

Edito

Les virus, spams ou piratages vous donnent déjà envie de jeter votre ordinateur ? Dans la famille « fléaux informatiques », le CRI vous présente le logiciel-espion, ou spyware. S'il n'est pas nouveau, il a cependant largement dépassé les seuils épidémiques critiques, et ses conséquences peuvent être graves. Pour tous ceux qui sous-estimeraient ces logiciels dont le nom semble emprunté à un James Bond, sachez que la menace ne prête pas à sourire : 30 000 spywares ont ainsi été recensés depuis leur première apparition en 1999, avec pas moins de 400 nouveaux venus par semaine. Les dégâts causés par les spywares, toujours plus ingénieux, sont estimés à plusieurs milliards de dollars pour la seule année 2004, et, pendant positif, le marché des anti-spywares prévoit un chiffre d'affaires de 106 millions de dollars en 2005.

Fidèle à sa politique de sécurité et d'information, ce premier CRI Pratique de l'année vous explique ce qu'est un logiciel espion, et, avant que vous ne décidiez définitivement de vous débarrasser de votre machine, vous donne tous les conseils nécessaire à sa protection.

Après le bêtisier des virus, la faune des logiciels espions

Apparentés aux cookies, aux vers, et autres chevaux de Troie, les logiciels-espions revêtent de multiples visages : spyware, adware, malware, parasiteware ou encore dialer... Quelques définitions s'imposent pour comprendre cette grande famille de programmes nuisibles.

Le adware (de l'anglais « advertising » (publicité) et « software » (logiciel)). Patriarche de la famille, le adware constitue la souche originelle du spywaring. Son rôle ? Collecter des données personnelles, concernant les habitudes de navigation de l'internaute. Considéré comme le plus anodin de l'espèce, il se « contente » de gérer l'affichage de bannières publicitaires ciblées selon les profils récoltés, de déclencher l'apparition de pop-up (ces petites fenêtres publicitaires qui s'ouvrent sans avertir et qui reviennent toujours malgré vos efforts pour vous en débarrasser), et peut aller jusqu'à modifier les sites web visités en leur ajoutant des liens vers des sites commerciaux précis.

Le spyware (de l'anglais « spy » (espion) et « software » (logiciel)). Il peut être traduit par « espioniciel » et est bien plus vicieux que son parent le adware. Le spyware collecte également des informations concernant vos habitudes de navigation, mais transmet ces données personnelles à des sociétés peu scrupuleuses qui utiliseront ou revendront les fichiers dans le but de vous inonder de spams.

Mais le spyware est bien plus dangereux, puisqu'il est capable d'espionner ce que vous tapez sur votre clavier : lorsque vous consultez votre compte bancaire, par exemple, il peut enregistrer votre mot de passe et le transmettre, avec les conséquences que l'on imagine...

Le malware (contraction de « malicious software »). Il appartient à la catégorie des programmes malveillants en tête dans le panthéon du banditisme informatique. Il s'agit de programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un ordinateur. Il a clairement pour objectif de nuire à l'intégrité d'un système.

Le dialer : ce programme malveillant ne concerne que les internautes connectés en mode RTC (connexion bas-débit par modem 56 Kb/s, passant par le réseau téléphonique). Tous les utilisateurs ayant une connexion ADSL et n'utilisant pas de modem RTC (y compris les modems internes) sont donc protégés. Un dialer est un logiciel qui connecte votre ordinateur à Internet en utilisant des numéros de téléphone surtaxés. Certains dialers utilisent même des connexions satellites dont les tarifs peuvent atteindre plusieurs euros par minute. Les communications effectuées par ce mode de connexion ne seront visibles que sur votre facture de téléphone...

Et les cookies ? Les cookies sont souvent assimilés à des logiciels espions. Pourtant, ils sont devenus incontournable à la navigation car nécessaires pour accéder à la plupart des sites web. Leur rôle est de personnaliser le contenu et les services proposés aux internautes. Par exemple, lorsque vous faites des achats en ligne, vous devez les placer dans un caddie virtuel. Les données correspondant aux achats effectués (prix, référence, quantité, ...) sont placées dans un cookie sur votre ordinateur. Elles permettent de personnaliser les pages affichées, d'enregistrer le contenu de votre caddie, ou encore d'afficher des informations vous concernant (nom, prénom, adresse de livraison...).

Un cookie est un simple fichier texte, de quelques Ko. Contrairement au spyware, le cookie n'est pas un programme et ne possède donc aucune fonction cachée lui permettant de récupérer à votre insu votre adresse e-mail ou vos mots de passe, et encore moins compromettre votre système. Il est également impossible d'attraper un virus par le biais d'un cookie. Enfin, seul le site web qui dépose un cookie sur un ordinateur peut l'utiliser : les informations qu'il contient ne sont pas accessibles par d'autres sites web.

