

Guide Nous aimons vous aider - pourquoi ne pas faire un don?



Forums



Support



Télécharger



Donner

[lien]

Présentation

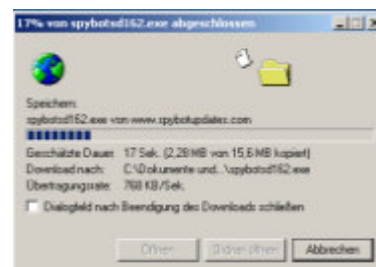
Ceci est un petit guide pour vous montrer les premières étapes à suivre pour supprimer de votre ordinateur les espioniciels (*le Spyware*) et d'autres cochonneries grâce à Spybot-Search&Destroy.

1. Télécharger

[lien]

Évidemment, la première chose que vous devez faire est de télécharger Spybot-S&D depuis notre page de téléchargement.

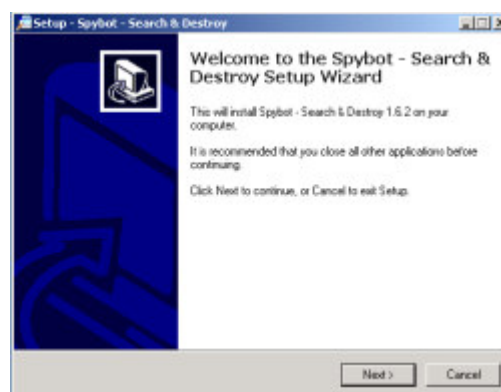
La page de téléchargement vous donne d'abord quelques informations sur les dons; si vous aimez le programme, je vous encourage à y revenir et à donner quelque chose. Mais en ce moment, vous voulez télécharger. Les téléchargements sont sur la même page, descendez de quelques lignes et cliquez sur *Spybot - Search & Destroy 1.6.2*. Sur la page suivante vous verrez une table avec quatre emplacements de téléchargement. Cliquer sur l'un d'eux vous amènera sur une page vous proposant de télécharger. Ces pages sont légèrement différentes les unes des autres, mais vous devriez pouvoir y trouver le lien de téléchargement sans problème.



2. Installation

[lien]

Le fichier que vous avez téléchargé s'appelle *spybotsd162.exe* ou quelque chose de similaire. Pour installer Spybot-S&D, tout ce que vous avez à faire est d'exécuter ce fichier, et le programme d'installation commencera (si vous l'avez téléchargé avec Internet Explorer, la boîte de dialogue de téléchargement vous a donné l'option de l'ouvrir directement). L'installateur vous montrera la licence et vous demandera l'emplacement d'installation. Vous pouvez conserver les réglages par défaut et continuer l'installation en cliquant sur le bouton *Suivant (Next)*.



Après la fin de l'installation, vous verrez une icône *Spybot - Search & Destroy* sur votre bureau et une ligne dans votre menu Démarrer. Cliquez dessus pour lancer Spybot-S&D pour la première fois.

3. La 1ère fois

[lien]

La première fois que vous lancez Spybot-S&D, il affichera un *Assistant*, une petite fenêtre qui vous aidera dans vos premiers pas. Celle-ci vous donne la possibilité d'ajouter ou d'enlever les icônes que vous avez ou non créées pendant l'installation, par exemple. Disons que vous voulez les garder, et passons à la page suivante.





Si vous utilisez un proxy dans Internet Explorer, Spybot-S&D vous affichera ce proxy et un bouton vous donnera la possibilité de l'utiliser également pour Spybot-S&D. Si la zone de texte est vide, vous n'en avez pas besoin, mais dans la plupart des cas elle affichera une adresse internet, et vous devriez conserver ce paramètre de proxy.

La page suivante traite les mises à jour. Il est très important d'être à jour. Les deux boutons situés sur cette page feront ces mises à jour, mais si vous voulez les faire ultérieurement, lisez ceci.

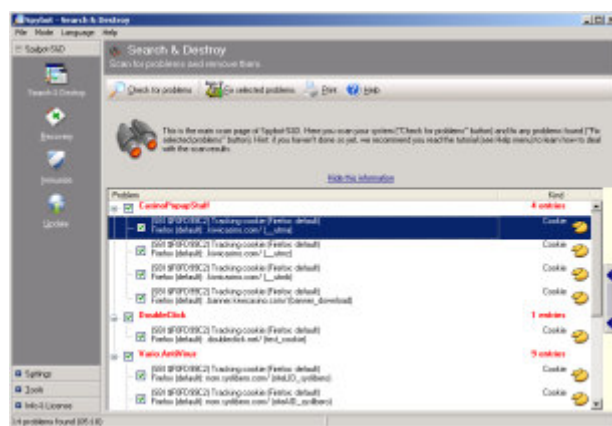
La dernière page des Astuces vous demande de lire le fichier d'aide. Le fichier d'aide est toujours une mine d'infos si vous ne savez pas quoi faire, donc lisez-le, ou au moins ses premières pages.

4. Effectuer un balayage

[lien]

Après la fin de ce guide, vous pouvez vous retrouver sur la page *Réglages* ou sur la page *Mise à jour*. Comme les réglages par défaut sont corrects pour le moment, et que vous avez déjà fait une mise à jour, ignorons-les pour l'instant et lançons le premier balayage.

La partie gauche du programme affiche une barre de navigation qui peut vous amener vers toutes les fonctions du programme. La première section (le bouton du haut) s'appelle *Spybot-S&D* et vous amène sur la page principale. En ce moment, vous ne voyez qu'une liste vide et une barre d'outils en bas. Le premier bouton de cette barre d'outils s'appelle *Vérifier tout* - c'est le bouton sur lequel vous devez cliquer pour lancer le balayage. Appuyez-vous sur votre dossier et regardez la progression de la recherche.



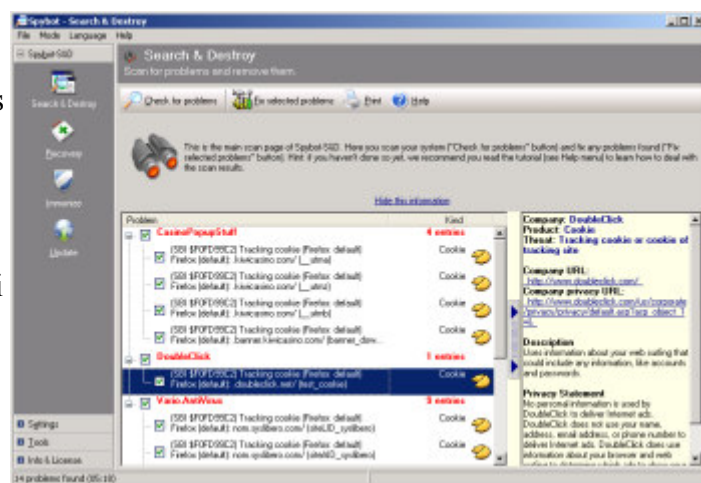
5. Interpréter les résultats

[lien]

Arrivé là, vous pourriez sauter directement au point 7, et supprimer les résultats. Au lieu de cela, nous vous conseillons de jeter un œil sur tous les trucs que Spybot-S&D a détectés. La première chose est de faire la distinction entre les **lignes en rouge**, qui représentent le **spyware** et les menaces similaires, et les **lignes en vert**, qui sont des **traces d'utilisation**.

Pour les traces d'utilisation (j'espère que vous avez suivi le lien pour voir à quoi cela correspond), la suppression n'est pas critique, mais dépend de vos préférences personnelles.

En laissant de côté pour l'instant les traces d'utilisation, vous devriez regarder les lignes en



rouge qui représentent les vraies menaces. Bien que vous puissiez bien sûr nous faire confiance sur le fait que nous avons choisi les cibles en utilisant des critères stricts, vous pouvez le vérifier vous-même en faisant un clic droit sur chaque produit et en lisant l'information produit qui s'affiche dans une nouvelle fenêtre en pop-up.

6. Créer des exceptions

[lien]

Tous les problèmes affichés en **rouge** sont considérés comme de **vraies menaces**, et on devrait s'en occuper. Mais en lisant la description du produit, vous pouvez malgré tout décider de conserver une menace, ou seulement une trace d'utilisation. Peut-être ne voulez-vous pas effacer la liste des derniers fichiers utilisés dans Word? Pour cela, vous avez trois options.

- Vous pouvez décider d'ignorer toutes les traces d'utilisation. Dans ce cas, ouvrez la page *Modules additionnels* dans la section *Réglages* du programme, et désactivez la ligne *Traceurs d'utilisation*.
- Ou si vous voulez juste garder toutes les traces d'un produit particulier, faites seulement un clic droit dessus dans la liste des résultats.
- Finalement, si vous ne voulez garder qu'un seul fichier, c'est possible de la même façon.

