AYI NEDJIMI Consultants

# Ransomwares : Pourquoi Vos Sauvegardes Ne Sauvent Plus

Catégorie : Cybersécurité Générale  Lecture : 6 min  Publié le : 23/03/2026  Auteur : Ayi NEDJIMI

*Les ransomwares ciblent vos sauvegardes en premier. Ayi NEDJIMI décrypte les techniques d attaque et la stratégie de backup résiliente à mettre en.*

Les ransomwares de 2026 ne chiffrent plus vos données en premier — ils détruisent vos sauvegardes. C'est leur première étape, systématique, méthodique, industrialisée. Avant même de lancer leur payload de chiffrement, les groupes modernes comme **LockBit 4.0**, **BlackCat ALPHV** ou **Interlock** passent des jours voire des semaines à cartographier et neutraliser votre stratégie de backup. Ils cherchent vos agents **Veeam**, vos snapshots **VMware**, vos sauvegardes cloud, vos NAS et vos Volume Shadow Copies. Ils les suppriment un à un, silencieusement, avant de déclencher le chiffrement. Si vous pensez que votre plan de reprise d'activité vous protège parce que vous avez des sauvegardes à 30 jours de rétention, cet article va vous déranger — et c'est exactement l'objectif. La résilience face aux ransomwares modernes nécessite une refonte complète de votre approche backup, bien au-delà de la simple règle 3-2-1.

## Ce que font réellement les ransomwares modernes avant de chiffrer

En 2024-2025, j'ai eu l'occasion d'analyser plusieurs incidents ransomware post-compromission dans le cadre de missions forensiques. Ce qui m'a frappé à chaque fois : les attaquants avaient passé entre 3 et 21 jours dans le réseau avant de déclencher le chiffrement. Durant cette phase de **reconnaissance active**, leur objectif principal n'était pas d'exfiltrer des données — c'était de comprendre et neutraliser la stratégie de sauvegarde de l'organisation.

Voici ce qu'ils font concrètement. Ils identifient vos solutions de backup en analysant les processus actifs et les connexions réseau. Ils repèrent vos snapshots VMware et vos points de restauration Windows. Ils localisent vos NAS et vos serveurs de sauvegarde en scannant les partages SMB. Et ensuite, ils suppriment tout ça — avant de chiffrer. Le groupe LockBit 4.0 a publié dans sa documentation interne une checklist explicite de neutralisation des sauvegardes. Ce n'est pas un hasard, c'est une méthodologie industrialisée. Les techniques les plus fréquemment observées : suppression des Volume Shadow Copies via `vssadmin delete shadows /all /quiet`, désactivation des agents de backup via les services Windows, corruption silencieuse des fichiers de sauvegarde, et dans les cas les plus sophistiqués, chiffrement ou suppression des sauvegardes stockées sur des partages réseau accessibles. La CISA documente cette tactique dans son guide StopRansomware comme l'une des plus critiques à contrer. Consultez également notre analyse de l'incident Marquis Financial pour un exemple concret des conséquences.

## Les erreurs de backup que j'observe systématiquement en audit

Première erreur, et la plus répandue : les sauvegardes accessibles depuis le domaine **Active Directory**. Si votre serveur Veeam est membre du domaine et que l'attaquant a compromis un compte admin de domaine, il a accès à vos sauvegardes. C'est aussi simple que ça. J'ai vu des organisations avec des budgets IT significatifs faire cette erreur fondamentale. Le serveur de backup doit être soit physiquement isolé, soit dans un domaine séparé avec des credentials dédiés non exposés sur le réseau principal. Notre guide du Tiering Model Active Directory explique comment cloisonner correctement ces accès.

Deuxième erreur : la règle 3-2-1 mal appliquée. Trois copies, deux médias différents, une hors-site — en théorie c'est bien. En pratique, je constate que le "hors-site" est souvent un NAS synchronisé en temps réel via un tunnel VPN sur le même réseau. Ce n'est pas une sauvegarde hors-site, c'est une deuxième cible. Troisième erreur : ne jamais tester la restauration. Des backups qui existent sur le papier mais qui échouent à la restauration, j'en vois régulièrement. La validation de l'intégrité des sauvegardes doit être automatisée et testée en conditions réelles au moins trimestriellement. Pour comprendre comment les attaquants se déplacent latéralement avant d'atteindre vos backups, notre guide de pentest Active Directory vous donnera la perspective de l'attaquant. Voir aussi notre guide sur la sécurisation Active Directory pour les défenses structurelles.

## La stratégie de backup qui résiste aux ransomwares en 2026

Voici ce que je recommande dans mes missions, basé sur ce qui fonctionne réellement face aux groupes modernes. D'abord, l'**air gap physique ou logique** : au moins une copie de sauvegarde doit être inaccessible depuis le réseau de production. Bandes magnétiques (LTO), disques durs déconnectés, ou stockage cloud avec authentification multi-facteurs et période de rétention avec suppression différée (les buckets S3 avec S3 Object Lock sont une bonne option). Ensuite, les **sauvegardes immuables** : certaines solutions comme Veeam Hardened Repository, Cohesity ou Rubrik permettent de créer des sauvegardes que même l'administrateur ne peut pas supprimer pendant la période de rétention définie. C'est la réponse technique directe à la neutralisation des VSS. Enfin, le **monitoring des sauvegardes** : alertes immédiates si un processus tente de supprimer les VSS, si l'agent de backup est arrêté, si les jobs de backup échouent plusieurs fois consécutives. Ces événements sont des signaux d'alarme ransomware à traiter comme des incidents critiques. Consultez le guide ransomware de la CISA pour les bonnes pratiques détaillées.

**Mon avis d'expert**
La majorité des organisations françaises que j'audite ont une fausse confiance dans leurs sauvegardes. Elles ont investi dans Veeam, elles ont des rétentions à 30 jours, elles cochent toutes les cases du PCA sur le papier. Mais quand je simule une compromission et que j'essaie de neutraliser leurs sauvegardes depuis un poste compromis dans le domaine, je réussis dans la grande majorité des cas. La vraie question à poser n'est pas "est-ce que j'ai des sauvegardes ?" mais "est-ce que mes sauvegardes survivraient à un attaquant ayant les droits admin sur mon domaine ?" Si vous ne connaissez pas la réponse, c'est probablement non.

### Comment savoir si mes sauvegardes Veeam sont accessibles depuis le domaine Active Directory ?

Vérifiez si votre serveur Veeam Backup & Replication est membre du domaine Active Directory (commande `systeminfo | findstr /i "domain"`). Si c'est le cas, tout compte administrateur de domaine compromis peut potentiellement accéder au serveur Veeam et supprimer les sauvegardes. La configuration recommandée est de sortir le serveur Veeam du domaine, d'utiliser un compte local dédié pour l'administration Veeam, et de configurer le Veeam Hardened Repository sur un serveur Linux non joint au domaine avec des accès SSH en mode clé uniquement.

### Qu'est-ce que l'immuabilité des sauvegardes et comment la mettre en place ?

L'immuabilité des sauvegardes signifie que les données de backup ne peuvent pas être modifiées ou supprimées pendant une période définie, même par un administrateur avec les droits maximaux. Sur AWS, cela se configure via S3 Object Lock en mode Compliance. Sur Linux, Veeam Hardened Repository utilise les attributs immuables du système de fichiers (chattr +i). Rubrik et Cohesity proposent des architectures nativement immuables. L'immuabilité est la protection la plus efficace contre la tactique de neutralisation des sauvegardes par les ransomwares modernes — même si l'attaquant a les droits root, il ne peut pas effacer les sauvegardes avant la fin de la période de rétention.

### À quelle fréquence tester la restauration des sauvegardes pour détecter les corruptions silencieuses ?

La recommandation minimale est un test de restauration complet trimestriel sur un environnement isolé, plus des tests partiels mensuels sur des fichiers ou VM individuels. Automatisez les tests de restauration dans votre outil de backup (Veeam SureBackup fait ça nativement). Pour détecter les corruptions silencieuses — une technique utilisée par certains ransomwares qui corrompent les sauvegardes sans les supprimer pour vous donner une fausse assurance — activez les checksums de vérification d'intégrité et planifiez des alertes en cas d'écart. Ne faites jamais confiance à une sauvegarde qui n'a pas été restaurée avec succès en environnement de test.

## FAQ

### Qu'est-ce que Ransomwares ?

Le concept de Ransomwares est détaillé dans les premières sections de cet article, qui couvrent les fondamentaux, les enjeux et le contexte opérationnel. Pour un accompagnement sur ce sujet, contactez nos experts.

## Conclusion

Les ransomwares modernes ont fait de la neutralisation des sauvegardes une étape systématique et méthodique de leur chaîne d'attaque. Une stratégie de backup conçue uniquement pour faire face aux pannes matérielles ou aux suppressions accidentelles ne résiste pas à un attaquant déterminé. La résilience face aux ransomwares exige un niveau supplémentaire de conception : isolation physique ou logique, immuabilité, surveillance active et tests réguliers en conditions adverses. Si votre PCA n'a pas été révisé avec cette réalité en tête, il ne vous protège pas — il vous donne juste une fausse sensation de sécurité.

**Sources et références :** CERT-FR · MITRE ATT&CK

## Mettre en place une gouvernance backup orientée résilience ransomware

Au-delà des mesures techniques, la résilience face aux ransomwares exige une gouvernance backup spécifique. Cela commence par un propriétaire clairement identifié pour la stratégie de sauvegarde — pas le responsable IT généraliste, mais un rôle dédié avec des responsabilités explicites sur les objectifs de RTO (Recovery Time Objective) et RPO (Recovery Point Objective) face à un scénario ransomware. Ces objectifs doivent être régulièrement testés et documentés, pas simplement définis sur le papier. La gouvernance inclut également un processus de validation des sauvegardes indépendant de l'équipe qui les gère — pour éviter que les mêmes personnes qui gèrent les backups soient aussi celles qui valident leur intégrité, créant un angle mort organisationnel. Pour structurer votre approche globale de sécurité avec ce type de rigueur, consultez notre guide sur l'audit et le monitoring de l'infrastructure IT et notre analyse des implications réglementaires de la sécurité des données — la perte de données suite à un ransomware engage aussi la responsabilité RGPD de votre organisation.

**Points clés à retenir**

- Les ransomwares modernes neutralisent les sauvegardes avant le chiffrement — c'est leur première priorité
- Serveur de backup membre du domaine AD = sauvegarde compromise si le domaine l'est
- Règle 3-2-1 nécessaire mais insuffisante : l'air gap réel et l'immuabilité sont indispensables
- Tester la restauration complète trimestriellement sur un environnement isolé — pas seulement les checksums

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

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