

Ransomware (rançongiciel)

Les criminels appliquent toute une série de stratégies pour soutirer de l'argent à leurs victimes inconscientes. Une de leurs méthodes favorites consiste à chiffrer les fichiers de l'utilisateur puis à lui demander une « rançon », en échange de quoi il pourra – peut-être – récupérer ses données.

Voici comment vous protéger contre les ransomwares :

- **Effectuez régulièrement une sauvegarde de vos données (backup).**

Une fois votre sauvegarde effectuée, veillez à bien déconnecter le support du système, sans quoi les données sauvegardées risqueraient elles aussi d'être verrouillées en cas d'infection de l'ordinateur par un rançongiciel.

- **Faites en sorte que les programmes et les plug-ins installés sur votre ordinateur soient toujours parfaitement à jour.**

Assurez-vous de disposer toujours de la dernière version disponible de tous vos logiciels, applications et plug-ins de navigation. Dans la mesure du possible, recourez systématiquement à la fonction de mise à jour automatique.

- **Faites preuve de prudence et de vigilance lorsque vous tombez sur des courriels douteux.**

La prudence est de mise pour tous les courriels inattendus, même lorsque ces derniers semblent provenir d'un contact connu. Ne suivez pas les instructions indiquées dans le message, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.

- **Utilisez un programme antivirus.**

Le programme de protection antivirus doit être constamment mis à jour par le biais des mises à jour automatiques. Un antivirus non actualisé risque en effet de ne pas reconnaître les derniers logiciels malveillants.

Fonctionnement

Tout va très vite : l'ouverture d'une pièce jointe infectée ou d'un site web piraté suffit parfois pour introduire un rançongiciel dans le système. Une fois inoculé, le programme malveillant efface ou chiffre l'ensemble des fichiers stockés, les rendant, de fait, complètement inutilisables.

Un écran de verrouillage apparaît sur le système, demandant à la victime de payer une rançon au hacker sous la forme d'un virement en monnaie virtuelle, en échange de quoi il procédera au déverrouillage de ses données. En choisissant une monnaie virtuelle, les cybercriminels savent qu'il sera très difficile de remonter jusqu'à eux.



La cible de prédilection des criminels reste les entreprises : dans la mesure où elles disposent de très grandes quantités de données confidentielles et stratégiques, elles sont souvent plus facilement disposées à payer de grosses sommes d'argent, pourvu d'éviter la perte de données cruciales. Cela dit, le risque d'infection par un ransomware et la perte des données qui en découle touche tout autant les particuliers.

Que faire en cas d'infection ?

La mesure la plus efficace doit être prise avant l'infection et consiste en la réalisation de copies de sauvegarde (backups) des données. Une infection du système reste possible et comporterait naturellement des désagréments et du travail pour réinstaller le système d'exploitation et les différents programmes, mais le principal est que vous aurez pu sauver vos données personnelles et les préserver contre d'autres menaces potentielles. Vous trouverez d'autres informations sur le sujet dans notre article « [Règle n°1 – Sauvegarder les données \(https://www.ebas.ch/fr/1-sauvegarder-les-donnees/\)](https://www.ebas.ch/fr/1-sauvegarder-les-donnees/) ».

Il est vivement déconseillé de payer toute forme de rançon ! Absolument rien ne garantit que la victime pourra effectivement retrouver ses données chiffrées. En cédant au chantage, on ne ferait qu'entretenir le modèle opérationnel des cybercriminels qui pourront ainsi poursuivre leurs attaques et racketter de nouvelles victimes.

Voici ce que vous devez faire en cas d'infection :**• Forcez l'arrêt de votre dispositif.**

Si vous remarquez un fonctionnement irrégulier de votre système et que vous l'imputez à la présence d'un ransomware ou autre logiciel malveillant, forcez l'extinction de votre appareil. « Forcer » l'arrêt signifie que vous devez mettre votre appareil hors tension, en débranchant le câble d'alimentation ou en appuyant pendant au moins 5 secondes sur le bouton d'allumage. C'est la seule chance dont vous disposez pour tenter de sauver le plus de données possible. Dans le cas d'un smartphone ou d'une tablette, plus difficiles à mettre hors tension, la seule solution est d'éteindre « normalement » votre dispositif.

• Nettoyez votre dispositif à l'aide d'un système Live de secours.

Si cela est possible, et réalisable, redémarrez votre dispositif avec un système Live de secours tels que par exemple « [Desinfect't](https://www.heise.de/download/product/desinfect-71642) (<https://www.heise.de/download/product/desinfect-71642>) » de la société « c't ». Ce système vous permettra d'analyser, de nettoyer et de sauvegarder vos données. Autrement, vous pouvez aussi confier votre appareil à un technicien qui se chargera lui-même de cette tâche.

• Utilisez des routines de déchiffrement si elles existent.

S'il existe déjà des routines de déchiffrement pour un ransomware, vous pouvez consulter un site dédié tel que www.nomoreransom.org (<https://www.nomoreransom.org/fr/index.html>). Une fois identifiée, la routine peut être téléchargée et utilisée sur votre appareil.

• Modifiez tous vos mots de passe.

Vous trouverez d'autres informations sur le sujet dans notre article « [Règle n°4 – Protéger les accès Internet](https://www.ebas.ch/fr/4-protoger-les-acces-internet/) (<https://www.ebas.ch/fr/4-protoger-les-acces-internet/>) ».

• Prévenez les autorités.

Prévenez l'Office fédéral de la cybersécurité (OFCS) en remplissant le [formulaire de signalement](https://www.report.ncsc.admin.ch/fr/) (<https://www.report.ncsc.admin.ch/fr/>) et portez plainte auprès du service de police local.

Breachstortion

Semblables aux attaques de ransomware, les attaques de type « breachstortion » ont récemment fait leur apparition dans le paysage des menaces informatiques. Dans ce cas, les criminels ne se limitent pas à verrouiller les données, mais menacent également leurs victimes (généralement des entreprises) de publier des informations sensibles et de nuire à leur réputation, à moins de payer une rançon.

Cette stratégie, qui repose sur la peur de la victime de voir sa réputation entachée, a pour but de mettre l'utilisateur encore davantage sous pression, dans le cas où l'impossibilité d'accéder à ses données ne suffisait pas à le décider à payer la rançon demandée.

Les rançongiciels (ou ransomware en anglais) font partie de la famille des logiciels malveillants appelés malwares. Ceux-ci se diffusent généralement via des pièces jointes ou des sites Internet infectés. Une fois installé, le rançongiciel verrouille les fichiers stockés sur l'ordinateur de la victime ainsi que sur tous les lecteurs réseau et supports de données connectés, comme par exemple les clés USB. À partir de là, la victime ne peut plus accéder à ses données.

Jouez à notre Ransomware Game !



[\(https://www.ebas.ch/fr/ransomware-game/\)](https://www.ebas.ch/fr/ransomware-game/)