

Diapo 11 (2005)

Les **spywares s'installent généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares)**. En effet, cela permet aux auteurs des dits logiciels de rentabiliser leur programme, par de la vente d'informations statistiques, et ainsi permettre de distribuer leur logiciel gratuitement. Il s'agit donc d'un modèle économique dans lequel la gratuité est obtenue contre la cession de données à caractère personnel.

Les spywares ne sont pas forcément illégaux car la licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé ! En revanche étant donné que la longue licence d'utilisation est rarement lue en entier par les utilisateurs, ceux-ci savent très rarement qu'un tel logiciel effectue ce profilage dans leur dos.

.....
Se protéger des spywares n'est pas chose facile. En effet, un **anti virus ne les détectera pas** puisqu'il ne détaille pas l'ensemble du code des programmes mais reconnaît des signatures au préalable identifiées. De plus, un espioiciel n'est pas un virus. Les éditeurs d'antivirus ne travaille donc pas sur ce "marché". <http://www.securiteinfo.com/attaques/divers/spyware.shtml>

En outre, **l'utilisation d'un firewall ne permettra généralement pas non plus la détection des espioiciels**. En effet, même si la routine provoque l'envoi d'un fichier par email à un destinataire non désiré la configuration du firewall, sauf exception, n'a pas pour but d'analyser ce qui sort du PC mais à l'inverse ce qu'il rentre. Le firewall n'a donc pas de moyen de savoir qu'un email est émis volontairement ou à l'insu de l'utilisateur. De plus, un firewall ne s'intéresse pas à la nature des fichiers qui transitent mais aux paquets qui voyagent sur le réseau. Il n'y a donc pas de moyen simple pour le firewall d'identifier comme des menaces l'exécution des routines et la passation d'informations.

.....
Règles générales de protection http://www.secuser.com/dossiers/spywares_generalites.htm

Depuis les scandales provoqués en 1999 par la découverte de spywares dans SmartUpdate (Netscape) et RealJukeBox (Real Networks), la pratique est devenue plus transparente dans le cas des spywares commerciaux, même si les abus restent nombreux. Quelques règles simples peuvent être observées :

- lisez attentivement les conditions d'utilisation d'un logiciel avant de l'installer. L'existence d'un spyware commercial et de ses fonctionnalités annexes y sont normalement signalées, même s'il faut bien souvent lire entre les lignes car le spyware y est présenté en des termes édulcorés voire trompeurs, voire parce que tout est fait pour que l'utilisateur évite de lire lesdites conditions d'utilisation. Si vous ne comprenez pas la langue dans laquelle est rédigée une licence d'utilisation vous ne devriez pas installer le logiciel concerné ;
- réfléchissez bien avant de dévoiler des informations personnelles. Dans le meilleur des cas, les conditions d'utilisation sont généralement conformes au droit américain, donc beaucoup moins protectrices en matière de vie privée qu'en Europe. Notamment ne donnez pas votre adresse email permanente chez votre fournisseur d'accès mais plutôt un compte d'email gratuit qui pourra être fermé en cas de spamming ;
- n'acceptez pas sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel. New.net, SaveNow et Webhancer sont ainsi proposés par défaut lors de l'installation de KaZaA, mais il suffit de décocher les cases correspondantes pour qu'ils ne soient pas installés ;

- installez un [firewall personnel](#) et surveillez les demandes d'autorisation de connexion à internet, afin de détecter toute application suspecte. C'est une autre bonne raison d'installer un firewall personnel ;
- informez-vous auprès de sites spécialisés. Secuser.com et sa lettre d'information hebdomadaire [Secuser News](#) aborde régulièrement la question des spywares au travers de l'actualité ou de dossiers ;
- gardez enfin à l'esprit qu'installer un logiciel n'est jamais une opération anodine : cela revient à autoriser le programme à effectuer toutes les opérations qu'il souhaite sur votre disque dur. Outre un spyware, un programme douteux peut contenir un virus ou un troyen, donc un minimum de précaution s'impose.

Les spywares commerciaux n'étant pas des virus ni des troyens, les antivirus ne permettent pas de les détecter. Scanner un fichier même avec un antivirus à jour n'assure donc pas de l'absence d'un spyware. Il existe cependant d'autres moyens de les détecter voire de les éliminer : il est ainsi utile d'exécuter un antispyware périodiquement ou après l'installation d'un logiciel douteux, pour s'assurer de ne pas avoir installé un spyware sans le savoir.

.....
 Il y a quelques mois Florian Bernard présentait Incredimail et SmileyCentral (équipes de bonhommes soleil) comme deux ennemis mortels de votre ordinateur...

