

Spyware : les éviter, s'en débarrasser

Il y a encore deux ans, le principal risque auquel était exposé l'utilisateur d'un ordinateur personnel était celui de voir sa machine infestée par un virus. Aujourd'hui et par le simple respect de quelques règles essentielles, on peut se prémunir presque complètement contre ce risque. Ces trois règles simples sont la mise à jour régulière à l'aide de Windows Update, la suppression systématique et avant ouverture de courriers électroniques d'origine inconnue et, enfin, l'utilisation d'un antivirus fréquemment mis à jour.

Le respect de ces trois règles « clefs » permet donc d'éviter l'immense majorité des virus, mais, hélas, ne prémunit pas l'utilisateur contre un risque nouveau, les spywares. Les joies de l'informatique étant ce qu'elles sont, à peine commence-t-on à maîtriser un domaine, qu'un nouveau mystère apparaît. Presque totalement ignorés par la majorité des antivirus, les spywares constituent une nouvelle menace pour l'utilisateur. Véritables « plaies du Web », ces logiciels espions sont de plus en plus gênants et difficiles à éviter, même pour l'utilisateur averti.

Les spywares ou logiciels espions : kézako ?

Un spyware est un logiciel qui s'installe à l'insu de l'utilisateur dans le but de diffuser de la publicité ou obliger à utiliser tel ou tel service payant pour, in fine, rapporter de l'argent à son créateur. Bien qu'ils ne soient pas considérés comme tels par les éditeurs d'antivirus (ou tout du moins pas encore tout à fait), les spywares se rapprochent en de nombreux points de leurs aînés destructeurs, les virus. Comme eux, ils s'installent souvent à l'insu de l'utilisateur et il est à peu près aussi difficile de s'en débarrasser. Une caractéristique différencie toutefois virus et spywares, caractéristique qui contribue à la pseudo légalité de ces derniers : ils ne cherchent pas à se reproduire.

De manière générale, on dénombre deux moyens de contamination pour les spywares. Le premier, redouté par de nombreux novices, n'est autre qu'Internet. Le schéma est classique : vous entrez sur un site web qui propose monts et merveilles (musique, logiciels ou jeux illégaux, contenu pornographique gratuit...) et vous demande avant d'accéder aux contenus ou services en question d'accepter l'installation d'un composant ActiveX similaire à ce que vous pouvez voir ci-contre. En acceptant, non seulement vous donnez les clefs de votre machine à l'éditeur du site Web pour y installer ce qu'il veut (logiciel espion, dialer, backdoor...), mais bien souvent, le site Web n'offre même pas ce qu'il a promis. Ce genre de site Web est bien entendu à éviter : qu'on se le dise, les généreux bienfaiteurs du Web sont rares et le gratuit coûte forcément à quelqu'un. Mieux vaut éviter que cela soit vous !

Pour rappel, le contrôle ActiveX est une technologie Microsoft qui permet à un site Web d'installer un composant logiciel sur l'ordinateur de l'internaute. Le risque lié à l'installation d'un composant ActiveX est tellement important qu'il est recommandé de ne jamais en installer à moins d'être absolument certain de sa provenance. On peut citer à ce sujet le site de mise à jour de Windows (windowsupdate.com), qui utilise cette technologie à bon escient et certains sites d'éditeurs de logiciels de sécurité : l'outil de recherche de virus en ligne de BitDefender ou le site de McAfee, par exemple, utilisent tout deux cette technologie sans que cela présente le moindre risque pour votre machine.

Le second mode de « diffusion » des spywares est aussi le plus répandu et le plus efficace. De nombreux éditeurs de logiciels gratuits utilisent en effet les spywares pour générer une petite rémunération. Ledit logiciel est accompagné, le plus souvent de manière invisible, d'un spyware qui s'active à l'installation. À l'utilisation du programme (voir même à tout moment) de la publicité est

affichée. Cette publicité permet à la société éditrice du spyware d'engranger des revenus, une partie de ces revenus étant redistribuée aux développeurs du soft. Cette intégration du spyware à des logiciels gratuits est donc et de loin la méthode de diffusion la plus efficace.

