pas de zero-day. Ils n'exigent pas un niveau d'expertise exceptionnel. Des frameworks comme BloodHound, Impacket, CrackMapExec et Certipy les rendent accessibles à des attaquants de niveau intermédiaire. Et pourtant, ils fonctionnent dans la grande majorité des environnements d'entreprise en 2026.

2026 : l'automatisation change l'échelle, pas la nature

Ce qui change en 2026, ce n'est pas l'invention de nouvelles techniques d'attaque AD. C'est l'industrialisation et l'automatisation de ces techniques existantes, couplées à l'émergence de l'IA comme copilote offensif.

Les frameworks comme BloodHound CE (Community Edition) ont atteint un niveau de maturité qui permet à un attaquant de niveau intermédiaire de cartographier un domaine de plusieurs milliers d'objets AD, d'identifier les chemins d'attaque les plus courts vers Domain Admin, et de générer automatiquement les commandes d'exploitation en moins d'une heure. Ce qui prenait des journées à un expert il y a cinq ans se fait maintenant en une session de travail pour quelqu'un de moyennement expérimenté.

L'IA augmente encore ce phénomène. Le cas du zero-day généré par IA documenté par Google GTIG en mai 2026 illustre que les modèles de langage peuvent maintenant participer à la découverte de vulnérabilités dans des logiciels réels, pas seulement à la rédaction de variants de malwares connus. Appliqué à AD, cela signifie que des configurations atypiques ou des

vulnérabilités dans des extensions propriétaires d'AD (ADFS, ADCS templates custom, extensions de schéma d'éditeurs tiers) pourraient être détectées et exploitées par des acteurs de menace augmentés par IA dans des délais bien plus courts que par le passé.

Les groupes de ransomware les plus actifs en 2026 — LockBit 4.0, RansomHub, Play, BlackBasta dans sa version restructurée — ont tous industrialisé la compromission Active Directory dans leurs chaînes d'attaque. Leurs affiliés disposent de runbooks détaillés couvrant l'ensemble des techniques mentionnées ci-dessus, de frameworks automatisés pour l'exécution, et de délais d'atteinte de Domain Admin qui se mesurent désormais en heures, plus en jours. Le rapport Mandiant M-Trends 2025 indique que le dwell time médian (temps entre compromission initiale et détection) reste autour de 10 jours dans les environnements sans MDR — une fenêtre plus que suffisante pour compromettre un domaine AD.

La combinaison automatisation + IA + maturité des frameworks offensifs crée une asymétrie croissante entre attaque et défense. Les défenseurs doivent bloquer chaque vecteur ; les attaquants doivent en réussir un seul. Cette asymétrie fondamentale ne se résout pas en ajoutant une couche d'outil de détection supplémentaire.

La dette technique AD : le problème que personne ne veut financer

Voici ce que je vois systématiquement quand j'audite des environnements Active Directory d'entreprises de taille moyenne à grande, tous secteurs confondus.

Des comptes de service créés il y a dix ans avec des mots de passe de 8 caractères jamais rotés depuis leur création initiale. Des GPO héritées de trois fusions-acquisitions successives, avec des couches de configuration contradictoires que personne n'ose toucher de peur de casser quelque chose en production. Des droits d'administration locale accordés à la louche sur des centaines de postes, parce qu'une application métier en 2012 le nécessitait et que le retrait de ce droit est potentiellement problématique. Des schémas ADCS déployés par un éditeur tiers en 2018 avec des templates ESC1 non revus depuis.

Des comptes dormants de prestataires, de stagiaires, d'anciens salariés — pas désactivés, parfois avec des membres de groupes à privilèges par erreur d'historique. Des délégations Kerberos

unconstrained sur des serveurs applicatifs vieux de 8 ans, incompatibles avec la délégation contrainte, impossibles à migrer sans refonte applicative. Des DCs sous Windows Server 2012 R2 (support étendu terminé depuis octobre 2023) maintenus en vie parce que « la migration, c'est pour le prochain exercice budgétaire ».

Ce n'est pas de la négligence. C'est de la dette technique accumulée sur vingt ans d'évolution d'un SI d'entreprise, dans un contexte où les équipes IT sont undersized, où les budgets de sécurité arrivent tard et insuffisamment, et où chaque intervention sur l'infrastructure Active Directory présente un risque de régression en production que les directions métier n'acceptent pas pendant les périodes clés de l'activité. Résultat : les nettoyages sont reportés, la surface d'attaque grossit, et les auditeurs trouvent les mêmes problèmes d'une organisation à l'autre, d'une année à l'autre.

