Thème de la semaine 2 : **Pourquoi moi?**

MOIS DE LA CYBER-SENSIBILISATION

Rançongiciel

Les employés du conseil scolaire, les enseignants et les élèves sont des cibles potentielles

Nous n'accordons habituellement pas beaucoup d'importance à la possibilité d'être des cibles pour les pirates informatiques en raison simplement de la nature de notre travail ou en tant qu'étudiant. Où que nous travaillions, enseignons ou apprenons, nous gérons chaque jour des renseignements, qu'il s'agisse de conseils scolaires, d'élèves ou de nos propres renseignements. Cela fait de nous des cibles pour les pirates informatiques.

La propagation des rançongiciels, une forme de logiciel malveillant qui verrouille et crypte les fichiers contenus dans l'ordinateur de la victime, est en hausse. Selon un rapport d'EmsiSoft, « En 2019, les États-Unis ont été frappés par une avalanche sans précédent et incessante d'attaques par rançongiciel qui ont touché au moins 966 organismes gouvernementaux, établissements d'enseignement et fournisseurs de soins de santé, pour un coût potentiel de plus de 7,5 milliards de dollars.

Le problème s'est aggravé pour les écoles de la maternelle à la 12e année aux États-Unis, en particulier pendant la pandémie de COVID, ce qui a incité le FBI à émettre une alerte de sécurité en juin 2020.

> *« Les rançongiciels constituent une forme de logiciel malveillant qui ciblent les employés du gouvernement. Il est de notre devoir de continuer à nous défendre contre ces menaces. Nous avons tous un rôle de premier plan à jouer dans la sécurité de l'information, puisque la majorité des cyberattaques découlent de l'erreur d'un utilisateur. Enseigner aux utilisateurs les pratiques exemplaires en matière de cybersécurité est le premier pas pour enrayer le problème des rançongiciels. »*
>
> **John Roberts**
> Directeur général de la sécurité de l'information
> Ministère des Services gouvernementaux et des Services aux consommateurs

Le Financial Post indiquait, dans un récent reportage, que les attaques par rançongiciel visaient des employés d'un organisme de santé du gouvernement canadien, non nommé, et une université participant activement aux recherches sur la COVID-19. Dans ces attaques, les pirates informatiques ont déployé des courriels d'hameçonnage contenant des pièces jointes infectées. Un clic sur la pièce jointe, par le destinataire, aurait entraîné le chiffrement de ses fichiers jusqu'au paiement de la rançon. Dans les deux cas, les attaques ont échoué.

Ces dernières années, un certain nombre d'incidents notables impliquant des rançongiciels ont touché des organisations de toutes sortes. Hormis les millions ou les milliards de dollars en pertes de revenus, ces attaques ont miné la confiance du public. Elles ont aussi mené à une exposition de renseignements sensibles. Dans de nombreux cas, il aura fallu satisfaire aux demandes de paiement des pirates informatiques pour reprendre le contrôle des systèmes informatiques rançonnés.

> *« Les employés du gouvernement sont les cibles potentielles de rançongiciels et d'autres types de cybercrimes, parce qu'ils pourraient fournir des services dont dépendent des collectivités, ce qui renseignements sous leur garde u précieuse pour les cybercriminels. »*
>
> **Jenny Alfandary**
> Directrice de l'information, Metrolinx

Les organismes victimes d'attaques par rançongiciel, ces dernières années, sont Garmin, LifeLabs, A. P. Moller-Maersk, Sony Pictures et l'agence de transport municipal de San Francisco. Certaines de ces attaques étaient si virulentes que les organismes infectés ont dû suspendre leurs activités habituelles et recourir à des transactions et à des communications non informatisées, comme dans le cas de l'attaque de Sony Pictures, où la société a dû communiquer avec ses employés au moyen de documents papier.

Comment les attaques par rançongiciel se déroulent-elles et qu'espèrent en tirer les pirates informatiques? Les pirates informatiques veulent en tirer un profit financier. Ils retiennent des systèmes informatiques en otage et forcent les entreprises et les particuliers à payer une rançon pour libérer les fichiers et les renseignements. Leurs demandes de paiement prennent habituellement la forme de cryptomonnaies, comme les bitcoins, pour éviter toute détection. En contrepartie du paiement, les pirates informatiques fournissent généralement une clé de déchiffrement qui permet à l'organisation ou à la personne touchée de récupérer ses renseignements et de reprendre ses activités. Dans de nombreux cas, la clé de déchiffrement ne restaure pas toutes les données et, parfois, elle ne fonctionne pas du tout.

De même, dans le cas de particuliers, les pirates informatiques cherchent à exploiter des possibilités en menaçant d'exposer des renseignements personnels pour obtenir un paiement. Les experts en cybersécurité recommandent de ne pas céder aux demandes de rançon des pirates informatiques, parce que rien ne garantit aux victimes qu'elles récupéreront leurs renseignements. Même après une récupération, rien ne dit que ces pirates informatiques ne cibleront pas de nouveau ces mêmes victimes. Que pouvez-vous faire pour vous protéger, vous et les renseignements que vous gérez chaque jour?

> *Le Mois de la sensibilisation à la cybersécurité est une campagne reconnue à travers le monde, qui a lieu chaque année en octobre, pour sensibiliser davantage le public à la sécurité en ligne, à la protection de la vie privée et à la cybersécurité. Cette activité, en cours tout le mois, à laquelle se greffent des programmes de formation de sensibilisation à la cybersécurité au travail, partout au Canada, doit nous rappeler à quel point il est important de toujours protéger nos renseignements, qu'il s'agisse d'un appareil personnel ou fourni pour le travail.*
>
> **Christine Beauchamp**
> Directrice par intérim, Centre d'appels et Détection des incidents
> Centre canadien pour la cybersécurité

Voici quelques astuces et de l'information permettant d'éviter d'être victime d'une attaque par rançongiciel :

- Rançongiciel 101 : Comment assurer votre cybersécurité
- Rançongiciel : Sauvegardez vos données, sinon…
- Vidéo: Maliciels et rançongiciels

En tant qu'employés du conseil scolaire, enseignants ou élèves il nous appartient à tous de protéger les renseignements auxquelles nous avons accès ou qui nous sont confiées. En faisant tous notre part, nous aidons à préserver la sécurité de nos lieux de travail, d'apprentissage et de nos domiciles.

Cet article a été adapté par ECNO, les membres participants d'OASBO ICT et le ministère de l'Éducation à partir d'un article produit d'une collaboration entre le ministère des Services gouvernementaux et des Services aux consommateurs, le personnel de gestion du risque en cybersécurité de Metrolinx et du Centre canadien pour la cybersécurité, dans le cadre de la sensibilisation à la sécurité sur Internet durant le Mois de la sensibilisation à la cybersécurité.