Mais la limite entre spyware et pratique commerciale douteuse n'est pas toujours facile à déterminer. Comment qualifier par exemple la fenêtre de mise à jour automatique d'un logiciel gratuit qui vous propose d'essayer ou d'installer un autre logiciel de l'éditeur, qui lui est payant ? À partir de quel moment un logiciel gratuit qui affiche une bannière de publicité pour se financer (adware) peut être qualifié de spyware ? Si l'utilisation d'un « dialer » (programme heureusement en perte de vitesse qui profite des lignes accès Internet RTC OU RNIS pour utiliser un numéro surtaxé et très cher en lieu et place du numéro normal de votre fournisseur d'accès) n'est pas le moins du monde équivoque, l'affichage d'une simple bannière de publicité au sein d'un logiciel gratuit n'est pas forcément critiquable.

En réalité, à partir du moment où il y a espionnage de l'utilisation de l'ordinateur et utilisation des ressources à l'insu de l'utilisateur, un logiciel peut être considéré comme un spyware. Toutefois, pour faire simple, nous utiliserons dans cet article le terme « spyware » un peu plus largement pour désigner tous les logiciels qui s'installent à l'insu de l'utilisateur, mais ne sont pas des virus (ne se reproduisent pas) et dont la finalité est de faire gagner de l'argent à leurs créateurs.

Eviter les spyware

Après avoir lu ce qui précède on pourrait conclure qu'un internaute qui n'installe jamais de logiciels autres que ceux du commerce et qui ne fréquente aucun site louche ne craint rien. C'est donc une des solutions pour se protéger complètement des spywares. Un peu excessive, convenons-en.

Malheureusement (ou heureusement, c'est selon), les logiciels commerciaux ne répondent pas forcément à tous les besoins et une grande partie des logiciels gratuits ne contiennent pas de spyware. Il convient donc de se poser la question à chaque logiciel téléchargé : « celui-ci peut-il contenir un spyware ? ». Un peu d'autopromotion ne faisant pas de mal, nous testons sur Clubic.com l'ensemble des logiciels que nous proposons en téléchargement ce qui limite les risques liés aux spywares. Sans pouvoir garantir que l'ensemble de la logithèque Clubic est exempte de spyware, nous faisons le maximum pour ne pas référencer les logiciels en contenant et lorsque c'est le cas, parce qu'un logiciel présente un réel intérêt et permet d'éviter leur installation (on pense par exemple à MSN Messenger Plus), nous le signalons.

On ne le dira jamais assez : lorsqu'un site Web vous propose d'installer un logiciel sur votre disque dur (à ne pas confondre avec le simple fait de télécharger un logiciel), il faut toujours se poser la question de la pertinence de cette installation. Les sites proposant du contenu illégal (logiciels et jeux piratés, musique illégale...) et les sites pornographiques utilisent souvent cette technique pour générer des revenus. Dans la plupart des cas, il faut refuser l'installation de logiciels par un site Web.

Nous reparlerons dans la suite de cet article de la protection permanente qu'offrent de plus en plus de logiciels antispyware. Avec une telle protection, l'antispyware, constamment en mémoire, se propose de supprimer les spywares avant même leur installation sur le disque dur. On se rapproche à ce niveau du fonctionnement d'un classique antivirus. Même si elle consomme des ressources, une telle protection peut aider à se prémunir des spywares.

Détecter les spywares

Le propre du spyware étant de se manifester pour inciter l'utilisateur à adopter une offre (publicité, service...), il est en général assez simple de se rendre compte de sa présence. L'action la plus couramment entreprise par un spyware consiste à modifier la page de démarrage et la page de recherche du navigateur. Une action un peu plus vicieuse consiste à ajouter une extension au navigateur, les fameux BHO (browser helper objects). Ces modules ajoutent des barres de menus ou des fenêtres publicitaires directement dans le navigateur.

Au palier de nuisance suivant, le spyware installe un logiciel qui se lance automatiquement au démarrage de Windows. Le spyware dispose ainsi de toutes les libertés pour vous envoyer une fenêtre de publicité même si le navigateur Web n'est pas ouvert. Qu'on se le dise : une page de démarrage modifiée ou un nouveau menu au sein du navigateur peut être synonyme de spyware. Une fenêtre intempestive (pop-up) qui s'affiche alors qu'aucun site Web n'est ouvert est synonyme de spyware.

