*Mai 2017*

# Un guide pour comprendre les maliciels et savoir protéger son entreprise

***Dan Longlade, CPA, CA,*** *est directeur principal à Collins Barrow SNT LLP.*
***Julie Chrétien*** *est coordonnatrice markéting à Collins Barrow SNT LLP.*

Dans l'environnement commercial actuel en perpétuel changement, la mondialisation numérique se déploie agressivement. Le monde étant plus connecté que jamais, c'est l'aube d'une ère nouvelle, celle des flux croissants de données et d'informations. La croissance d'Internet et de l'utilisation des technologies numériques a à la fois transformé et perturbé le monde des affaires. Un univers hyperconnecté a fait naitre de nouvelles brillantes possibilités, mais a également entrainé une croissance de la cybercriminalité.

Selon le Norton 2016 Cyber Security Insights Report (rapport d'indices de sécurité), 689 millions de gens dans 21 pays ont été victimes d'un cybercrime en 2016. D'une année à l'autre, le nombre d'entreprises qui subit des pertes à cause de ce fléau augmente à un rythme alarmant.

Une infrastructure TI robuste est la pierre angulaire de la gestion de la sécurité et la première étape vers la protection de son propre environnement numérique contre le cybercrime. Pour réduire les risques de vulnérabilité et protéger vos ordinateurs et appareils adéquatement, il est important de comprendre les diverses menaces qui existent.

### Maliciel

Amalgame des mots « malicieux » et « logiciel », le maliciel est une forme de logiciel intrusif conçu pour infiltrer votre ordinateur et endommager votre système sans votre consentement. « Maliciel » est un terme générique qui englobe un vaste éventail de menaces incluant les virus informatiques, les logiciels espions, les vers informatiques, les rançongiciels, les chevaux de Troie, les alarmgiciels, les maliciels furtifs et autres programmes malveillants. Pami les divers virus maliciels figurent des logiciels de piratage de navigateurs, comme CryptoLocker, MyDoom, Storm Worm et Slammer.

### Advanced persistent threat (APT)

Une menace persistante avancée (ou APT) constitue une attaque furtive prolongée au moyen de laquelle une personne non autorisée force l'accès à un réseau pour y voler des données. L'APT consiste habituellement en plusieurs attaques distinctes.

### Pourriel

Un message courriel commercial groupé non sollicité qui est envoyé à un vaste nombre de destinataires et qui se résume principalement à de la publicité.

### Hameçonnage

Un courriel envoyé par un pirate déguisé en entité respectable qui, par la ruse, pousse des personnes à divulguer des informations sensibles, comme des mots de passe et des numéros de carte de crédit.

### Harponnage

Un courriel d'usurpation qui cible un individu ou un groupe afin qu'ils révèlent des informations sensibles. Le harponnage consiste en une arnaque par courriel ou par communication électronique qui cible une personne, une organisation ou une entreprise précise. Bien qu'il soit destiné à voler des données pour des raisons malveillantes, les cybercriminels peuvent aussi l'utiliser pour installer des maliciels sur l'ordinateur d'un utilisateur cible.

### L'usurpation

Un courriel avec une fausse identité qui dupe ou leurre votre système ou vous-même. L'usurpation par courriel est la

*Mai 2017*

# Un guide pour comprendre les maliciels et savoir protéger son entreprise

contrefaçon d'un entête de courriel visant à faire croire que le message provient de quelqu'un ou de quelque part d'autre que de la véritable source. Les distributeurs de pourriels utilisent souvent l'usurpation dans l'espoir que les destinataires ouvrent, voire répondent même à leur sollicitation.

**Rançongiciel/cryptage**

Un logiciel malveillant que les cybercriminels utilisent pour séquestrer votre ordinateur ou vos fichiers informatiques en échange d'une rançon; ils exigent un paiement de votre part pour que vous puissiez les récupérer. Malheureusement, les rançongiciels deviennent des outils de plus en plus populaires qui permettent aux auteurs de maliciels d'extorquer l'argent des entreprises autant que des consommateurs. Il y a une variété de rançongiciels qui peut s'insinuer dans l'appareil d'une personne, mais comme toujours, ces techniques se résument soit à des tactiques d'ingénierie sociale ou à l'exploitation des vulnérabilités logicielles pour installer en silence un rançongiciel sur l'appareil d'une victime.

