

tuto Spybot

tesgaz

8 septembre 2006

S'il existe des logiciels indispensables, **Spybot-S and D** est à classer dans cette catégorie, véritable couteau Suisse du nettoyage de logiciels espions, **Spyware, BHO, Adware, Malware, trojans, enregistreur de frappe au clavier, etc** N'ont plus qu'à bien se tenir!!!

Fort d'une base de données d'environ 25000 références Spybot-S and D est gratuit (freeware).

ses mises à jour sont régulières (environ toutes les 3 semaines),

Spybot-S and D permet de supprimer tous les espions qui polluent notre PC dès l'installation du système d'exploitation (n'est-ce pas Alexa qui est inclus d'origine dans XP) voir ceci.

Enfin que des programmes qui sont souvent néfastes au bon fonctionnement de son PC, donc totalement inutiles.

Attention ce logiciel fonctionne différemment des autres logiciels anti-spyware, il recherche directement les clés connues des programmes malveillants dans la base de registre et les supprime.

Ce qui veut dire que l'entrée néfaste sera supprimée, mais pas le dossier dans votre système d'exploitation.

Petite visite guidée d'une utilisation simple et efficace de ce logiciel.

1 Page d'accueil

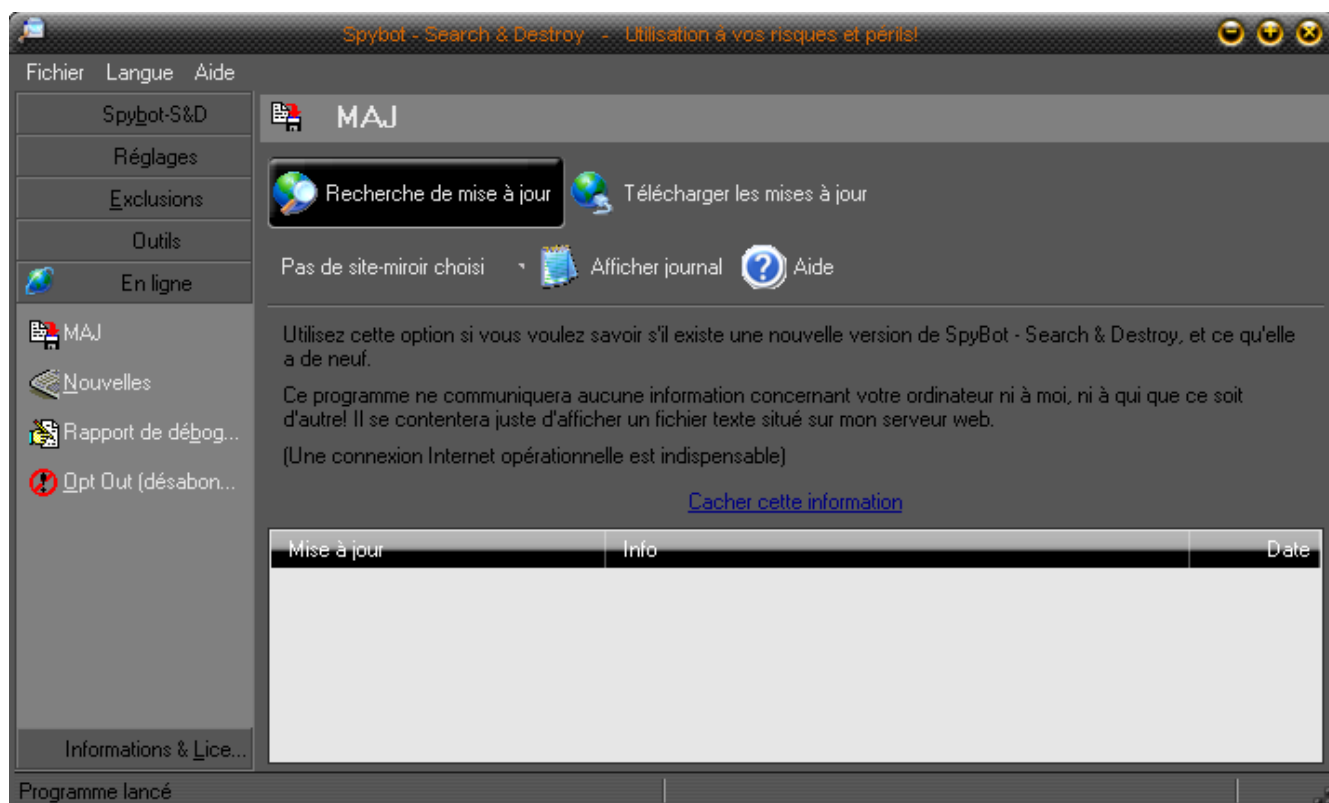
Pour démarrer le logiciel, vous avez 2 possibilités :

"**SpyBot**" ou "**SpyBot (advanced mode)**", il est préférable de choisir "**SpyBot (advanced mode)**"= qui permet d'avoir toutes les options au démarrage du logiciel.



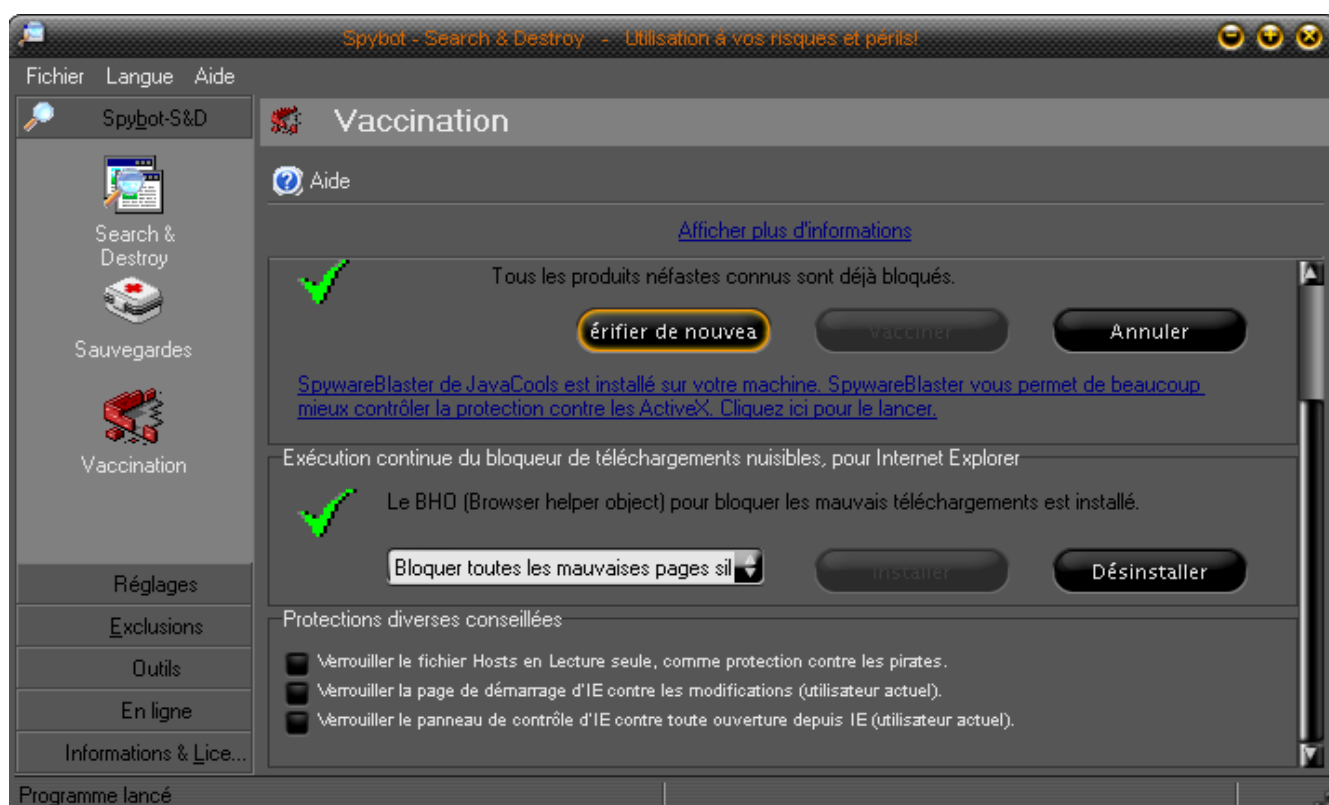
La première chose à faire une fois que votre logiciel est opérationnel, c'est de faire la **"mise à jour immédiate"** des définitions de spywares, pour cela, il vous suffit de cliquer sur la touche **"MAJ"** de votre écran de droite.

