

Attaques AD 2025 : Bilan et Tendances Emergentes en 2026

Catégorie : Attaques Active Directory Lecture : 6 min Publié le : 20/11/2025 Auteur : Ayi NEDJIMI

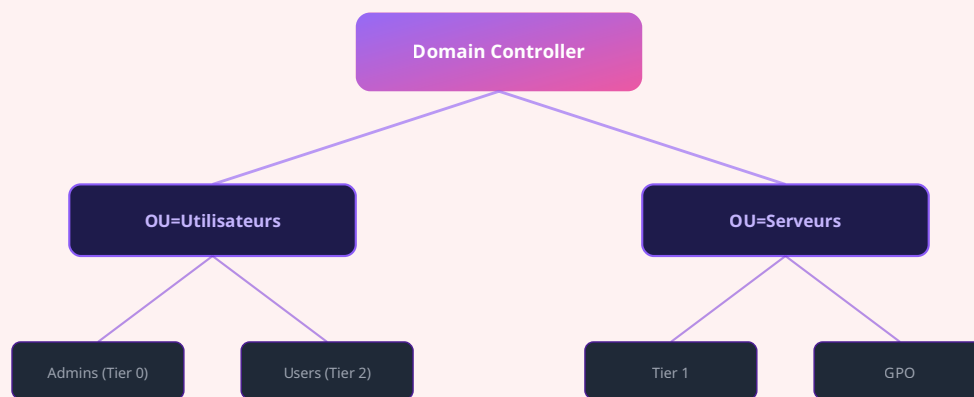
Bilan complet des attaques Active Directory en 2025 : nouvelles techniques, statistiques clés et tendances pour 2026. Guide technique complet avec.

Bilan complet des attaques Active Directory en 2025 : nouvelles techniques, statistiques clés et tendances pour 2026. Les équipes de sécurité et les professionnels du domaine y trouveront des recommandations applicables immédiatement. La sécurisation d'Active Directory représente un défi majeur pour les entreprises modernes. Les attaquants ciblent systématiquement ces infrastructures critiques, exploitant des configurations par défaut ou des privilèges excessifs pour compromettre l'ensemble du système d'information. Cet article fournit une analyse technique approfondie des mécanismes d'attaque et des contre-mesures efficaces, basée sur des retours d'expérience terrain et les recommandations des autorités de référence comme l'ANSSI et le MITRE. Ce guide couvre les aspects essentiels de attaques ad 2025 bilan tendances : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

Contexte et Enjeux

La sécurité d'**Active Directory** reste un enjeu majeur pour les entreprises en 2025-2026. Avec la multiplication des attaques élaborées, les équipes IT doivent constamment adapter leurs défenses. Les environnements hybrides combinant AD on-premise et **Entra ID** (anciennement Azure AD) ajoutent une complexité supplémentaire.

Pour comprendre les fondamentaux, consultez notre article sur [Rbcd Attaque Defense](#). Les techniques d'attaque évoluent rapidement, comme détaillé dans [Adcs Certificats Attaque Defense](#).



Architecture Active Directory - Modele de tiering

Notre avis d'expert

Les risques liés à l'identité hybride AD/Azure AD sont systématiquement sous-évalués. Nos audits révèlent que la synchronisation entre environnements on-premises et cloud crée des chemins d'attaque que ni l'équipe infrastructure ni l'équipe cloud ne surveillent efficacement.

Analyse Technique Détaillée

L'approche technique repose sur plusieurs vecteurs d'attaque complémentaires. Les **pentesters** et red teamers utilisent ces techniques pour identifier les failles dans les configurations AD. La compréhension de la **chaîne d'attaque** complète est essentielle pour mettre en place des défenses efficaces.

Les outils comme **BloodHound**, Impacket et Rubeus permettent d'automatiser la détection des chemins d'attaque. Selon les recommandations de ANSSI, la surveillance des événements critiques (Event ID 4769, 4662, 4724) est indispensable. Notre guide [Pass The Hash Attaque Defense](#) détaille les procédures d'audit.

La complexité des environnements modernes nécessite une approche en couches. Le **modele de tiering** recommande par Microsoft et l'ANSSI reste la référence pour segmenter les accès privilégiés.

Savez-vous combien de comptes à privilèges existent réellement dans votre domaine ?

Stratégies de Defense et Remediation

La remediation doit être progressive et priorisée. Commencez par les **quick wins** : désactiver NTLM ou possible, activer le Protected Users group, configurer le tiering. Ensuite, abordez les chantiers de fond comme la migration vers le **passwordless** et le renforcement du Conditional Access.

- **Etape 1** : Audit complet avec les scripts recommandés — voir [Sidhistory Injection](#) [Attaque Defense](#)
- **Etape 2** : Remediation des configurations critiques
- **Etape 3** : Mise en place du monitoring continu
- **Etape 4** : Tests de penetration réguliers

Cas concret

Le groupe Conti utilisait systématiquement des attaques Kerberoasting pour extraire les tickets de service des comptes Active Directory dotés de SPN. L'analyse de leurs playbooks, fuités en 2022, a révélé une méthodologie industrialisée de compromission AD applicable en moins de 48 heures.

Plusieurs outils gratuits facilitent l'audit et le durcissement d'Active Directory. PingCastle, Purple Knight et ADRecon fournissent des rapports détaillés. Les références de NIST complètent ces outils avec des bonnes pratiques validées. Pour approfondir, consultez [Acl Abuse](#) [Attaque Defense](#).

Questions frequentes

Comment securiser un environnement Active Directory ?

