

Vous souhaitez combattre les « SPYWARES » ?
Cette brochure va vous aider



■ 1 - Introduction

Un spyware (ou logiciel espion) est un logiciel qui s'installe à l'insu de l'utilisateur dans le but de diffuser de la publicité ou d'obliger ce dernier à utiliser des services payants.

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 : ces derniers ne cherchent pas à se reproduire.

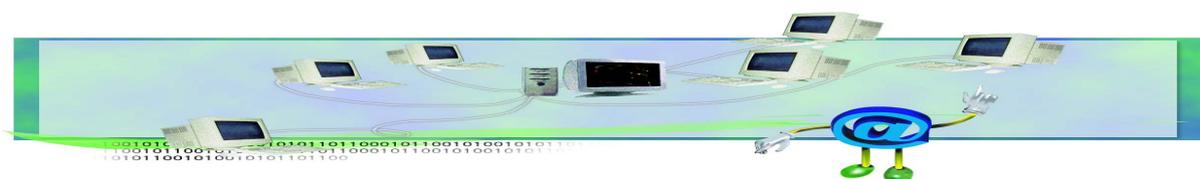
Dans tous les cas, ils représentent une atteinte à la vie privée, et de surcroît les programmes ainsi installés à votre insu grèvent petit à petit les performances de votre machine, jusqu'à la rendre inutilisable dans les cas extrêmes ...

Il convient donc d'être vigilant et de se débarrasser de ces gêneurs le plus rapidement possible !

A noter que vous trouverez en dernière page de ce document les définitions d'un certain nombre de termes techniques employés ici.

Sommaire:

Introduction	Page 1
Comment contracte t-on des spywares ?	Page 2
Les outils pour les combattre	Page 3
Comment obtenir et installer Spybot	Page 4
Comment configurer SpyBot	Page 6
Comment utiliser SpyBot	Page 7
Spybot : fréquence d'utilisation et mises à jour	Page 9
Quelques définitions utiles	Page 12



■ 2 - Comment contracte t-on des spywares ?

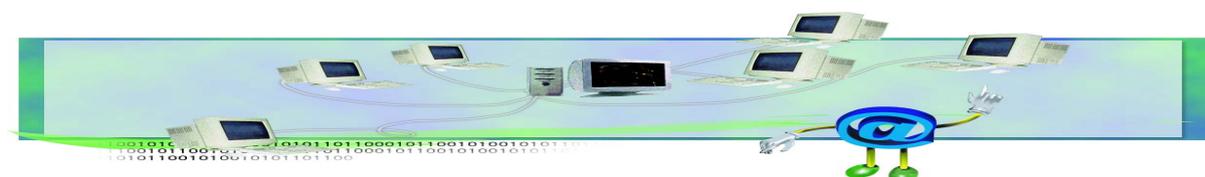
Première possibilité : lors d'une connexion à l'Internet, vous entrez sur un site web et celui-ci vous demande, avant d'accéder à certains contenus ou services, d'accepter l'installation d'un composant appelé « ActiveX » similaire à ce que vous pouvez voir ci-dessous.



En acceptant, vous donnez les « clefs » de votre machine à l'éditeur du site Web pour y installer ce qu'il veut. Ce genre d'adresse est bien entendu à éviter, **sauf s'il s'agit d'un site dont vous êtes sûr** ; par exemple la figure ci-dessus montre l'installation d'un ActiveX issu de *Microsoft Corporate* (l'éditeur du contrôle). Vous avez, entre autres, besoin d'installer ce contrôle afin de permettre la mise à jour via *Microsoft Windows Update*. Il est donc recommandé de n'installer un ActiveX que si vous êtes certain(e) de sa provenance

Le second mode de contamination est très répandu et sans doute le plus efficace. De nombreux éditeurs de logiciels gratuits utilisent les spywares pour générer une rémunération. Ledit logiciel est accompagné, le plus souvent de manière invisible, d'un spyware qui s'active à l'installation. Cette méthode s'avère très courante à l'heure actuelle.

En connaissant mieux le fonctionnement et les objectifs des spywares, il est plus simple de les éviter et de s'en débarrasser. Certaines machines peuvent rapidement « héberger » une collection impressionnante de Spywares ! Dans certains cas, on aura même tendance à recourir à une réinstallation complète du système ... Heureusement dans la plupart des cas, la suppression des spywares est chose faisable avec les bons outils, un peu de rigueur et de la patience.



■ 3 - Les outils pour les combattre :

Des « anti-spywares » ont été conçus sur le modèle des anti - virus, afin d'en détecter la « signature ». Utilisables facilement y compris par des non - initiés, ils permettent de détecter un espion même s'il n'est pas actif, mais ils restent tout de même dépendants de la mise à jour du fichier des signatures.

