Souhir ZAIMI

Veille n°3 – Active Directory et les ransomwares

En 2025, les ransomwares exploitent AD comme point d'entree pour compromettre rapidement les reseaux entiers. Apres un acces initial, les attaquants elevent leurs privileges, puis utilisent les GPO pour deployer le malware. Le delai median intrusion-chiffrement s'est reduit a 5 jours, avec des couts d'attaque atteignant 5 millions de dollars en moyenne.

Comment les ransomwares exploitent Active Directory

Apres un acces initial (phishing, identifiants compromis), les attaquants cartographient l'AD, elevent leurs privileges via Kerberoasting ou Pass-the-Hash, puis deploient le ransomware sur toutes les machines via les GPO. Le delai median entre l'intrusion et le chiffrement est desormais de seulement 5 jours (Gridinsoft, 2025).

Cas reels d'attaques (2025)

En janvier 2025, un prestataire de sante suisse a vu 3 000 postes chiffres en 51 secondes, avec 800 Go de donnees exfiltrees. Le groupe Play ransomware a touche 900 entites selon le FBI. En France, 74 % des organisations ont ete ciblees en 2024 et plus d'une sur deux a subi une attaque reussie (Semperis, aout 2025).

Impact sur les entreprises

Le cout moyen mondial d'une attaque atteint 5,08 millions de dollars en 2025. En France, l'arret du SI coute plus de 200 000 euros pour une PME. Les ransomwares pratiquent desormais la triple extorsion : chiffrement, vol de donnees et attaques DDoS simultanees. 69 % des entreprises attaquees ont paye la rancon, dont 30 % plusieurs fois.

Moyens de prevention

Segmenter le reseau via le Tier Model, maintenir des sauvegardes isolees et immuables, activer le MFA sur tous les comptes privilegies (63 % des incidents debutent par un compte compromis), deployer des outils EDR/XDR pour la detection en temps reel, et organiser des exercices de simulation d'attaques reguliers pour tester la resilience de l'organisation.

Notions cles

Ransomware
: Logiciel malveillant chiffrant les donnees d'une victime et exigeant une rancon pour la dechiffrement. Devenus une menace majeure pour les entreprises.

Acces initial
: Premiere etape d'une attaque cybernetique permettant a l'attaquant de penetrer le reseau, souvent via phishing ou identifiants compromis.

Elevation de privileges
: Technique permettant a un attaquant d'obtenir des droits d'acces superieurs (par exemple passer d'utilisateur a administrateur).

Triple extorsion
: Tactique d'attaque combinant le chiffrement de donnees, le vol et la publication d'informations sensibles, et les attaques DDoS simultanees.

Sauvegardes immuables
: Copies de donnees qui ne peuvent pas etre modifiees ou supprimees, meme par les administrateurs, pour se proteger contre le chiffrement ransomware.

EDR/XDR
: Outils de detection et de reponse (EDR: au niveau des points terminaux, XDR: etendu a tout le reseau) permettant de detecter les activites malveillantes en temps reel.

Sources

• Gridinsoft – Ransomware 2025 : Statistiques et Tendances (fevrier 2026)
https://gridinsoft.com/article/ransomware

• Bitsight – 2026 Ransomware Statistics & Deep Web Threat Trends
https://www.bitsight.com/underground/ransomware

• Brightdefense – 500+ Ransomware Statistics for 2026
https://www.brightdefense.com/resources/ransomware-statistics/