7. Supprimer les menaces trouvées

[lien]

Maintenant, vous êtes au courant de tout ce que vous avez trouvé. C'est le moment d'utiliser le bouton *Corriger les problèmes*.

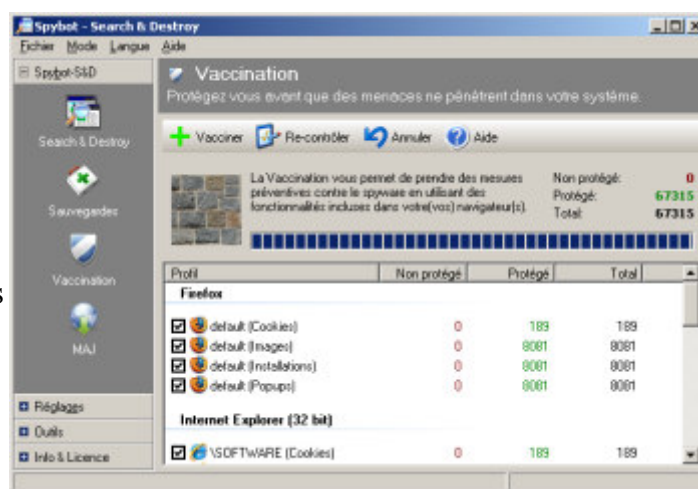
Si vous pensez supprimer aussi les traces d'utilisation, vous pouvez trouver que cocher toutes les lignes en vert est un sacré boulot. C'est pour une raison très simple - vous obliger, vous le débutant - à regarder les résultats. Une fois que vous saurez ce que vous êtes en train de faire, il existe un bouton caché Cocher tous les problèmes.

8. Résident

[lien]

Si vous utilisez la protection en temps réel de Spybot-S&D contre les espioniciels (spyware), les mauvais espions ne rentreront pas dans votre système. Actuellement il existe trois types de protection différents.

La fonction **Vaccination** empêche par exemple les cookies traceurs de rentrer dans votre système. La Vaccination fonctionne avec Mozilla Firefox, Internet Explorer et Opera, et vous permet de régler certains paramètres du navigateur de façon à bloquer des installateurs d'espioniciels connus, (et des nuisibles similaires), déjà inscrits dans la base de données de Spybot-S&D. Vous activez la fonction Vaccination en cliquant sur *Spybot-S&D* → *Vaccination* dans la barre de navigation sur la gauche.

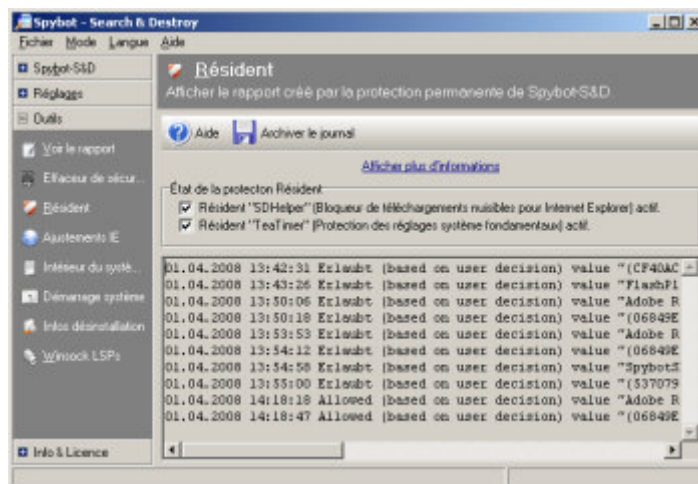


Résident SDHelper est une deuxième couche de protection pour IE. La fonction Vaccination

bloque les installeurs selon l'ID (*identifiant*) de leur ActiveX, tandis que SDHelper bloque les nuisibles qui essaient de rentrer en utilisant une autre méthode. Ainsi Internet Explorer ne peut pas télécharger de fichiers néfastes. Vous activez SDHelper en cliquant sur *Outils* → *Résident* dans la barre de navigation sur la gauche (pour cela Spybot-S&D doit être exécuté en *mode Avancé*). Là vous pouvez cocher la case située devant *Résident SDHelper* "(Bloqueur de téléchargements nuisibles pour Internet Explorer) actif afin d'activer SDHelper.

