Introduction

Un constat s'impose : il est devenu impératif de sécuriser son PC car l'usage d'Internet implique de nombreux risques. D'autre part, l'utilisation généralisée des liaisons sans fil ne fait qu'aggraver les problèmes de sécurité liés à l'usage d'Internet.

Force est de constater que de plus en plus d'informations en tout genre sont présentes sur nos PC ou supports de stockage externes (images, vidéos, documents). En cas de perte ou de vol de son PC ou d'un support de stockage externe, les préjudices peuvent être très importants en fonction de la nature des informations.

Il est donc particulièrement important d'identifier les menaces et de savoir protéger efficacement votre PC face à ces dangers.

Quelles sont les menaces ?

Il existe essentiellement deux grands types de menaces liés à Internet : les logiciels malveillants et le piratage. Les deux types de menaces peuvent être liés, un logiciel malveillant pouvant aider au piratage d'un PC. On compte à l'heure actuelle des centaines de milliers de logiciels malveillants, avec des types et des modes de propagation extrêmement variés.

Si votre PC n'est pas connecté à Internet, vous n'êtes pas à l'abri du vol ou de la perte de votre PC (particulièrement si celui-ci est portable) ou d'un support de stockage comme une clé USB.

Nous allons vous présenter les principaux types de logiciels malveillants, puis nous ferons un point sur le piratage.

Les virus

Qu'est-ce qu'un virus ?

Un virus est un programme capable de se propager à d'autres ordinateurs en s'insérant dans des logiciels. Outre le fait de se reproduire, un virus peut effectuer d'autres actions qui peuvent être nuisibles à l'ordinateur infecté ou à d'autres ordinateurs reliés par réseau. La gravité d'une infection est très variable, cela peut aller du simple message à une perte de l'intégralité de vos données.

Les virus constituent cependant une menace de moins en moins importante pour votre PC au profit d'autres formes de programmes malveillants.

Le terme « virus » est souvent mal employé, pour désigner toutes sortes de logiciels malveillants. Ceci vient principalement du fait qu'historiquement les virus ont été les premiers logiciels malveillants. De plus, l'appellation logiciel antivirus, qui ne lutte pas seulement contre les virus, vient renforcer cette confusion.

Comment réduire les risques d'infection ?

- Utilisez un pare-feu efficace.
- Utilisez un logiciel antivirus et mettez les bases à jour très régulièrement.
- Scannez avec un logiciel antivirus tout support inscriptible venant de l'extérieur contenant des programmes (clé USB, cartes mémoire, CD, DVD).
- Évitez d'installer des logiciels de provenance inconnue ou douteuse.
- Téléchargez les logiciels depuis le site des éditeurs plutôt que depuis des sites tiers.

Les vers

Qu'est-ce qu'un ver ?

Un ver est un programme qui se répand le plus souvent par courrier électronique en profitant des failles de sécurité des logiciels de messagerie. Dès qu'un ver a infecté un ordinateur, il tente d'infecter d'autres ordinateurs en s'envoyant lui-même grâce au carnet d'adresses du logiciel de messagerie.

Cette menace est en forte progression car ce logiciel est plus facile à réaliser qu'un virus. Leur vitesse de propagation peut être foudroyante en infectant plusieurs dizaines de milliers d'ordinateurs en quelques heures. D'où l'importance de mettre à jour très régulièrement les bases virales de son antivirus.

Comment réduire les risques d'infection ?

- N'ouvrez pas un e-mail d'un expéditeur inconnu.
- En cas de doute concernant une pièce jointe, scannez-la grâce à un antivirus.
- Évitez de surfer sur des sites web aux contenus douteux.
- Utilisez un pare-feu efficace.
- Utilisez un logiciel antivirus et mettez à jour les bases très régulièrement.
- Installez les mises à jour de sécurité de votre logiciel de messagerie.

Les chevaux de Troie

Qu'est-ce qu'un cheval de Troie ?

Un cheval de Troie est un programme d'apparence anodine (jeu, utilitaire, etc.) qui va effectuer des actions nuisibles sans l'autorisation de l'utilisateur. Un cheval de Troie peut aussi faciliter l'intrusion de pirates informatiques sur votre ordinateur.

Un cheval de Troie n'est pas un virus, car il ne peut pas se reproduire. La capacité de reproduction d'un virus étant l'une de ses caractéristiques essentielles.

Comment réduire les risques d'infection ?

- Évitez d'installer des logiciels de provenance inconnue ou douteuse.
- Scannez avec un logiciel antivirus tout support inscriptible contenant des programmes (clé USB, cartes mémoire, CD, DVD).
- Méfiez-vous des pièces jointes contenant un fichier exécutable.
- Utilisez un pare-feu efficace.
- Utilisez un logiciel antivirus et mettez à jour les bases très régulièrement.

Les logiciels espions

Qu'est-ce qu'un logiciel espion ?

Un logiciel espion est un programme inclus dans un autre programme s'installant à l'insu de l'utilisateur. Il collecte des informations ensuite transférées à une personne tierce.