Ainsi, vous arrivez sur l'écran de mise à jour :



Vous cliquez sur **”Recherche de mise à jour”** une fois les mises à jour trouvées, il vous suffit de cliquer sur **”Télécharger les mises à jour”** à la suite, vous faites **”Installer”**, une fenêtre CMD va s’ouvrir afin d’installer les mises à jour. Maintenant que les mises à jour sont installées, revenons à l’écran d’accueil

Sur la partie gauche de l’écran, cliquez sur **”Vaccination”**



Sur la partie droite cliquez sur **”Vacciner”**, vous devriez avoir maintenant une icône en forme de V verte qui vous signale que la vaccination est effectuée.

En dessous, si vous utilisez le logiciel **”SpywareBlaster”** vous aurez une indication qui vous permet de le lancer pour faire une mise à jour de ce logiciel (qui inscrit des clés en lieu et place des programmes espions les plus connus), et ensuite, la dernière chose à vérifier, c’est de voir que le système bloque les **BHO** (browser helper object)

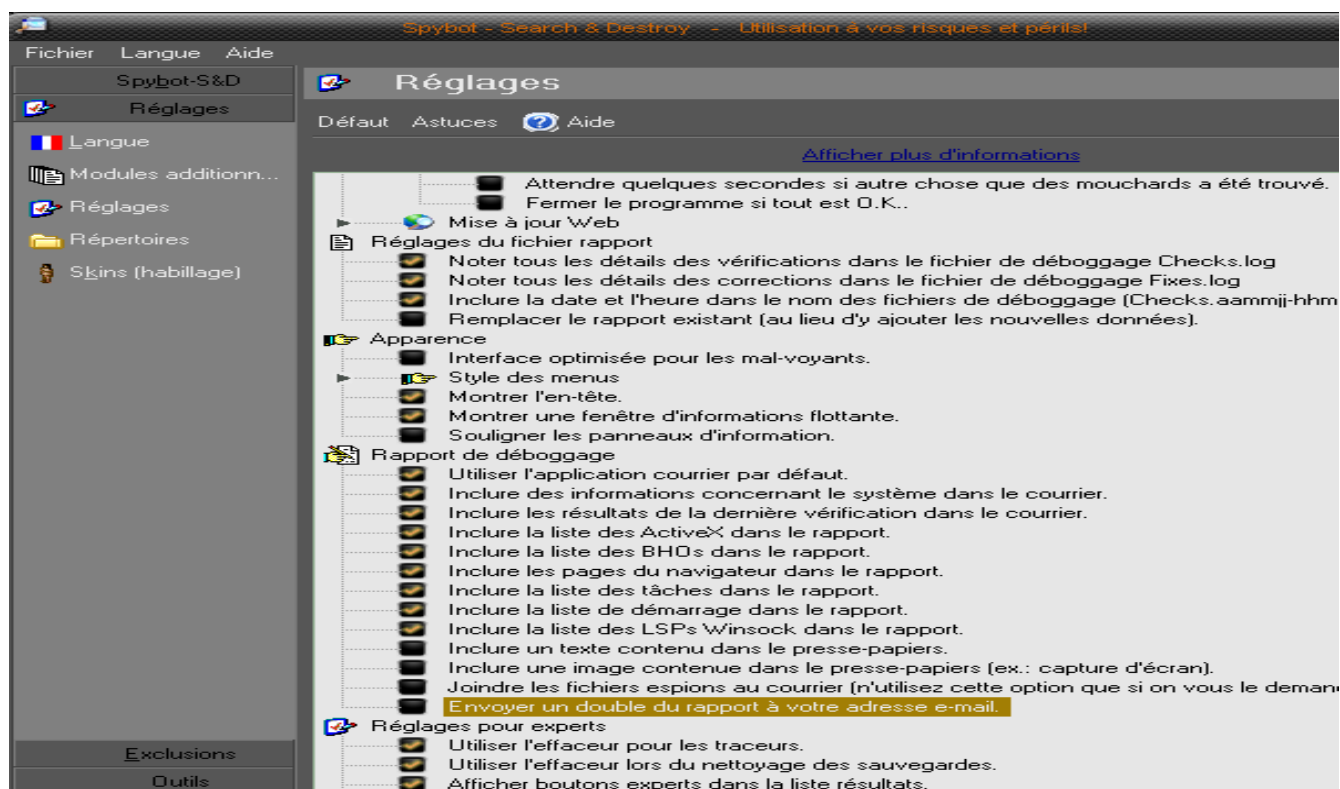
En dessous 3 options sont disponibles :

- **Verrouiller le fichier hosts** (installez d’abord le fichier hosts et activez cette option)
- **Verrouiller la page de démarrage IE** (choisissez votre page d’accueil et activez cette option)
- **Verrouiller le panneau de contrôle de IE** (paramétrez votre IE et activez cette option)

Conseil : Activez le verrouillage de ces 3 options, nous verrons dans le détail, l’intérêt du fichier hosts un peu plus bas.