La bonne nouvelle : cette dette est adressable. La mauvaise : elle nécessite un investissement en temps et en expertise que la plupart des organisations sous-estiment, et une volonté politique de prendre des risques de régression calculés pour traiter les problèmes structurels plutôt que de les contourner par des détections compensatoires.

Ce qui fonctionne vraiment pour réduire le risque

Après des années d'audits et de missions de réponse à incident sur des environnements AD compromis, voici ce qui réduit réellement le risque — pas ce qui génère le plus de slides dans les présentations commerciales.

Le tiering Active Directory (aussi appelé Privileged Access Workstation ou PAW model) est la mesure structurelle la plus efficace que je connaisse. Le principe : séparer les comptes d'administration en niveaux (Tier 0 : DC et ADCS, Tier 1 : serveurs, Tier 2 : postes), interdire rigoureusement la connexion interactive des comptes Tier 0 sur des systèmes Tier 1 ou Tier 2, et utiliser des postes dédiés pour chaque niveau. Cette mesure coupe les chemins d'escalade de privilèges les plus courants et rend la compromission d'un poste utilisateur incapable d'aboutir directement à Domain Admin. Elle est difficile à mettre en oeuvre dans les organisations avec une dette technique élevée — mais c'est exactement pour cette raison qu'elle est si efficace quand elle est déployée.

La rotation des comptes de service vers gMSA (group Managed Service Accounts) traite le Kerberoasting à la source. Les gMSA ont des mots de passe de 120 caractères aléatoires, rotés automatiquement tous les 30 jours, non extractables par des outils standards. La migration est souvent possible pour la plupart des comptes de service courants, et le coût de la migration est largement inférieur au coût d'une compromission via Kerberoasting.

L'activation de Protected Users sur les comptes à privilèges empêche leur utilisation avec NTLM (forçant Kerberos), désactive la délégation Kerberos unconstrained, et réduit la durée de vie des tickets Kerberos. Cette mesure est souvent invisible pour les utilisateurs légitimes mais coupe plusieurs vecteurs d'attaque simultanément. Elle ne coûte rien à déployer — juste l'ajout au groupe AD Protected Users.

L'audit régulier avec BloodHound CE du côté défensif — oui, le même outil que les attaquants — permet d'identifier et de corriger proactivement les chemins d'attaque avant que les adversaires ne les exploitent. Cartographier son propre domaine avec BloodHound une fois par trimestre, corriger les chemins courts vers Domain Admin, vérifier la régression au trimestre suivant. C'est simple, gratuit, et extrêmement efficace quand c'est pratiqué systématiquement.

Le monitoring spécifique AD (pas seulement la collecte de logs) avec des outils dédiés comme Microsoft Defender for Identity (anciennement ATA), Semperis DSP, ou des règles SIEM ciblées sur les patterns d'attaque AD (DCSync attempts, AS-REP requests anormaux, LDAP enumeration massive, modifications d'ACL sensibles) permet de détecter les phases de reconnaissance et d'exploitation avant qu'elles n'aboutissent. La détection fonctionne si elle est configurée correctement et si les alertes sont traitées — deux conditions souvent non réunies simultanément.

La rotation du compte krbtgt deux fois par an (ou après toute suspicion de compromission) limite la validité des Golden Tickets potentiellement générés par un attaquant ayant eu accès au hash krbtgt. C'est une mesure de remédiation essentielle après tout incident AD et une bonne pratique préventive souvent négligée.

Ce qui ne fonctionne pas — et pourtant tout le monde le vend

Autant être direct sur ce qui ne résout pas le problème AD, même si c'est commercialement populaire.

L'achat d'un XDR ou d'un SIEM supplémentaire n'adresse pas la dette technique. Si votre réseau a des milliers de comptes Kerberoastables avec des mots de passe faibles, un XDR de plus ne changera pas fondamentalement l'exposition. La détection est utile — indispensable, même — mais elle traite les symptômes, pas la cause.

