# COMMENT PRÉVENIR LES RANÇONGICIELS ET S'EN REMETTRE

SEPTEMBRE 2021 | ITSAP.00.099

## QU'EST-CE QU'UN RANÇONGICIEL?

Un rançongiciel est un type de maliciel qui bloque l'accès aux fichiers ou aux systèmes jusqu'à ce que l'utilisateur verse une somme d'argent. Le rançongiciel peut se servir de votre réseau pour infecter tous les appareils qui y sont connectés. Il y a deux principaux types de rançongiciels:

- **Le cryptorançongiciel** retire les accès à vos fichiers en les remplaçant par des données chiffrées.
- **Le rançongiciel cryptoverrouilleur** vous empêche de vous connecter à votre appareil.

Les dispositifs sont souvent infectés par un rançongiciel lorsqu'on clique sur des liens ou qu'on télécharge des pièces jointes qui se trouvent sur des sites Web non sécurisés, dans des courriels d'hameçonnage ou sur les médias sociaux. Les auteurs de menace explorent souvent vos réseaux pour trouver de l'information qu'ils pourraient exfiltrer et surveillent vos méthodes de communications avant de déployer un rançongiciel.

Si votre dispositif est infecté par un rançongiciel, vous recevrez un avis de rançon à votre écran vous indiquant que vos fichiers ont été chiffrés et qu'ils seront inaccessibles jusqu'à ce qu'une rançon soit payée. Les auteurs de menace risquent de vous menacer de détruire vos données de façon permanente, ou de les rendre publiques, si vous ne payez pas la rançon dans un délai précis. On demande habituellement la rançon en monnaie numérique, comme des bitcoins, étant donné que le transfert est difficile à retracer. Des cartes de crédit prépayées ou des cartes-cadeaux peuvent également être demandées.

## COMMENT MON ORGANISATION PEUT-ELLE SE PRÉPARER?

Il y a plusieurs façons de minimiser les risques d'attaque par rançongiciel et de préparer votre organisation en conséquence.

**Planifiez.** Élaborez un plan d'intervention en cas d'incident pour déterminer comment votre organisation surveillera et détectera les incidents et comment elle interviendra par la suite, comme dans le cas d'une attaque par rançongiciel. Votre plan doit également comprendre un plan de sauvegarde, de reprise, et de communication. Votre plan d'intervention devrait établir les rôles que vos employés devront jouer et les instructions détaillées qu'ils devront suivre en cas d'incident.

**Sensibilisez vos employés à la sécurité.** Donnez à vos employés de la formation personnalisée sur la cybersécurité et la gestion des dispositifs pour éviter qu'ils tombent dans le piège d'activités malveillantes comme des courriels d'hameçonnage et le téléchargement de fichiers infectés.

**Mettez vos plans à l'essai.** Faites l'essai de votre plan d'intervention en cas d'incident et de votre plan de reprise en effectuant des simulations et des exercices préparatoires. Les mises en situation devraient évaluer l'efficacité de vos mesures d'intervention et mettre en lumière ce qu'il convient d'améliorer.

**Pensez à une cyberassurance.** Faites des recherches sur les fournisseurs de cyberassurance et sur les diverses polices d'assurance pour déterminer si votre organisation pourrait en tirer des avantages.

## COMMENT PUIS-JE PROTÉGER MON ORGANISATION?

**Sauvegardez vos données**. Mettez en place un plan de sauvegarde des données de votre organisation. Une copie de sauvegarde vous permettra de récupérer vos données et d'accéder à vos systèmes essentiels dans l'éventualité d'un incident. Vous devez faire des copies de sauvegarde régulièrement pour vous assurer qu'elles comportent les données les plus à jour. Créez le plus de barrières de sécurité que possible entre vos systèmes de production et vos copies de sauvegarde et veillez à ce que ces dernières soient stockées hors ligne sans connexion à Internet ou à des réseaux locaux. Les auteurs de menace peuvent infecter vos copies de sauvegarde avec des rançongiciels si ces dernières sont connectées à vos réseaux, ce qui minerait vos efforts de restauration. Il est également essentiel de mettre à l'essai votre processus de sauvegarde et de récupération pour vous assurer que votre restauration est rapide et efficace.

