Les ransomwares

Par Patrick Sentinel – 29a.ca

Ce qu'il faut savoir sur les ransomwares (ou comment éviter que vos fichiers finissent en otage)

Imaginez que vous êtes tranquillement chez vous, en train de siroter un café, quand tout à coup… votre ordinateur vous envoie un message d'alerte : "Vos fichiers sont chiffrés. Payez une rançon pour les récupérer." Non, ce n'est pas une blague, c'est un **ransomware**. Les ransomwares, ces logiciels malveillants qui prennent vos fichiers en otage, sont devenus la **plaie (je pèse le mot)** du numérique moderne. Mais pas de panique ! Voici ce qu'il faut savoir pour éviter de finir avec un ordinateur séquestré.

1. Les ransomwares, c'est quoi ?

Un ransomware, c'est un logiciel malveillant qui entre dans votre système, **verrouille** vos fichiers et vous demande une rançon pour les récupérer (d'où le nom, "ransom" signifiant "rançon" en anglais). Imaginez un voleur numérique qui entre chez vous, change toutes les serrures, et ne vous laisse rentrer qu'une fois que vous avez payé. Mais ici, il n'y a pas de serrurier pour vous sauver, et il est peu probable que les cybercriminels honorent leur "promesse" une fois payés.

Petite précision : En payant la rançon, il n'y a **AUCUNE** garantie que vous retrouverez vos fichiers. Souvent, l'arnaqueur disparaît une fois l'argent reçu, sans laisser de clés pour déverrouiller vos précieuses données, crap crap 😐.

2. Comment ça arrive ?

Les ransomwares ne surgissent pas de nulle part. Ils arrivent souvent sous forme de pièces jointes infectées, de liens cliquables ou de fichiers téléchargés sur un site douteux. Vous cliquez, l'ordinateur s'infecte, et hop ! Vos fichiers sont bloqués avant même que vous ayez eu le temps de crier : "mouton !!!".

Les techniques courantes : Les courriels de phishing sont parmi les méthodes favorites pour propager les ransomwares. Un courriel qui semble venir de votre banque, d'un colis à récupérer ou même d'un ami. Attention à ce que vous ouvrez !

3. Les différents types de ransomwares

Il existe plusieurs variantes de ransomwares, chacune avec sa petite touche personnelle pour rendre vos journées plus "intéressantes" :

- **Le ransomware de cryptage** : Le plus classique. Il chiffre tous vos fichiers pour les rendre illisibles, puis exige une rançon pour vous donner la clé de déchiffrement.
- **Le ransomware de verrouillage** : Celui-ci bloque complètement votre appareil, souvent en affichant un grand message menaçant. Pas d'accès aux fichiers, pas d'accès à l'appareil. Il vous faut une clé pour le déverrouiller.
- **Le scareware** : Moins dangereux, mais tout aussi agaçant, il fait semblant de bloquer votre système en affichant de fausses alertes et des messages effrayants. Heureusement, il est parfois possible de s'en débarrasser avec une simple analyse antivirus.

4. Comment éviter de se faire piéger par un ransomware ?

La meilleure défense contre un ransomware, c'est de ne **JAMAIS** l'inviter chez vous ! Voici quelques astuces simples pour éviter d'en faire l'expérience :

- **Faites des sauvegardes régulières** : Le meilleur moyen de ne pas céder aux menaces, c'est de ne pas avoir besoin des fichiers bloqués. Sauvegardez vos données sur un disque externe ou dans le cloud, et faites-le régulièrement. Je sais qu'il faut y investir quelques minutes de son temps mais ça va vous prendre plus de temps à remettre tout en ordre si vous n'avez pas de *backup*.
- **Ne cliquez pas sur tout et sur n'importe quoi** : **Avant** d'ouvrir une pièce jointe ou de cliquer sur un lien, demandez-vous si c'est vraiment fiable. Les courriels suspects, les pièces jointes inattendues et les liens étranges sont à éviter.
- **Utilisez un antivirus** : Choisissez un bon antivirus et assurez-vous qu'il est à jour. Il pourra détecter les ransomwares avant qu'ils n'entrent dans votre système.
- **Mettez vos logiciels à jour** : Les ransomwares aiment les failles de sécurité. Gardez vos logiciels et votre système d'exploitation à jour pour réduire les risques (un article sur les mises à jour est déjà disponible).
- **Désactivez les macros** : Certains ransomwares se cachent dans des fichiers *Word* ou *Excel*. Si on vous demande d'activer les macros, réfléchissez-y à deux fois, surtout si le document vient d'une source non vérifiée.

5. Que faire si on est victime d'un ransomware ?

Pas de panique ! Même si la situation est stressante, il y a des étapes à suivre :

- **Déconnectez-vous du réseau** : Si votre appareil est infecté, coupez immédiatement la connexion Internet et déconnectez les périphériques externes pour éviter la propagation.
- **Ne payez pas la rançon** : Comme mentionné, **rien ne garantit** que vous retrouverez vos fichiers, désolé mais c'est la vie. Il faut plutôt être préventif et éviter que ça nous arrive.
- **Consultez un professionnel** : Certains ransomwares ont déjà été neutralisés, et il existe parfois des outils de décryptage pour les variantes connues. Cherchez de l'aide auprès d'un expert en cybersécurité ou consultez des sites officiels comme

No More Ransom qui offrent des solutions gratuites pour certains types de ransomwares.

6. Pourquoi les ransomwares existent-ils encore ?

Simple : parce que ça marche malheureusement! Les ransomwares sont rentables pour les cybercriminels, car beaucoup de victimes cèdent à la panique et paient la rançon. De plus, c'est une technique relativement simple à mettre en place pour les pirates. Tant qu'il y aura des gens pour payer, il y aura des ransomwares.

Conclusion : mieux vaut prévenir que guérir !

Les ransomwares sont un véritable fléau, mais avec un peu de prudence, il est possible de s'en protéger. En suivant quelques bonnes pratiques (sauvegardes, antivirus, vigilance et autres protections), vous réduisez considérablement les risques. Souvenez-vous : en ligne, chaque clic compte, et mieux vaut réfléchir avant de cliquer. Votre ordinateur et vos fichiers vous en remercieront !