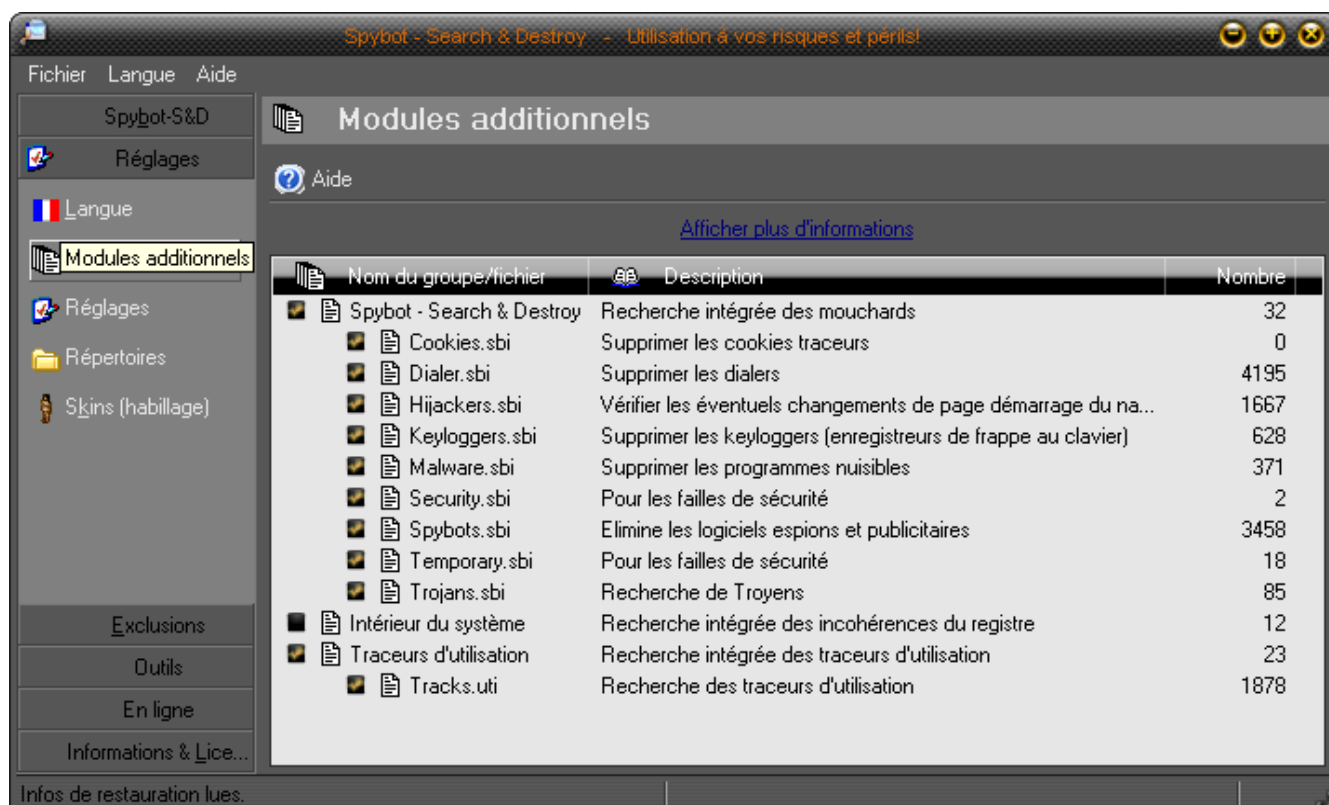
2 Ecran Réglage

Réglages- ”global”



C'est ici que vous mettez les options d'ouverture du programme, les réglages de choix d'utilisation, de rapport ou d'apparence, etc.. Activez ou désactivez les cases en fonction de vos désirs.

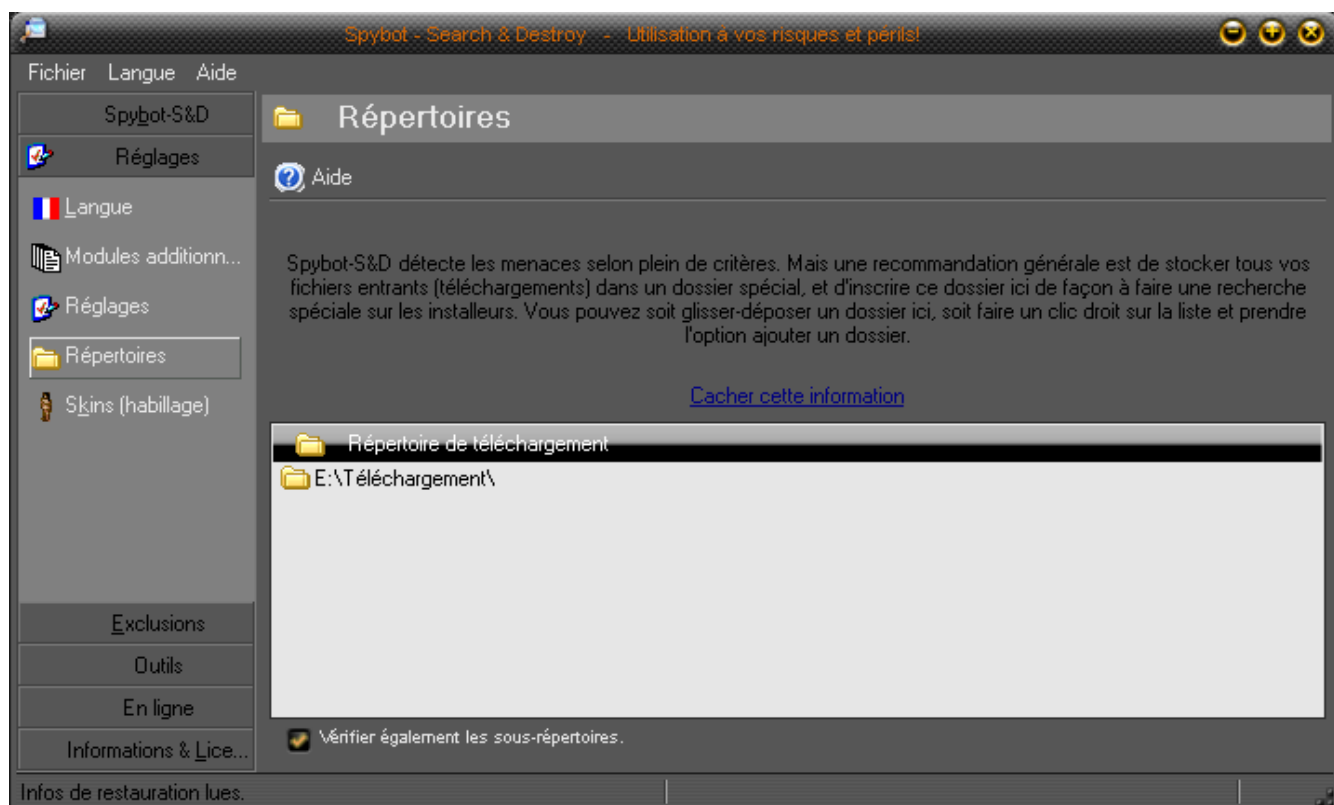
Modules Additionnels



715 435

Ici, il faut activer toutes les cases des **”modules”** de Spybot-SD, ce sont ces modules qui permettent la recherche des espions dans votre base de registre et qui sont régulièrement mis à jour.