Le spyware peut aussi (et en cela il se rapproche du virus), utiliser la connexion Internet de la machine sur laquelle il est installé pour envoyer des courriers électroniques non désirés (spam) à d'autres internautes : comme la lutte antispam s'accroît, il devient de plus en plus difficile pour les spammeurs d'envoyer eux-mêmes les courriers indésirables, sous peine de risquer des poursuites judiciaires. L'utilisation en masse de machines infestées par des spywares est un bon relai pour envoyer du spam. Une connexion Internet ralentie peut donc, elle aussi, être synonyme de spyware.

Certains spyware modifient parfois le fichier "hosts" de Windows. C'est un fichier très sensible dans la mesure où il indique aux navigateurs Internet comment convertir une adresse web (<http://www.mabanque.com>) en adresse IP (192.231.12.18). Imaginez un spyware qui vous fasse ainsi croire que vous êtes sur le site de votre banque alors que vous naviguez en fait sur une copie de celui-ci.

L'utilisation périodique d'un logiciel antispyware est bien entendu recommandée pour s'assurer que la machine n'a pas été récemment infestée par un spyware.

Le nombre de logiciels permettant de se débarrasser des spywares est croissant, certains sont gratuits, d'autres payants. On en distingue toutefois deux dont la présence historique leur donne une longueur d'avance sur tous les autres. Qui plus est, ils sont gratuits. Il s'agit de Ad-Aware et de Spybot Search&Destroy. Avant de nous lancer dans l'utilisation de ces logiciels, nous pouvons signaler une méthode simple pour commencer notre ménage.

Supprimer les spywares avec l'Ajout / Suppression de programmes

Cela paraît presque idiot, mais il est possible de supprimer certains spywares simplement en les désinstallant comme on le ferait avec n'importe quelle application par l'intermédiaire de la fonction de désinstallation de Windows : Ajout et suppression de programmes (Menu Démarrer / Panneau de Configuration / Ajout et Suppression de Programmes). Il n'y a aucune raison, sauf cas exceptionnel, qu'apparaissent dans ce menu des logiciels que vous n'avez pas vous-même installés. En cliquant sur le lien « cliquez ici pour obtenir des informations sur le support technique », s'affiche le nom de l'éditeur ce qui devrait aider à identifier (ou non) le programme. De la même manière, il se peut qu'en désinstallant le logiciel qui a « amené » le spyware, le spyware soit lui aussi désinstallé. Cela ne coûte en général pas grand-chose d'essayer. Il sera toujours possible, si besoin est, de le réinstaller par la suite.

Voici une liste non exhaustive des spywares que l'on peut supprimer avec cette fonction de Windows : Active Alert, B3D Projector, BackWeb, Bridge, ClickTheButton, CometCursor, CommonName, DownloadWare, eXact Search, Ebates Moe Money Maker, Flingstone Bridge, GoHip, HotBar, HuntBar, IEDriver, IEPlugin, Internet Optimizer, Interstitial Ad Delivery by n-CASE, IPInsight, MediaLoads, MySearchBar, NetworkEssentials, New.net, NewtonKnows, PAD Lookups by n-CASE, SaveNow, SubSearch, TopText, WeatherCast, WhenUSearch, Win32 BI Application, Xupiter

Les antispywares

La menace étant croissante, les solutions antispywares sont de plus en plus nombreuses. Nous avons choisi dans cet article de nous attarder sur les logiciels qui proposent une fonction d'analyse (scanneur). Les trois gratuits Ad-Aware, Spybot Search&Destroy et Microsoft Antispyware font partie de la liste à laquelle nous avons ajouté quatre payants que l'on peut acheter sans difficulté en France : SpySweeper, Pest Patrol, McAfee Antispyware et Effaceur 8.

