10 conseils empiriques pour récupérer ses données suite à une cyberattaque par ransomware

Quand restaurer ses sauvegardes n'est pas possible !

RECOVEO
AU SERVICE DE VOS DONNÉES

Sommaire

10 réflexes à adopter pour préserver ses données suite à une attaque ransomware :

Rançongiciel : un phénomène en pleine explosion

Le paysage informatique de ces dernières années a été marqué par l'explosion fulgurante d'un nouveau type d'attaques informatiques de plus en plus sophistiquées et virulentes :

les ransomwares ou rançongiciels

Un ransomware, comme son nom l'indique, est un type de logiciel malveillant (malware) qui infecte votre système et chiffre vos données dans le but de vous extorquer une rançon.

+ 300%

C'est l'augmentation des coûts engendrés par les ransomwares de 2017 à 2021 pour atteindre **20 milliards de $**

source : Cybersecurityventures

Selon une étude de février 2022, la France a le taux d'attaques par ransomware **le plus élevé au monde : 81 %** des entreprises interrogées ont été confrontées à au moins une infection par rançongiciel.

De la TPE à la grande entreprise en passant par les administrations publiques, tout le monde est susceptible d'être attaqué par des groupes de **cybercriminels aguerris et organisés** pour lesquels c'est devenu un business juteux.

En 2021, une attaque ransomware a eu lieu toutes les **11 secondes**

source : Idagent

4 options pour la reprise d'activité

Restaurer depuis une sauvegarde récente

Dans le cas où les sauvegardes sont disponibles, suffisamment récentes et saines, c'est la meilleure option.

Mais ça n'est pas toujours possible !

Reconstruire les données à partir de zéro

L'impact sur le temps de reprise d'activité et les coûts engendrés par la reconstitution des données et les pertes d'exploitation sont souvent considérables.

Payer la rançon et tenter de déchiffrer

L'ANSSI déconseille cette option qui ne garantit pas la restitution des données, finance la cybercriminalité et peut inciter à de nouvelles attaques.

Faire appel à un laboratoire spécialisé

Un laboratoire de récupération de données peut être en capacité de retrouver des fichiers à partir de serveurs ou de sauvegardes attaqués par un ransomware.

Pourquoi ce guide ?

Il existe une pléthore de livres blancs traitant des ransomwares.
Il s'agit majoritairement de conseils préventifs pour s'en prémunir, sécuriser les failles et restaurer les sauvegardes qui sont publiés par des organismes d'état, les éditeurs d'antivirus et de solutions de sauvegarde.

Mais que faire dans le cas fréquent où **il n'existe pas de sauvegarde exploitable ?**
Il peut s'agir de sauvegardes anciennes, incomplètes ou souvent sabotées par les cyberattaquants.

Payer la rançon ou repartir de zéro : quelle alternative ?

Quels sont **les bons gestes à adopter** pour se laisser des chances de récupérer tout ou partie des données ?

Ce livre blanc édité par un **laboratoire spécialisé en récupération de données** a pour but de donner des conseils concrets et empiriques pour préserver ses données suite à une attaque ransomware.

01

Isoler les postes du réseau

La majorité des ransomwares scannent le réseau interne ciblé pour se propager et **chiffrer l'ensemble des systèmes connectés.**