Résident TeaTimer empêche que des fichiers indésirables soient installés – peu importe comment – sur votre système. Il surveille en permanence les processus appelés/lancés. Si des processus connus pour être malicieux veulent démarrer, TeaTimer les arrête immédiatement, et vous donne le choix entre trois options sur la façon de traiter ce processus à l'avenir:

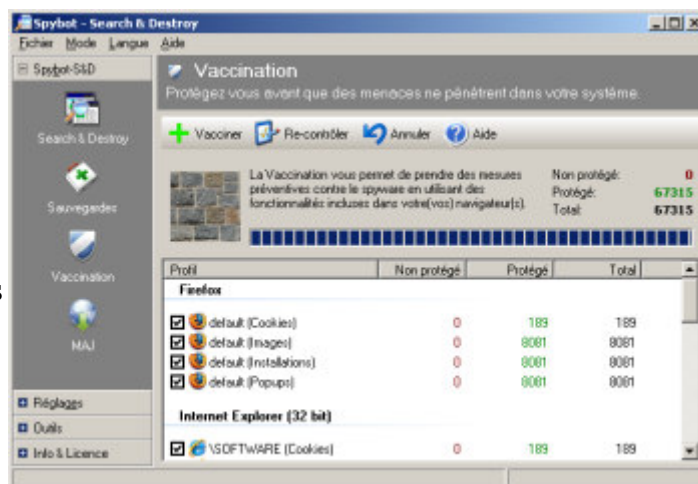
- être averti si le processus veut de nouveau démarrer
- tuer automatiquement le processus
- autoriser l'exécution du processus



Il y a aussi la possibilité de supprimer le fichier associé à ce processus.

Si vous utilisez la protection en temps réel de Spybot-S&D contre les espioniciels (spyware), les mauvais espions ne rentreront pas dans votre système. Actuellement il existe trois types de protection différents.

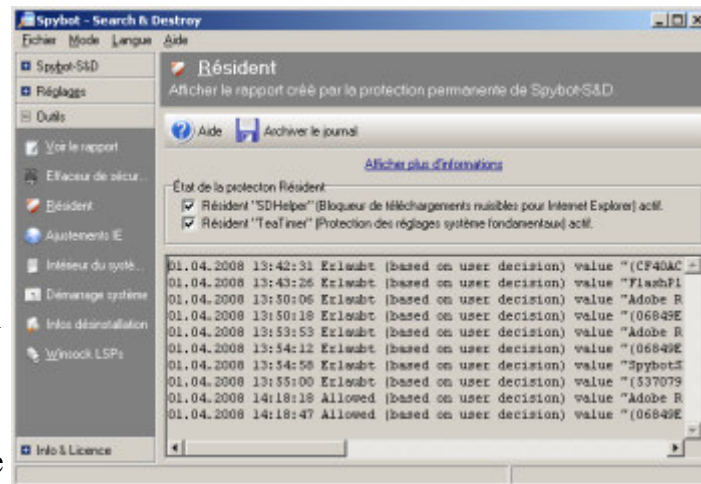
La fonction **Vaccination** empêche par exemple les cookies traceurs de rentrer dans votre système. La Vaccination fonctionne avec Mozilla Firefox, Internet Explorer et Opera, et vous permet de régler certains paramètres du navigateur de façon à bloquer des installeurs d'espioniciels connus, (et des nuisibles similaires), déjà inscrits dans la base de données de Spybot-S&D. Vous activez la fonction Vaccination en cliquant sur *Spybot-S&D* → *Vaccination* dans la barre de navigation sur la gauche.



Résident SDHelper est une deuxième couche de protection pour IE. La fonction Vaccination bloque les installeurs selon l'ID (*identifiant*) de leur ActiveX, tandis que SDHelper bloque les nuisibles qui essaient de rentrer en utilisant une autre méthode. Ainsi Internet Explorer ne peut pas télécharger de fichiers néfastes. Vous activez SDHelper en cliquant sur *Outils* → *Résident* dans la barre de navigation sur la gauche (pour cela Spybot-S&D doit être exécuté en *mode Avancé*). Là vous pouvez cocher la case située devant *Résident SDHelper* "(Bloqueur de téléchargements nuisibles pour Internet Explorer) actif afin d'activer SDHelper.