Afin de vérifier la pertinence de chacune de ces solutions, nous avons utilisé plusieurs logiciels qui contiennent des variantes différentes de spyware : le fameux Kazaa, mais aussi des logiciels complètement infestés de spywares dont on taira le nom par prudence. L'utilisation croisée de chacun des antispywares permet d'identifier quels sont ceux qui se comportent le mieux. Il est par contre complètement impossible de comparer les antispywares en se basant sur le nombre de spywares détectés tant leur manière d'effectuer un décompte est différente. Pest Patrol identifie par exemple comme spyware tout fichier stocké dans le répertoire d'installation d'un logiciel contenant un spyware. Tous les fichiers provenant de l'installation de Kazaa (y compris les images .bmp ou les fichiers textes) sont comptabilisés comme spyware et chaque élément est affiché comme ayant la même importance dans l'interface. Les antispywares nomment aussi parfois les spywares différemment ce qui complique la comparaison.

Le tableau ci-dessous récapitule les possibilités de plusieurs outils antispyware.

	Scanneur	Protection permanente	Prix	Editeur	Outils inclus (hors analyse et résident)
Ad-Aware SE Personal	Oui	Oui (payant)	Gratuit ou payant	Lavasoft	Aucun
Spybot Search&Destroy	Oui	Oui	Gratuit	Safer Networking	<ul style="list-style-type: none"> - Suivi des modifications IE - Incohérences du registre - Démarrage système - Effaceur de sécurité
SpySweeper	Oui	Oui	29,95€	Webroot Software	<ul style="list-style-type: none"> - Suivi des démarrages automatiques - Suivi des modifications IE - Suivi des fichiers hôtes - Protection service Windows Messenger
Effaceur Expert 8	Oui	Oui	29,95€	Micro Application	<ul style="list-style-type: none"> - Suivi des démarrages automatiques - Effacement des traces (Internet, applications, Windows) - Effacement définitif - Popup blocker - Défragmenteur mémoire
Pest Patrol	Oui	Oui	39,95€	Computer Associates	aucun
Microsoft Antispyware	Oui	Oui	Gratuit	Microsoft	<ul style="list-style-type: none"> - Suivi des démarrages automatiques - Suivi des fichiers hôtes - Suivi des modifications IE - Effacement des traces (Internet, applications, Windows) - Restauration IE
McAfee Antispyware	Oui	Oui	29,99\$	McAfee	aucun

Conclusion

En connaissant mieux le fonctionnement et les objectifs des spywares, il est plus simple de les éviter et de s'en débarrasser. Autant nous aurions tendance à conseiller une réinstallation complète dans le cas d'une infection virale (nous avons tous tenté de supprimer un virus pendant une demi-journée pour nous rendre compte qu'il était plus rapide de réinstaller sa machine), autant la suppression des spywares est chose faisable avec les bons outils, un peu de rigueur et de la patience.

Après avoir soumis les sept antispywares de ce guide à un grand nombre de logiciels espions, on peut déjà conclure qu'il n'existe aucun antispyware « ultime ». Notre préférence va à Spysweeper qui possède la meilleure base de définitions, une interface claire et détaillée et des outils de nettoyage intéressants, mais il n'est hélas pas suffisant seul pour éliminer complètement la menace. Spybot et Microsoft Antispyware, nos deux gratuits préférés nous semblent indispensables et tout à fait complémentaires à Spysweeper. Ad-Aware, pourtant précurseur est lui en retrait face aux deux autres gratuits. McAfee Antispyware et Effaceur 8, pourtant payant, sont insuffisants pour lutter efficacement contre les spywares. Pour terminer, Pest Patrol n'est clairement pas utilisable.

On ne comprend vraiment pas pourquoi aucun des logiciels ne propose la création d'un CD autobootable de nettoyage qui éviterait le problème des spywares résidents. Pas un des logiciels de ce guide n'a en effet été capable de se débarrasser des spywares les plus acharnés (type « elitebar »). Un dernier conseil pour terminer. Pour éviter les spywares, préférez les logiciels commerciaux ou Open Source qui en sont exempts (NDLR : du moins, on l'espère pour les éditeurs) et lorsque vous installez un logiciel gratuit (freeware), préférez les éditeurs qui mentionnent explicitement que leur logiciel ne contient pas de spyware, le mensonge est assez rare sur la question.