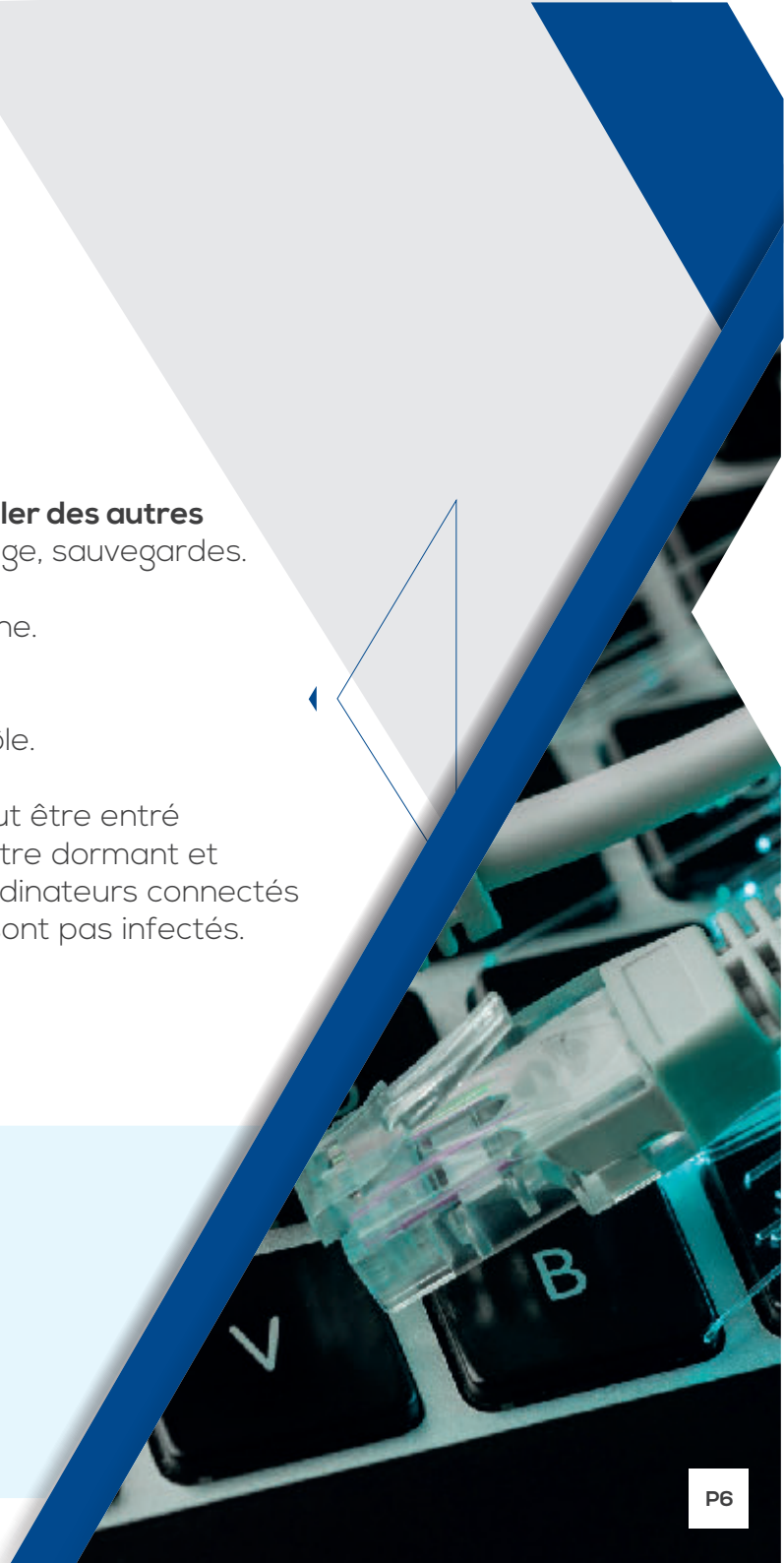
La première chose à faire lorsqu'un ordinateur est suspecté d'être infecté est de **l'isoler des autres ordinateurs et des périphériques de stockage** : postes utilisateurs, serveurs de stockage, sauvegardes.

Déconnectez-le du réseau (câblé et Wi-Fi) et de tout périphérique de stockage externe. Les vers cryptés recherchent activement les connexions et les autres ordinateurs, vous voulez donc empêcher que cela se produise. Vous ne voulez pas non plus que le logiciel rançon communique sur le réseau avec son centre de commande et de contrôle.

Sachez qu'il peut y avoir plus d'un patient zéro, ce qui signifie que le logiciel rançon peut être entré dans votre entreprise ou votre maison par le biais de plusieurs ordinateurs, ou peut être dormant et ne pas encore se manifester sur certains systèmes. Traitez avec suspicion tous les ordinateurs connectés et en réseau et appliquez des mesures pour vous assurer que tous les systèmes ne sont pas infectés.

Les vecteurs d'attaque ransomware les plus courants sont les fichiers infectés, les attaques distantes de serveurs mal sécurisés et le protocole RDP.

source : Sophos



02

Déterminer le périmètre de l'infection

Le plus souvent, le logiciel de rançon ou groupe de hacker qui l'utilise s'identifie lui-même lorsqu'il demande une rançon. Dans le cas contraire, il existe de nombreux sites qui vous aident à identifier les logiciels de rançon, notamment ID Ransomware.
Le site No More Ransom fournit le Crypto Sheriff pour aider à identifier les logiciels de rançon.

L'identification du logiciel de rançon vous aidera à comprendre quel type de ransomware vous a infecté, comment il se propage, quels types de fichiers il affecte etc.

Si la machine infectée est identifiée, **vérifiez quels emplacements réseaux étaient accessibles à partir de ce poste** pour prioriser la vérification des machines ou ressources qui auraient pu être contaminées.