- Votre ordinateur s'arrête brusquement sans raison apparente?
- Votre ordinateur est parfois d'une lenteur de tortue, sans raison apparente?
- Votre ordinateur affiche de mystérieux messages d'erreur lorsque vous naviguez sur l'Internet?
- Ou alors tout bloque et vous obtenez un écran bleu avec des messages incompréhensibles?
- Vous n'arrivez plus à ouvrir certains liens sur l'Internet?
- Vous recevez beaucoup de messages publicitaires sous forme de popups ou de courrier-spam?
- Vous avez toutes sortes de bugs dans votre ordinateur, sans cause apparente?
- Certains programmes fonctionnent de manière étrange?

Il y a de fortes chances qu'une partie des problèmes - ou la totalité - viennent de Incredimail ou de Smiley Central, ou des deux à la fois...

Ces deux programmes gratuits (il en existe une version non gratuite, mais guère plus recommandable) sont des ennemis de votre ordinateur et ne peuvent causer que des problèmes, des bugs, des arrêts brusques de votre ordinateur, des troubles de fonctionnement de d'autres programmes, des difficultés de navigation sur le web, etc.

En outre, ces deux programmes sont PLEINS de spyware (modules d'espionnage) qui s'installent à votre insu sur votre ordinateur et qui suivent à la trace toutes vos opérations. Le programme Incredimail, notamment, installe un module-espion qui communique directement des renseignements à votre sujet aux propriétaires du programme, à Tel-Aviv, en Israël. Ces renseignements concernent votre ordinateur, les programmes qui y sont installés, votre adresse Internet, vos archives, vos navigations sur le web, etc. Autant Incredimail que Smiley Central, une fois installés, établissent une communication à votre insu avec différents sites où des données sont recueillies à votre sujet.

Les deux programmes créent ensuite des liens qui inondent votre ordinateur de messages variés, y compris des popups

de sites pornographiques, etc.

En outre Incredimail utilise une part énorme des ressources de votre système, notamment au niveau de la mémoire RAM, ce qui ralentit votre ordinateur et, très souvent, cause des arrêts et des gels de tout le système. Les mêmes problèmes surviennent chez ceux à qui vous avez envoyé des messages Incredimail.

Le code-source des courriers d'Incredimail contient un lien de téléchargement des images à partir d'un site EXTÉRIEUR, ce qui ouvre littéralement votre ordinateur à tout venant. A cause de ce lien extérieur, votre ordinateur devient une cible potentielle d'infection par des virus, des vers, des chevaux de Troie, etc.

Mais ici vous devez exercer votre propre jugement dans cette affaire...

Voir aussi → Fred Langa 10 octobre 2002

.....

Comment détecter la présence d'un spyware ?

http://www.secuser.com/dossiers/spywares_generalites.htm

Le plus simple pour détecter la présence d'un spyware est de procéder par des moyens indirects, à savoir son activité, la présence de fichiers caractéristiques ou le nom du logiciel suspect. Les moyens ci-dessous sont assez faciles à mettre en oeuvre, mais ne concernent que les spywares commerciaux ainsi que les mouchards dont l'existence a été découverte.

Il existe ainsi des **listes de spywares**, consultables en l'état, sous forme de moteurs de recherche ou encore d'utilitaires dédiés. Près d'un millier de logiciels (spywares intégrés ou programmes associés à un spyware externalisé) ont ainsi été recensés, dont Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA ou encore iMesh :

C'est pourquoi des **antispywares** ont été conçus sur le modèle des antivirus, afin de détecter les spywares sur la base de signatures. Utilisables facilement même par des non initiés, ils permettent de détecter un spyware même s'il n'est pas actif, mais restent dépendants de la mise à jour du fichier des signatures. OptOut étant abandonné, **le plus performant des antispywares gratuits actuels est Ad-Aware** (LavaSoft), qui a par ailleurs le mérite d'exister en version française :

Dans la Presse section techno, dimanche le 13 février 2005 , page A2

Sacré Kazaa !

Il n'y a pas que les utilisateurs qui rouspètent contre les programmes qui s'installent automatiquement avec le logiciel Kazaa. **Même les employés de Kazaa Media Desktop s'en plaignent.** Selon un rapport interne, les employés du célèbre programme d'échange de fichiers blâment leurs employeurs pour la **quantité phénoménale de logiciels intégrés qui se greffent à Kazaa.** (On comprend notre compagnie qui doit faire **de la publicité**, mais quand **ces logiciels alourdissent le système informatique et le ralentissent**, ce n'est pas juste pour l'utilisateur). À preuve, les employés disent qu'ils n'installent pas Kazaa sur leur ordinateur personnel.