Se protéger Lutter contre les espiogiciels

Votre ordinateur a un comportement anormal : des fenêtres publicitaires s'ouvrent à tort et à travers lorsque vous surfez sur Internet, l'adresse de votre page de démarrage a changé sans votre accord… Cela signifie que vous avez été infecté par un espiogiciel. Rien de grave, à condition de vous en débarrasser.

« A l'insu de votre plein gré »

Un espiogiciel, plus connu sous son nom anglais de *spyware*, est un programme chargé de recueillir des informations sur l'utilisateur de la machine sur lequel il est installé. Son but est de récolter et de transmettre ces informations, c'est pourquoi on l'appelle parfois mouchard.

En général, un espiogiciel s'installe en même temps qu'un autre logiciel, le plus souvent des gratuiciels (freewares) ou des partagiciels (sharewares). Ainsi, l'auteur rentabilise son programme grâce à la vente d'informations statistiques. On peut donc parler d'un véritable modèle économique où la gratuité du logiciel est obtenue contre la cession de données personnelles. D'autant que les espiogiciels ne sont pas illégaux. Souvent, la licence d'utilisation qui accompagne le logiciel précise qu'un tel programme va être installé. Mais qui lit une licence d'utilisation en entier ? Si vous faites encore cet effort, méfiez-vous des formules du type «peut contenir un logiciel vous avertissant occasionnellement d'informations importantes», en anglais «*may include software that will occasionally notify you of important news*».

Savoir +

Ce que l'espiogiciel peut savoir

Un espiogiciel peut savoir :

- **les sites internet que vous visitez**
- **les mots-clés que vous saisissez dans les moteurs de recherche**
- **les achats que vous réalisez sur Internet**
- **les informations de paiement bancaire (numéro de CB, Visa…) pour les plus sournois**
- **et d'une manière générale, tout ce qu'il y a dans votre machine**

Se Lutter contre les espiogiciels protéger

Comme pour les virus, quelques **précautions** simples permettent de les éviter. Et même en cas d'infection, la situation n'est pas dramatique. Des programmes spécialisés les éliminent, comme le font les antivirus avec les codes malicieux.

Comme tout bon espion, le *spyware* est difficile à détecter. La meilleure façon de **s'en protéger**, c'est encore de ne pas installer de logiciels dont la provenance n'est pas sûre. En particulier, les gratuiciels, les partagiciels et les logiciels d'échange de fichiers de pair à pair. D'autant plus que la désinstallation d'un logiciel ne supprime que rarement l'espiogiciel qui l'accompagne.

Si la première parade consiste à ne pas installer n'importe quoi, a fortiori si vous êtes un adepte des logiciels de pair à pair ou des sites peu recommandables, elle ne suffit pas pour assurer une protection sans faille.

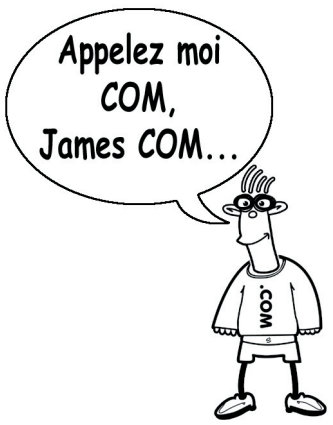
Savoir +

Comment l'espiogiciel nuit à votre machine ?

Outre le désagrément causé par le fait de se savoir épié, les espiogiciels nuisent aussi à l'ordinateur :

. en consommant de la mémoire vive
. en utilisant de l'espace disque
. en sollicitant le processeur
. en empêchant le fonctionnement normal de certaines applications(plantage machine systématique)
. en ouvrant des écrans publicitaires ciblés en fonction de l'information collectée lorsque vous surfez sur Internet
. en utilisant de la bande passante

Il faut la **combiner à une autre méthode** qui consiste à mettre à jour votre navigateur et à éviter l'exécution de scripts Active X avec Internet Explorer. Par défaut, celui-ci est paramétré pour ne les exécuter qu'après confirmation. Pour le vérifier, cliquez sur le menu Outils/Options d'Internet Explorer. Dans l'onglet Sécurité de la fenêtre Options Internet, vérifiez que le niveau de sécurité Moyen est associé à la zone sécurité Internet. Seuls les contrôles Active X dotés d'un certificat s'exécutent automatiquement. Ce qui devrait vous éviter un certain nombre de désagréments. Si vous utilisez le navigateur Firefox, notez que le succès aidant, il risque de devenir la prochaine cible des *spywares*.



Se protéger Lutter contre les espiogiciels

Pour vous débarrasser des espogiciels, il faut utiliser un **antispyware**. Les trois plus connus sont :

Spybot Search & Destroy que vous pouvez télécharger gratuitement :
http://www.spybot.info/fr/mirrors/index.html

Ad-Aware que vous pouvez télécharger gratuitement :
http://lavasoft.element5.com/default.shtml.fr

http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10045910.html?part=dl-ad-aware&subj=dl&tag=top5

Microsoft Antispyware que vous téléchargez gratuitement en version béta :
http://www.zdnet.fr/telecharger/windows/fiche/0,39021313,39105760s,00.htm

Selon les journaux et les sites spécialisés, ce sont les trois meilleurs gratuiciels pour lutter contre les espiogiciels. Néanmoins, ces outils ont un inconvénient majeur : chaque logiciel ne reconnaît pas les mêmes spywares. Ainsi, un espiogiciel détecté par un programme ne l'est pas forcément par un autre. Une bonne solution consiste à les combiner. Comme pour les antivirus, une mise à jour régulière est nécessaire pour qu'il reste efficace.

Pour **neutraliser** les logiciels espions, vous pouvez aussi installer un pare-feu qui les empêchera de se connecter à Internet et de transmettre les informations collectées sur votre machine. Le *spyware* sera toujours installé sur votre machine, mais son action sera enrayée.

Rassurez-vous, si un *spyware* peut être très nuisible, il suffit généralement d'une dizaine de minutes pour l'éradiquer ou, au moins, le neutraliser.

Savoir +

Le publiciel, un espiogiciel spécialisé

Peu virulent, mais très fréquent, le publiciel est un espiogiciel qui affiche des publicités ciblées, sous la forme de bannières ou de fenêtres «pop-up». En fonction des informations récupérées sur votre ordinateur (sites visités, achats effectués en ligne…), ils affichent la réclame censée vous intéresser. Ils effectuent donc un véritable profil de l'utilisateur. La conséquence principale d'une telle infection est la gêne occasionnée : les pages sont plus longues à télécharger et vous ne pouvez plus surfer sans être renvoyé vers des «pop-up» publicitaires. En anglais, on le nomme adware, contraction des mots adversiting (publicité) et software (logiciel).

Les plus perfides

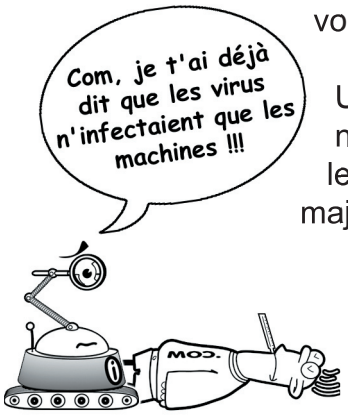
Il existe d'autres spécialistes de l'espionnage. Les internautes qui utilisent une connexion bas débit via une ligne téléphonique classique doivent se méfier plus particulièrement des composeurs (*dialers* dans la langue de Shakespeare) qui appellent – à l'insu de l'utilisateur – un numéro surtaxé. Méfiez-vous aussi des *keyloggers* qui peuvent transmettre à un tiers toutes les frappes clavier, votre numéro de carte de crédit par exemple.

Se protéger « Lutter contre les virus informatiques »

Vous avez un accès à Internet, vous utilisez le courrier électronique ou les disquettes de votre petit frère, alors vous avez forcément été confronté à un virus, peut-être même sans vous en apercevoir. Rassurez-vous, on s'en débarrasse plus facilement que de la grippe.