Les anti-spywares les plus performants - dans la famille des logiciels gratuits - sont actuellement *Spybot* et *Ad-Aware* (qui ont en plus le mérite d'exister en version française).

Il s'agit là d'une solution « ultime ». Les anti-spywares ne vous mettent pas à l'abri de toute contamination. Toutefois certains de leurs paramètres peuvent vous éviter bien des malheurs.

Les pare - feux sont une autre solution pour parer à d'éventuelles contaminations. Ils se basent sur les éléments sortants et entrants dans votre système en auscultant ce que l'on appelle des « ports ». Certains de ces produits sont également gratuits.

Leur paramétrage peut toutefois s'avérer être complexe à mettre en œuvre pour un « débutant ». Cependant, pour les détenteurs du système d'exploitation Microsoft Windows XP Service pack 2 ou Vista, un pare feu simple est à leur disposition de façon intégrée. Il peut être activé et surtout désactivé très simplement en cas de problème de communication.

Pour vérifier si le pare - feu de Windows est activé, cliquez sur « Démarrer - Panneau de configuration - Centre de sécurité - Pare - feu Windows ».

Si vous disposez d'un réseau local composé de plusieurs machines en réseau, il est également possible d'avoir recours à une solution de Pare - feu centralisée.



■ 4 - Comment obtenir et installer Spybot

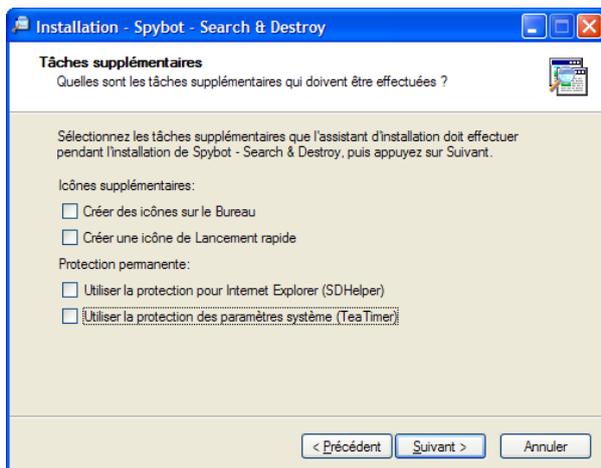
Rendez vous sur <http://www.safer-networking.org/fr/home/index.html> et cliquez sur le lien permettant de télécharger l'utilitaire

Si le site de Safer Networking n'était pas disponible, veuillez utiliser le lien <http://www.telecharger.com>

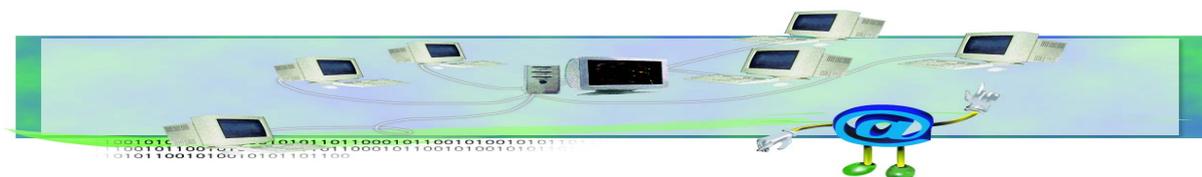
Dans la page qui s'affiche, tapez le mot clé « spybot » dans la zone « rechercher » comme le montre la figure ci-contre, puis cliquez sur « OK ».



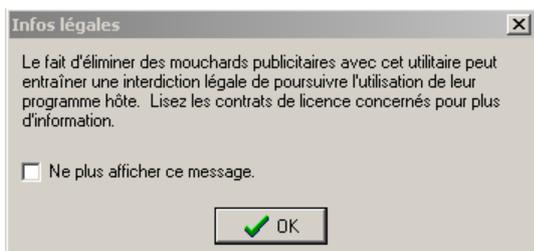
Après avoir téléchargé le programme, exécutez- le.



L'assistant d'installation se lance. Cliquez sur « *Suivant* » pour passer d'écran en écran. Si vous ne souhaitez pas que Spybot soit trop « interventionniste », vous pouvez décocher les cases de protections résidentes « Tea - timer ». Dans ce cas, il vous suffira de lancer une analyse Spybot de temps en temps, ou lorsque vous suspectez une infection...