Les formations de sensibilisation sur le phishing n'ont qu'un impact marginal sur les vecteurs AD classiques. La majorité des compromissions AD documentées en 2026 ne débutent pas par un utilisateur qui clique sur un lien malveillant. Elles débutent par une exploitation directe d'un service exposé, par un credential spray sur un service d'authentification exposé, ou par la compromission d'un partenaire avec une relation de confiance AD. Le phishing est un vecteur, pas LE vecteur dominant dans les incidents AD de grande envergure.

Les scans de vulnérabilités périodiques sans suivi de remediation génèrent des rapports que personne ne lit jusqu'au bout et des plans de remédiation que personne ne déploie. J'ai vu des organisations avec des rapports d'audit AD pointant les mêmes problèmes critiques depuis quatre ans consécutifs. Le problème n'est pas le manque de visibilité — c'est le manque de capacité et de volonté à traiter les problèmes structurels identifiés.

La désactivation de NTLMv1 seul, sans désactivation de NTLMv2 et sans traitement des délégations Kerberos unconstrained, n'apporte qu'une protection très partielle contre les attaques relay. NTLMv2 est toujours relayable dans de nombreux scénarios. La vraie protection nécessite une combinaison de mesures — signature SMB obligatoire, LDAP signing et channel binding, désactivation de NTLM où Kerberos est possible, gestion des délégations — et non une seule switch de configuration.

Le « durcissement d'une GPO template » copié d'un benchmark CIS ou DISA sans compréhension du contexte de l'organisation aboutit souvent à des régressions en production, une déstabilisation des équipes IT, et une désactivation du durcissement en urgence lors du premier incident. La sécurité par template ne remplace pas la compréhension des flux légitimes du SI.

AVIS DrXPERT

Mon avis d'expert

Active Directory restera une surface d'attaque critique tant que les organisations n'adresseront pas leur dette technique structurelle avec un budget et un portage politique adéquats. La réponse à CVE-2026-41089 — comme à toutes les vulnérabilités AD avant elle — n'est pas « patcher et surveiller ». Elle est « patcher, auditer les chemins d'attaque, traiter la dette qui amplifie l'impact, et construire une architecture où Domain Admin n'est pas atteignable depuis n'importe quel poste utilisateur via quelques étapes de pivot ». Ce n'est pas plus compliqué que ça sur le papier. C'est juste politiquement et budgétairement difficile — et c'est exactement pour ça que les attaquants continuent de gagner.

Conclusion : le problème est connu, la solution aussi — il reste la volonté

Active Directory en 2026 n'est pas un problème technique non résolu. Les défenses existent, elles sont documentées, certaines sont gratuites à déployer. Le tiering AD, les gMSA, Protected Users, la rotation krbtgt, l'audit BloodHound défensif — ce sont des mesures dont l'efficacité est prouvée et dont la mise en oeuvre ne nécessite pas des millions d'euros d'investissement.

Ce qui manque dans la grande majorité des organisations, c'est la combinaison d'un portage politique fort pour traiter la dette technique, d'une équipe ayant l'expertise pour la détecter et la corriger méthodiquement, et d'un budget pour financer les projets de nettoyage qui n'ont pas de ROI immédiatement mesurable mais qui réduisent drastiquement le risque de compromission totale.

CVE-2026-41089 ne sera pas le dernier. Le prochain est déjà quelque part dans la base de code Netlogon, ou dans ADCS, ou dans Kerberos. La question n'est pas de savoir si une prochaine vulnérabilité critique Active Directory sera découverte — c'est quand. La vraie question est : quand cette vulnérabilité sera-t-elle exploitée dans votre SI, est-ce que l'attaquant aura les chemins libres pour atteindre Domain Admin, ou est-ce que vous aurez fait le travail de fond pour l'en empêcher ?

C'est là la différence entre une organisation qui survit à un incident AD et une organisation qui passe trois mois à reconstruire son SI de zéro après une opération ransomware.

Besoin d'un regard expert sur votre sécurité ?

Discutons de votre contexte spécifique.

Prendre contact

À RETENIR

Points clés à retenir

Trente ans et toujours n°1 des vecteurs de compromission

Les chemins d'attaque classiques qui fonctionnent toujours en 2026

2026 : l'automatisation change l'échelle, pas la nature

La dette technique AD : le problème que personne ne veut financer

Ce qui fonctionne vraiment pour réduire le risque

Sources et références

ANSSI — Bonnes pratiques de sécurité

CISA — Ressources cybersécurité

ENISA — Threat Landscape 2024