Détecter les virus

Se faire infecter par un virus n'est pas catastrophique, même s'ils peuvent perturber sérieusement le fonctionnement normal de votre ordinateur (messages incongrus, exécution de tâches non sollicitées, perturbation du système et des logiciels installés, pertes de données…) voire l'endommager physiquement en s'attaquant à votre disque dur. Pour vous contaminer, les virus utilisent les moyens de communication des données : le courrier électronique, les disquettes et les CD, mais aussi le téléchargement. En fait, dès que vous copiez des données sur votre disque dur, vous prenez un risque. Sauf si vous les contrôlez à l'aide d'un antivirus.



Une fois enregistrés sur votre disque dur, la majorité des virus ne deviennent nuisibles que si vous lancez le programme ou si vous ouvrez le fichier dans lequel ils résident. Installer un antivirus permet de les détecter et, dans la majorité des cas, de les éradiquer sans effort.

Se protéger
Lutter contre les virus informatiques

Eliminer les virus

Un antivirus ne peut pas détruire un programme malicieux qu'il n'est pas capable d'identifier, comme si vous aviez été immunisé contre la grippe et qu'une souche plus virulente apparaissait : le vaccin serait alors inefficace. Une piqûre de rappel s'impose. En informatique, une visite mensuelle sur le site de l'éditeur pour mettre à jour votre antivirus augmentera son efficacité : il reconnaîtra tous les virus apparus depuis la dernière mise à jour. Dans le pire des cas, vous devrez patienter quelques jours, le temps que des ingénieurs trouvent un antidote. Malheureusement, ce n'est pas aussi simple en médecine…

Que faire si vous êtes infecté par un virus ?

Il faut :

- Eviter d'utiliser votre ordinateur. Ne plus poster de messages, ne plus vous connecter à d'autres machines, ne plus enregistrer de disquettes ni de CD…
- Prévenir les personnes que vous auriez pu contaminer depuis une autre machine ou par téléphone.
- Tenter d'identifier la source d'origine du virus (nouvelle disquette, derniers messages…), tout en sachant qu'il existe des virus dormants, programmés pour se déclarer à une date définie.
- Si le virus est nouveau, consulter les sites spécialisés, notamment celui de Microsoft puisque la plupart des virus portent leurs attaques sur ses produits les plus utilisés (Outlook, Internet Explorer). *A contrario*, les utilisateurs de Mac, de logiciels libres sont moins exposés aux contaminations. N'hésitez pas à demander à une personne plus compétente si vous ne vous en sortez pas.

On trouve deux types d'antivirus : les payants, disponibles sous licences commerciales et les gratuits, la plupart du temps réservés à une utilisation privée et non commerciale. Pour une version propriétaire, comptez moins de 60 euros, avec des mises à jour gratuites durant la première année. Ensuite, vous devrez vous acquitter annuellement d'un droit d'abonnement pour bénéficier de ce service (moins de 10 euros).
Parmi les antivirus qui ont la confiance des internautes, on peut citer les logiciels gratuits tels que avast ! Virus Cleaner, BitDefender Free Edition, Clean Sasser (créé spécialement pour exterminer le virus Sasser), AVG Free Edition…

Se protéger
Lutter contre les virus informatiques

Les fichiers dont il faut se méfier

Si jamais vous recevez un courriel d'une de vos connaissances et que le message est rédigé en anglais, langue de prédilection des propagateurs de virus, **méfiez-vous** ! Enregistrez ce fichier sur le disque dur sans l'ouvrir. Et si l'extension du fichier est contenu dans cette liste, vérifiez-le avec un antivirus à jour.

.mdb .mde .bat .pif .com .xls .xlt .js
.ppt .pps .vbs .exe .scr .doc .dot .reg

Rappelez-vous aussi que les virus sont rusés et que pour vous tromper, certains fichiers arrivent avec des extensions doubles. Par exemple, achillezavatta.jpg.bat vous apparaîtra sous la forme achillezavatta.jpg sous Outlook si Windows est paramétré pour cacher les extensions. Ce n'est pas une image au format .jpg, mais bien un programme malicieux.

Soyez aussi prudent si vous recevez ou téléchargez des données incluses dans des fichiers compressés (zip…).