**Adoptez le principe du droit d'accès minimal.** Gérez et surveillez les comptes et les accès des utilisateurs en appliquant le principe du droit d'accès minimal, selon lequel les employés devraient seulement avoir les accès et privilèges nécessaires à la réalisation de leurs tâches. Restreignez les privilèges administratifs et exigez une confirmation pour chaque action qui nécessite des droits d'accès et des autorisations de niveau élevé.

**Mettez à jour vos systèmes et appliquez les correctifs.** Obtenez les mises à jour et les correctifs qui corrigeront les vulnérabilités et les bogues connus de vos logiciels, microprogrammes, et systèmes d'exploitation. Les auteurs de menace peuvent facilement exploiter les systèmes et les dispositifs non corrigés ou qui ne sont pas pris en charge.

**Désactivez les macros.** Assurez-vous de désactiver les macros par défaut afin de réduire les risques de propagation des rançongiciels par des pièces jointes de Microsoft Office.

**Segmentez vos réseaux.** Divisez votre réseau en plus petites sections. Ainsi, il sera plus difficile pour un rançongiciel d'infecter l'ensemble du réseau.

**Mettez en place des outils de sécurité.** Installez un antimaliciel et un antivirus sur vos appareils afin de détecter les activités malveillantes et sécurisez votre réseau à l'aide d'un pare-feu pour protéger les dispositifs connectés. Pensez à installer un filtre DNS (système de noms de domaine) sur vos appareils mobiles pour bloquer les sites Web malveillants et filtrer le contenu nuisible. Vous pouvez également mettre en œuvre le protocole DMARC (Domain-based Message Authentication, Reporting and Conformance), un système d'authentification et de rapports qui aide à protéger les domaines de votre organisation contre l'usurpation, l'hameçonnage et d'autres activités malveillantes.

**Obtenez l'aide de professionnels de la cybersécurité.** Dans le cas d'un cyberincident, le fait de communiquer tout de suite avec un professionnel de la cybersécurité peut vous aider à restaurer vos systèmes et vos données plus rapidement qu'avec votre personnel de TI en interne.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

## COMMENT REPRENDRE MES ACTIVITÉS APRÈS UNE ATTAQUE?

Les étapes suivantes peuvent vous aider à éliminer un rançongiciel ou à réduire sa propagation.


1. **Isolez le dispositif immédiatement.** Mettez vos dispositifs hors connexion pour arrêter la propagation du rançongiciel à d'autres dispositifs connectés. Certaines souches de rançongiciels sont conçues pour rester en dormance sur un dispositif et se propager discrètement à d'autres dispositifs connectés aux réseaux avant de chiffrer les fichiers. Dans de tels cas, il est possible que vous ne puissiez pas arrêter la propagation du rançongiciel.
2. **Déterminez le type de rançongiciel.** Utilisez les informations de la note de rançon (p. ex., les URL listées) et les nouvelles extensions dont vos fichiers chiffrés ont hérité afin d'alimenter vos recherches sur de possibles attaques récurrentes et d'identifier le rançongiciel. Si vous trouvez un outil de déchiffrement en ligne, allez à l'étape 3.
3. **Retirez le rançongiciel.** Utilisez l'outil de déchiffrement en ligne pour retirer le rançongiciel de vos dispositifs, ce qui devrait déchiffrer vos fichiers et les rendre accessibles.