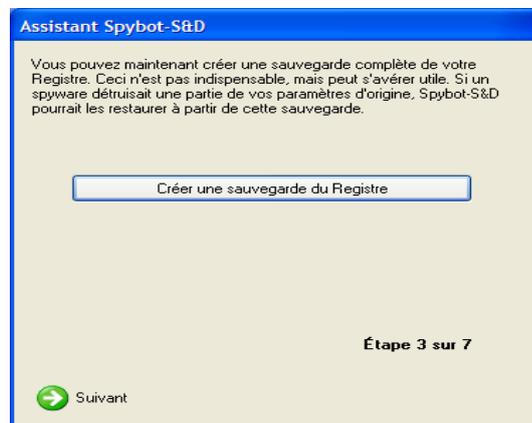
■ 5 - Comment configurer SpyBot



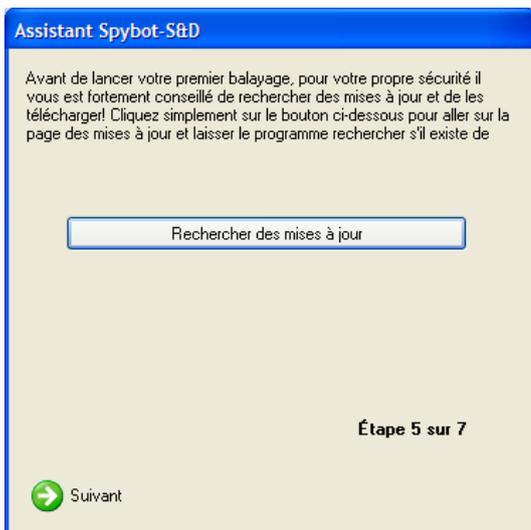
Nous allons à présent entrer dans le paramétrage de Spybot. Lors de la fin de l'étape précédente, une fenêtre similaire à celle ci-dessous apparaît.

Cochez la case *Ne plus afficher ce message* puis *OK*.

Une nouvelle fenêtre vous propose de sauvegarder le registre. Effectuez cette sauvegarde grâce à la commande *Créer une sauvegarde du registre*. Cette opération peut prendre plusieurs minutes. Cliquez ensuite suivant :



Sur la fenêtre suivante, *Internet doit être connecté*.



Cliquez sur *Recherche de mises à jour*

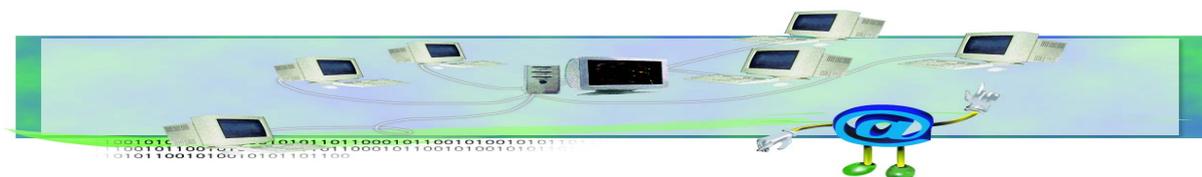
Lorsque vous téléchargez des mises à jour, la machine vous demande d'opter pour un serveur où aller chercher le téléchargement. Si vous n'avez pas de contrainte particulière, sélectionnez une machine en Europe (par exemple Safer-Networking #1).

Les mises à jour importantes sont normalement déjà sélectionnées, veillez dans tous les cas à récupérer au moins les mises à jour « anti-rootkits », « immunization database », « detection rules », « Fixes », « Main update » si elles vous sont proposées.

Cliquez sur « Télécharger », vous constatez l'avancement des mises à jour .

Une fois l'opération terminée, cliquez sur *Quitter*.

De la même manière que précédemment cliquez sur *Vacciner le système* puis sur *Suivant*. La dernière étape du paramétrage consiste à cliquer sur *Commencer à utiliser le programme*.



■ 6 - Comment utiliser SpyBot

L'utilisation de Spybot est simple sur la fenêtre ci-dessous repérez l'icône

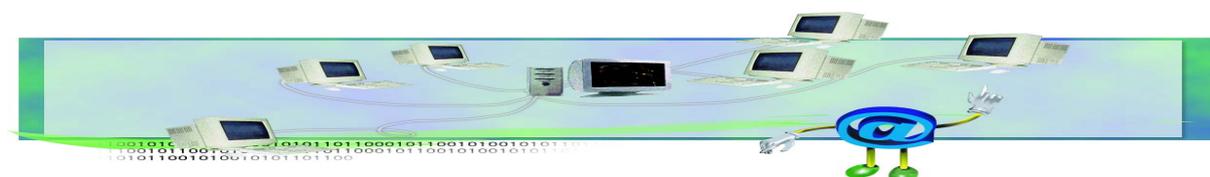


Vous obtenez le tableau suivant. Pour chercher d'éventuels spywares cliquez sur *Vérifier tout* suffit.



Vous pouvez noter la progression de l'analyse grâce à la barre de défilement située en bas de votre fenêtre. Cette recherche peut prendre un certain temps voire beaucoup de temps (jusqu'à 15 minutes pour les cas les plus longs).

A la fin du contrôle, deux options s'offrent à vous. Pour les non - infecté, la mention « Félicitation », sinon un tableau similaire à celui ci-dessous apparaît.



Problème	Genre
<input checked="" type="checkbox"/> Advertising.com	2 éléments
<input checked="" type="checkbox"/> Avenue A, Inc.	1 éléments
<input type="checkbox"/> BackWeb lite	56 éléments
<input checked="" type="checkbox"/> DoubleClick	1 éléments
<input checked="" type="checkbox"/> HitBox	2 éléments
<input checked="" type="checkbox"/> MediaPlex	1 éléments
<input checked="" type="checkbox"/> ValueClick	1 éléments

Les lignes rouges signalent les problèmes détectés. Il s'agit donc du nom des spywares trouvés sur votre poste. Vous pouvez également noter le nombre d'éléments enregistrés pour chaque spyware.

Pour vous en débarrasser, sélectionnez tous les éléments trouvés (ci cela n'est pas déjà fait) à l'aide de *la case à cocher* situé devant chacun puis cliquez sur *Corriger les problèmes*.

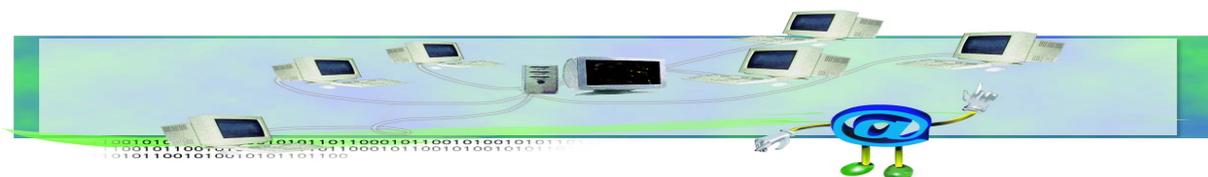
La fenêtre suivante s'affiche. Cliquez sur **Oui** et voilà votre PC désinfecté de tous ses spywares.



Le message suivant s'affiche : cliquez sur **Ok** et vous pouvez quitter le programme à l'aide de la croix en haut à droite.



A noter : certains spywares ne peuvent être enlevés lors de cette correction. Si cela s'avère être le cas, un message vous demandant de scanner votre ordinateur s'affiche. Il n'est pas nécessaire de l'effectuer. Toutefois par mesure de sécurité, contactez votre service de maintenance afin de palier à ce problème.



■ 7 - Spybot : fréquence d'utilisation et mises à jour :

Comme précisé plus haut, Spybot est aux spywares ce que Norton est aux virus. Toutefois, il ne contrôle pas en permanence votre disque dur pour parer aux infections comme le fait un anti - virus. C'est cette différence majeure qui va vous obliger à effectuer des contrôles réguliers. Il est nécessaire de scanner votre disque dur, à l'aide de Spybot, si possible une fois par semaine.

Il s'avère, tout comme pour les Anti - virus, nécessaire de faire des mises à jour. Ces mises à jour permettent à Spybot de connaître la liste des infections les plus récentes. Les mises à jours doivent être effectuées avant chaque nouveau contrôle. Il est bon de savoir qu'un anti - spywares, tout comme un anti- virus, non mis à jour, revient à réduire notablement sa protection.

Mises à jour à effectuer à chaque utilisation de Spybot.

Pour effectuer les mises à jour il vous faut lancer Spybot pour cela :

Double cliquez sur l'icône présente sur votre bureau.

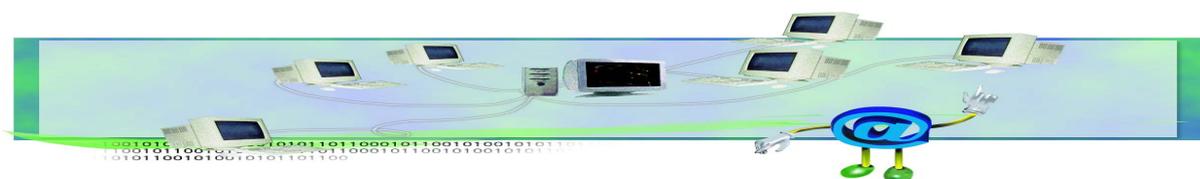


Si celle-ci ne se trouve pas sur votre bureau, vous la trouverez dans *Démarrer, Programmes* puis *Spybot - Search & Destroy*.