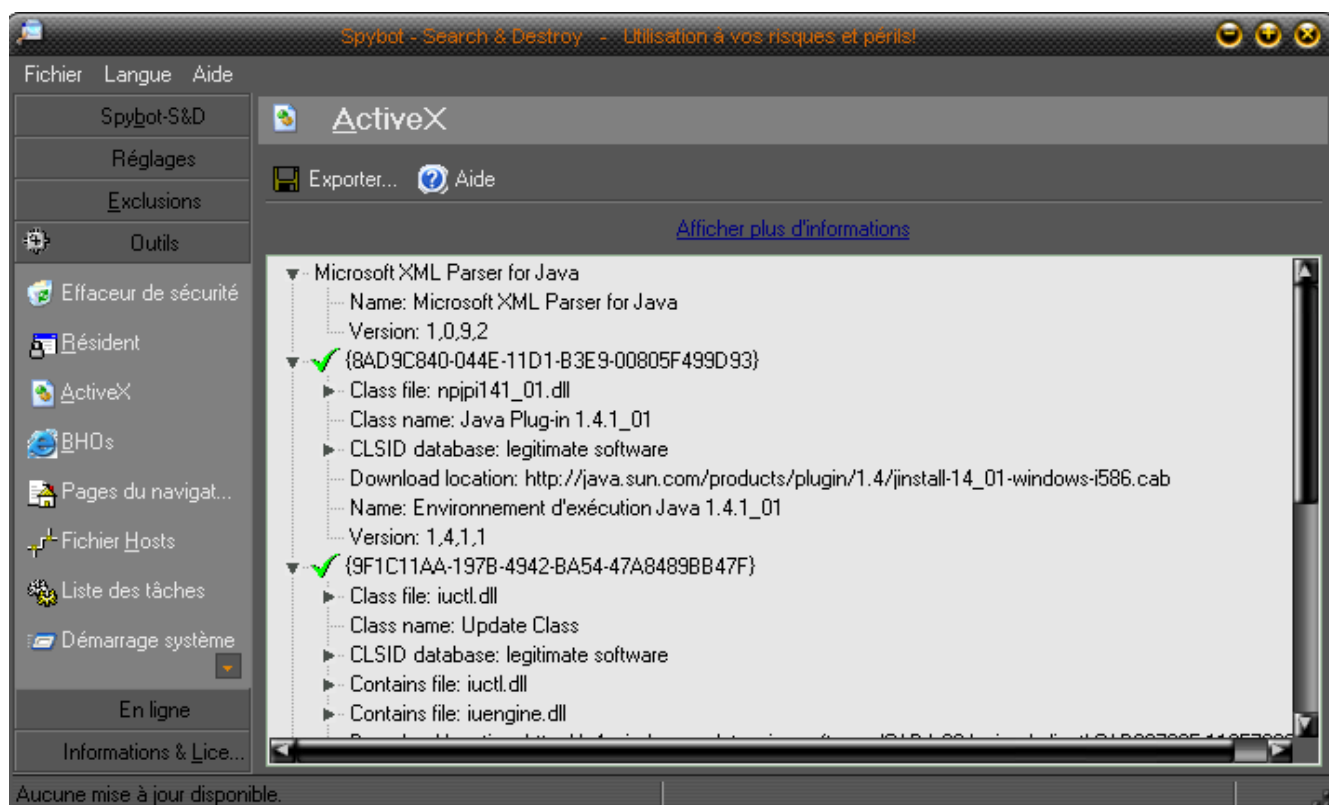
Réglages - Répertoires



Ici, vous indiquez votre répertoire de **”téléchargement”** par défaut, afin que Spybot-SD puisse faire une recherche sur les installeurs, n’oubliez pas d’activer la case **”Vérifier également les sous-répertoires”**. =Réglages - Skins Vous pouvez modifier la présentation de votre logiciel, c’est par ici que ça se passe.

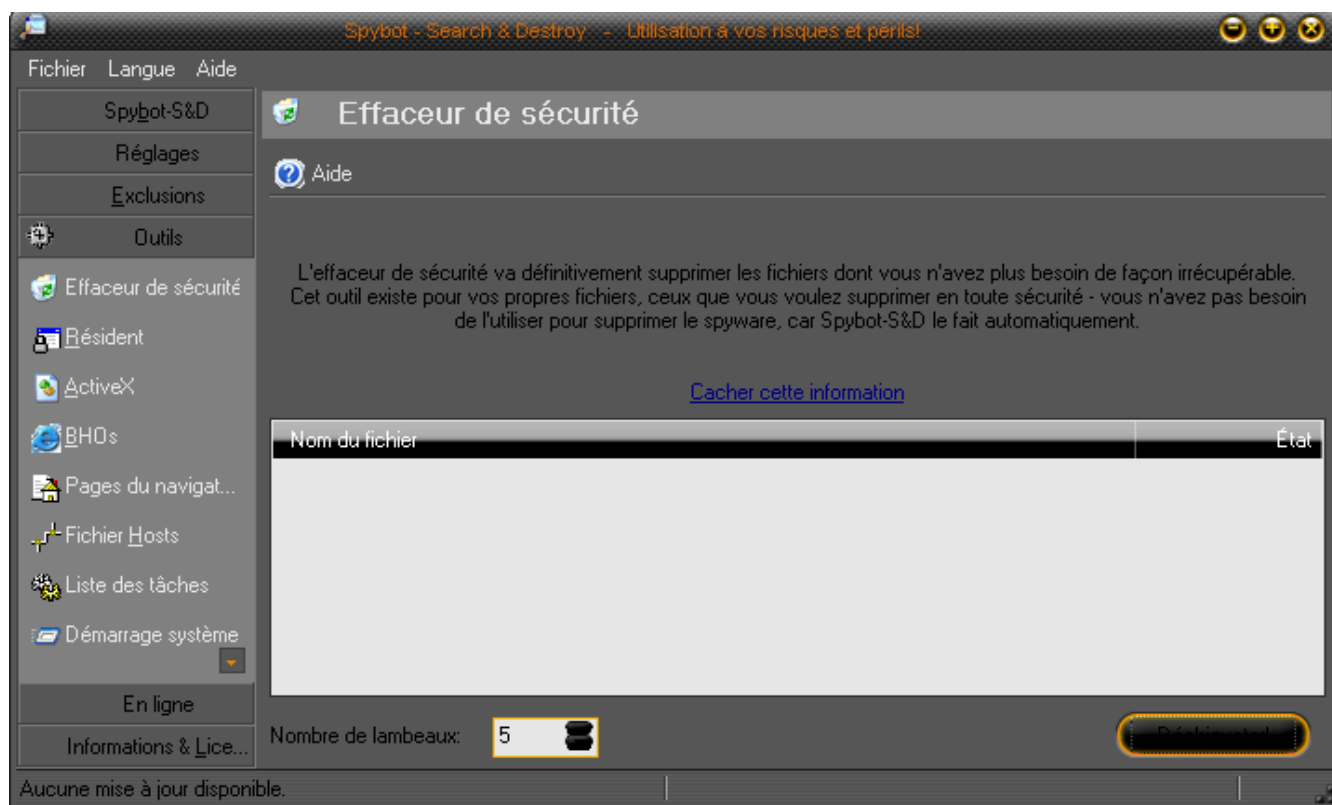
3 Ecran OUTILS

Outils-ActiveX



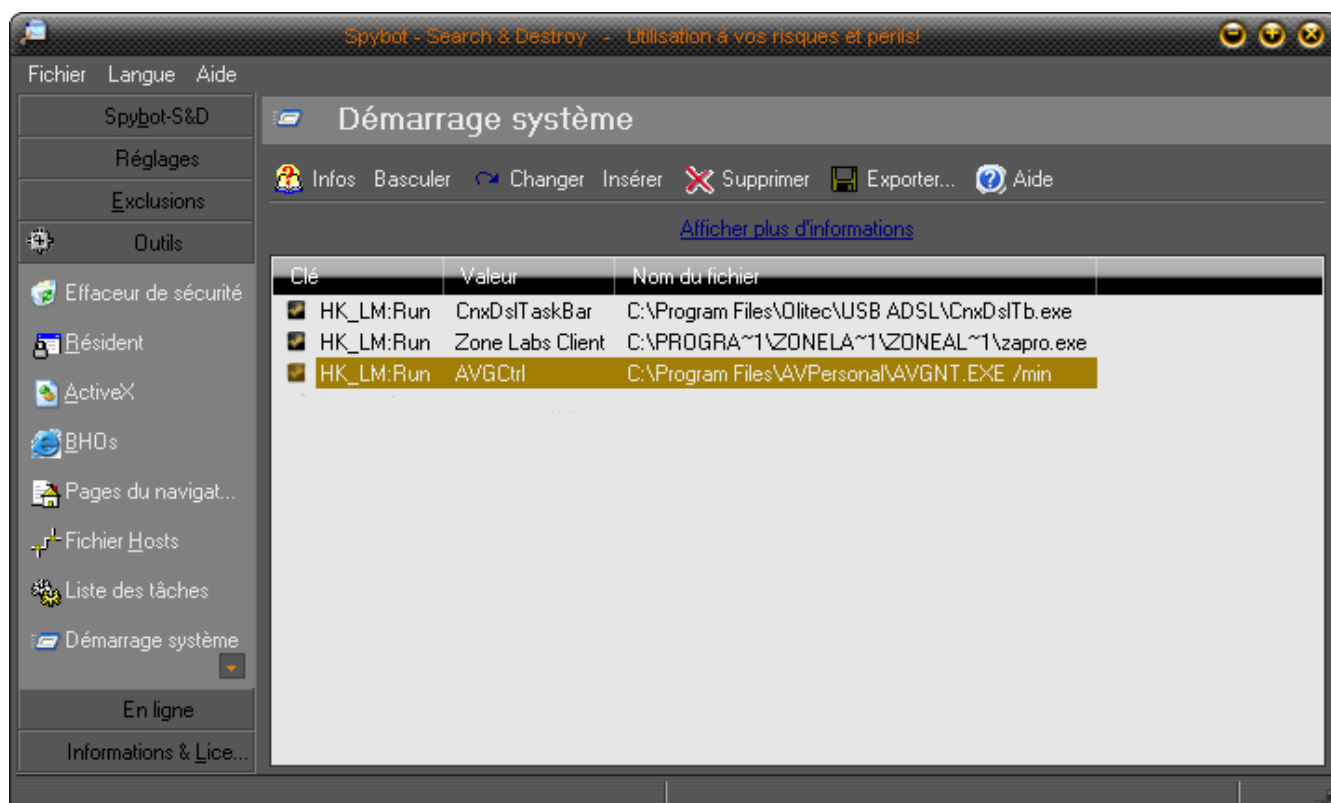
Cet écran permet de visualiser les contrôles ActiveX présents sur votre PC, ceux avec un "V vert" indiquent l'élément comme "légal", ceux avec un "V rouge" indiquent l'élément comme "néfaste", ceux sans indication ne sont pas encore dans la base de données. (vérifiez leurs chemins)