Comment attrape-t-on les spywares ?

Les spywares sont présents sur le Web. Vous courez des risques dans les cas suivants :

- ◇ En visitant un site web douteux : site pour adultes, site de recherche de fichiers piratés, site de jeux...
- ◇ En téléchargeant un logiciel gratuit : logiciel de peer-to-peer (kazaa, notamment), de démonstration de jeux, ...
- ◇ En remplissant un formulaire en ligne.
- ◇ Mais aussi, parfois, par le biais de votre messagerie, en activant un lien présent dans un spam. (Pour rappel, ne répondez jamais aux spams et ne cliquez jamais sur les liens qu'ils proposent ! Reportez-vous au **CRI Pratique n°4 consacré aux spams**).

À savoir :

La présence d'un spyware dans un logiciel gratuit est toujours mentionnée dans les termes de sa licence. L'utilisateur installe donc le spyware de son plein gré. Cependant, une telle mention est la plupart du temps perdue dans un jargon incompréhensible, et même une lecture attentive des termes de la licence ne permet de déceler l'existence du parasite...

Les méfaits des spywares ?

- ◇ Des bannières publicitaires correspondant à votre profil s'affichent de manière inexplicée.
- ◇ Des pop-up surgissent.
- ◇ De nouveaux liens apparaissent.
- ◇ Votre boîte aux lettres électronique est inondée de spams.
- ◇ Vos données personnelles sont piratées.
- ◇ Le système est instable et ralentit : les spywares existent sous forme de fichiers binaires, scripts, exécutables .exe ou fichiers .dll, qui s'installent dans le répertoire système de la machine et fonctionnent comme un service afin de pouvoir être activés au démarrage. En modifiant la base de registre, ils déstabilisent à moyen terme le système d'exploitation.
- ◇ Votre connexion Internet "rame" : le débit de votre liaison est diminué parce que votre ligne est polluée par l'activité parfois frénétique des spywares, qui occupent votre ligne pour renvoyer un maximum d'informations vous concernant.
- ◇ Vous ne pouvez plus démarrer un programme : les liens ou boutons de certains programmes deviennent inactifs ; l'activation et la désactivation de l'état de veille deviennent quasiment impossibles ou excessivement lentes.
- ◇ Votre navigateur Internet Explorer adopte un comportement étrange : la page de démarrage change aléatoirement et toutes vos tentatives pour corriger la configuration échouent ; il se lance seul et affiche des publicités ; des favoris, bien souvent pornographiques, apparaissent dans votre dossier Favoris ; des barres d'outils s'ajoutent toutes seules.
- ◇ Votre facture téléphonique ne correspond pas à votre consommation.

Cette liste n'est pas exhaustive. Mais ces symptômes, isolés ou cumulés, doivent attirer votre attention ; ils sont autant de traces de la présence de spywares sur votre ordinateur.

Comment se prémunir ?

Comme pour les virus ou les spams, il n'existe aucune recette miracle... Quelques réflexes simples à acquérir vous permettront cependant d'échapper aux spywares :

◇ Installez un fire-wall (ou pare-feu), utilisé principalement pour :

Un fire-wall est le gardien de la porte virtuelle de votre réseau : il vérifie et vous alerte, si vous l'avez configuré ainsi, de tout ce qui circule depuis votre machine vers l'extérieur, dans le sens entrée ou dans le sens sortie.

Les fonctions du fire-wall sont nombreuses : il permet notamment de se protéger contre les tentatives d'intrusion, et donc d'espionnage. Mais s'il est recommandé pour se protéger des spywares, c'est aussi parce qu'il surveille tous les programmes qui tournent sur votre machine. Son fonctionnement est simple : à chaque fois qu'un programme essaie pour la première fois d'accéder à l'extérieur du réseau, le fire-wall vous alerte, et inscrit ce programme dans une sorte de registre. Vous n'avez plus qu'à préciser si vous souhaitez, à chaque fois que le programme en question se lancera, que le fire-wall vous avertisse ou non de l'action.

Le fire-wall ne peut empêcher un programme de fonctionner, de même qu'il est incapable de repérer un programme malveillant. C'est à vous de l'autoriser à vous alerter à chaque fois (sauf pour les applications que vous utilisez couramment) et de surveiller les données qu'il vous transmet. Attention, lorsque vous effectuez la mise à jour de vos logiciels, le fire-wall ne les reconnaîtra plus et vous devrez le reconfigurer.

Le CRI met plusieurs fire-wall à votre disposition sur son serveur ftp. Cet outil est indispensable pour une informatique en réseau sécurisée : ne le négligez pas !

Le prochain CRI Pratique (mois de mars) sera consacré aux fire-wall, à leur installation et à leur configuration.

=> Téléchargez votre firewall sans risque sur le serveur ftp du CRI :
<ftp://ftp.pub.cri74.org/pub/win9x/firewall/>

◇ Installer un logiciel antispyware :

Un anti-spyware est destiné à éliminer les indésirables, mais ne peut le faire que lorsque ceux-ci sont déjà installés sur la machine. Il se différencie de l'anti-virus qui empêche le programme malveillant de pénétrer le système en lui bloquant l'accès. Il est donc indispensable de lancer régulièrement l'anti-spyware (au moins à chaque téléchargement) de manière à vérifier qu'aucun espioniciel ne s'est introduit dans le système. L'anti-virus est donc un outil de prévention (à la condition expresse qu'il soit mis à jour régulièrement, sinon il ne peut pas reconnaître les derniers virus), tandis que l'anti-spyware est un outil de "guérison".

Tous les anti-spyware suivants sont gratuits mais ne sont pas libres. Vous pouvez les télécharger sans risque sur le serveur ftp du CRI : <ftp://ftp.pub.cri74.org/pub/win9x/anti-spyware/>

- Spybot Search & Destroy

Télécharger Spybot Search & Destroy :

<ftp://ftp.pub.cri74.org/pub/win9x/anti-spyware/Spybot-SearchAndDestroy/>

Site officiel : <http://www.safer-networking.org/fr/home/index.html>

- **Ad aware** : des fichiers additionnels permettent de localiser le logiciel dans plusieurs langues dont le français (<http://manuelsdaide.com/>)

Télécharger Ad Aware : <ftp://ftp.pub.cri74.org/pub/win9x/anti-spyware/Ad-Aware/>

Site officiel : <http://www.lavasoftusa.com/>

◇ **Utilisez et mettez à jour régulièrement un logiciel anti-virus**

L'association de l'anti-virus et de l'anti-spyware est incontournable : un spyware peut très bien pénétrer votre système par le biais d'un virus.

=> **Téléchargez votre antivirus sans risque sur le serveur ftp du CRI :**
<ftp://ftp.pub.cri74.org/pub/win9x/antivirus>

◇ **Et surtout, « surfez » de manière responsable !** L'informatique en réseau comporte des risques qu'il faut connaître. De petites habitudes très simples vous permettront d'en éliminer beaucoup :

- Ne visitez pas des sites web douteux.
- Ne remplissez pas n'importe quel formulaire en ligne, ou alors interrogez-vous sur la pertinence des réponses à donner (donner une adresse e-mail secondaire pour les spams, ...).
- N'acceptez jamais systématiquement un message émis par un site web : on vous propose de télécharger un programme afin de vous faire bénéficier d'offres promotionnelles extraordinaires ? Il est certain qu'un spyware est installé dans ce programme, et que vous ne recevrez jamais d'offres... Ne cochez donc pas de manière compulsive les cases "oui" ou "ok" dès qu'une fenêtre de dialogue s'affiche sur un site web.
- N'acceptez pas sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel : il suffit de décocher les cases correspondantes pour qu'ils ne soient pas installés.
- Informez-vous auprès de sites spécialisés (en recherchant sur Google), et n'hésitez pas à contacter le **référént informatique** de votre structure qui pourra vous aider à identifier et vous débarrasser d'un spyware.
- Enfin, n'oubliez pas qu'installer un logiciel n'est pas une opération anodine puisqu'elle autorise un 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 : il est indispensable de prendre un minimum de précautions !

Les logiciels libres et les spywares

Ils ne s'entendent pas du tout ! En effet, le code source du logiciel libre est par définition clairement affiché, et scanné par des milliers d'informaticiens à l'affût de la moindre faille ; il est donc impossible d'y cacher un programme espion. Vous pouvez télécharger sans risque les logiciels libres, surtout à partir de sites web qui vérifient les programmes avec minutie avant de les proposer (Framasoft.net par exemple).

Enfin, s'équiper d'un navigateur libre, Firefox par exemple (200 000 téléchargements quotidiens, et 20 millions d'internautes conquis à ce jour ! Et vous ?), permet de limiter considérablement les risques liés aux spywares.

Conclusion

Un peu de bon sens, des outils anti-spyware et un fire-wall vous protégeront efficacement contre ce fléau.

Un dernier conseil : laissez agir votre anti-spyware plutôt que de vous attaquer vous-même à l'élimination du programme ! En effet, la désinstallation du logiciel suspect ne supprime pas forcément le spyware, et peut même supprimer d'autres programmes sains et vitaux pour le système !

LIENS UTILES

- ◇ www.spychecker.com : moteur de recherche de spywares
- ◇ www.secuser.com : sa lettre d'information aborde régulièrement le sujet des spywares et donne la liste des derniers logiciels espions recensés.