22 jours

C'est le temps d'arrêt occasionné par une attaque ransomware en 2021.
Ce temps est en augmentation constante.

source : Statista

03

Réaliser un état des lieux du matériel de stockage

Dans le cas où vous constatez que l'infection s'est propagée aux serveurs de stockage, ou que ceux-ci ont été pris pour cible suite à une intrusion, il convient de répertorier :

- le nombre de serveurs touchés
- les répliques éventuelles
- les systèmes de stockage utilisés : type de RAID, nombre de disques, volumes de stockage
- l'organisation des données : nombre, tailles et formats de partitions, LUNs ou machines virtuelles

Ces informations doivent être les plus précises et exhaustives possibles pour qu'un prestataire spécialisé en récupération de données dispose du **maximum d'informations techniques** sur l'architecture et puisse proposer une **prise en charge optimale**.

81%

C'est la proportions des organisations françaises qui ont déclaré avoir été confrontées à au moins une infection par rançongiciel selon une étude de 2021.

source : Proofpoint

04

Évaluer les données impactées

S'il s'avère que les systèmes de stockage sont infectés et que les données ont été chiffrées, il convient d'**énumérer et d'évaluer les données perdues :**

- typologies de fichiers : bases de données, fichiers bureautique, machines virtuelles, PAO/DAO etc.
- criticité des données : fichiers les plus importants à récupérer en priorité
- services et utilisateurs les plus impactés par la perte des données
- emplacement de stockage et volumétrie par type de donnée

Cette cartographie des informations perdues et à récupérer est capitale pour prendre du recul sur l'opérationnel et accélérer la reprise d'activité en priorisant les dossiers. Il n'est pas recommandé de s'attaquer d'un seul coup à l'ensemble de l'architecture, mais plutôt d'envisager un retour à la normale en plusieurs paliers : données indispensables à une reprise d'activité dégradée, puis les données secondaires (nécessaires mais pas indispensables) avant de terminer par les documents de type archives par exemple.

D'après l'assurance Allianz,
les incidents cyber représentent le risque n°1 pour les sociétés à l'échelle internationale en 2022.

source : Allianz Global Corporate & Speciality

05

Éviter les mauvaises manipulations

Afin de ne pas amoindrir les chances de récupérer des données et de ne pas compromettre les preuves, il est recommandé de **ne pas écrire ou effectuer de manipulations sur les serveurs.**

D'après notre expérience, les mauvaises manipulations les plus souvent effectuées sont :

- utilisation d'outils de récupération
- reformatage du serveur
- désinfection via des outils antivirus ou antimalware
- effacement de fichiers suspects
- redémarrages successifs du serveur

pas de clonage préalable des disques = risque important de perte de données

Ces manipulations semblent instinctives et valables de prime abord, mais sans sécurité (clonage préalable), elles provoquent souvent des **dommages irréparables et compromettent les chances de réussite**.
Dans la panique, il est tentant d'essayer tout ce qui est en son pouvoir avant de prendre conseil ou de se tourner vers une expertise externe.
C'est compréhensible mais c'est aussi un mauvais réflexe qui, dans le cadre complexe des cyberattaques et ransomwares, provoque **plus de dégâts qu'il n'apporte de solution.**

C'est la baisse du taux de succès moyen sur des dossiers de récupération pour lesquels il y a eu des manipulations préalables.

source : Recoveo

06

Arrêter les serveurs de stockage

Une fois les serveurs de stockage identifiés et les données impactées cartographiées, il convient **d'arrêter les systèmes de stockage et ne pas les redémarrer.**

Beaucoup de ransomwares détectent les redémarrages et peuvent corrompre les systèmes d'exploitation ou effacer des fichiers aléatoirement.

De plus, les redémarrages système génèrent des écritures dans le système de fichiers et l'espace libre qui peuvent écraser des zones utiles et **réduire les chances de retrouver des données.**

Dans la mesure du possible, il est préférable de faire un dump de la mémoire pour conserver des traces à des fins d'investigation forensic :
https://hackernewsdog.com/best-memory-dump-tools-for-forensics

Clonez les supports, sauvegardez la mémoire, et arrêtez toute utilisation des serveurs au plus vite pour **maximiser les chances d'une reprise d'activité rapide.**

80%

des entreprises qui choisissent de payer une rançon pour retrouver l'accès à leurs systèmes chiffrés font face à une **nouvelle attaque** par la suite.

source : Cybereason

07

Répertorier les systèmes de sauvegarde

Les meilleures chances de récupérer des données dans des cas d'attaques ransomware viennent souvent des **systèmes de sauvegarde qui sont attaqués mais plus rarement chiffrés**.