Savoir +

Le ver, un membre éminent de la famille des virus

Le ver est un programme capable de s'auto-reproduire et de se déplacer à travers un réseau. Il peut propager une version fonctionnelle et complète de lui-même vers d'autres ordinateurs. Il fonctionne de manière indépendante et n'a pas besoin d'un support physique ou logique (disque dur, programme hôte, fichier joint...) pour se diffuser. C'est ce que l'on appelle un virus réseau. Son but est de se répandre d'ordinateur en ordinateur via les connexions réseau en se reproduisant à l'infini. A cause de leur vitesse de reproduction, ils ont pour principal effet de saturer la bande passante.
Un antivirus à jour permet de se débarrasser de quasiment tous les vers.

Prévenir, c'est guérir

Plutôt que de traquer le virus dans toutes les parties de votre disque, évitez-les. Cette liste de conseils devrait vous y aider.

- Avant d'ouvrir une pièce jointe contenant un fichier exécutable (se terminant par .exe, .com, .sys, .pif…), scannez-la avec votre antivirus. D'une manière générale, méfiez-vous des courriels de grande taille dont vous ne connaissez pas la provenance.
- Analyser vos disquettes, CD et DVD avant de les lire.
- Paramétrez Windows pour que le logiciel de messagerie que vous utilisez affiche systématiquement les extensions de fichiers.

Se protéger « Lutter contre les virus informatiques »

. Enregistrez et testez tous les fichiers que vous téléchargez sur Internet, surtout si vous faites du « peer to peer » ou que les données ne proviennent pas d'un site « institutionnel», sûr. Même si les antivirus vérifient toutes nouvelles données sensibles avant que vous ne les lanciez, mieux vaut ne pas « exécuter » directement le fichier mais l'enregistrer sur le disque dur (option « enregistrement » plutôt que « ouvrir avec… »). Comme pour une pièce jointe, vous pourrez analyser le fichier avec votre antivirus avant de l'exécuter.

. Créez un Recue Disk afin de pouvoir analyser son disque dur et éliminer le virus sous MS-DOS lorsque l'ordinateur est contaminé et que vous n'arrivez plus à retourner sous Windows.

. Partitionnez votre disque dur, séparez les données des applications pour éviter de contaminer la totalité de votre disque, l'idéal étant d'avoir un deuxième disque dur.

De toute façon, ce n'est pas la peine d'en faire une jaunisse si jamais votre machine est « vérolée ». Le remède existe ou va être mis au point. Se débarrasser d'un virus est donc une opération plus facile qu'on le croit et suivre quelques règles de bases permet d'éviter la plupart des infections.

En résumé

Pour mettre son ordinateur et celui des autres à l'abri

Il faut :

. Installer un antivirus, un pare-feu pour éviter une contamination ou l'invasion d'un Troyen.
. Faire une image de votre disque dur avec un « ghost » afin d'éviter de tout réinstaller en cas de panne.
. Sauvegarder fréquemment vos données.
. Faire le ménage : vider la corbeille, supprimer les fichiers temporaires…
. Défragmenter votre disque dur.
. Faire un ScanDisk, même si l'opération est longue, tous les trois mois afin de réparer les par ties (clusters) abîmées, le changer si une grande proportion de clusters sont inexploitables.
. Surveiller le comportement de votre machine (souris qui n'obéit plus, impression non-sollici tée, ralentissement du disque dur…).
. Vous créer une deuxième adresse mail que vous consacrerez aux usages « publics » : forums, chats, achats en ligne, lettres de diffusion…

Il ne faut pas :

. Ouvrir ou lancer des logiciels de provenance douteuse (site warez, pirate, de pair à pair…), il est préférable les enregistrer sur le disque et les scanner avec un antivirus avant de les ouvrir.
. Ouvrir un courriel indésirable, répondre à un mail dont l'expéditeur vous est inconnu.

Si vous n'utilisez pas votre ordinateur personnel :

. Inspecter l'ordinateur avec un antispyware, si c'est possible.
. Vérifier si un utilisateur de la machine peut installer un logiciel. En cas de doute, il ne faut pas vous connecter à des sites sécurisés, comme celui de votre banque.