AYI NEDJIMI Consultants

# Ransomware : Anatomie d'une Attaque, Kill Chain et

Catégorie : Techniques de Hacking  Lecture : 10 min  Publié le : 08/03/2026  Auteur : Ayi NEDJIMI

*Analyse complète du ransomware en 2026 : kill chain en 7 phases, double et triple extorsion, techniques d'accès initial, mouvement latéral.*

**Avertissement :** Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

La **triple extorsion**, observée depuis 2021, ajoute une troisième dimension de pression qui peut prendre plusieurs formes. Les variantes les plus courantes incluent : des attaques **DDoS** contre l'infrastructure de la victime pour amplifier la pression opérationnelle, le **harcèlement direct** des clients, partenaires ou patients dont les données ont été volées (observé notamment dans le secteur de la santé), et des **menaces envers les dirigeants** personnellement identifiés. Certains groupes comme **ALPHV/BlackCat** ont même signalé les violations à la SEC et aux régulateurs au nom des victimes pour les contraindre au paiement, exploitant ainsi les obligations réglementaires contre les organisations ciblées. Analyse complète du ransomware en 2026 : kill chain en 7 phases, double et triple extorsion, techniques d'accès initial, mouvement latéral. Ce guide couvre les aspects essentiels de ransomware anatomie kill chain contre : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

**Attention : L'extorsion sans chiffrement, la tendance de 2025-2026**

Un nombre croissant de groupes, à l'instar de **Cl0p** et de **BianLian** (qui a abandonné le chiffrement début 2024), se concentrent exclusivement sur le vol et la menace de divulgation de données. Cette approche présente plusieurs avantages pour les attaquants : elle est plus rapide (pas besoin de déployer un ransomware sur chaque endpoint), plus discrète (moins de signaux détectables par les EDR), et cible directement la peur réglementaire et réputationnelle des organisations. L'absence de chiffrement complique également la qualification juridique de l'attaque et l'intervention des assureurs cyber.

## 2.3 Le modèle Ransomware-as-a-Service (RaaS)

Le modèle RaaS a transformé le ransomware en une véritable industrie avec une division du travail spécialisée. Au sommet se trouvent les **opérateurs/développeurs** qui créent et maintiennent le ransomware, l'infrastructure de C2, les sites de négociation et les portails de fuite. Ils recrutent des **affiliés** (ou "pentesters" dans le jargon interne) qui réalisent les intrusions et le déploiement. Les revenus sont partagés selon des ratios variables : LockBit proposait un split 80/20 en faveur de l'affilié, tandis que d'autres groupes pratiquent des ratios de 70/30 ou 60/40.

L'objectif de cette phase est d'obtenir les privilèges les plus élevés possibles, idéalement un accès Domain Admin dans les environnements Active Directory. Les techniques de Kerberoasting sont systématiquement utilisées pour extraire les tickets TGS des comptes de service configurés avec des SPN, puis les soumettre à un cracking offline. Les mots de passe faibles sur les comptes de service restent remarquablement fréquents, permettant souvent d'obtenir des credentials à hauts privilèges en quelques heures de cracking.

Les **exploits d'élévation de privilèges locaux** constituent un autre vecteur important. Les vulnérabilités du type PrintNightmare (CVE-2021-34527), PetitPotam (CVE-2021-36942) et les vulnérabilités récurrentes du noyau Windows sont régulièrement exploitées. La **manipulation de tokens** Windows (T1134) permet d'usurper l'identité de processus à hauts privilèges via des techniques comme le token impersonation ou le token duplication. Les attaques de type NTLM relay restent également très efficaces pour escalader les privilèges dans les environnements où la signature SMB n'est pas activée ou où les protocoles d'authentification legacy sont encore présents.

## 3.4 Phase 4 : Évasion Défensive (TA0005)

L'évasion des solutions de sécurité est une préoccupation constante tout au long de la chaîne d'attaque, mais elle s'intensifie une fois que les attaquants disposent de privilèges élevés. La technique la plus directe consiste à **désactiver ou dégrader les solutions antivirus et EDR**. Les outils comme GMER, PCHunter, Process Hacker ou le Defender Control sont utilisés pour terminer les processus de sécurité. L'abus de pilotes noyau vulnérables signés (technique "Bring Your Own Vulnerable Driver" ou BYOVD) est devenu une méthode standard : les attaquants chargent un pilote légitime mais vulnérable, puis l'exploitent pour terminer les processus de l'EDR en mode noyau, contournant ainsi les protections anti-tamper.

Le **bypass AMSI** (Antimalware Scan Interface) est systématiquement réalisé pour permettre l'exécution de scripts PowerShell malveillants sans détection. Les techniques de **timestomping** sont utilisées pour modifier les horodatages des fichiers malveillants et compliquer l'investigation forensique. Les secrets de l'environnement sont exploités pour se fondre dans le trafic légitime, par exemple en utilisant des identifiants de comptes de service existants plutôt que de créer de nouveaux comptes suspects. L'effacement sélectif des journaux d'événements Windows (Event Log clearing) et la désactivation de Sysmon complètent l'arsenal défensif des attaquants.

Malgré des années de sensibilisation, les services d'accès distant exposés sur Internet restent un vecteur d'entrée majeur. Des scans Shodan et Censys révèlent régulièrement des centaines de milliers d'instances RDP directement accessibles sur Internet, dont une proportion significative avec des identifiants par défaut ou des mots de passe faibles. Les appliances VPN non patchées, en particulier les concentrateurs Fortinet, Citrix NetScaler, Palo Alto GlobalProtect et Ivanti Connect Secure, constituent des cibles de choix.

L'absence de **MFA** sur ces points d'accès amplifie considérablement le risque. Une étude de CISA indique que plus de **50%** des incidents ransomware impliquant un accès VPN ou RDP concernaient des comptes sans MFA activé. La recommandation est claire : tout service d'accès

distant exposé sur Internet doit être protégé par une authentification multi-facteurs résistante au phishing (FIDO2/WebAuthn plutôt que OTP SMS ou push notifications vulnérables aux attaques de fatigue MFA).

## 5.5 Supply chain : le vecteur le plus critique

Les attaques supply chain représentent le vecteur d'accès initial ayant le plus fort potentiel d'impact. En compromettant un fournisseur de logiciel ou de service utilisé par de nombreuses organisations, les attaquants peuvent simultanément toucher des centaines ou milliers de victimes. L'attaque Kaseya VSA par REvil (juillet 2021) et les campagnes Cl0p contre les solutions de transfert de fichiers illustrent ce modèle. En 2025-2026, les fournisseurs de services managés (MSP) et les éditeurs de logiciels SaaS restent des cibles privilégiées car leur compromission offre un effet de levier maximal.

**Point clé : La convergence des vecteurs d'accès**
En 2026, les groupes ransomware les plus efficaces combinent plusieurs vecteurs d'accès de manière opportuniste. Un affilié typique surveille simultanément les publications de CVE critiques, achète des logs d'infostealers contenant des accès VPN d'entreprise, mène des campagnes de phishing ciblé et se fournit auprès d'IAB. Cette approche multi-vecteurs rend la prévention particulièrement complexe et renforce la nécessité d'une défense en profondeur couvrant l'ensemble de la surface d'attaque.

Les **canary files** (fichiers leurres) constituent un mécanisme de détection simple mais extrêmement efficace contre le ransomware. Des fichiers portant des noms attractifs (par exemple, `Salaires_2026.xlsx`, `Mots_de_passe_admin.docx`, `Plan_strategique_confidentiel.pdf`) sont placés à des emplacements stratégiques (partages réseau, répertoires utilisateurs, serveurs de fichiers). Toute modification ou accès à ces fichiers déclenche une alerte immédiate. Le mécanisme est particulièrement efficace car le ransomware chiffre méthodiquement tous les fichiers qu'il rencontre, déclenchant inévitablement les alertes sur les canary files.

Les **honeypots** réseau, tels que des faux serveurs avec des services RDP, SMB ou des partages de fichiers apparemment intéressants, peuvent également piéger les attaquants lors de la phase de mouvement latéral. Des solutions comme CanaryTokens (gratuit et open-source), Thinkst Canary ou Attivo/SentinelOne Identity permettent un déploiement rapide et une intégration aux workflows SOC existants.

**Mesures défensives : Détection - Les essentiels**

- **SIEM centralisé** avec corrélation de logs et règles de détection spécifiques ransomware (Sigma rules)
- **EDR avec behavioral analytics** : détection des comportements suspects (exécution PowerShell encodée, injection de processus, accès LSASS)
- **NDR (Network Detection and Response)** : identification des mouvements latéraux, exfiltrations et communications C2
- **Canary files et honeypots** : déployer des leurres sur les partages réseau et serveurs de fichiers pour une détection précoce

- **Monitoring Active Directory** : surveiller les modifications de GPO, créations de comptes, Kerberoasting, DCSync
- **Alertes sur les sauvegardes** : notification immédiate en cas d'arrêt des services de sauvegarde ou de suppression de points de restauration
- **Threat Intelligence** : intégrer les IoC des groupes ransomware actifs dans les solutions de détection

### 6.3 Réponse : Contenir et Éradiquer

La réponse à un incident ransomware doit être rapide et structurée. L'**isolation** est la première priorité : les systèmes infectés doivent être immédiatement déconnectés du réseau pour empêcher la propagation, tout en préservant l'état des machines pour l'analyse forensique (ne pas éteindre mais isoler). Le **confinement** réseau peut inclure la désactivation temporaire de certains segments réseau, le blocage du trafic SMB entre VLANs, et la réinitialisation des mots de passe des comptes compromis.

La question du paiement est l'une des plus débattues en cybersécurité. Les positions des autorités sont claires : l'**ANSSI**, le **FBI**, **Europol** et la majorité des agences nationales de cybersécurité **déconseillent fermement le paiement** car il finance l'écosystème criminel, ne garantit pas la récupération des données (environ 20% des organisations qui paient ne récupèrent pas leurs données), ne garantit pas la suppression des données volées, et peut exposer l'organisation à des sanctions si le groupe ransomware est sous le coup de mesures restrictives (OFAC).

Cependant, la réalité opérationnelle confronte certaines organisations à des situations où le paiement peut sembler la seule option viable : absence de sauvegardes exploitables, systèmes vitaux inaccessibles (notamment dans le secteur de la santé), et impact financier du temps d'arrêt dépassant le montant de la rançon. Si la décision de payer est prise, elle doit l'être en concertation avec un conseil juridique spécialisé, et la négociation doit être menée par des professionnels expérimentés qui peuvent souvent obtenir une réduction significative (40 à 60%) du montant initial demandé.

## 7.4 Obligations légales et notification

En France et en Europe, un incident ransomware impliquant des données personnelles déclenche plusieurs obligations légales :

- **RGPD (Article 33)** : notification à la **CNIL** dans un délai de **72 heures** après la prise de connaissance de la violation. Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, celles-ci doivent également être informées directement (Article 34).
- **NIS 2 (Directive 2022/2555)** : pour les entités essentielles et importantes, notification à l'**ANSSI** dans un délai de **24 heures** pour l'alerte précoce, suivi d'une notification complète dans les 72 heures et d'un rapport final dans le mois.
- **DORA (Règlement 2022/2554)** : pour les entités financières, notification spécifique auprès de l'**ACPR/AMF** selon des délais stricts.

- **Plainte pénale** : dépôt de plainte auprès de la police nationale (OCLCTIC/C3N) ou de la gendarmerie nationale (ComCyberGend) pour permettre l'enquête et la poursuite des attaquants.

## Mise en œuvre détaillée

La **communication de crise** doit être préparée en amont avec des templates de communication pré-rédigés pour les différentes parties prenantes (direction, employés, clients, partenaires, médias, régulateurs). La transparence, tout en préservant la confidentialité de l'investigation, est généralement la meilleure approche. Les organisations qui tentent de dissimuler un incident s'exposent à des sanctions réglementaires aggravées et à une perte de confiance plus importante lorsque l'incident est finalement révélé.

### 7.5 Leçons apprises et amélioration continue

Le retour d'expérience (RETEX) post-incident est une étape souvent négligée mais essentielle. Un rapport d'incident complet doit documenter la chronologie détaillée de l'attaque, les faiblesses exploitées, l'efficacité de la réponse et les recommandations d'amélioration. Ce rapport alimente le plan d'amélioration continu de la sécurité et permet de justifier les investissements nécessaires en matière de cybersécurité. Des exercices de simulation (tabletop exercises) reproduisant le scénario de l'incident doivent être conduits régulièrement pour valider la préparation des équipes.