L'intrusion dans le système informatique peut remonter à plusieurs mois mais les hackers doivent aller très vite lorsqu'ils déclenchent leur attaque et ciblent en priorité les serveurs de stockage.

Face aux volumes importants et à la capacité de calcul plus limitée des systèmes de sauvegarde, les cybercriminels vont généralement déployer moins d'efforts et tenter de les **saboter** :

- réinitialisation de volume NAS
- écrasement de LUN ou cible iSCSI
- effacement de containers de sauvegardes ou machines virtuelles

Cas récurrent : sauvegardes à chaud de machines virtuelles via le logiciel Veeam sur un NAS de forte capacité qui est saboté parallèlement au chiffrement du serveur source.

Il convient de **répertorier tous les systèmes de sauvegarde existants**, récents ou anciens ou ayant pu contenir des sauvegardes car chacun est susceptible d'avoir été endommagé différemment et d'avoir un potentiel de récupération différent.

Sur les 10 derniers dossiers de ransomware reçus en diagnostic, les sauvegardes étaient chiffrées dans **seulement 10% des cas** (90% de sabotage).

source : Recoveo

08 Vérifier et préserver les sauvegardes

Lorsque des sauvegardes automatiques sont planifiées, la première chose à faire est de **stopper leur déclenchement** au risque que de voir les données être écrasées par des fichiers infectés. Cela ne doit normalement pas arriver si les systèmes de sauvegarde ont été déconnectés du réseau.

Dans le cas où les sauvegardes sont disponibles, elles doivent être **vérifiées avec précaution :**

- Ne connectez jamais la sauvegarde à une machine potentiellement infectée, même pour une simple vérification.
- Ne formatez pas le serveur infecté pour restaurer la sauvegarde par-dessus.
- Utilisez une machine neuve et hors-réseau pour effectuer ces vérifications.

Ces restaurations hâtives peuvent avoir comme conséquence **l'endommagement de sauvegardes saines ou un nouveau chiffrement des serveurs** lorsque les sauvegardes sont infectées.

Dans le cas fréquent où les sauvegardes ont été sabotées lors de l'intrusion, il est recommandé d'**arrêter au plus vite le matériel afin d'empêcher toute écriture néfaste** générée par le système d'exploitation et des modifications irrémédiables dans le système de fichiers.

L'expérience montre que le potentiel de récupération des données est bien meilleur sur des systèmes de sauvegarde qui sont rapidement stoppés.

En moyenne, les organisations qui payent la rançon restaurent **65% des fichiers chiffrés.**

source : Sophos

09

Se faire accompagner par des experts externes

Lorsque vous ne disposez pas des ressources ni de l'expertise requise pour faire face à une attaque par rançongiciel, il peut être nécessaire de se **faire accompagner par des experts externes :**

- Experts en cybersécurité afin d'identifier puis combler les failles de sécurité et ainsi de protéger votre infrastructure d'une nouvelle attaque
- Experts dans le domaine du stockage et des solutions de sauvegarde pour réintégrer et sécuriser les données
- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Commission nationale de l'informatique et des libertés (CNIL) en cas de violation de données personnelles

Pour plus d'informations : **cybermalveillance.gouv.fr**

02/02/2022

Après Axa, Generali décide de ne plus couvrir le paiement des rançons.

source : BFM Business

10

Se faire accompagner par des experts en récupération de données

Si vos sauvegardes sont défaillantes, faire appel à un **laboratoire spécialisé en récupération de données est une solution qui a fait ses preuves.**

Le but n'est pas forcément de décrypter les fichiers infectés, mais de tenter de trouver des données exploitables à partir des différentes sources de stockage.

Chaque cas d'attaque est différent et nécessite de procéder à un audit des systèmes de stockage :

Serveurs de stockage :

- rechercher des failles dans l'attaque et évaluer si l'ensemble des serveurs ont été chiffrés
- évaluer les possibilités de récupérer des données supprimées ou d'anciennes versions
- rechercher des données sur d'anciens serveurs réinitialisés

Systèmes de sauvegarde (plus rarement chiffrés) :

- déterminer le type de sabotage mis en place : suppression de volume, réinitialisation, écrasement de volume, effacement de containers de sauvegardes ou machines virtuelles
- évaluer les possibilités de récupérer des données supprimées
- extraire des données de sauvegardes corrompues, sabotées ou en panne

RAID//2 RECOVEO

Les 10 commandements

Rappel de la liste des 10 réflexes à adopter pour préserver ses données suite à une attaque ransomware et favoriser une reprise d'activité la plus rapide possible :