Outils -Effaceurs



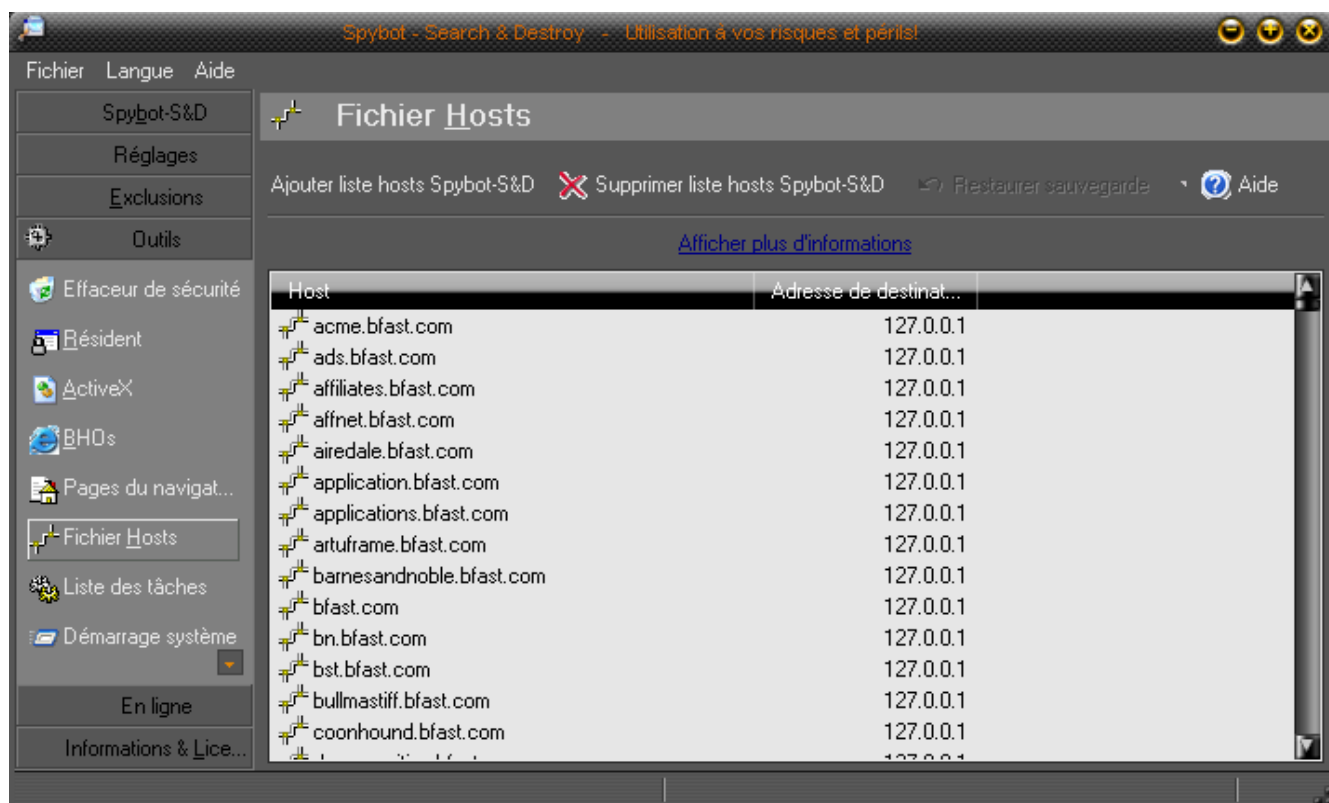
Cet outil supprime des fichiers de façon définitive, il suffit de faire un **”glisser- déposer”** du fichier depuis votre explorateur, Spybot se chargera de le supprimer en même temps que le nettoyage.

Outils - Démarrage



Remplace la fenêtre de ” **démarrage de MSCONFIG**” , il vous permet de visualiser les programmes chargés au démarrage de votre session, vous pouvez les supprimer ou en ajouter à partir de là.

Outils -HOSTS



Si vous n'avez pas de fichier "hosts" autre que celui installé par défaut dans Windows, je vous conseille d'en télécharger un, l'intérêt d'un tel fichier réside dans le fait que vous pouvez bloquer des sites indésirables pendant votre surf (tous les sites publicitaires ou les pop-up indésirables qui en font partie et qui s'ouvrent sans votre permission).

Mais qu'est-ce que c'est "hosts" ?

[Hosts est un carnet d'adresses IP dans un fichier qui agit comme un serveur DNS (Domaine Name Server) utilisé en local. Lorsque vous entrez une adresse comme `http://www.tf1.fr/` dans votre navigateur, le fichier **Hosts** est consulté pour voir si vous avez l'adresse IP correspondant à ce site. Si elle est trouvée, votre ordinateur l'appelle et ouvre le site.

S' il ne la trouve pas, c'est le serveur DNS de votre FAI qui la fournit.

Chaque PC a sa propre adresse IP qui se nomme "localhost" avec l'adresse IP **127.0.0.1**, elle est utilisée pour se reporter à elle-même en local.

Donc tous les noms des sites associés à cette adresse IP seront automatiquement renvoyés à votre PC, et votre PC n'ira pas sur le réseau pour rechercher les adresses inscrites et de ce fait n'ouvrira pas les pages associées à l'adresse IP **127.0.0.1**

Exemple :127.0.0.1 localhost

127.0.0.1 tf1.fr n'ira pas chercher la page sur le réseau et n'ouvrira pas la page associée (donc la page sera bloquée) 195.68.47.6 tf1.fr ouvrira la page de tf1 sans passer par le serveur DNS de votre FAI Si tf1 n'est pas indiqué dans votre fichier hosts, c'est le serveur DNS de votre FAI qui prendra le relais et permettra d'ouvrir la page de TF1

Voici un fichier hosts à télécharger <http://www.mvps.org/winhelp2002/hosts.zip>

Il vous suffit de remplacer votre fichier "hosts" par celui que vous venez de télécharger à l'endroit indiqué ci-dessous. Par la suite, vous pouvez ajouter ou supprimer des adresses dans la

liste afin de l'adapter à votre surf.

Le fichier HOSTS se trouve dans :

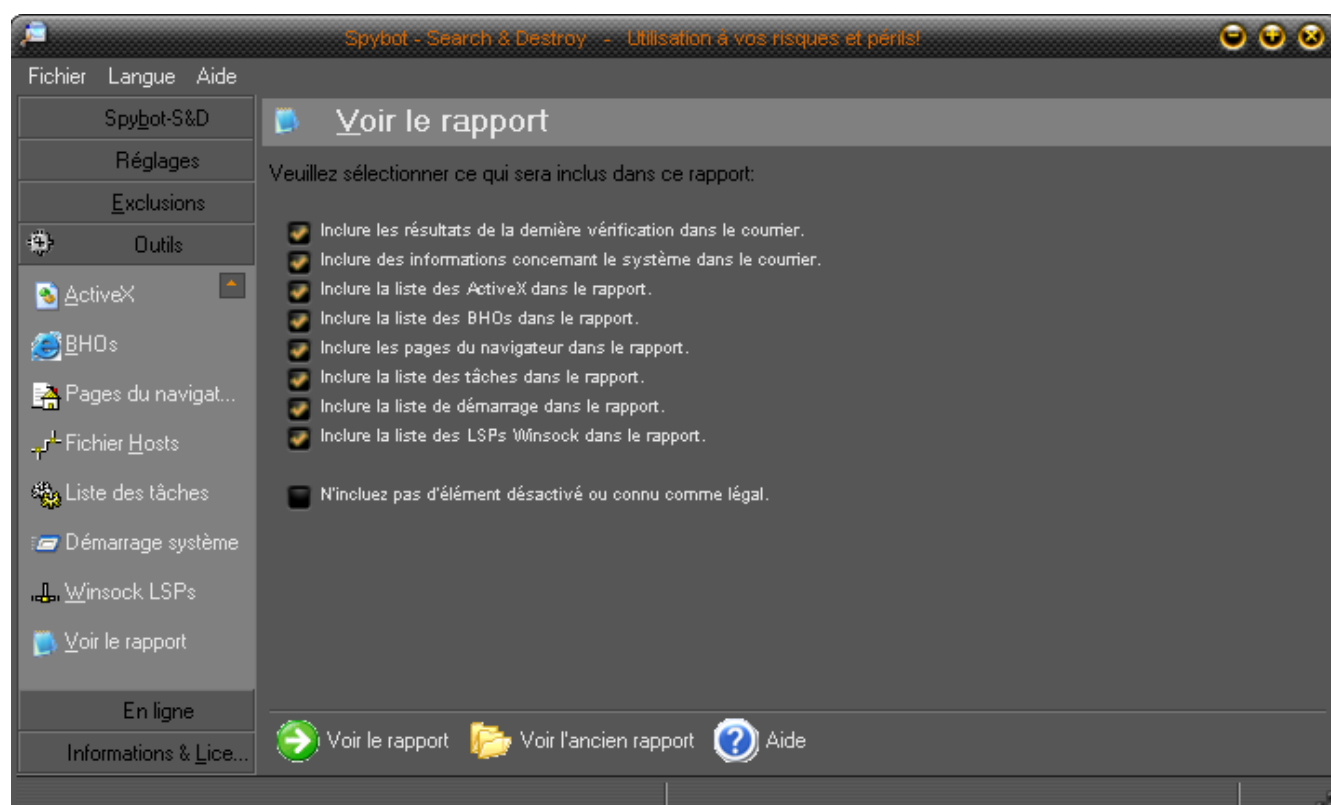
Windows XP = C :32

Windows 2K = C :32

Win 98= C :

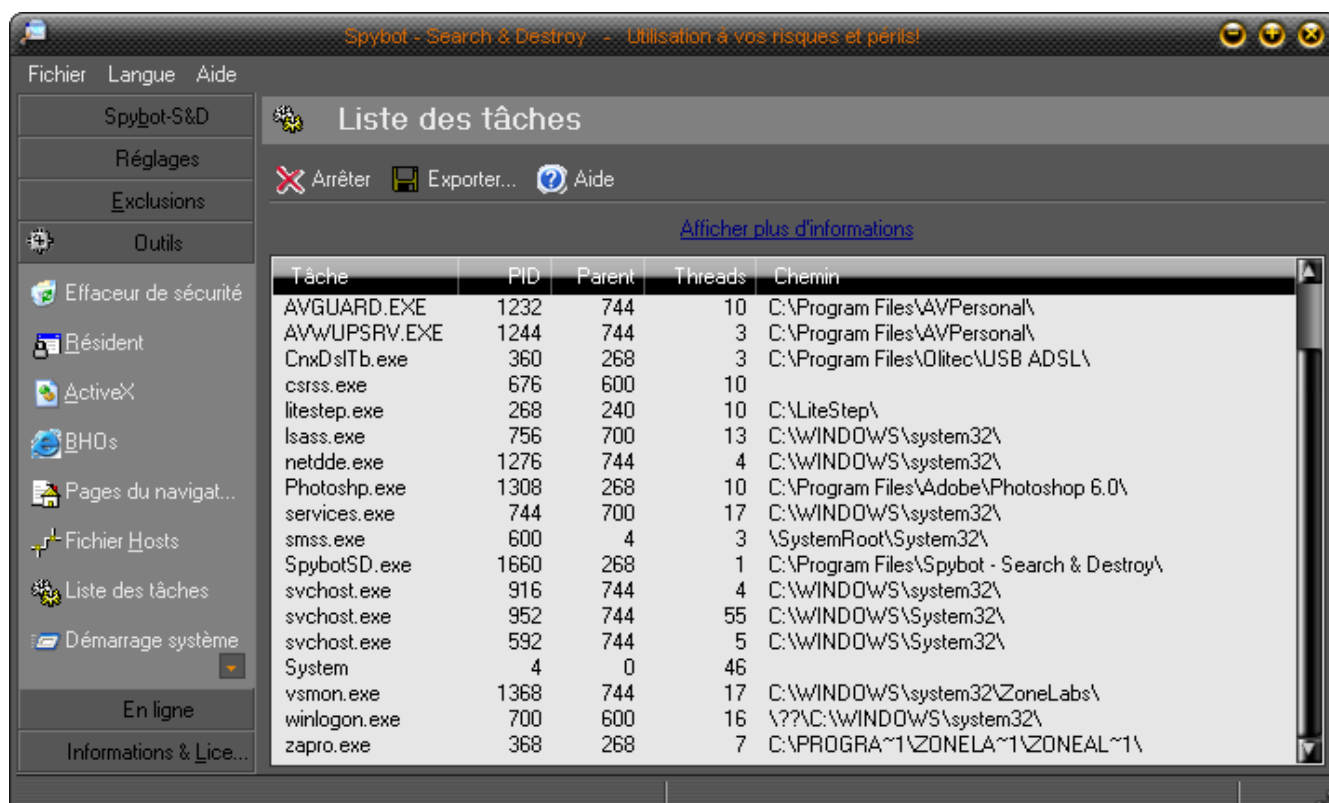
Pour en savoir plus sur le fichier HOSTS : <http://speedweb1.free.fr/frames2.php?page=securite10>

Outils-rapports



Permet de mettre diverses informations concernant votre machine, je vous conseille d'activer toutes les options, vous pouvez visualiser le rapport en cliquant sur la touche **”Voir le rapport”** ou visualiser tous les anciens rapports existants depuis l'installation du logiciel

