

Ransomware : comprendre et se prémunir

Le scénario qui met une PME à l'arrêt en une nuit — et les défenses qui font vraiment la différence.

14 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/ransomware

Un ransomware (rançongiciel) chiffre l'ensemble de vos fichiers et exige une rançon pour les restituer — presque toujours doublée d'une menace de publication des données volées. Les TPE/PME sont des cibles privilégiées : moins protégées, elles paient plus souvent. Ce guide détaille l'anatomie complète d'une attaque, les défenses par ordre d'efficacité, les signaux qui permettent de détecter l'intrusion avant le chiffrement, et la conduite à tenir si le pire arrive.

1. Anatomie d'une attaque

Contrairement à l'image du virus qui frappe au hasard, une attaque par ransomware moderne est un cambriolage méthodique qui se déroule sur des jours, parfois des semaines :

1. L'intrusion

L'attaquant entre par une des portes classiques : identifiants volés ou hameçonnés, accès distant mal protégé, faille non corrigée. À ce stade, rien de visible — il dispose d'un simple pied dans la porte, souvent le poste d'un seul collaborateur.

2. La reconnaissance et l'escalade

Pendant des jours, il explore : cartographie du réseau, recherche des sauvegardes (pour les détruire), vol de mots de passe supplémentaires jusqu'à obtenir un compte administrateur. Il exfiltre discrètement les données les plus sensibles — contrats, données clients, paie — qui serviront au chantage.

3. Le chiffrement et l'extorsion

Le déclenchement a lieu au pire moment pour vous : nuit, week-end, veille de fête. En quelques heures, serveurs et postes sont chiffrés, les sauvegardes accessibles en ligne détruites, et une note de rançon s'affiche. La « double extorsion » est devenue la norme : payer pour déchiffrer, et payer pour que les données volées ne soient pas publiées.

CAS CONCRET

Déroulé type constaté en PME : lundi, un employé saisit ses identifiants sur une fausse page Microsoft 365. Mercredi, l'attaquant se connecte au VPN (pas de MFA) et explore le réseau. Le week-end suivant, à 2 h du matin, tout est chiffré — y compris le NAS de sauvegarde, resté connecté au réseau. Lundi matin, l'entreprise découvre la note de rançon et repart de zéro.

2. Les portes d'entrée

- Le phishing : une pièce jointe ou un lien ouvre l'accès initial — de loin le vecteur le plus courant
- Les accès distants mal protégés : un bureau à distance (RDP) exposé sur Internet ou un VPN sans double authentification se force ou s'achète (les identifiants volés se revendent quelques euros)
- Les failles non corrigées sur les équipements exposés : pare-feu, VPN, serveurs de messagerie — les

attaquants scannent Internet en permanence à la recherche des versions vulnérables

- La réutilisation de mots de passe ayant fuité sur d'autres services
- Plus rarement : un prestataire ou un logiciel compromis servant de relais (attaque par la chaîne d'approvisionnement)

3. Les défenses, par ordre d'efficacité

Aucune protection n'est absolue, mais chaque couche fait chuter la probabilité de succès ou l'ampleur des dégâts :

Survivre : les sauvegardes

C'est la défense qui transforme une catastrophe en mauvais week-end. Règle 3-2-1 avec une copie hors ligne ou immuable — c'est-à-dire impossible à modifier ou supprimer même avec des droits administrateur, car les attaquants cherchent et détruisent systématiquement les sauvegardes accessibles depuis le réseau. Et des tests de restauration réguliers : une sauvegarde jamais testée est une hypothèse.

Bloquer l'entrée

- MFA sur tous les accès distants (VPN, RDP, messagerie) et comptes administrateurs — neutralise le vol d'identifiants
- Jamais de RDP exposé directement sur Internet : toujours derrière un VPN
- Mises à jour rapides des équipements exposés (pare-feu, VPN) — sous quelques jours pour les failles critiques

Limiter la propagation

- Utilisateurs non administrateurs de leur poste : l'attaquant qui compromet un compte standard reste confiné
- Comptes administrateur dédiés, utilisés uniquement pour administrer
- Segmentation du réseau : les serveurs critiques et les sauvegardes dans des zones séparées
- EDR supervisé sur postes et serveurs : détecte le comportement de chiffrement et isole la machine

Réduire le facteur humain

- Sensibilisation continue au phishing (voir notre guide dédié)
- Culture du signalement sans blâme : la détection précoce vient souvent d'un employé qui ose dire « j'ai cliqué »

4. Détecter l'intrusion avant le chiffrement

Entre l'intrusion et le chiffrement s'écoulent des jours : chaque signal détecté dans cette fenêtre peut sauver l'entreprise.

- Connexions VPN ou messagerie à des heures inhabituelles, ou depuis des pays inhabituels
- Alertes de l'EDR même « mineures » : outils de scan, tentatives de désactivation de l'antivirus
- Comptes verrouillés en série ou tentatives de connexion échouées massives
- Nouveaux comptes administrateurs que personne n'a créés, règles de transfert email inconnues
- Ralentissements ou activité disque inexplicable sur les serveurs, sauvegardes qui échouent soudainement

5. L'attaque survient : la conduite à tenir

- Isoler immédiatement : débrancher le câble réseau et couper le Wi-Fi des machines touchées — sans les éteindre, la mémoire contient des traces précieuses pour l'analyse (parfois même des clés de chiffrement)
- Couper les accès distants (VPN) et changer les mots de passe critiques depuis un poste sain
- Mettre les sauvegardes à l'abri : déconnecter physiquement celles qui ont survécu avant toute autre action
- Appeler votre prestataire IT et votre assureur cyber — la plupart des contrats imposent une déclaration immédiate
- Photographier la note de rançon et ne rien effacer
- Déposer plainte et notifier la CNIL sous 72 h si des données personnelles sont concernées
- Restaurer uniquement après nettoyage complet : restaurer sur un réseau encore compromis, c'est tout re-perdre le lendemain

ATTENTION

Ne payez pas la rançon. Aucune garantie de récupérer les données (les outils de déchiffrement fournis sont souvent défectueux), aucune garantie de non-publication, et le paiement vous signale comme « bon client » pour une prochaine attaque. Avant toute décision, vérifiez sur nomoreransom.org si un outil de déchiffrement gratuit existe pour la souche qui vous touche.

6. Après l'incident : reconstruire et durcir

- Identifier la porte d'entrée avec l'aide d'un expert — sinon elle resservira
- Reconstruire les systèmes depuis des supports sains plutôt que « nettoyer » : les attaquants laissent des portes dérobées
- Réinitialiser tous les mots de passe de l'entreprise, sans exception
- Tirer le bilan à froid : quelles défenses ont manqué, dans quel ordre les mettre en place
- Informer honnêtement clients et partenaires concernés — la transparence maîtrisée coûte moins cher que la rumeur

L'essentiel à retenir

01 Mettre en place la règle 3-2-1 avec une copie hors ligne ou immuable

02 Tester une restauration complète au moins une fois par an

03 Activer la MFA sur tous les accès distants et comptes admin

04 Ne jamais exposer de RDP directement sur Internet

05 Supprimer les droits administrateur des comptes utilisateurs

06 Déployer un EDR supervisé sur postes et serveurs

Questions fréquentes

Une petite entreprise est-elle vraiment une cible ? Nous n'avons rien d'intéressant à voler.

Les attaques de masse ne choisissent pas : des robots scannent tout Internet et frappent ce qui est vulnérable, quel que soit le nom sur la porte. Et votre valeur n'est pas ce qu'un attaquant peut revendre, c'est ce que VOUS êtes prêt à payer pour retrouver votre facturation, vos dossiers clients et votre production. C'est précisément le calcul du ransomware.

Notre antivirus nous protège-t-il du ransomware ?

Partiellement. Un antivirus à signatures bloque les souches connues, mais les attaques sérieuses utilisent des outils inédits ou détournent des outils légitimes du système. Un EDR comportemental fait beaucoup mieux, à condition que ses alertes soient surveillées. Et aucun outil ne remplace les sauvegardes hors ligne : c'est l'unique garantie de pouvoir repartir.

Payer la rançon est-il légal ?

En France, ce n'est pas illégal en soi (sauf si le destinataire est sous sanctions internationales), et la loi exige un dépôt de plainte sous 72 h pour qu'un assureur puisse rembourser une rançon. Mais toutes les autorités — ANSSI, cybermalveillance.gouv.fr — le déconseillent fermement : payer ne garantit rien et entretient l'écosystème criminel.

Combien de temps faut-il pour s'en remettre ?

Avec des sauvegardes saines et un plan de reprise : de quelques jours à deux semaines pour l'essentiel. Sans sauvegardes exploitables : plusieurs semaines à plusieurs mois, avec une perte définitive de données — et une entreprise sur deux dans ce cas ne s'en remet pas. La différence entre les deux scénarios se joue entièrement avant l'attaque.

Pour aller plus loin

[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — fiche rançongiciel et assistance — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiels-ransomwares

No More Ransom — outils de déchiffrement gratuits — www.nomoreransom.org/fr/index.html

ANSSI — Attaques par rançongiciels, tous concernés — cyber.gouv.fr/publications/attaques-par-rancongiels-tous-concernes

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr