Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)

Cybersécurité

Vous avez reçu un message douteux contenant des pièces jointes ? Vous avez retrouvé par hasard une clé USB ? Gare aux « rançongiciels » (ou « ransomware ») ! Vos données peuvent-être chiffrées et prises en otage contre rançon. Voici 5 conseils pour minimiser les risques.

Qu'est-ce qu'un ransomware ?

Vous êtes de plus en plus nombreux à recevoir des messages douteux contenant des pièces jointes ou des liens vous invitant à les ouvrir.

Prenez garde, des logiciels malveillants appelés « rançongiciels » ou « ransomware » peuvent s'y cacher. Leur but : chiffrer (coder) vos données pour vous les rendre moyennant une rançon. Bien entendu, la payer ne garantit pas la récupération de vos données. Mieux vaut donc vous prémunir contre ce type d'attaque.

Pour se prémunir d'un ransomware, effectuez des sauvegardes régulières de vos données

C'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne !

Lire aussi : Sécurité de vos données : les 7 méthodes de piratage les plus courantes

N'ouvrez pas les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel

Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels. Restez donc très vigilants ! Certains messages paraissent tout à fait originaux.

Apprenez à distinguer des emails piégés (ou autres formes de récupération de vos données) sur la Hack Academy.

Vous avez un doute ? Contactez le messager par un autre biais.

Lire aussi : Sécurité sur le web : découvrez le nouveau site web cybermalveillance.gouv.fr

Pour se prémunir d'un ransomware, apprenez à identifier les extensions des fichiers douteuses

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ? Ne les ouvrez surtout pas ! Exemples : pif ; .com ; .bat ; .exe ; .vbs ; .lnk… Attention à l'ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l' Agence nationale de la sécurité des systèmes d'information (ANSSI), il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

Lire aussi : 10 règles à respecter pour être (presque) sûr de vous faire pirater votre ordinateur

Pour se prémunir d'un ransomware, mettez à jour vos principaux outils

On ne vous le dira jamais assez : Windows, antivirus, lecteur PDF, navigateur… Veillez à leurs mises à jour ! Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications.

Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

Lire aussi : Comment protéger ses données personnelles ?

Pour se prémunir d'un ransomware, utilisez un compte « utilisateur » plutôt qu' « administrateur »

Nous vous l'avions déjà conseillé, ne naviguez pas depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

Lire aussi : Sécurité sur le web : découvrez le nouveau site web cybermalveillance.gouv.fr

RANÇONGICIELS
COMMENT S'EN PRÉMUNIR?

Mode d'emploi

Les rançongiciels sont des **programmes informatiques malveillants** de plus en plus répandus. Leur objectif : chiffrer vos données puis vous demander d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Bien entendu, la **payer ne garantit pas la récupération de vos données**. Mieux vaut donc vous prémunir contre ce type d'attaque !

LES CONSIGNES À SUIVRE

APPRENEZ À IDENTIFIER LES EXTENSIONS douteuses des fichiers

N'OUVREZ PAS LES MESSAGES dont la provenance ou la forme est suspecte

UTILISEZ UN COMPTE UTILISATEUR plutôt qu'*administrateur*

METTEZ À JOUR vos outils principaux

SAUVEGARDEZ RÉGULIÈREMENT vos données