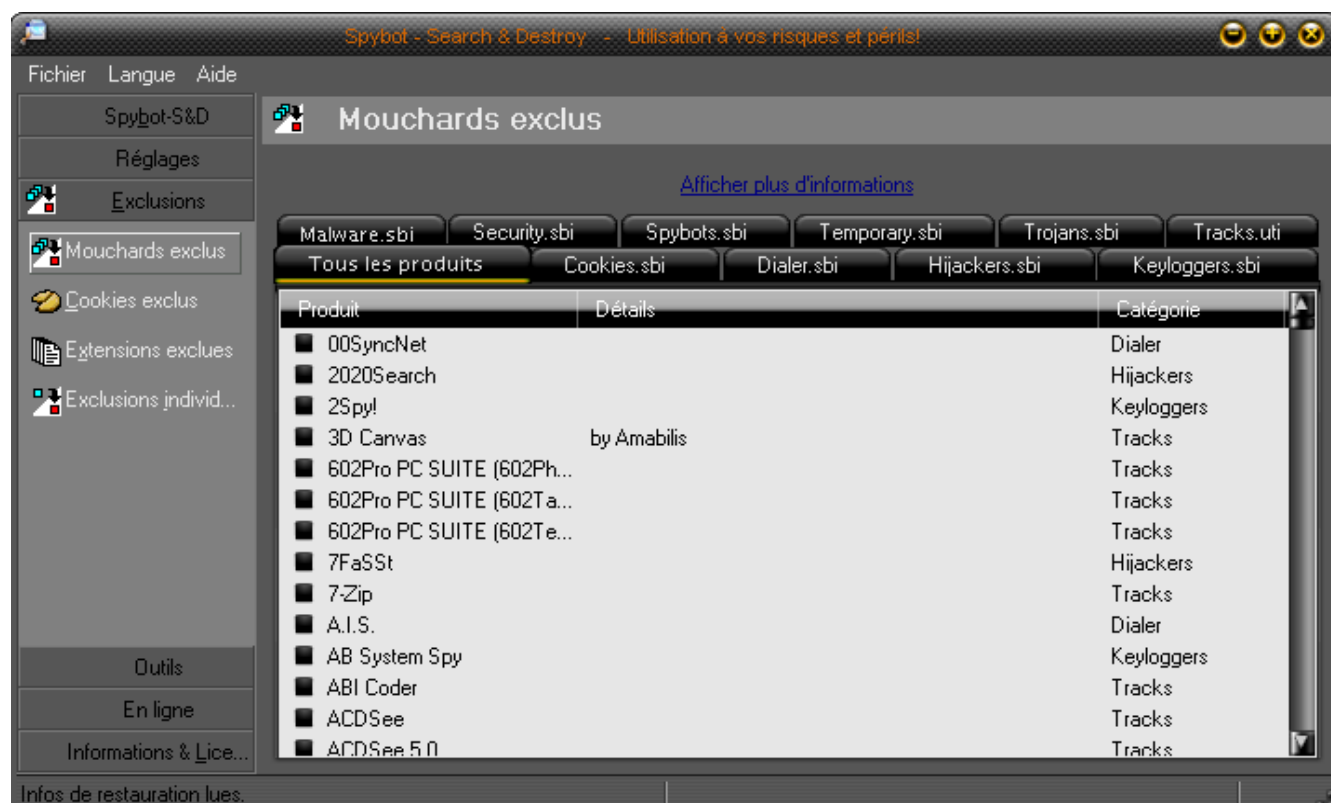
Outils - Tâches



Vous permet de visualiser les processus en cours sur votre PC comme le fait le gestionnaire des tâches de Windows, l'avantage, c'est qu'il vous indique le chemin des programmes ouverts.

4 Ecran Exclusions

Exclusions - Mouchards



Ces diverses listes de programmes et mouchards connus, vous permettent d'en désactiver un ou plusieurs .

Pourquoi débloquent un mouchard ?

Il arrive parfois que spybot bloque sur l'analyse d'un mouchard, retenez son nom, arrêtez l'analyse et venez ici l'exclure afin que le prochain scanne se déroule sans encombre.

les autres options :

- Exclusion des cookies :

Donne la liste des cookies déjà exclus de votre navigateur, il ne seront pas détruits pendant la phase de nettoyage.

- Extension exclues :

Donne la liste des extensions de programmes déjà exclues, les fichiers ayant cette extension ne seront pas détruits pendant la phase de nettoyage

-Exclusion individuelle :

Ici, c'est vous qui mettez des fichiers à exclure de l'analyse

5 Information Licence

Infos mouchards



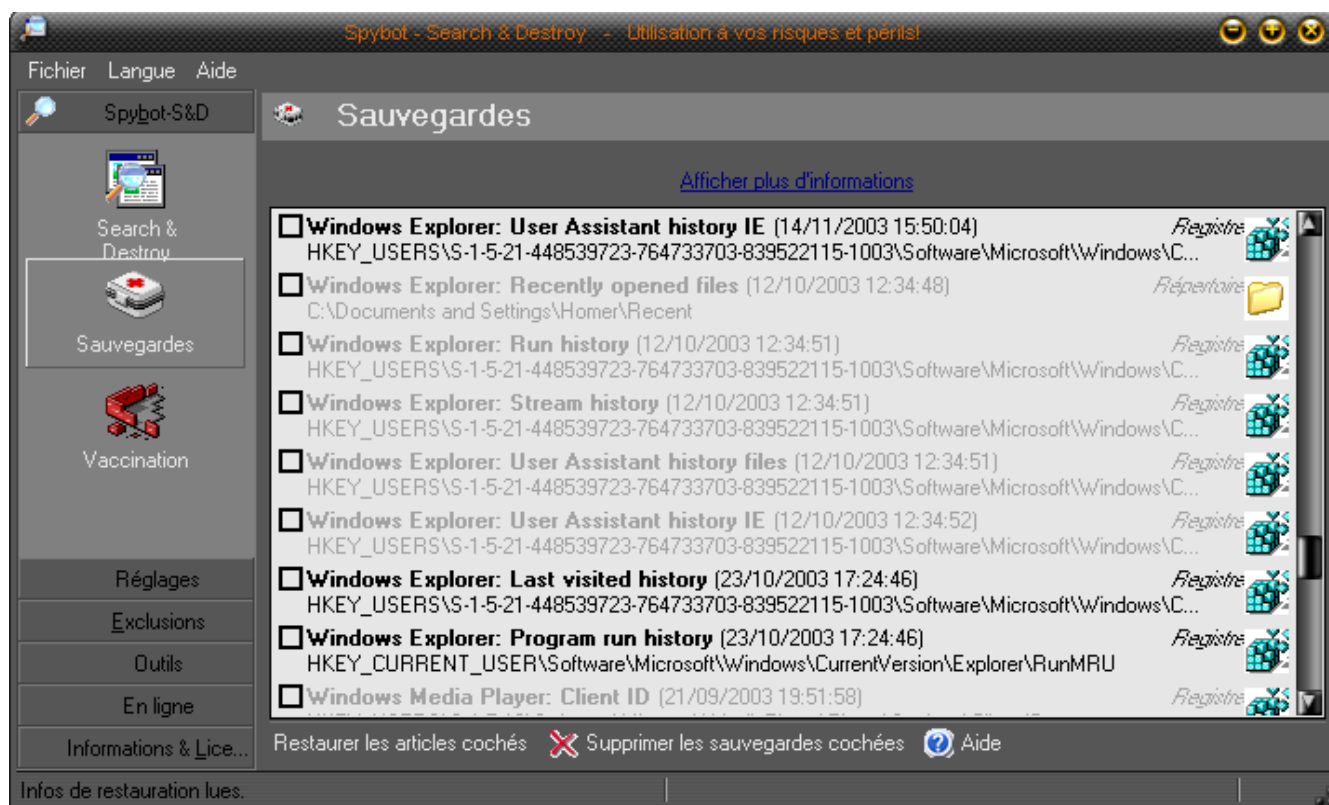
C'est la base de connaissance de spybot, chaque mouchard est inscrit avec les diverses informations le concernant, **très instructif!!** Avant de supprimer une entrée, vous pouvez chercher le nom du mouchard ici, et voir quelles sont ses intentions!

Dons

Ce logiciel est gratuit (Freeware), mais rien ne vous empêche d'envoyer un don pour la continuation de son développement .

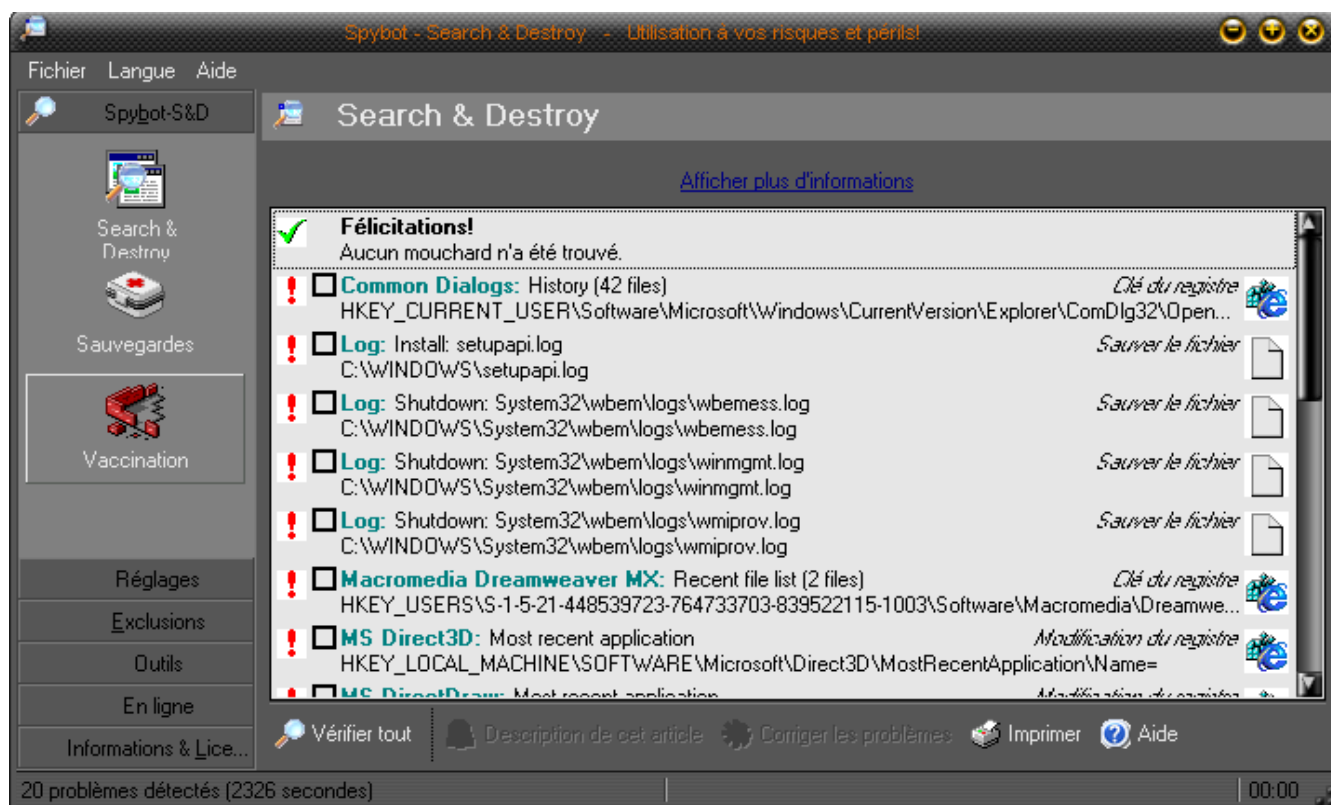
6 Ecran D'Accueil

Sauvegarde

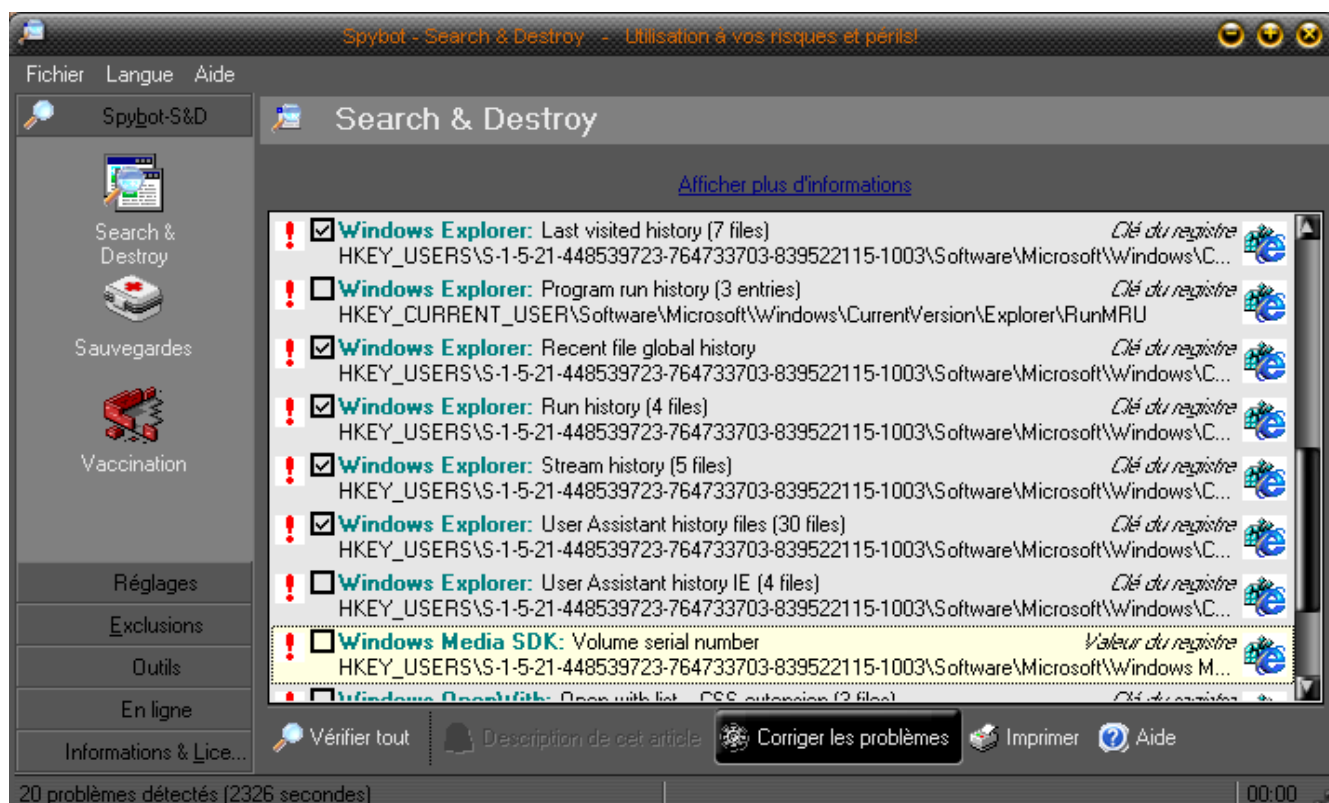


Nous voici de retour à la page d'accueil, c'est ici que vous pouvez restaurer une entrée supprimée si par exemple, votre système est devenu instable depuis ce nettoyage. Voilà, nous avons fait le tour des options et du logiciel, passons aux choses sérieuses. Le nettoyage, c'est parti.

Nettoyage



Sur la page d'accueil toujours, cliquez sur **"Vérifier tout"**, le résultat s'affiche au fur et à mesure des entrées contaminées trouvées. **Corriger les problèmes**



Une fois l'analyse effectuée, si tout s'est bien passé, il vous félicite ! Sinon, vous aurez une liste d'espions trouvés, souvent impressionnante quand c'est la première analyse !

Pour le reste, les entrées trouvées sont principalement des fichiers de logs de certains logiciels, il suffit juste de supprimer les entrées corrompues, certaines entrées peuvent être réparées dans la base de registre, ce sont souvent des clés invalides ou obsolètes, spybot vous préviendra.

Votre PC, sera reconnaissant de ce nettoyage.

A ce jour, depuis que j'utilise Spybot-SD, je n'ai jamais rencontré de dysfonctionnement de mon PC après nettoyage. Maintenant que votre PC est propre, bon surf à tous

Tesgaz le : 03/12/2003