**Point clé : Le temps est l'ennemi**
Dans un incident ransomware, chaque minute compte. Les études montrent qu'une détection et un confinement rapides (dans les premières heures) peuvent réduire l'impact de **70 à 90%** par rapport à une détection tardive (après déploiement du ransomware). C'est pourquoi la préparation (playbooks, exercices, outils pré-déployés) et la capacité de détection précoce (EDR, NDR, canary files) sont les investissements les plus rentables en matière de défense anti-ransomware.

Pour approfondir ce sujet, consultez notre outil open-source burpsuite-automation qui facilite l'automatisation des tests d'intrusion web.

## Questions frequentes

### Comment mettre en place Ransomware dans un environnement de production ?

La mise en place de Ransomware en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

### Pourquoi Ransomware est-il essentiel pour la securite des systemes d'information ?

Ransomware constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

### Quelles sont les bonnes pratiques pour Ransomware en 2026 ?

Les bonnes pratiques pour Ransomware en 2026 incluent l'adoption d'une approche Zero Trust, l'automatisation des controles de securite, la mise en œuvre d'une veille continue sur les vulnerabilites et l'integration des recommandations des organismes de reference comme l'ANSSI et le NIST.

**Sources et références :** MITRE ATT&CK · OWASP Testing Guide

## 8. Conclusion : Anticiper l'Avenir du Ransomware

Le ransomware en 2026 représente une menace mature, industrialisée et en constante évolution. Les tendances actuelles dessinent un avenir où les attaques seront plus rapides (kill chains de moins de 24 heures), plus critiques (combinaison de chiffrement, vol de données et destruction), et plus difficiles à attribuer (multiplications des rebrandings et des programmes RaaS). L'intégration de l'IA dans l'arsenal offensif -- génération de phishing personnalisé, automatisation de la reconnaissance, évasion adaptative des EDR -- va accélérer cette évolution.

Face à cette menace, les organisations doivent adopter une posture de **résilience cyber** qui va au-delà de la simple prévention. La question n'est plus "si" mais "quand" une attaque ransomware surviendra. La clé réside dans la capacité à **détecter précocement** (avant le déploiement du ransomware), à **contenir rapidement** (limiter le scope de la compromission) et à **restaurer efficacement** (grâce à des sauvegardes testées et immuables). L'investissement dans la sécurité doit être envisagé comme un coût opérationnel permanent, pas comme une dépense ponctuelle.

Les cadres réglementaires européens (NIS 2, DORA, Cyber Resilience Act) imposent désormais des exigences minimales de cybersécurité et de notification qui obligent les organisations à structurer leur approche. La collaboration entre le secteur privé, les autorités de cybersécurité (ANSSI, ENISA, CISA) et les forces de l'ordre (Europol, FBI) est également essentielle pour perturber l'écosystème criminel et augmenter le coût des opérations pour les attaquants.

En complément de cet article, nous vous recommandons la lecture de nos analyses détaillées sur les techniques d'évasion EDR/XDR, les méthodes de post-exploitation et pivoting, l'exploitation de Kerberos dans Active Directory, et les frameworks C2 modernes. La maîtrise de ces sujets complémentaires est indispensable pour construire une défense holistique contre les menaces ransomware actuelles et futures.

**Point clé : Les 5 actions prioritaires contre le ransomware**

1. **Sauvegardes 3-2-1-1-0** avec au moins une copie immuable/offline, testée mensuellement
2. **MFA résistant au phishing** (FIDO2/WebAuthn) sur tous les accès critiques

3. **EDR/XDR** sur tous les endpoints avec protection anti-tamper et mode blocage
4. **Patch management accéléré** pour les systèmes exposés (<48h pour les CVE critiques)
5. **Playbook de réponse à incident** documenté, testé trimestriellement par exercice de simulation

## Références et ressources externes

- MITRE ATT&CK -- Framework de référence pour les tactiques, techniques et procédures adverses
- No More Ransom -- Outils de déchiffrement gratuits pour de nombreuses familles de ransomware
- CISA StopRansomware -- Ressources et alertes de l'agence américaine de cybersécurité
- ANSSI -- Agence nationale de la sécurité des systèmes d'information
- Ransomlook.io -- Suivi en temps réel des groupes ransomware et de leurs victimes
- CNIL - Violations de données -- Guide de notification des violations de données personnelles

---

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

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