01 Isoler les postes du réseau
02 Déterminer le périmètre de l'infection
03 Réaliser un état des lieux du matériel de stockage
04 Évaluer les données impactées
05 Éviter les mauvaises manipulations
06 Arrêter les serveurs de stockage
07 Répertorier les systèmes de sauvegardes
08 Vérifier et préserver les sauvegardes
09 Se faire accompagner par des experts externes
10 Se faire accompagner par des experts en récupération de données

Les **spécialistes de Recoveo** sont à votre écoute n'importe quand et à n'importe quelle heure via leur **cellule d'urgence dédiée 24/7**. Ils peuvent ainsi répondre à vos interrogations et vous orienter vers la **meilleure solution** en fonction de votre problématique.

Cas concrets de récupération de données

Exemple n° 1 : Communauté de communes de la région Rhône-Alpes

Juillet 2020

Problématique

Des hackers ont profité d'un accès mal sécurisé ouvert pour un agent en télétravail pour s'introduire dans le système informatique et chiffrer le serveur de stockage principal pendant la nuit.
Les sauvegardes Veeam ont été sabotées en parallèle du chiffrement du serveur.
Dans la panique, le DSI a utilisé des logiciels de récupération de données sans résultat.

Matériel

2 NAS QNAP de 12 To répliqués qui ont été réinitialisés par les cybercriminels grâce à un accès administrateur.

Données perdues

6 machines virtuelles VMWare contenant des bases de données Oracle et SQL Server issues du logiciel Magnus (Berger-Levrault), le serveur de partage de fichiers bureautiques utilisés par les agents et le serveur de mails Exchange.

Résultat

Récupération parfaite de l'archive Veeam contenant l'intégralité des sauvegardes valides des 6 machines virtuelles à partir du NAS n°2.
Les écritures générées au préalable par les logiciels de récupération sur le NAS n°1 ne permettent pas d'obtenir de résultat exploitable.

Temps de restitution des données

4 jours

Cas concrets de récupération de données

Exemple n° 2 : PME du Nord de la France

Novembre 2021

Problématique

Ce client spécialisé dans le génie mécanique s'est fait infecter par le ransomware Ranzylocked qui a chiffré l'ensemble du serveur de production.
Les sauvegardes Veeam stockées sur un NAS ont été effacées avant le chiffrement du serveur.
L'activité est totalement paralysée et les employés sont au chômage technique.

Matériel

Serveur de production Dell de 8 x 1 To (SSD) en RAID 5
NAS de sauvegarde Synology de 3 x 8 To en RAID 5

Données perdues

5 machines virtuelles Hyper-V (dont Exchange, Sage, partage de fichiers, logiciel métier)

Résultat

Des fichiers Veeam sont rapidement retrouvés sur le NAS effacé, mais ils sont endommagés.
Un outil est développé pour parvenir à extraire le contenu des fichiers vbk corrompus.
Les 5 fichiers vhdx sont récupérés et testés en bon état.

Temps de restitution des données

3 jours

À propos de Recoveo

Laboratoire expert en récupération de données **depuis 2001**, **Recoveo** recense de nombreux succès suite l'explosion des attaques par ransomware, avec un **taux de réussite approchant les 80%**.

Nos clients sont des **grand comptes, collectivités locales ou territoriales, PME ou ETI** dans **différents secteurs d'activité** : santé, industrie, audiovisuel, bâtiment, services informatiques, etc.

Sur un volume de **33 serveurs** réceptionnés en 2021 suite à des cyberattaques :

- 490 To de volume de stockage traités
- Taux de réussite moyen de 81 %
- Délai moyen inférieur à 8 jours

Entreprise **100% française, Recoveo** assure la **confidentialité et la souveraineté des données** traitées dans ses laboratoires.

Recoveo a été auditée et labellisée par la société spécialisée en cybersécurité **Ubcom** qui récompense 3 atouts majeurs :

- la **souveraineté** des données
- la **méthodologie** de travail
- la **sécurité** renforcée

Ce guide a été réalisé par Recoveo, laboratoire expert en récupération de données depuis 2001.

Suite à de nombreuses demandes d'interventions post cyberattaque, Recoveo a souhaité partager son retour d'expérience afin d'éviter tout risque d'aggravation de l'environnement dans le cadre d'infection par ransomware.

Pour plus d'informations et de conseils : **recoveo.com** / **raid112.com**

0 805 385 607 Service & appel gratuits

RECOVEO
AU SERVICE DE VOS DONNÉES