PROTEGER SON ORDINATEUR

Définition d'un virus

Le virus est un programme informatique capable d'infecter d'autres programmes en les modifiant afin d'y intégrer une copie de lui-même qui pourra avoir légèrement évolué. A la manière de son frère biologique, il se reproduit rapidement à l'intérieur de l'environnement infecté à l'insu de l'utilisateur.

Indépendamment de sa fonction reproductive, le virus contient généralement une charge qui peut causer des dégâts insignifiants ou redoutables.

Cependant un virus, aussi bien conçu soit-il, ne peut se propager sans votre aide. En effet un programme infecté doit être exécuté pour que le virus soit actif. Tant qu'on n'y touche pas, le programme infecté est inoffensif. Cependant, certains programmes, sont parfois paramétrés pour effectuer automatiquement des actions potentiellement dangereuses sans véritable intervention de l'utilisateur. Ainsi, l'ouverture automatique d'un e-mail dans le volet de visualisation peut tout à fait ouvrir un fichier infecté si votre application n'a pas été patchée contre cette faille.

En matière de sécurité informatique, l'ignorance est votre pire ennemie !

Il existe d'autres programmes potentiellement dangereux que l'on confond assez souvent avec les virus : il s'agit des chevaux de Troie, des vers et des bombes logiques. La différence réside dans le fait que ces programmes ne possèdent pas la capacité de se multiplier sur le système infecté.

Définition d'un ver

Le ver est un programme capable de fonctionner de manière indépendante. Il peut propager une version fonctionnelle et complète de lui-même vers d'autres machines.
Contrairement au virus, le vers n'a pas besoin d'infecter et de parasiter un programme ou un support physique et il est incapable de se reproduire sur le système infecté. Il n'existe donc sur celui-ci qu'une seule copie du ver. Aujourd'hui, le ver est considéré comme un sous-ensemble de la famille des virus.
Les vers récupèrent l'ensemble des adresses de courriers contenues dans le carnet d'adresses et les fichiers internet temporaires pour s'auto distribuer aux correspondants, ce qui garantit une diffusion massive.

Définition d'un cheval de Troie

On les appelle souvent des Troyens ou Trojans, mais c'est une mauvaise transposition du terme anglais. Les chevaux de Troie sont des programmes simples. Tout comme les vers, ils sont incapables de se reproduire sur le système infecté : l'utilisateur d'un système infecté n'a donc en général qu'une seule copie à trouver et détruire pour s'en débarrasser. Ils sont également incapables de se propager par eux-mêmes. Tapis entre les lignes de code d'un programme, ils attendent que vous double-cliquiez sur l'icône du programme qui les héberge pour devenir les maîtres de votre PC.
Les chevaux de Troie ou Trojans se nichent ainsi à l'intérieur de programmes gratuits ou commerciaux qui semblent anodins aux yeux de l'utilisateur : patchs ou mises à jour, utilitaires, logiciels de jeux, écrans de veille etc.
L'action la plus pernicieuse reste la prise de contrôle à distance de l'ordinateur. En effet, un cheval de Troie peut ouvrir un port de l'ordinateur à la communication ou profiter d'une faille de sécurité sans que l'utilisateur s'en aperçoive. Une fois installé, le Trojan agit comme l'élément serveur d'un logiciel de prise en main à distance classique.

Définition d'une bombe logique

Les bombes logiques présentent des caractéristiques similaires aux chevaux de Troie (incapacité de se reproduire et de se propager). Mais à la différence de ceux-ci qui sont immédiatement opérationnels au lancement du logiciel hôte, les bombes logiques sont programmées pour s'activer quand survient un événement précis (comme les bombes traditionnelles). Cet évènement, déterminé par le programmeur malveillant, peut être une date particulière, une combinaison de touches, une action spécifique ou un ensemble de conditions précises. De manière générale, à l'instar des bombes réelles, les bombes logiques visent à faire le plus de dégâts possible sur le système en un minimum de temps.
Ainsi la fameuse bombe logique Tchernobyl s'est activée le 26 avril 1999, jour du 13ème anniversaire de la catastrophe nucléaire en reformatant le disque dur des malheureux utilisateurs qui étaient infectés...

PROTEGER SON ORDINATEUR

Définition d'un spyware

Logiciels espions qui s'installent sur l'ordinateur à l'insu de l'utilisateur, soit à partir d'une page Web infectée, soit à partir d'un programme. Ils ne détériorent pas les fichiers du disque dur, mais peuvent voler des données confidentielles.

Définition d'un dialer

Littéralement, un dialer signifie "composeur de numéro". C'est un programme qui sert tout simplement à composer des numéros, le plus souvent des numéros de téléphone. Pour vous connecter à internet, vous devez avoir recours à un dialer afin de composer le numéro de votre fournisseur d'accès internet, celui-ci est sans aucun danger, il est même indispensable. Certaines personnes et obscures sociétés peu scrupuleuses ont imaginé d'utiliser des dialers afin de s'enrichir à vos dépens.

Définition d'un hijacker

Un hijacker modifie les réglages de votre navigateur par l'intermédiaire d'une page web piégée par un contrôle ActiveX ou un JavaScript par exemple. C'est, entre autres, parce qu'il est le plus populaire (et aussi le plus vulnérable aux failles de sécurité) que Internet Explorer est le plus souvent victime de hijackers. Des navigateurs comme Firefox sont très rarement hijackés. Plus concrètement, si lors de votre navigation vous tombez sur une telle page, les effets peuvent être variés : modification de votre page de démarrage, de votre page de recherche, de votre liste de favoris...
Le but recherché est de vous forcer à passer par certains sites. Des webmasters peu scrupuleux ont recours à ce genre de procédés pour gonfler le nombre de visites sur leur site afin de vendre des espaces de publicité plus cher sur leurs pages.

Définition du phishing

L'hameçonnage (ou filoutage), appelé en anglais phishing, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.