Résident TeaTimer empêche que des fichiers indésirables soient installés – peu importe comment – sur votre système. Il surveille en permanence les processus appelés/lancés. Si des processus connus pour être malicieux veulent démarrer, TeaTimer les arrête immédiatement, et vous donne le choix entre trois options sur la façon de traiter ce processus à l'avenir:

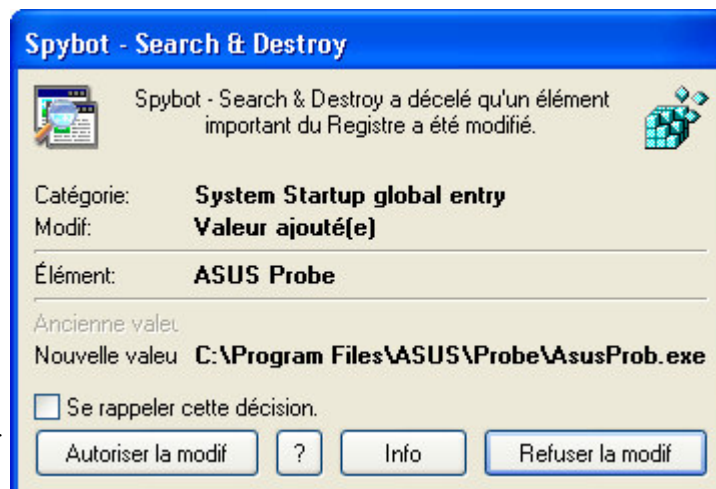
- être averti si le processus veut de nouveau démarrer
- tuer automatiquement le processus
- autoriser l'exécution du processus



Il y a aussi la possibilité de supprimer le fichier associé à ce processus.

Si quelque chose essaie de modifier des clés de Registre cruciales, TeaTimer le détectera. TeaTimer peut vous protéger contre de telles modifications en vous donnant le choix: Vous pouvez soit *Autoriser* soit *Refuser* la modification. TeaTimer tourne en permanence en arrière-plan.

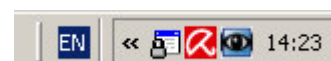
Depuis Spybot-S&D 1.6, TeaTimer utilise notre base de données dans laquelle les fichiers sont classés comme bons ou dangereux. Cette base de données contient plusieurs centaines de milliers d'éléments et s'accroît en permanence. Néanmoins, de temps en temps il y a des fichiers qui n'y sont pas encore inscrits. Dans ce cas, et également si vous utilisez d'anciennes versions de Spybot-S&D, Résident TeaTimer va vous demander votre autorisation pour chaque modification. Si vous n'êtes pas certain(e) de devoir autoriser cette modification, voici un simple principe de base:



Si vous êtes en train d'installer quelque chose et/ou si vous estimez que le fichier qui doit être installé est bon parce que vous connaissez son nom, vous pouvez continuer en autorisant la modification du Registre (il en est de même si vous ou Spybot-S&D êtes en train de supprimer une application). Mais si le message surgit à l'improviste pendant que vous surfez sur le web, vous devriez vous méfier. Dans ce cas il est préférable de refuser la modification du Registre.

Vous activez Résident TeaTimer en cliquant sur *Outils* → *Résident* dans la barre de navigation sur la gauche (Spybot-S&D doit s'exécuter en *Mode Avancé*). Là vous pouvez cocher la case située devant *Résident TeaTimer* ("Protection des réglages système fondamentaux) actif afin d'activer TeaTimer.

Bien entendu, il est possible de changer chaque décision que vous



avez prise. Cela peut s'avérer nécessaire si vous avez refusé un processus qui ultérieurement se révèle être utile. Pour ce faire, il suffit de faire un clic droit sur l'icône de TeaTimer dans la Zone de notification - c'est celle qui est bleue avec un cadenas. (Si vous ne voyez pas cette icône, c'est probablement parce qu'elle est masquée. Cliquez simplement sur les flèches "<<" de la Zone de notification pour afficher toutes les icônes masquées.) Dans la petite fenêtre qui apparaît, cliquez sur *Réglages* pour modifier votre liste des modifs de registre et processus autorisés/bloqués.

Aperçu de l'article

- Comment reprendre une sauvegarde du Registre
- Comment désactiver temporairement Spybot-S&D
- Comment télécharger Spybot-S&D
- Comment exclure un produit de la recherche
- Comment désactiver le proxy
- Comment effectuer une restauration
- Comment activer le bouton *Tout sélectionner*
- Comment exporter la liste de démarrage
- Comment modifier la langue
- Comment désinstaller
- Comment mettre à jour