Canadians Connected
Canadiens branchés

Fiche-conseils sur la cybersécurité destinée aux consommateurs

Protégez-vous des logiciels malveillants

« Malveillant » est un terme général utilisé pour qualifier des programmes nuisibles qui peuvent endommager votre ordinateur ou tout autre dispositif qui se connecte au Web, notamment les téléphones intelligents, les baladeurs MP3 et les tablettes tactiles.

Que fait le logiciel malveillant?

Il existe plusieurs types de programmes malveillants : les virus, les chevaux de Troie, les vers informatiques et les trousses administrateur pirate. Ils ont en commun la capacité d'exécuter une ou plusieurs des actions suivantes une fois qu'ils ont contaminé votre dispositif numérique :

Endommager votre système. La forme la plus simple de programme malveillant n'a pour but que d'endommager, d'une façon ou d'une autre, votre système. Pour ce faire, il peut réécrire ou écraser des données ou des programmes stockés sur votre disque dur (comme votre carnet d'adresses électroniques) ou exécuter une ou plusieurs copies de lui-même. Ces deux actions réduisent l'efficacité d'exécution de votre ordinateur : premièrement parce qu'il y a moins d'espace disponible sur votre disque dur (et dans certains cas, parce que des fichiers importants ont été modifiés ou supprimés) et deuxièmement, parce que le programme malveillant recourt au processeur de votre dispositif pour s'exécuter.

Changer le fonctionnement de votre système. Un type courant de logiciels malveillants modifie votre navigateur Internet (Internet Explorer, Firefox, Chrome ou Safari) vous laissant voir du contenu Web modifié (notamment des bannières publicitaires différentes), ou bien il change votre page d'accueil, ou encore, il vous dirige vers de faux sites Web dans le but de recueillir vos renseignements personnels

Compromettre l'intégrité de vos renseignements personnels. Certains types de programmes malveillants peuvent lire les données stockées dans votre système, dont vos renseignements financiers ou vos noms d'utilisateur et vos mots de passe, puis les transmettre à leur concepteur. Une autre catégorie de programmes malveillants nommés enregistreurs de frappe enregistrent et transmettent automatiquement tout ce que vous saisissez au clavier.

Utiliser votre système pour se propager. Peu importe la raison pour laquelle ils ont été conçus, la plupart des programmes malveillants visent à se propager à d'autres systèmes. Par

exemple, le virus « ILOVEYOU » envoyait des copies de lui-même aux 50 premiers contacts du carnet d'adresses électroniques du système qu'il avait contaminé.

Prendre les commandes de votre ordinateur. Alors que certains programmes malveillants ont été conçus à la seule fin de plaisanter, d'autres visent à « recruter » des ordinateurs dans un réseau de zombies, soit un groupe de systèmes qui ont tous été infectés par le même programme malveillant utilisé afin d'exécuter des attaques coordonnées sur des sites Web ou de transmettre des pourriels.

La façon dont un logiciel malveillant contamine vos dispositifs

Tout contact entre votre ordinateur ou votre dispositif et un autre système, même dans le cadre d'une activité aussi simple que la visite d'un site Web, peut mener à une contamination par un programme malveillant. Toutefois, voici quelques activités plus risquées que d'autres :

Télécharger des fichiers. Lorsque vous téléchargez des fichiers, vous permettez à un autre ordinateur de sauvegarder quelque chose sur votre disque dur. Plusieurs programmes malveillants en tirent profit en agissant comme imposteur ou en utilisant un fichier légitime pour pénétrer dans votre système par un accès à califourchon. Il est préférable de ne jamais télécharger un fichier à moins d'avoir la certitude de sa légitimité et de celle de sa source.

Ouvrir des pièces jointes aux courriels. Bien qu'ouvrir la pièce jointe d'un courriel semble moins risqué que de télécharger un fichier, ces deux actions le sont tout autant l'une que l'autre. Puisque le logiciel malveillant est souvent conçu de façon à envoyer des copies de lui-même à toutes les adresses électroniques du carnet d'un système contaminé, il ne faut pas tenir pour acquis qu'une pièce jointe est sans danger tout simplement parce que vous en connaissez l'expéditeur. Il ne faut jamais ouvrir une pièce jointe sans que l'expéditeur ait confirmé son intention de vous l'envoyer.

Visiter des sites Web suspects. Se connecter à un site Web au moyen de votre navigateur peut, à cause de scripts (programmes qui envoient des directives à votre navigateur) malveillants, contaminer votre système. Les sites malveillants proposent souvent du contenu gratuit ou d'autres mesures incitatives pour attirer les utilisateurs. Bien que les sites de partage de fichiers, de pornographie et autres sites issus du marché gris soient plus susceptibles d'héberger des scripts malveillants, il faut savoir que même les sites bien établis peuvent être piratés et utilisés pour propager des programmes malveillants. Aussi, évitez les sites dont les offres semblent « trop belles pour être vraies ».

Cliquer sur des liens inconnus. Même si vous ne visitez pas de sites malveillants intentionnellement, cliquer sur le mauvais lien peut vous y conduire. Avant de cliquer sur un lien, laissez-y votre curseur pendant un instant pour vous assurer que l'adresse URL (adresse Web) qui s'affiche y correspond. Les utilisateurs de réseaux sociaux comme Facebook et Twitter ont souvent recours à des raccourcis d'adresse URL tels que Bit.ly. La prudence extrême est toujours de mise si ces liens apparaissent d'eux-mêmes ou si leur contenu semble bizarre. Aussi, quelques programmes (notamment l'extension Verify pour Firefox) permettent de voir l'adresse URL complète.

Utiliser des dispositifs de stockage non sécuritaires. Des dispositifs de stockage, notamment les clés USB, les minidisques durs ou même les lecteurs de musique ou de vidéo numériques, peuvent également contenir des programmes malveillants. Par exemple, en 2008, le système informatique du département de la Défense des États-Unis a été contaminé par un virus stocké sur une clé USB. On ne doit jamais utiliser une clé USB ni tout autre dispositif de stockage provenant d'une source qui n'est pas digne de confiance. Il est préférable, avant d'utiliser tout dispositif de stockage, même ceux que vous venez tout juste d'acheter, de lancer une analyse antivirus à partir d'un ordinateur qui n'est pas connecté à Internet et qui ne contient pas de données sensibles. Vous pouvez également demander au fabricant de votre antivirus si son logiciel prend en charge l'analyse des dispositifs de stockage avant le lancement (des programmes malveillants sur les clés USB peuvent s'exécuter automatiquement aussitôt que vous les branchez à votre ordinateur, et ce, sans vous donner l'occasion de les analyser pour y détecter les virus).

Comment protéger votre système

En plus d'éviter les activités risquées, il existe plusieurs autres façons efficaces de réduire les risques de contamination de votre système :

Mettre à jour le système et le navigateur régulièrement. Les fabricants de logiciels distribuent régulièrement des programmes de correction et des mises à jour pour parer aux plus récents bogues et aux dernières menaces à la sécurité. En mettant régulièrement votre logiciel à jour, vous le protégez des risques connus. Il est particulièrement important de mettre à jour votre navigateur étant donné qu'il sert de passerelle principale entre votre ordinateur et le Web. Vous pouvez établir la fréquence de mise à jour de votre logiciel à partir des paramètres de votre ordinateur (pour Windows, cliquez sur Panneau de configuration, puis sur Centre de sécurité et enfin, sur Mises à jour automatiques. En ce qui concerne les systèmes Mac, cliquez sur le menu Apple, puis sur Mise à jour de logiciels). Également, ne manquez pas de vérifier vos logiciels tiers périodiquement. Bien que ces logiciels soient souvent mis à jour au moyen d'une fonction automatisée établie par défaut, ce n'est pas toujours le cas. En général, pour vérifier si la fonction de mise à jour automatique est activée sur des ordinateurs Mac ou avec système d'exploitation Windows, on doit cliquer sur les menus Aide ou ?, puis sur Préférences ou Propriétés.

Utiliser un logiciel antivirus. Il existe plusieurs programmes, notamment Norton, Symantec, AVG et Avast, spécialement conçus pour détecter, bloquer et supprimer les programmes malveillants. Ce sont des logiciels commerciaux, mais AVG et Avast proposent tous deux des versions gratuites (mais dénuées de certaines fonctions, par exemple le blocage des pourriels et des courriels d'hameçonnage) qui offrent une protection contre la plupart des vers et des programmes malveillants. Pour sa part, Microsoft propose Microsoft Security Essentials, un programme antivirus gratuit destiné aux systèmes Windows.

Installer un pare-feu et activer la fonction de sécurité du routeur. Le pare-feu constitue la défense de première ligne de votre système et son rôle consiste à empêcher les ordinateurs avec lesquels vous entrez en contact de le modifier. Vous trouverez la fonction pare-feu dans le panneau de configuration à partir duquel vous pourrez l'activer. De plus, si vous utilisez un routeur sans fil pour accéder à Internet, vous devez en activer la fonction de sécurité et établir un mot de passe pour le rendre inaccessible à d'autres utilisateurs.

Pour obtenir plus de renseignements :

Veuillez consulter la Fiche-conseils sur la sécurité destinée aux consommateurs de l'Autorité canadienne pour les enregistrements Internet (ACEI) et HabiloMédias est disponible au www.acei.ca et sur le site Web www.habilomedias.ca, même que d'autres ressources favorisant la littératie numérique.

L'ACEI est fière de commanditer Habilo Médias et le travail essentiel dont il s'acquitte au nom de la population canadienne.

Habilo Médias