les "malwares" : typologie

Principaux types de programmes malveillants

Il existe des dizaines de milliers de programmes malveillants et de nouveaux sont créés chaque jour.

Le terme "virus" ne représente qu'une partie des menaces : le générique "malware" (programme malveillant), contraction de l'expression anglophone *malicious software*, convient mieux.

Il désigne tout **programme ou logiciel spécifiquement conçu ou modifié à des fins malhonnêtes ou frauduleuses**.

Voici un aperçu de la diversité de ces menaces :

Cheval de Troie

Désigne un programme exécutable qui ne se multiplie pas, mais recourt à des systèmes pour effectuer des opérations malveillantes telles que l'ouverture des ports aux pirates. Sous prétexte d'éradiquer des virus sur votre ordinateur, les chevaux de Troie sont des applications qui y introduisent de nouveaux virus. Les solutions antivirus conventionnelles peuvent détecter et supprimer les virus, mais pas forcément les chevaux de Troie, notamment ceux qui ont déjà pénétré votre système.

Virus

Les virus informatiques sont de petits programmes logiciels conçus pour se propager d'un ordinateur à l'autre et en perturber le fonctionnement.
Un virus peut corrompre ou supprimer des données de votre ordinateur, utiliser votre programme de messagerie pour se propager à d'autres ordinateurs ou même effacer tout le contenu de votre disque dur.
Les virus se propagent principalement par les pièces jointes à des courriers électroniques ou par les messages instantanés. C'est pourquoi il est essentiel de ne jamais ouvrir les pièces jointes aux courriers électroniques si vous ne connaissez pas l'expéditeur et si l'envoi n'était pas prévu.
Les virus peuvent prendre la forme de pièces jointes, comme des images amusantes, cartes de vœux ou fichiers audio et vidéo.
Ils peuvent également se propager par le téléchargement de fichiers sur Internet. Ils peuvent être dissimulés dans des logiciels illicites et autres fichiers et programmes que vous téléchargez.

Ver

Un ver informatique est un logiciel conçu pour se copier lui-même depuis un ordinateur vers un autre ordinateur sans interaction humaine. Contrairement à un virus informatique, un ver peut se copier lui -même automatiquement.
Les vers peuvent se dupliquer pour atteindre un nombre considérable. Par exemple, un ver peut envoyer des copies de lui-même à chaque contact de votre carnet d'adresses, pour ensuite envoyer d'autres copies aux contacts de vos contacts, et ainsi de suite.
Certains vers se propagent très rapidement. Ils encombrent les réseaux et peuvent vous faire perdre beaucoup de temps, ainsi qu'à l'ensemble des internautes, lors de l'affichage de pages Web.

Logiciel espion

Un "logiciel espion" ou "spyware"désigne communément un logiciel réalisant, le plus souvent sans obtention de votre accord préalable, des actions telles que :

- Affichage de publicités
- Recueil d'informations personnelles
- Modification de la configuration de votre ordinateur

Cela ne signifie pas que tous les logiciels générant des publicités ou suivant vos activités en ligne sont malveillants. Par exemple, vous pouvez vous abonner à un service de musique gratuit, mais « payer » ce service en acceptant de recevoir des publicités ciblées. Si vous comprenez et acceptez les termes de cet accord, vous avez peut-être considéré que c'est un compromis équitable. Vous pouvez également accepter que cette société suive vos activités en ligne afin de vous envoyer des publicités appropriées.
Ces programmes ont la capacité de modifier la page d'accueil ou la page de recherche de votre navigateur ou d'ajouter à votre navigateur des composants supplémentaires indésirables ou superflus. Ces programmes compliquent aussi sensiblement la restauration de vos paramètres d'origine.
Le plus important dans tous les cas est de savoir si vous (ou la personne qui utilise votre ordinateur) comprenez ou non ce que va faire ce logiciel et si vous acceptez qu'il soit installé sur votre ordinateur.

Faux logiciels de sécurité

Également connus sous le nom de "scareware". Généralement présentés comme antivirus / anti espions, ils s'affichent comme des opérations positives du point de vue de la sécurité (en proposant le nettoyage de votre poste, celui-ci étant systématiquement "très infecté"). Malheureusement, ils ne fournissent qu'une sécurité limitée voire inexistante, génèrent des alertes erronées ou trompeuses ou tentent de leurrer les utilisateurs en les faisant participer à des transactions frauduleuses.

M.A.J. le 14/02/2018

Dans cette rubrique

- Conditions d'utilisation
- Documentations

Généralités

Les "malwares"
Les vecteurs d'infection / la protection
Le pare-feu
Liens utiles

Procédures

Conditions d'utilisation
Acquisition / installation
Assistance / contacts
En cas d'infection...

Postes personnels : TrendMicro Internet Security

Modalités d'acquisition de licence

Rectorat de Nantes
4, rue de la Houssinière
BP 72616 - 44326 Nantes CEDEX 03
Tél. 02 40 37 37 37