Il existe deux grandes catégories de logiciels espions :

Les enregistreurs de touches

Les enregistreurs de touches stockent dans un fichier toutes les touches que vous avez frappées sur le clavier. Le fichier est ensuite envoyé à une personne malveillante qui a installé le dispositif.

Les logiciels publicitaires ou Adware

Cette famille n'est généralement pas très agressive. Les objectifs sont multiples et variés :

- Modification de la page de démarrage de votre navigateur.
- Installation d'un module de recherche sur votre navigateur.
- Redirection sur un site web.

- Fenêtres publicitaires.
- Vol des informations concernant votre vie privée (comme par exemple les sites que vous visitez le plus souvent ou les mots-clés de recherche que vous utilisez).

Comment se protéger ?

Il est difficile de se protéger des logiciels espions, car tout programme installé peut potentiellement embarquer ce type de programme.

Le seul moyen de se protéger efficacement est d'installer un logiciel spécialisé dans la protection contre les logiciels espions. À l'heure actuelle, aucune solution ne peut vous garantir une protection à 100 % contre ce type de menace.

L'hameçonnage

Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une technique de piratage où le cyberdélinquant usurpe l'identité d'une institution financière ou d'un site de renom pour obtenir des informations confidentielles. Les attaques par hameçonnage sont réalisées par le biais d'e-mails ou de sites web malveillants destinés à soutirer au destinataire des renseignements, le plus souvent d'ordre financier (numéro de carte bancaire, code confidentiel de carte bleue, codes confidentiels de sites de paiement en ligne).

Comment réduire les risques d'hameçonnage ?

- Ne répondez pas aux e-mails non sollicités.
- Ne révélez à personne vos mots de passe.
- Ne donnez aucune information sensible sans avoir vérifié l'identité du demandeur par exemple par téléphone ou par courrier.
- Vérifiez la sécurité du site web avant d'envoyer des informations sensibles sur Internet.
- Utilisez WOT pour vous prémunir des sites web à risque (cf. Pour une meilleure sécurité, un peu plus loin dans ce chapitre).

Le piratage

Le piratage informatique prend plusieurs formes :

- La copie illégale de logiciel ou le fait de supprimer les protections contre la copie.
- L'intrusion sur un PC ou un ensemble de PC distants.
- L'usurpation d'une connexion internet le plus souvent sans fil.

Nous allons nous intéresser plus particulièrement aux deux dernières formes.

Les risques d'intrusion sur le PC d'un particulier sont faibles car les principales motivations des cyberdélinquants sont :

- le défi technique ou intellectuel,
- l'appât du gain en récupérant des informations facilement monnayables (numéro de carte bancaire, informations confidentielles…).

Le plus souvent, le pirate va utiliser des failles de sécurité logicielles ou matérielles, voire s'appuyer sur un cheval de Troie pour prendre le contrôle du PC.

L'intrusion sur le PC d'un particulier ne répond pas à ces motivations. Par contre, les entreprises sont particulièrement exposées à ce type de menace.

L'usurpation d'une connexion internet est fréquente. Les particuliers sont beaucoup plus touchés que les entreprises du fait de leur méconnaissance en matière de sécurité des réseaux sans fil.

Les premiers réflexes

Sur le marché français, la plupart des fournisseurs d'accès internet vous fournissent une box (Livebox, Freebox, SFR box, etc.). Ces boîtiers contiennent un routeur, un pare-feu et un modem. Le pare-feu permet d'ouvrir ou de fermer des ports qui sont autant de points d'entrée pour les virus, logiciels malveillants ou pirates. La box effectue aussi une traduction d'adresses entre votre réseau et le réseau internet, afin de "masquer" les machines de votre réseau. Ceci est une très bonne chose, car elles permettent de se protéger d'un très grand nombre d'infections et d'intrusions.

Le routeur, quant à lui, s'occupe de diriger les échanges entre vos ordinateurs et Internet. Tout ordinateur supplémentaire connecté à votre box pourra ainsi accéder à Internet.

Toutes les versions de Windows offrent un pare-feu qui constitue un second "rideau" de protection.

Il reste néanmoins des failles majeures :

- Le pare-feu intégré dans la box n'assure pas forcément un niveau de sécurité optimal.
- Le pare-feu de Windows offre un niveau de sécurité parfois faible lié à des failles de sécurité.

- La configuration par défaut du système de sécurité pour les connexions sans fil (Wi-Fi) présente en général un niveau de protection insuffisant, rendant l'usurpation de la connexion facile.
- Le système d'exploitation Windows est connu pour ses nombreuses failles de sécurité.

Il convient donc, dans un premier temps, d'évaluer l'efficacité du pare-feu.

Évaluer l'efficacité du pare-feu

Je vous propose d'évaluer l'efficacité de votre pare-feu en vous rendant sur un site internet permettant de tester la sécurité de votre PC à l'adresse suivante : http://www.zebulon.fr/outils/scanports/test-securite.php

Attention : ce test n'est pas suffisant pour évaluer l'efficacité d'un pare-feu dans le cadre d'une entreprise.

- Cette page apparaît puis cliquez sur **Testez la sécurité de votre PC**.