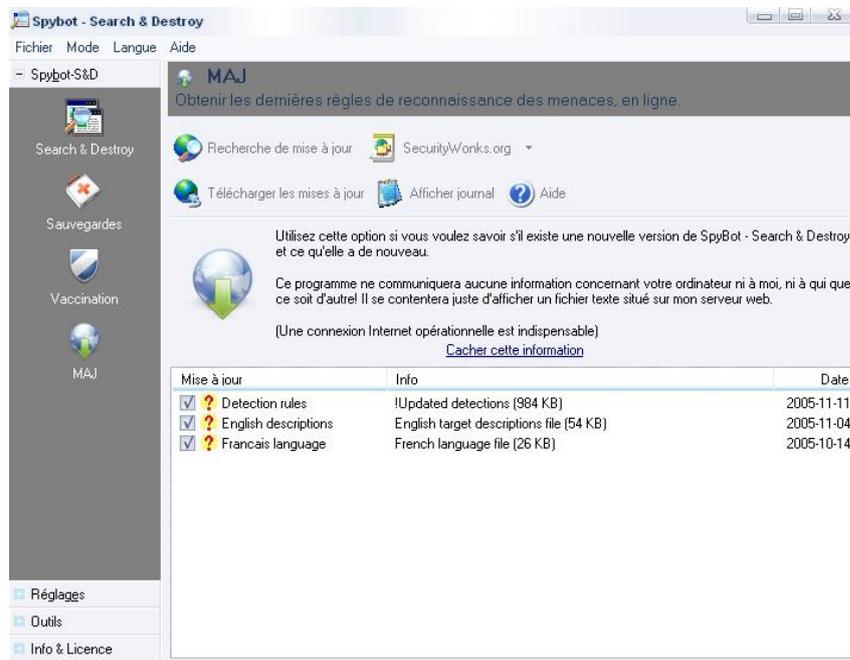
Un clic sur *Recherche de mise à jour* vous donnera la totalité des mises à jour disponibles.



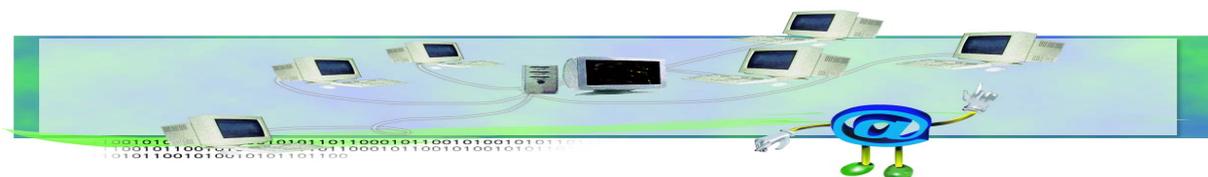
Nota : Internet doit au préalable être connecté



Vous obtiendrez la fenêtre si dessous.



Sélectionnez toutes les mises à jour à l'aide des *cases à cocher*. Puis *cliquez sur* « Télécharger les mises à jour ». N'oubliez pas de vacciner à nouveau ensuite.



■ 8 - Quelques définitions utiles :

SPYWARE.

Contraction de spy et software. Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers, comme transmettre les données saisies grâce au clavier par exemple.

KEYLOGGER.

Type de spyware spécialisé pour espionner les frappes au clavier sur l'ordinateur qui l'héberge, et pour les transmettre via Internet à une adresse où un pirate pourra les exploiter. Un keylogger peut donc recueillir et transmettre vos mots de passe, code de carte bancaire, intitulé sous lequel vous ouvrez une session...

CHEVAL DE TROIE.

Désigne tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate...

SPAM

Technique de marketing utilisant les adresses e-mail pour envoyer des messages publicitaires. Certaines messageries sont parfois saturées par un "spamming" trop important.

MALWARE

Mot bâti par analogie à software. Il désigne tout type de programme nocif introduit sur un ordinateur à l'insu de l'utilisateur. Il regroupe les virus, vers, spywares, keyloggers, chevaux de Troie,...

ACTIVEX

Technologie développée par Microsoft pour installer un petit programme enrichissant les fonctionnalités de votre navigateur

FIREWALL

En français "Pare-feu". Système protégeant le réseau local de l'entreprise contre les intrusions pouvant venir de l'extérieur (Internet). Ce système est un filtre, il peut permettre également de mettre en place des restrictions de connexion pour les machines de l'entreprise qui veulent se connecter sur certaines ressources externes.

© Agence landaise pour l'informatique

