

Les adwares

Les adwares, d'advertising (publicité en anglais), cousins des spywares, sont centrés sur l'affichage publicitaire. Ils constituent d'ailleurs la souche originelle de ces parasites.

Ces logiciels souvent inoffensifs vont principalement soit vous bombarder de bandeaux de publicité spécifiques soit vous inonder de pop-up.

Les malwares

Les malwares, contraction de " malicious software " sont des programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un ordinateur. Les malwares sont à la navigation Web ce que sont virus ou vers pour le mail et Internet. Mais ces malwares peuvent aussi être constitués de javascripts ou applets java hostiles. Contrairement aux spywares et adwares, les malwares ont clairement pour objectif de nuire à l'intégrité d'un système.

C'est pour cela que les antivirus détectent et éliminent une grande partie des malwares sans toutefois pouvoir jamais atteindre 100% d'efficacité : il reste donc indispensable de n'exécuter un programme ou un fichier joint que si sa sûreté est établie avec certitude, le doute profitant toujours aux malwares.

Les malwares sont les principaux responsables des comportements anormaux d'Internet Explorer. Certains malwares utilisent des techniques très évoluées et se révèlent très difficiles à éradiquer

Les spywares

(ou espioniciels) sont par définition des logiciels intrusifs. Tellement intrusifs qu'un grand nombre d'utilisateurs en hébergent depuis plusieurs mois sans même s'en rendre compte. Le problème provient du fait que de nombreux spywares sont inclus et installés avec des logiciels dits adwares utilisant un mode de diffusion très répandu car très rentable.

Votre système en contient peut-être quelques uns, d'ailleurs, à moins que vous n'ayez jamais surfé... ni jamais installé de logiciels gratuits de partage de fichier (peer to peer),... d'accélérateur de téléchargement,... d'enregistreurs de mots de passes. Actuellement, les fichiers les plus téléchargés sur les sites spécialisés sont des adwares pour la plupart.

Un adware est un programme pouvant paraître gratuit mais qui est en fait supporté par la publicité ou des services tiers. Son concepteur ou éditeur touche une rétribution qui varie selon le nombre d'installations. Une gratuité toute fictive pour l'utilisateur car il paye "en nature" alors qu'il existe toujours des équivalents libres ou simplement épurés de leurs fonctions douteuses.

Les spywares peuvent effectuer des modifications sur votre système, se charger au démarrage, récupérer toutes sortes de données vous concernant, établir et enregistrer des statistiques sur vos transferts de fichiers ou les sites que vous visitez. Ces données servent à alimenter des bases de données d'entreprises marketing ou publicitaires, d'établir des profils ou tout simplement de vous fichier.

Souvent installés à votre insu, ils savent se montrer discret sur la machine qu'ils parasitent, et dont ils utilisent la connexion et les ressources, pouvant même en perturber ou ralentir les performances.

Les spywares peuvent avoir différentes missions :

- collecter des informations sur vos habitudes de surf.
- voir quelle utilisation vous faites de votre ordinateur.

- vous cibler géographiquement....
- récupérer vos données personnelles et tout ce que vous frappez sur votre clavier (par l'intermédiaire d'un petit logiciel installé à votre insu appelé KEYLOGGER.
- encoder vos données personnelles, ne vous permettant plus l'accès à celles ci.
- installer un "dialer", un programme qui coupe la connexion établie et tente de joindre un numéro d'appel surtaxé vers des sites pornographiques (ou d'autres contenus). Ils peuvent être installés par mégarde en cliquant simplement sur OK dans une d'une fenêtre Javascript d'Internet Explorer (en utilisant ActiveX)etc ... etc

Cheval de Troie

En anglais : Trojan horse. Un cheval de Troie (Trojan horse) est un programme malicieux qui ne peut pas se reproduire lui-même; il doit être installé volontairement par l'utilisateur, souvent par accident. Parmi les techniques de propagation de virus informatiques, le cheval de Troie est la plus utilisée par les créateurs de virus. Comme son nom le laisse entendre, elle consiste à placer le programme infecté à l'intérieur d'un autre programme ou d'un document dont une partie est exécutable (script d'un document HTML, par exemple). Mais son exécution, ou son ouverture, entraîne l'activation du virus, qui infecte de façon plus ou moins nuisible le système de l'utilisateur et se propage à d'autres ordinateurs.

Backdoor

Un "backdoor" est un type particulier de Trojan qui permet à un attaquant de contrôler l'ordinateur de sa victime à distance

Virus

Petit logiciel parasite créé par jeu (dangereux) ou dans un but de sabotage.

Se transmettant par disquette ou par Internet, les virus sont de petits programmes qui infectent d'autres programmes et fichiers informatiques. Indétectable par l'utilisateur tant qu'il n'a pas produit son effet (mais pouvant être repéré par un logiciel antivirus), le virus peut être relativement inoffensif (affichage d'un message, par exemple) ou très nocif (destruction de données, pannes, etc.).

Ver

Un ver est un virus qui à la particularité de se reproduire par réseau.

Hacker

Passionné d'informatique ayant un goût prononcé pour le déchiffrement de code de bas niveau et la confection rapide de petits programmes

Ce terme anglais est dérivé du verbe to hack, qui signifie hacher, couper avec vigueur. On parle alors de hackers malveillants, pour ne pas confondre dans un même opprobre quelques individus mal intentionnés et une énorme majorité de passionnés ne pensant pas à mal. Enfin, notons que les crackers (ou "craqueurs") sont un sous-ensemble de hackers se consacrant plus particulièrement à l'étude et à la neutralisation des systèmes de protection contre la copie de certains logiciels

Keylogger

Les keyloggers (de l'anglais Keystroke Logger, enregistreur de frappes de touches) sont des petits programmes espions qui enregistrent toutes les frappes sur les touches d'un clavier relié à un ordinateur infecté. Régulièrement, le keylogger envoie les informations ainsi collectées au pirate. Les keyloggers les plus sophistiqués ne se contentent pas d'enregistrer les frappes sur le clavier mais effectuent également des captures d'écran.

Des logiciels espions dits de surveillance sont également conçus. Ceux-ci ont pour but d'utiliser tous les équipements mis à leur disposition sur l'ordinateur de la victime tels que :

- Webcam – capture vidéo de l'environnement autour de l'ordinateur,
- Microphone – capture audio de l'environnement et des communications autour de l'ordinateur,
- Captures d'écran – capture d'images de l'activité de l'ordinateur
- Capture d'informations diverses – mots de passes, identifiants de connexions,

pour stocker puis transmettre ces informations à des tiers.

Tracking cookies

Les tracking cookies sont à la base des cookies, rien de plus normal sur Internet, mais, à la différence des cookies classiques qui sont eux dédiés et accessibles au seul site Internet qui les a transmis, les tracking cookies sont accessibles à plusieurs sites Internet ce qui a pour effet de permettre aux sites associés à ces tracking cookies de tracer l'activité de l'utilisateur sur Internet, les sites visités et les actions faites sur chacun des sites visités.

En soi, les tracking cookies ne constituent pas un risque pour le système informatique sur lequel ils sont implantés mais peuvent constituer une forte atteinte à la vie privée des internautes.

Les sociétés qui exploitent les tracking cookies ont le plus souvent pignon sur rue et sont souvent des régies publicitaires.

Dialer

Un dialer est un tout petit programme, généralement installé sans aucune action de la part de la future victime. Une fois installé, le dialer déconnecte la connexion active pour se reconnecter automatiquement, généralement par un numéro surtaxé, à autre provider pour proposer un accès proposant d'autres types de contenus (jeux, mp3, cracks, sexe...)

En général la re-connexion via dialer est invisible aux yeux des internautes.

Il est à noter que les dialers agissent par des lignes téléphoniques du réseau commuté (via un modem RTC) et n'ont pas d'impact sur les lignes DSL en l'absence de modem RTC connecté.