La securisation d'Active Directory repose sur plusieurs piliers : l'implémentation du modèle de tiering, la restriction des privilèges administratifs, la surveillance des événements critiques, le déploiement du Protected Users group, la désactivation des protocoles obsolètes comme NTLM et la mise en place d'audits réguliers.

Qu'est-ce que le modele de tiering Active Directory ?

Le modèle de tiering est une architecture de sécurité recommandée par Microsoft et l'ANSSI qui segmente les accès privilégiés en trois niveaux : Tier 0 pour les contrôleurs de domaine, Tier 1 pour les serveurs membres et Tier 2 pour les postes de travail, empêchant ainsi la propagation latérale des attaquants.

Pourquoi les attaques Active Directory sont-elles si fréquentes ?

Les attaques Active Directory sont fréquentes car AD reste le système d'authentification central de la majorité des entreprises. Les configurations par défaut sont souvent permissives, les privilèges excessifs répandus et les techniques d'exploitation bien documentées, ce qui en fait une cible privilégiée pour les attaquants.

La mise en pratique de ces concepts nécessite une approche méthodique et structurée. Les équipes techniques doivent d'abord évaluer leur niveau de maturité actuel sur le sujet, identifier les lacunes prioritaires et définir un plan d'action réaliste. L'implémentation progressive, avec des jalons mesurables, garantit une adoption durable et efficace des pratiques recommandées.

Les organisations qui réussissent le mieux dans ce domaine adoptent une culture d'amélioration continue. Cela implique des revues régulières des processus, une veille technologique active et une formation permanente des équipes. Les indicateurs de performance doivent être définis dès le départ pour mesurer objectivement les progrès réalisés et ajuster la stratégie si nécessaire.

L'intégration de ces pratiques dans les processus existants de l'organisation est un facteur clé de succès. Plutôt que de créer des workflows parallèles, il est recommandé d'enrichir les procédures actuelles avec les contrôles et les vérifications nécessaires. Cette approche réduit la résistance au changement et facilite l'adoption par les équipes opérationnelles.

Recommandations de durcissement

La sécurisation d'un environnement Active Directory passe par une approche méthodique. Le modèle de tiering proposé par Microsoft — avec une séparation stricte des comptes administrateurs Tier 0, Tier 1 et Tier 2 — reste la fondation de toute architecture sécurisée. Pourtant, dans la majorité des audits, on constate que ce modèle n'est que partiellement appliqué.

LAPS (Local Administrator Password Solution) est un autre pilier souvent négligé. Sans LAPS, un seul mot de passe administrateur local compromis peut ouvrir la voie à un mouvement latéral massif. La documentation Microsoft détaille la mise en œuvre, mais l'implémentation sur un parc hétérogène prend du temps et de la planification.

Points de contrôle prioritaires

Les chemins d'attaque les plus courants dans un AD passent par : les délégations Kerberos non contraintes, les comptes de service avec des SPN et des mots de passe faibles (cible du Kerberoasting), les GPO mal configurées qui exposent des credentials, et les ACL permissives sur des objets sensibles comme AdminSDHolder.

BloodHound permet de cartographier ces chemins en quelques minutes. Si vous ne l'avez jamais lancé sur votre environnement de production, la découverte risque d'être instructive. La réalité est souvent plus complexe que ce que les schémas théoriques laissent supposer.

Consultez les recommandations de l'ANSSI et le référentiel MITRE ATT&CK TA0004 (Privilege Escalation) pour structurer votre approche défensive.

Contexte et enjeux actuels

Impact opérationnel

Pour approfondir ce sujet, consultez notre outil open-source ad-attack-simulator qui facilite la simulation d'attaques Active Directory en environnement contrôlé.

Les sujets techniques en cybersécurité exigent une approche rigoureuse, fondée sur l'expérimentation et la validation en conditions réelles. Les environnements de laboratoire — qu'ils soient construits avec Proxmox, VMware Workstation ou des services cloud éphémères — sont indispensables pour tester les techniques, les outils et les contre-mesures avant tout déploiement en production.

L'un des écueils les plus fréquents dans la mise en œuvre de solutions techniques de sécurité est le gap entre la documentation officielle et la réalité du terrain. Les guides de déploiement supposent souvent un environnement propre et standardisé, là où la plupart des organisations gèrent un patrimoine applicatif hétérogène, avec des dépendances croisées et des configurations héritées.

Approche méthodique recommandée

Pour chaque implémentation technique, la méthodologie suivante a fait ses preuves : audit de l'existant, définition des prérequis, déploiement en environnement de test, validation fonctionnelle et sécurité, déploiement progressif en production avec rollback plan, puis monitoring post-déploiement. Chaque étape doit être documentée.

Les référentiels MITRE ATT&CK et MITRE D3FEND fournissent un cadre structuré pour aligner les mesures techniques sur les menaces réelles. D3FEND, en particulier, cartographie les contre-mesures défensives face aux techniques d'attaque, ce qui facilite la priorisation des investissements en sécurité.

La documentation interne — runbooks, playbooks, procédures d'exploitation — est le maillon souvent manquant. Sans elle, la connaissance reste dans la tête des experts, et chaque départ ou absence crée un risque opérationnel. Avez-vous documenté vos procédures critiques de manière à ce qu'un nouveau membre de l'équipe puisse les exécuter de manière autonome ?

Sources et références : [MITRE ATT&CK Privilege Escalation](#) · [ADSecurity.org](#)

Conclusion

La sécurisation d'Active Directory est un processus continu qui nécessite une vigilance constante. Les nouvelles menaces de 2026 renforcent la nécessité d'adopter une approche proactive, combinant audit régulier, monitoring en temps réel et formation des équipes.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2025 — Reproduction interdite sans autorisation.