Les spywares Version 1.0 par Sebastien VELLOZZI

- Date de création : Décembre 2004
- Date de MAJ: Décembre 2004
- Commentaire : ce document est basé en grande parti sur l'article sur les spywares de Emmanuel JUD paru sur le site http://www.secuser.com
Certains passages ont été reformulés ou abrégés pour être plus digestes.
- Lien direct : http://www.secuser.com/dossiers/spywares_generalites.htm

1. Définition :

Un spyware, en français "espiogiciel" ou "logiciel espion", est un programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs (mail, nom, prénom, telephone, ...) et de les envoyer à son concepteur ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Deux types de spywares

Une première classification des spywares peut être établie en tenant compte de leur fonction, à savoir le commerce ou le renseignement :

* les spywares commerciaux collectent des données sur leurs utilisateurs et interagissent de manière visible avec eux, en gérant l'affichage de bannières publicitaires ciblées, en déclenchant l'apparition de fenêtres pop-up, voire en modifiant le contenu des sites web visités afin par exemple d'y ajouter des liens commerciaux. Ce sont les spywares les plus courants. Leur existence est généralement mentionnée dans la licence d'utilisation du logiciel concerné, mais souvent dans des termes ambigus et/ou dans une langue étrangère, ce qui fait que l'utilisateur n'est pas correctement informé. Ils se présentent généralement sous la forme de logiciels gratuits, pour les éditeurs desquels ils constituent une source de revenu ;
* les mouchards collectent également des données sur leurs utilisateurs mais le font dans la plus totale discrétion. La surveillance et la réutilisation éventuelle des données collectées se font à l'insu des utilisateurs, généralement dans un but statistique ou marketing, de débogage ou de maintenance technique, voire de cybersurveillance. L'existence de ces mouchards est délibérément cachée aux utilisateurs. Ils peuvent concerner n'importe quel logiciel, qu'il soit gratuit ou commercial, mais de par leur fonction ils sont peu fréquents.

Une seconde classification peut être opérée en fonction de la nature des spywares, à savoir leur constitution logicielle :

* le spyware intégré (ou interne) est incorporé dans le code d'un programme ayant une fonction propre pour lui donner en plus la possibilité de collecter et de transmettre via internet des informations sur ses utilisateurs. Les logiciels concernés sont par exemple Gator, New.net, SaveNow, TopText, Alexa ou Webhancer ainsi que la totalité des mouchards. Le spyware et le programme associé ne font qu'un et s'installent donc simultanément sur l'ordinateur de l'utilisateur ;
* le spyware externalisé est une application autonome dialoguant avec le logiciel qui lui est associé, et pour le compte duquel elle se charge de collecter et de transmettre les informations sur ses utilisateurs. Ces spywares sont conçus par des régies publicitaires ou des sociétés spécialisées comme Radiate, Cydoor, Conducent, Onflow ou Web3000, avec lesquelles les éditeurs de logiciels passent des accords. Le spyware de Cydoor est par

exemple associé au logiciel peer-to-peer KaZaA, et s'installe séparément mais en même temps que lui.

Une nouvelle tendance encore plus contestable concerne les utilisateurs du navigateur Internet Explorer. Certains spywares comme Gator cherchent à s'installer automatiquement sur le poste de l'internaute au moyen de la technologie ActiveX, lors de la visite de pages web peu recommandables.

2. Comment s'en protéger ?

* être vigilant, c'est à dire:
- Lire les licences des logiciels que vous installez. Tout y est précisé de manière plus ou moins claire certes, en particulier le spyware et les données qu'il envoie.
- Ne pas installer des compléments de programmes à l'aveuglette sans savoir ce qu'il fait. A ce niveau, méfiez vous des cases pré-cochées lors de l'installation d'un logiciel :).
- Faites attention à vos informations personnelles. Bien souvent les logiciels/systèmes d'exploitation respectent le droit américain bien plus permissif que le droit européen sur les informations personnelles
- Evitez de surfer sur des sites "douteux" ou proposant des kits de connection spécifiques pour accéder à la partie membre du site.

* Installer un firewall. Celui vous permettra de contrôler tout ce qui sort ou entre de votre machine via internet.

* Installer un antispyware
Ci dessous une liste non exhaustive d'antispyware gratuit:
- Adware : http://www.lavasoft.de
- Spybot - Search & Destroy : http://www.safer-networking.org/fr/index.html
- Spy sweeper : http://www.webroot.com/wc/productcs/spysweeper/index.php
- Spy Audit : http://www.spychecker.com/download/download_spyaudit.html
- X-Cleaner : http:///www.spychecker.com/download/download_xcleaner.html

Adware est le plus connu et un des plus performants. Mais ma préférence va à Spybot - Search & Destroy. Ce dernier est aussi performant que son camarade. De plus, il est entièrement en français (développé par des gentils gars bien de chez nous! Cocorico!!). Son gros point fort est qu'il ne se limite pas qu'à la détection et l'élimination de spyware. En effet, Spybot est capable de:
- détecter les trojans et autres keylogger,
- renforcer la sécurité de votre Internet Explorer favori en bloquant les contrôles activeX douteux (ActiveX : Technologie capable d'être téléchargé et exécuté par un navigateur web, et permettant l'accès depuis celui-ci aux éléments d'un environnement Microsoft.),
- surveiller les modifications apportées à votre base de registres à votre insu si vous installez le logiciel "tea timer" fournit avec.

3. Conclusion

Les spywares sont une des menaces de l'internet. Ce document vous a sensibilisé à ce nouveau fléau et les moyens de vous en préserver. Les logiciels présentés, en particulier Spybot, sont subjectifs car il existe autant de solutions pour se protéger que d'informaticiens dans ce monde. Maintenant libre à vous de vous protéger ou de tirer le diable par la queue à ce niveau. Pour ceux qui voudraient approfondir le sujet, je vous conseille d'aller sur #nohack ou de prendre votre moteur de recherche préféré.