Voici quelques mesures suggérées pour se défendre contre tout type de cybercrime :

1. Investir dans des solutions de sauvegarde et effectuer des restaurations périodiques pour s'assurer que le système fonction de manière optimale
2. Afficher les extensions de fichiers cachés
3. Filtrer les exécutables de vos courriels
4. Désactiver les fichiers fonctionnant depuis les dossiers AppData/LocalAppData
5. Corriger ou mettre à jour son logiciel
6. Utiliser une suite de sécurité reconnue
7. Suspicieux? Déconnectez-vous du Wifi ou débranchez-vous du réseau immédiatement

Afin de prévenir le fait que vous ou votre entreprise fassiez partie des statistiques en matière de cybercriminalité, il est important de développer des stratégies de cybersécurité.

Le fait d'identifier les courriels hostiles peut s'avérer une tâche ardue. Bien que certains messages soient manifestement frauduleux, d'autres peuvent se révéler tellement efficaces et convaincants qu'ils parviennent à déjouer même les utilisateurs les plus expérimentés et versés technologiquement. Pour se protéger contre les menaces par courriel, il est capital d'être suspicieux envers tous les courriels et d'évaluer toutes les pièces jointes ainsi que les hyperliens. La Gendarmerie royale du Canada suggère d'appliquer les dix trucs de prévention du cybercrime suivants :

1. Utiliser un mot de passe solide – combiner des lettres, des nombres et des caractères spéciaux
2. Sécuriser son ordinateur – activer son pare-feu, utiliser des logiciels antivirus
3. Maitriser les médias sociaux – s'assurer que son profil est réglé à privé
4. Sécuriser ses appareils mobiles – télécharger des applications de sources fiables uniquement
8. Installer les dernières mises à jour du système d'exploitation – activer la mise à jour automatique
9. Protéger ses données – utiliser le cryptage
10. Sécuriser son réseau sans fil – réviser et modifier les paramètres par défaut
11. Protéger son identité numérique – activer les paramètres de confidentialité
12. Éviter les arnaques – vérifier la source du courriel

Appeler la bonne personne à l'aide – consulter un technicien informatique certifié pour renforcer ses défenses contre les

*Mai 2017*

# Un guide pour comprendre les maliciels et savoir protéger son entreprise

courriels hostiles et éviter de devenir une cybervictime, suivre la règle : arrêter, observer et réfléchir.

**ARRÊTER**
Confirmer l'identité de l'expéditeur

- Connaissez-vous cette personne?
- Attendez-vous un courriel?

**OBSERVER**
Évaluer l'objet du courriel – observer, mais sans cliquer

- Semble-t-il y avoir une urgence?
- Est-ce qu'on vous demande d'envoyer de l'argent à un ami dans le besoin?
- Est-ce que l'objet est vague?
- Le langage employé est-il menaçant?

**RÉFLÉCHIR**
Se poser des questions

- Pourquoi ai-je reçu ce courriel?
- Cette pièce jointe est-elle valide?
- Est-ce que je connais l'expéditeur?
- Qu'est-ce qu'on me demande (argent, renseignements personnels, confirmations de carte de crédit)?
- Me demande-t-on des renseignements personnels?
- Y a-t-il des fautes d'orthographe ou de grammaire?

**ACTIONS**

- Toujours avoir des copies de sauvegarde sur place et ailleurs
- Effectuer des tests de restauration
- Investir dans les antivirus
- Surplomber les hyperliens afin de confirmer leur itinéraire
- Éduquer tout le monde sur l'identification des cyberattaques
- Maintenir le système d'exploitation de son ordinateur à jour
- Mettre en œuvre des politiques de mot de passe complexe
- Investir du temps pour développer et mettre à jour les politiques Internet et de sécurité
- Dénoncer l'activité informatique suspecte à un professionnel de TI
- Ne jamais transférer de courriel suspect aux autres, même pas au service de TI

Un récent rapport sur les menaces de sécurité Internet réalisé par Symantec a révélé que les attaques de rançongiciels sont en hausse au Canada. Le rapport a classé globalement le Canada au quatrième rang des pays les plus souvent touchés par les rançongiciels et les arnaques par médias sociaux. Environ 1 641 attaques de logiciels de rançon ont touché les Canadiens chaque jour en 2015, d'après le rapport. Puisque les cyberattaques sont plus courantes, le fait d'avoir une infrastructure TI fiable est crucial. Il faut toujours agir avec prudence. Cela pourrait très bien vous sauver, ainsi que votre entreprise, de la faillite.

**Ressources :**

- 2016 Norton Cyber Security Insights Report
- Palmares des 10 meilleurs trucs de prévention du cybercrime de la Gendarmerie royale du Canada
- Rapport de sécurité Internet par Symantec

***Dan Longlade, CPA, CA,*** *est directeur principal à Collins Barrow SNT LLP.* ***Julie Chrétien*** *est coordonnatrice markéting à Collins Barrow SNT LLP.*