



Spyware

Pour plus de sécurité, adoptez les réflexes CASES !

Les spywares ou logiciels espion envahissent nos ordinateurs ! Ces petits programmes informatiques se multiplient à l'aide de logiciels (généralement gratuits) diffusés et téléchargeables sur Internet (freewares et sharewares) ou distribués sur des CD-ROM et DVD-ROM. Certains logiciels propriétaires sont porteurs de spywares.

1. Spyware, c'est quoi ?

Un spyware est un logiciel espion. C'est un programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs 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 de l'utilisateur. Les spywares ont pour objectif primaire, d'espionner le comportement de l'internaute et de transmettre ensuite, à son insu, les informations collectées aux créateurs et éditeurs de logiciels afin d'alimenter une gigantesque base de données.

2. Qui est concerné ?

Toute personne accédant à Internet est concernée. Il est difficile de connaître avec précision le nombre d'utilisateurs affectés, car le spyware s'exécute généralement avec discrétion et dans l'ignorance totale du propriétaire de l'ordinateur. Et même s'ils connaissent sa présence, beaucoup ne le voient pas comme une menace, tout au plus un vague inconfort. Ils ne prennent donc aucune action pour s'en débarrasser et n'avertissent pas leur administrateur réseau. Néanmoins, l'explosion du Spam ces



deux dernières années pourrait souligner la gravité du problème posé par les logiciels espions. Veuillez aussi consulter notre publication sur les risques 2004.

3. Comment cela fonctionne-t-il ?

Un spyware « s'attrape » en général en naviguant sur Internet, ainsi qu'en téléchargeant des logiciels gratuits (freeware) ou de publicité (adware). Il est tout particulièrement fréquent dans les programmes de messagerie instantanée (ICQ), les lecteurs audio (RealPlayer) et les systèmes « peer-to-peer » (Kazaa, Limewire).

Le spyware lui-même est un programme autonome ou associé à un logiciel prévu pour tout autre chose. Il utilise alors des techniques comme l'ingénierie sociale ou celles des chevaux de Troie.

3.1 Types de spywares 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 d'y ajouter par exemple 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.

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, de marketing, de débogage ou de maintenance technique, voire de cybersurveillance. L'existence de ces mouchards est délibérément cachée aux utilisateurs.

Le spyware intégré (ou interne) est un programme exécutable inclus dans le code source d'un logiciel ayant une fonction propre, pour lui donner la possibilité de collecter et de transmettre des informations par Internet. Ces spywares sont téléchargeables séparément ou sont proposés à l'installation en même temps que d'autres programmes gratuits, eux-mêmes généralement des spywares, grâce à des accords entre éditeurs de logiciels. C'est le cas notamment de Gator, New.net, SaveNow, TopText, Alexa et Webhancer.

Le spyware externalisé est une application autonome dialoguant avec le logiciel principal qui lui est associé, et dont la seule fonction est de se charger de la "relation client" : collecte et transmission d'informations, affichage de bannières publicitaires, etc. 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 également des accords. Le spyware de Cydoor est par exemple associé au logiciel « peer-to-peer » KaZaA, et s'installe en même temps que lui.

3.2 Exemples

Cydoor - Spyware qui ouvre des fenêtres « pop-up » pendant la navigation sur Internet. Il ré-achemine également toutes les demandes Internet vers des serveurs tiers afin de capturer vos habitudes. Cydoor ne peut pas être désinstallé en utilisant la fonction « uninstall » de Windows et aucun logiciel de désinstallation n'est fourni.

Gator - fournit une fonctionnalité qui semble être utile, mais qui est tout à fait dangereuse. Il fournit l'option de se rappeler le nom de l'utilisateur, les mots de passe et les informations des cartes que vous employez pour accéder à des sites pour l'e-commerce. Ces informations sont stockées sur votre ordinateur. Bien que l'information soit chiffrée (encryptée), elle peut être consultée par Gator ou par des intrus.

4. Le spyware est-il légal ?

Selon la législation européenne, « chacun a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » (Convention pour la Protection des Droits de l'Homme et des Libertés Fondamentales). La directive 95/46 de la Communauté Européenne indique que « les données à caractère personnel sont toute information concernant une personne physique identifiée ou identifiable », et stipule que l'utilisation de ces données n'est pas licite, «...sauf consentement explicite de la personne concernée...».

De son côté, la directive 2002/58 de la Communauté Européenne traite du statut des spywares et autres technologies aux mêmes caractéristiques. Elle stipule que « (...) les logiciels espions, les pixels invisibles (web bugs), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné. ».

Il semblerait donc que la législation protège les droits de l'utilisateur d'Internet. Cependant, même si certaines affaires sont déjà passées devant la justice (par exemple Doubleclick, condamné en 2002, aux Etats-Unis, à payer 450 000 dollars et à respecter la vie privée des utilisateurs d'Internet), tout problème lié à l'utilisation d'Internet rentre difficilement dans un cadre légal. En attendant que le côté légal soit éclairci, l'utilisateur d'Internet doit prendre des mesures pour protéger sa vie privée.

5. Comment se protéger ?

Se protéger des spywares n'est pas

chose facile. En effet, un anti-virus ne les détecte pas puisqu'il ne détaille pas l'ensemble du code des programmes mais reconnaît des signatures identifiées au préalable. De plus, un spyware n'est pas un virus. L'utilisation d'un firewall correctement configuré (un firewall qui analyse à la fois les flux entrants et sortants) peut détecter éventuellement les spywares qui essaient d'envoyer des données vers l'extérieur. Si le code informatique provoque l'envoi d'un fichier par email à un destinataire non désiré, le firewall n'a pas de moyen de savoir qu'un email est émis volontairement ou à l'insu de l'utilisateur et ne le bloque pas (firewall applicatif). Cependant, l'un des moyens existants pour suspecter un spyware sur une machine est de voir un flux de paquets nettement supérieur au flux habituel passer via le firewall ou le modem. Mais là encore, c'est très difficile à détecter.

Il existe sur le net de nombreux sites référençant des spywares. Cependant aucun ne peut prétendre avoir une liste exhaustive des spywares existants. De même, certains outils permettent la détection de logiciels identifiés comme ayant des spywares, mais les utiliser ne garantit pas une sécurisation à 100% du PC.

C'est pourquoi des anti-spywares ont été conçus sur le modèle des antivirus, afin de détecter les spywares sur la base de signatures. Facilement utilisables, même par des non initiés, ils permettent de détecter un spyware même s'il n'est pas actif, mais ils restent dépendants de la mise à jour du fichier des signatures.

Liens utiles

[Spychecker](#) - moteur de recherche de spywares

[ZoneAlarm](#) - firewall personnel de ZoneLabs

[AdAware](#) - antispyware de Lavasoft

[Spybot](#) - autre excellent antispyware

[Windows Anti-spyware](#) - antispyware de Microsoft

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu