Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Feuille-info sur la technologie

Se protéger contre les rançongiciels

Juillet 2016

Les rançongiciels sont de plus en plus courants et constituent une menace sérieuse à la sécurité des documents électroniques. La présente feuille-info destinée aux institutions publiques et aux organismes du secteur de la santé de l'Ontario explique comment se protéger contre ces logiciels.

QU'EST-CE QU'UN RANÇONGICIEL?

Un rançongiciel est un type de logiciel malveillant qui chiffre des fichiers dans votre appareil ou ordinateur, y compris les unités mappées ou de réseau, afin de vous extorquer de l'argent en échange de la clé nécessaire pour les déchiffrer. Ce logiciel vous empêche donc d'utiliser vos données, que vous ne pouvez récupérer qu'en payant une rançon.

COMMENT LES ORDINATEURS EN SONT-ILS INFECTÉS?

Les pirates informatiques utilisent différentes techniques pour installer des rançongiciels dans les ordinateurs. Ces techniques se divisent en gros en deux catégories : l'hameçonnage et les exploits logiciels.

Hameçonnage

L'hameçonnage est une attaque en ligne lors de laquelle un pirate informatique envoie à une ou plusieurs personnes une communication électronique non sollicitée, comme un courriel, un billet de média social ou un message transmis par messagerie instantanée, qui vise à amener par tromperie le destinataire à révéler des renseignements délicats ou à télécharger un logiciel malveillant.

Dans le cas de l'hameçonnage, le pirate informatique essaie souvent d'imiter une correspondance « officielle » concernant une opération commerciale courante, par exemple, un avis d'expédition ou une facture d'une société de messagerie. Le pirate peut également essayer de faire croire qu'il s'agit d'une « affaire urgente », comme une facture impayée ou un avis de vérification. Des formes plus évoluées d'hameçonnage (appelées « harponnage ») sont destinées à des personnes ou à des établissements précis.

Le rançongiciel peut être installé si le destinataire ouvre un fichier joint ou clique sur un hyperlien dans le corps du message.

Exploits logiciels

Le code de programmation employé pour faire fonctionner les applications et programmes dans votre ordinateur peut présenter des lacunes en matière de sécurité. Les pirates informatiques peuvent exploiter ces lacunes pour installer des logiciels malveillants dans votre ordinateur.

Dans le cas des rançongiciels, les pirates infectent souvent un site Web avec un certain nombre d'exploits (également appelés « trousses d'exploits ») et tentent d'attirer des visiteurs par l'hameçonnage ou l'affichage de fenêtres surgissantes, ou en faisant passer leur site pour un site Web légitime.

Si vous visitez un site Web piraté et si les logiciels de votre ordinateur présentent des lacunes connues des pirates, un rançongiciel pourrait être installé.

PROTÉGEZ VOTRE ORGANISME

En vertu des lois ontariennes sur l'accès à l'information et la protection de la vie privée, les institutions publiques doivent prendre des mesures « raisonnables » pour assurer la sécurité des documents dont elles ont la garde, et les organismes du secteur de la santé doivent faire de même à l'égard des renseignements personnels sur la santé. Pour vous protéger contre les rançongiciels, vous devriez évaluer le risque qu'ils posent pour vos données et prendre des mesures préventives telles que les suivantes :

- **Formation du personnel.** Les employés devraient connaître la menace que représentent les rançongiciels, comment ceux-ci s'installent et comment les prévenir. Par exemple, ils devraient faire preuve de prudence lorsqu'ils ouvrent des pièces jointes ou cliquent sur des liens dans des courriels de l'extérieur qu'ils n'attendaient pas. En cas de doute, ils devraient vérifier si la communication est légitime avant de cliquer.
- **Copies de sécurité.** Vous devriez faire une copie de sécurité des documents électroniques régulièrement. Après utilisation, ces copies devraient être débranchées du réseau et conservées « hors ligne ». Elles devraient aussi être vérifiées de temps à autre pour confirmer qu'il est possible de récupérer les documents. La période de conservation des copies de sécurité devrait également être examinée en tenant compte du fait que les rançongiciels peuvent fonctionner en arrière-plan pendant des jours avant d'être décelés.
- **Logiciel antivirus.** Un logiciel permettant de prévenir, de déceler et d'éliminer les logiciels malveillants devrait être installé et réglé pour effectuer des vérifications en temps réel, en plus des vérifications périodiques.

- **Mise à jour des logiciels.** Tous les logiciels et systèmes d'exploitation devraient être mis à jour régulièrement et toute rustine devrait être installée. Si possible, réglez les mises à jour pour qu'elles se fassent automatiquement.
- **Mise en quarantaine des courriels.** Les courriels de l'extérieur de votre organisme qui contiennent en pièce jointe des fichiers exécutables, des fichiers d'archives ou des fichiers comportant du contenu actif, comme des documents Microsoft Office, devraient être bloqués ou mis en quarantaine. Le destinataire devrait être informé et invité à vérifier si le courriel est légitime avant d'y avoir accès.
- **Limitation des droits d'accès.** Les comptes utilisateurs devraient être assortis uniquement des privilèges et droits d'accès nécessaires pour les tâches professionnelles de chaque utilisateur. Par exemple, si un utilisateur n'a pas besoin d'accéder à certaines unités de réseau ni d'installer des logiciels, cet accès et ce privilège devraient être désactivés dans son cas. L'utilisation de comptes d'administrateurs devrait aussi être strictement limitée.
- **Restriction du contenu actif.** La capacité des utilisateurs d'exécuter du code intégré dans des documents devrait être limitée. Par exemple, les macros des documents Microsoft Office émanant de l'extérieur de votre organisme devraient être bloquées, et les fichiers JavaScript devraient s'ouvrir par défaut au moyen d'un éditeur de texte tel que Notepad.
- **Attaques simulées.** Pour vérifier si vos employés sont sensibilisés à ce problème et évaluer l'efficacité de votre formation, vous pouvez envoyer des attaques simulées d'hameçonnage à vos employés. Vous pourrez vous appuyer sur les résultats de ces simulations pour mieux sécuriser vos données.

RÉAGISSEZ EN CAS D'INCIDENT

Si un ordinateur de votre réseau a été compromis, vous devez agir immédiatement pour atténuer les effets de l'attaque, notamment en prenant les mesures suivantes :

- Débranchez l'ordinateur infecté de tous les réseaux, y compris les réseaux sans fil [Wi-Fi, Bluetooth, communication en champ proche (CCP)].
- Déterminez la gravité de l'infection, et notamment la proportion des fichiers locaux et partagés qui ont été compromis ou chiffrés.
- Tentez d'identifier la souche du rançongiciel et de déterminer s'il existe un outil de déchiffrement.
- Évaluez les possibilités qui s'offrent à vous et déterminez le meilleur moyen de régler le problème. Il est notamment recommandé de réinstaller le système d'exploitation sur l'ordinateur infecté à même une source propre et de récupérer les fichiers à partir des copies de sécurité. Ensuite, vous devriez vérifier l'ordinateur et toutes les ressources touchées pour vous assurer qu'il ne reste aucun signe d'infection.

- Modifiez vos mesures préventives afin de combler les lacunes sur le plan de la sécurité qui ont été mises au jour lors de l'incident.

Les institutions publiques et organismes du secteur de la santé qui ont été victimes d'une infection par rançongiciel devraient s'adresser au Bureau du commissaire à l'information et à la protection de la vie privée pour obtenir des conseils et une orientation. Vous pouvez nous joindre au 1 800 387-0073 ou à info@ipc.on.ca.