4. **Réinitialisez le dispositif et effacez toutes les données qu'il contient.** Si aucun outil de déchiffrement n'est disponible en ligne pour la souche de rançongiciel à laquelle vous faites face, effacez toutes les données de votre dispositif de façon sécuritaire et réinstallez le système d'exploitation.
5. **Restaurez vos systèmes et vos données à partir de votre copie de sauvegarde.** Analysez vos copies de sauvegarde pour vous assurer qu'aucun rançongiciel ou autre logiciel malveillant ne s'y trouvent. Stockez vos copies de sauvegarde hors ligne pour atténuer les risques qu'un rançongiciel les infecte. Une fois que vous êtes confiant, restaurez vos systèmes et vos dispositifs à partir de vos copies de sauvegarde.
6. **Mettez à jour vos systèmes et appliquez les correctifs.** Mettez à jour tous vos dispositifs, votre matériel et vos logiciels. Appliquez les correctifs à votre système d'exploitation et assurez-vous que tout antivirus, antimaliciel et pare-feu est à jour.

7. **Changez vos mots de passe.** Réinitialisez vos justificatifs d'identité, y compris les mots de passe de tous vos systèmes, dispositifs et comptes. Les auteurs de menace conservent habituellement ces informations pour des attaques futures. Pensez à utiliser des phrases de passe pour vos dispositifs puisque celles-ci sont plus robustes et plus faciles à retenir.
8. **Offrez de la formation.** Formez vos utilisateurs sur la cybersécurité pour réduire le risque d'attaques futures. La formation devrait porter sur toutes les mesures préventives qui permettent de se protéger contre les attaques par rançongiciel, comme apprendre à identifier reconnaître des pièces jointes et des courriels suspects. Servez-vous des menaces courantes et des incidents passés pour rester à jour et vous préparer pour le futur.

### DEVRAIS-JE LE SIGNALER?

Bien que ça ne vous apparaisse peut-être pas essentiel sur le moment, il est important de signaler tout incident lié à un rançongiciel aux organismes d'application de la loi, au Centre canadien pour la cybersécurité et au Centre antifraude du Canada. Si vous êtes la première organisation à en être la cible, les organismes d'application de la loi seront mis au courant et pourront surveiller d'autres attaques possibles. Ces organismes peuvent également vous aider à atténuer les risques et vous soutenir dans vos efforts de reprise.

## LES RISQUES ASSOCIÉS AU PAIEMENT D'UNE RANÇON

La décision de payer un auteur de menace pour qu'il vous redonne l'accès à vos fichiers et à vos dispositifs est difficile, et vous vous sentirez probablement pressé de répondre à ses demandes. Avant de payer, communiquez avec votre poste de police local et signalez le cybercrime. Il n'est habituellement pas recommandé de payer la rançon pour les raisons suivantes:

- Payer la rançon ne garantit pas l'accès à vos fichiers. Les auteurs de menace pourraient demander encore plus d'argent après que vous avez payé une première rançon.
- Payer une rançon encourage les auteurs de menace à continuer d'infecter vos dispositifs et ceux d'autres organisations avec des rançongiciels puisqu'ils s'attendent à ce que vous continuerez de payer à chaque attaque.
- Les auteurs de menace peuvent utiliser des maliciels effaceurs qui ont l'apparence d'un rançongiciel. Dans ce cas, vos fichiers ne seront pas récupérables puisque les maliciels les modifient ou les suppriment de façon permanente une fois que la rançon est payée.
- Vos données ont probablement été copiées et peuvent être divulguées par les auteurs de menace à des fins financières. Ils pourraient également continuer de vous extorquer de l'argent avec les copies des données.
- Votre paiement pourrait être utilisé pour soutenir d'autres attaques par rançongiciel ou des organisations terroristes.

## POUR EN SAVOIR PLUS

Pour obtenir des précisions sur certains points clés, consultez les publications connexes ci-dessous, qui se trouvent sur le site Web du Centre pour la cybersécurité (cyber.gc.ca).

- *Directive de mise en œuvre : protection du domaine de courrier*
- *Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)*
- *Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)*
- *Êtes-vous victime de piratage? (ITSAP.00.015)*
- *Les outils de sécurité préventive (ITSAP.00.058)*
- *Sauvegarder et récupérer vos données (ITSAP.40.002)*
- *Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)*
- *Reconnaître les courriels malveillants (ITSAP.00.100)*

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada