SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

Site : http://aviquesnel.free.fr/Mederic

9 mars 2009

Numéro 94

Sommaire

Le Service Pack SP2 RC de Vista disponible pour le grand public

A peine quelques jours après l'avoir mis à disposition des testeurs des programmes MSDN et Technet, le Service Pack 2 en version Release Candidate (SP2 RC) de Windows Vista est déjà disponible pour le grand public.

C'est aussi le cas du SP2 RC de Windows Server 2008 et tous deux sont téléchargeables sur cette page ou directement via Windows Update via l'installation d'un outil supplémentaire disponible ici .

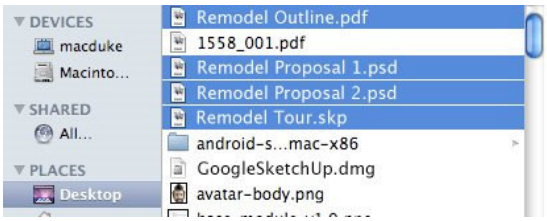
Il donne aussi quelques indications sur les changements majeurs qu'introduisent ces versions, les plus signifiants étant la gravure de disque blu-ray en standard, l'intégration du stack de connexion Bluetooth 2.1 et l'arrivée du moteur de recherche Windows Search 4.0.

Mise à jour de FireFox en version 3.0.7

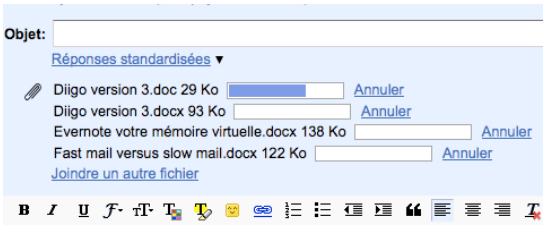
Le 4 mars, Mozilla a également publié une mise à jour pour Firefox, la version 3.0.7. Celle-ci corrige 8 vulnérabilités, dont 6 qualifiées de critiques. Ces bugs affectent principalement l'utilisation de mémoire par les extensions, les librairies PNG et le moteur JavaScript. Selon Mozilla, des attaquants pourraient, dans certaines circonstances, s'appuyer sur des corruptions mémoire pour exécuter arbitrairement du code.

Avec GMail charger plusieurs pièces jointes simultanément

Une nouvelle fonction vous permet de charger plusieurs pièces jointes simultanément sur GMail. Lorsque vous rédigez un courriel sur GMail et que vous sélectionnez “Joindre un fichier” une fenêtre vous permettant de sélectionner vos fichiers apparaîtra.



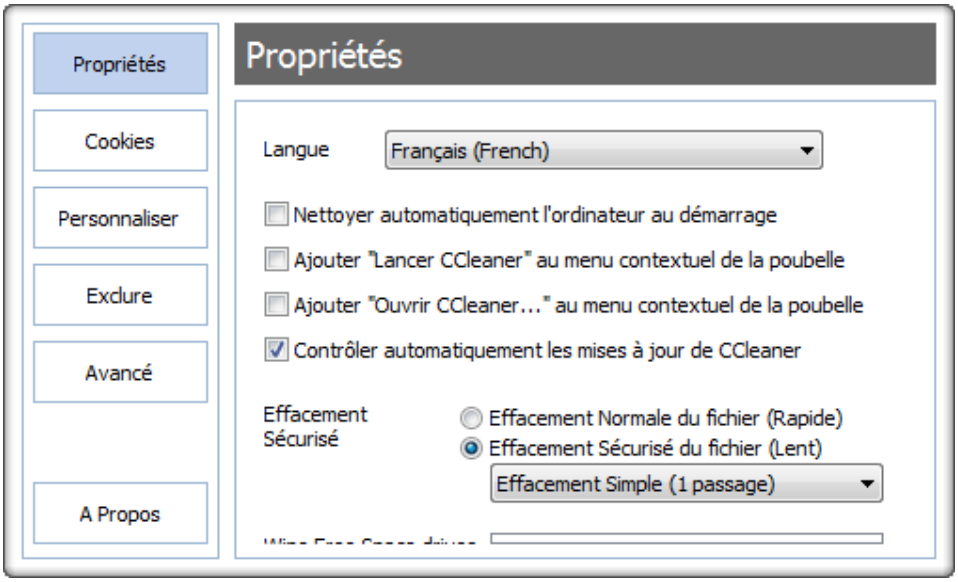
Pour charger plusieurs fichiers, vous n'avez qu'à appuyer sur la touche Cmd (Pomme) sur Mac et Ctrl sous Windows et sélectionner vos fichiers. Vous verrez vos fichiers apparaître sur votre courriel. Une jauge de progression vous permettra de connaître l'état de chargement de vos pièces jointes.



Si vous êtes incapable d'avoir accès à la fenêtre vous permettant de charger plusieurs fichiers simultanément, débranchez-vous de votre compte GMail et reconnectez-vous à nouveau. Il était déjà possible de charger plusieurs documents en pièce jointe sur GMail en utilisant le module dragdropupload. Mais cette nouvelle fonction native facilite grandement le chargement des pièces jointes

Effacement sécurisé des données avec CCleaner

Le logiciel de nettoyage **CCleaner** est doté d'une fonctionnalité intéressante apparue il y a quelques temps déjà. En effet, cet outil permet la suppression sécurisée de vos données. Pour activer cette option, il suffit de se rendre dans l'onglet "Propriétés" des options du logiciel. Vous aurez alors la possibilité de sélectionner l'option **Effacement Sécurisé** afin que les données supprimées le soient définitivement, sans pour autant qu'il soit possible par la suite de récupérer ces informations à l'aide d'un logiciel spécialisé (comme Recuva du même éditeur par exemple).



La suppression définitive des données se fait par des réécritures puis effacements successifs de données aléatoires à l'emplacement des fichiers supprimés. Le logiciel dispose pour cela de quatre algorithmes différents qu'il vous sera possible de choisir (simple, DOD 5220.22-M, NSA ou Gutmann). Ainsi, le nombre de passages pourra varier de 1 à 35. Bien entendu, une telle suppression demandera beaucoup plus de temps qu'un effacement classique et non sécurisé.

Mais la dernière version du logiciel CCleaner estampillée 2.17 apporte également de nouvelles fonctionnalités, voyez plutôt :

- Nouvelle fonctionnalité "**Wipe Free Space**" (ou *nettoyage de l'espace libre*) présente dans le nettoyage avancé de l'onglet *Windows*
- La barre de progression a été modifiée pour passer de 0 à 100%.
- Amélioration du nettoyage de l'historique de Safari.
- Amélioration de la vitesse de l'outil de désinstallation.
- Ajout de la traduction ukrainienne.
- Modifications mineures dans l'architecture.
- Autres corrections mineures de bugs.

Plus que jamais, CCleaner est un excellent logiciel de nettoyage gratuit qui apporte au travers de cette version de nouvelles fonctionnalités très appréciables.

Spybot Search & Destroy 2008

Spybot - Search & Destroy peut détecter et supprimer plusieurs sortes de spyware de votre ordinateur. Le spyware est une sorte de menace relativement nouvelle que les programmes anti-virus ne traitent pas encore. Si vous voyez des barres d'outils dans votre Internet Explorer que vous n'avez pas installées intentionnellement, si votre navigateur se plante, ou si la page de démarrage de votre navigateur a changé à votre insu, votre PC est probablement infecté par du spyware. Mais même si vous ne voyez rien, vous pouvez être infecté, parce qu'arrive de plus en plus de spyware qui silencieusement suit à la trace votre comportement lorsque vous surfez, de façon à créer votre profil commercial, et à vendre ce dernier à des sociétés de publicité. Spybot-S&D est gratuit, donc il n'y a pas de mal à essayer de voir si quelque chose a farfouillé dans votre ordinateur :)

Spybot-S&D peut aussi effacer les traces d'utilisation, une fonction intéressante si vous partagez votre ordinateur avec d'autres utilisateurs et si vous ne voulez pas qu'ils sachent ce que vous avez fait. Et pour les utilisateurs professionnels, il permet de corriger certaines incohérences du Registre et de créer des rapports complets.

Attention :

SpyBot Search & Destroy est un scanner d'emplacements privilégiés uniquement - il n'analyse absolument pas un ordinateur entier et ne l'a jamais fait. Vous devez compléter le travail de SpyBot Search & Destroy par une analyse de vos fichiers avec un scanner anti-trojans traditionnel comme Ad-Aware et un scanner antivirus traditionnel comm Avast. SpyBot Search & Destroy empêchera les parasites de s'exécuter, de s'identifier dans la base de registre ou dans d'autres emplacements privilégiés, de se lancer automatiquement etc. ... mais les fichiers restent en place.

Dans Réglages > Répertoires, vous pouvez désigner un ou des répertoires à analyser (voire des volumes entiers avec leurs sous-répertoires) .

Cibles : tous les parasites non viraux.Trojans, Backdoors, HackTools, Batch Viruses, Batch Trojans, Internet-Worms, IRC-Worms, email-Worms, Instant-Messaging-Worms, File-sharing Networks Worms, JavaScripts, Webserver-Scripts, VBS-Scripts, Virus-Construction Kits, Denial of Service Tools (DoS), Distributed Denial of Service Tools (DDoS), Flooder, Keylogger, Nuker, Sniffer

- A telecharger sur Clubic ici
- Cliquez sur l'exécutable puis sélectionnez votre langue et cliquez sur OK

- Accepter les termes et cochez Je comprends et j'accepte.....
- Puis cliquez sur Suivant
- Soit vous le modifier en cliquant sur Parcourir et en sélectionnant un en répertoire différent, soit vous le laissez par défaut

- Cliquez ensuite sur Suivant

- Cochez les trois options suivantes : Langues supplémentaires, Skins pour changer l'aspect, Téléchargez les mises à jour immédiatement
- Security Center Integration
- Separate Secure Shredder Application
- Puis cliquez sur suivant

- Laissez tout par défaut
- Puis cliquez sur suivant

Permanent protection

- Cocher Tea Timer
- Cocher SDHelper si vous utilisez Internet Explorer
- Cliquez ensuite sur Suivant

- Vous êtes maintenant prêt à installer Spybot
- Cliquez maintenant sur le bouton Installer

Qu'est-ce que Résident TeaTimer?

Résident TeaTimer est un outil de Spybot-S&D qui surveille en permanence les processus qui sont appelés/lancés. Il détecte immédiatement les processus connus pour être malveillants qui veulent démarrer et les arrête, en vous donnant quelques options sur la façon de traiter ces processus à l'avenir. Vous pouvez demander à TeaTimer:

- de vous informer quand le processus essaiera de démarrer de nouveau
- de tuer automatiquement le processus
- ou d'autoriser l'exécution du processus

Il y a aussi une option pour supprimer le fichier associé à ce processus.

De plus, TeaTimer détecte quand quelque chose veut modifier certaines clés vitales du Registre. TeaTimer peut aussi vous protéger contre de telles modifications en vous donnant le choix: Vous pouvez soit *Autoriser* soit *Refuser* ce changement. Comme TeaTimer tourne en permanence en arrière-plan, il utilise quelques ressources, environ 5 MB.

Résident de Spybot-S&D surveille la création ou la suppression des Browser Helper Objects (qui sont des extensions pour Internet Explorer, augmentant parfois sa fonctionnalité, mais souvent utilisés aussi dans un but malveillant). Un BHO est un petit programme qui ajoute des fonctionnalités à Internet Explorer de Microsoft. Des exemples de BHO sont des barres d'outils additionnelles affichées dans Internet Explorer, mais aussi des fonctions cachées. L'adware et le spyware ainsi que les pirates de navigateur utilisent souvent des BHOs pour

afficher des pubs ou suivre vos traces sur l'internet, parce qu'un BHO a accès à chaque URL que vous visitez et peut vous rediriger, ou afficher d'autres pages que celles que vous avez demandées (des pubs, par exemple).

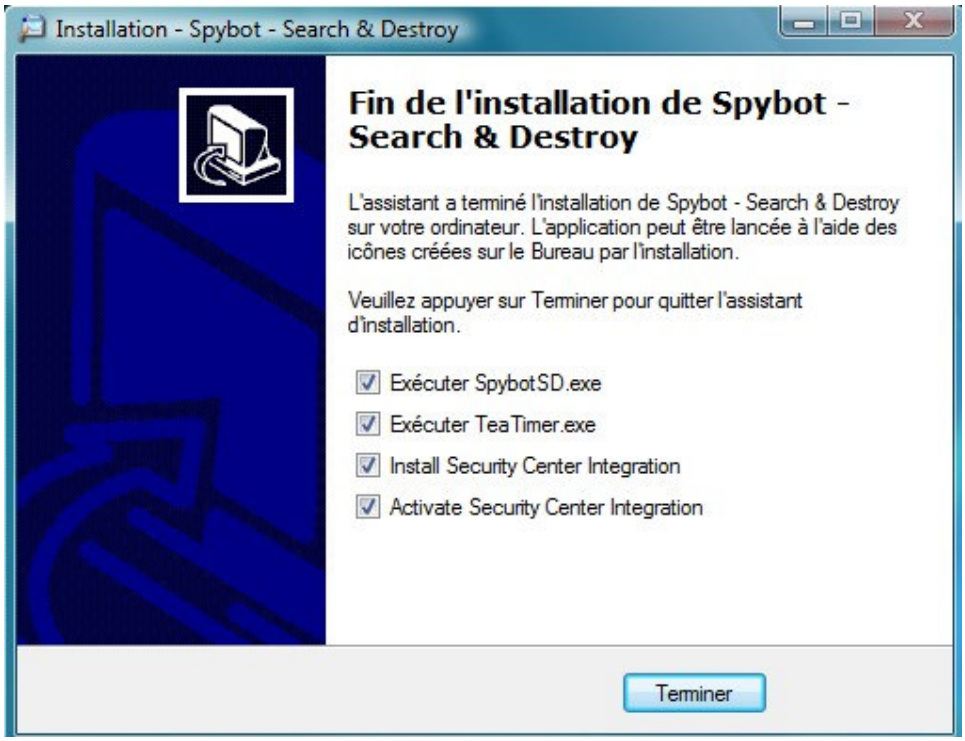
Résident de Spybot-S&D examine toutes les applications qui sont lancées sur votre ordinateur. Il connaît les mêmes fichiers néfastes que le scan à la demande de *Spybot-S&D*, et s'il rencontre une application qu'il sait être une menace, il l'arrêtera automatiquement.

Résident de Spybot-S&D surveille tous les paramètres de pages de démarrage et de recherche, et vous avertit s'ils sont modifiés,

TeaTimer vous signale toute tentative de modification des clés de Registre qu'il surveille, sans préjuger si elle est bonne ou mauvaise. Il y a tellement de clés de Registre qu'il est impossible de les classer par défaut (acceptable ou non). L'utilisateur doit donc décider s'il veut ou non autoriser la modif. TeaTimer crée des fichiers "clichés" (photos instantanées) lorsque vous le lancez pour la première fois, puis l'outil compare l'état actuel du Registre avec les fichiers "clichés".

Si vous voulez créer de nouveaux fichiers "clichés", arrêtez TeaTimer via l'icône de *Résident* puis relancez-le manuellement depuis le dossier d'installation de Spybot S&D (double clic sur TeaTimer.exe). Il n'y a pour l'instant aucune possibilité de masquer les popups qui vous signalent qu'une modif de clé est bloquée/autorisée. La seule façon de contourner cela est de créer de nouveaux fichiers "clichés".

F**in de l'installation** : cocher les 4 propositions présentées

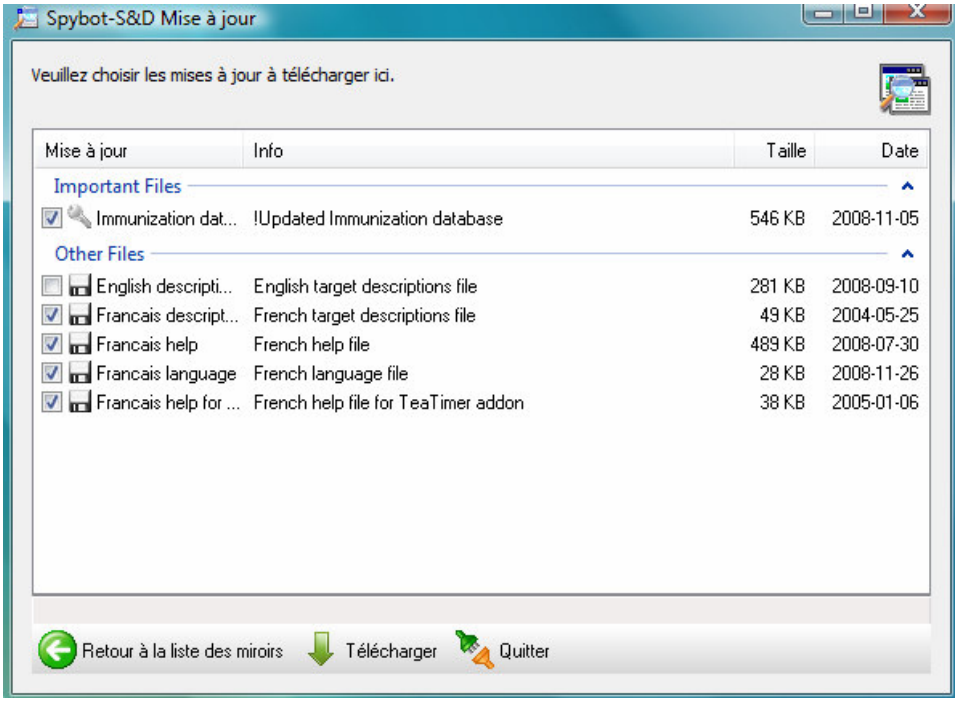


Il est inutile de créer une sauvegarde du registre. Il vaut mieux avoir pris un point de restauration avant de commence l'installation de Spybot.

Cliquer sur Commencer à utiliser le programme

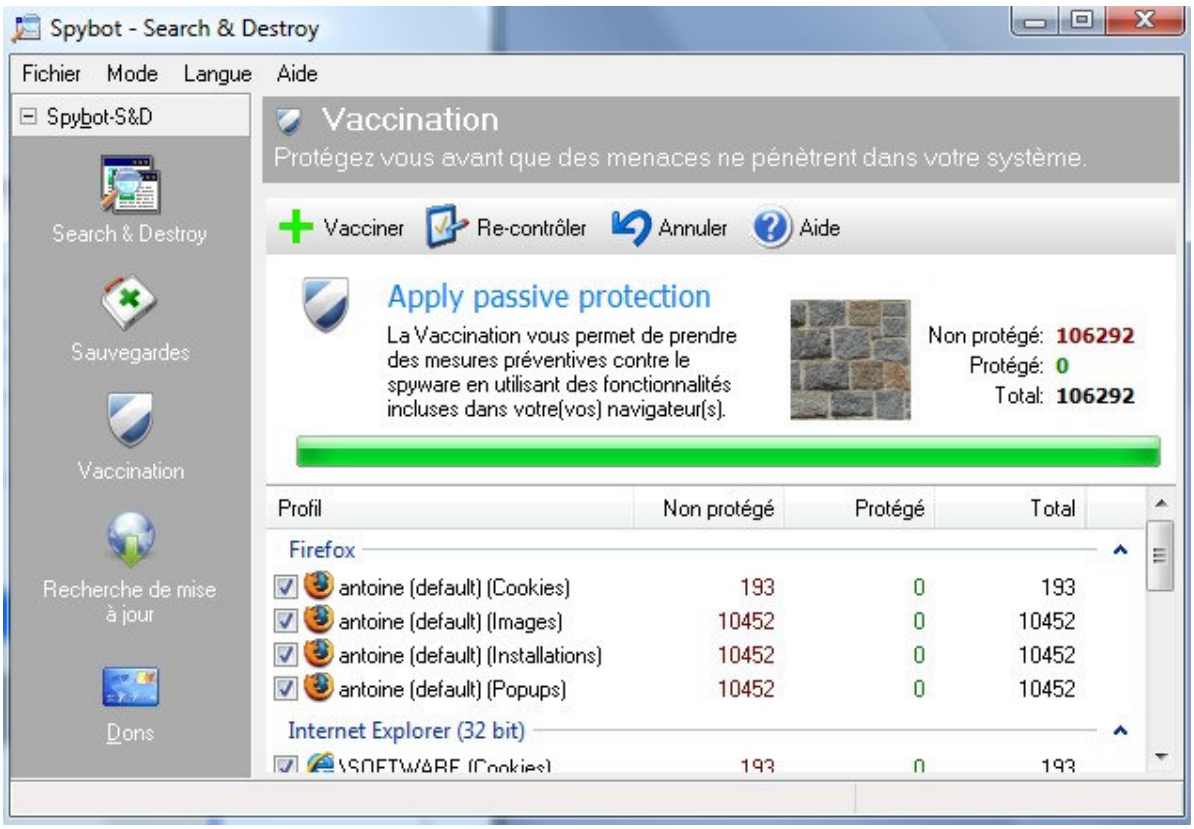
- Cliquez sur Rechercher des mises à jour
- Cliquez sur le bouton Télécharger toutes les mises à jour

Choisir un site de téléchargement



Cliquer sur Télécharger puis sur Quitter

Maintenant il faut vacciner l'ordinateur. Mais pour cela il faut être en mode Administrateur. Donc il faut quitter Spybot, et le relancer en mode Adminstrateur (clic droit sur l'icône de Spybot)



Vacciner Search & Destroy

Depuis la version 1.2, Spybot-S&D vous permet de vacciner votre ordinateur contre certains spywares. Il offre actuellement trois immunisations différentes:

Immunité permanente d'Internet Explorer

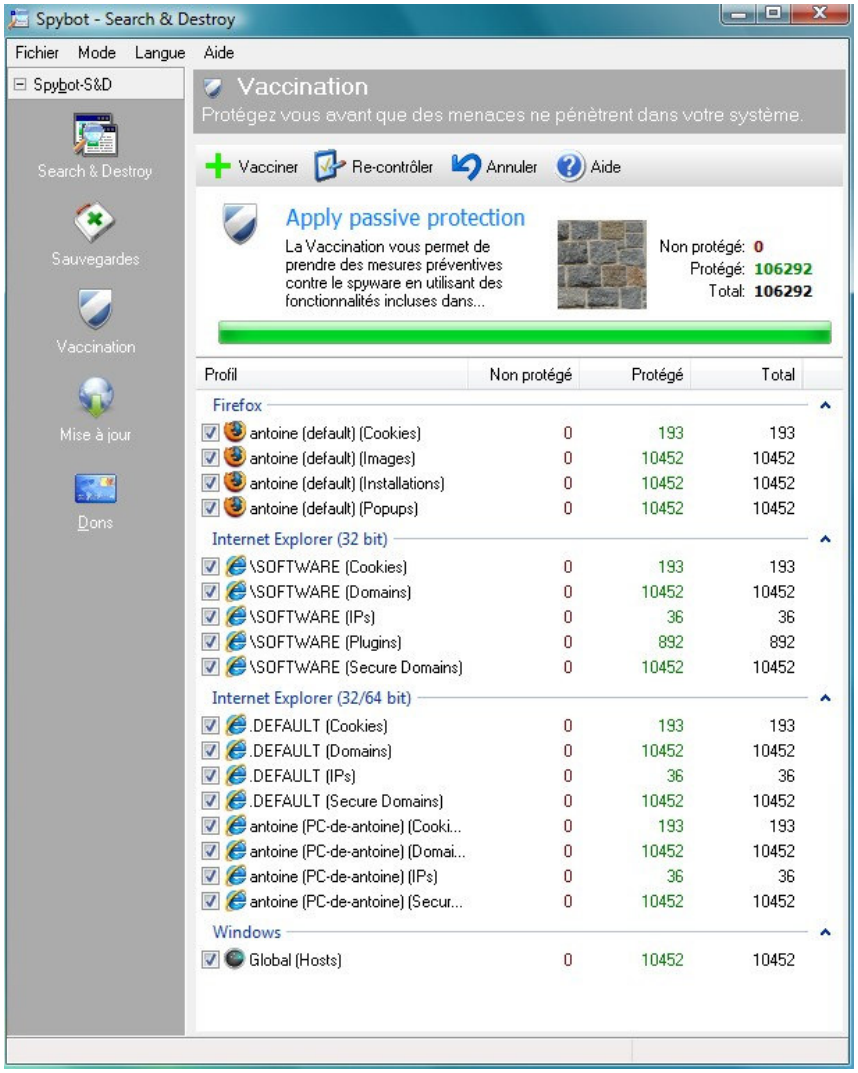
L'immunité permanente agit sur certaines options de contrôle d'Internet Explorer qui sont en partie visibles dans l'interface d'Internet Explorer, et en partie cachées seulement dans le Registre. Elle ajoute des domaines connus pour contenir de mauvaises choses aux Sites sensibles, bloquant ainsi l'installation de code exécutable depuis ces pages; elle ajoute aussi des options de blocage de code exécutable nuisible d'après son ID, et elle fait en sorte que des cookies traceurs connus ne soient pas acceptés par Internet Explorer.

En bref: cela modifie Internet Explorer, par des moyens officiels, afin de bloquer un tas de trucs néfastes que Spybot-S&D connaît.

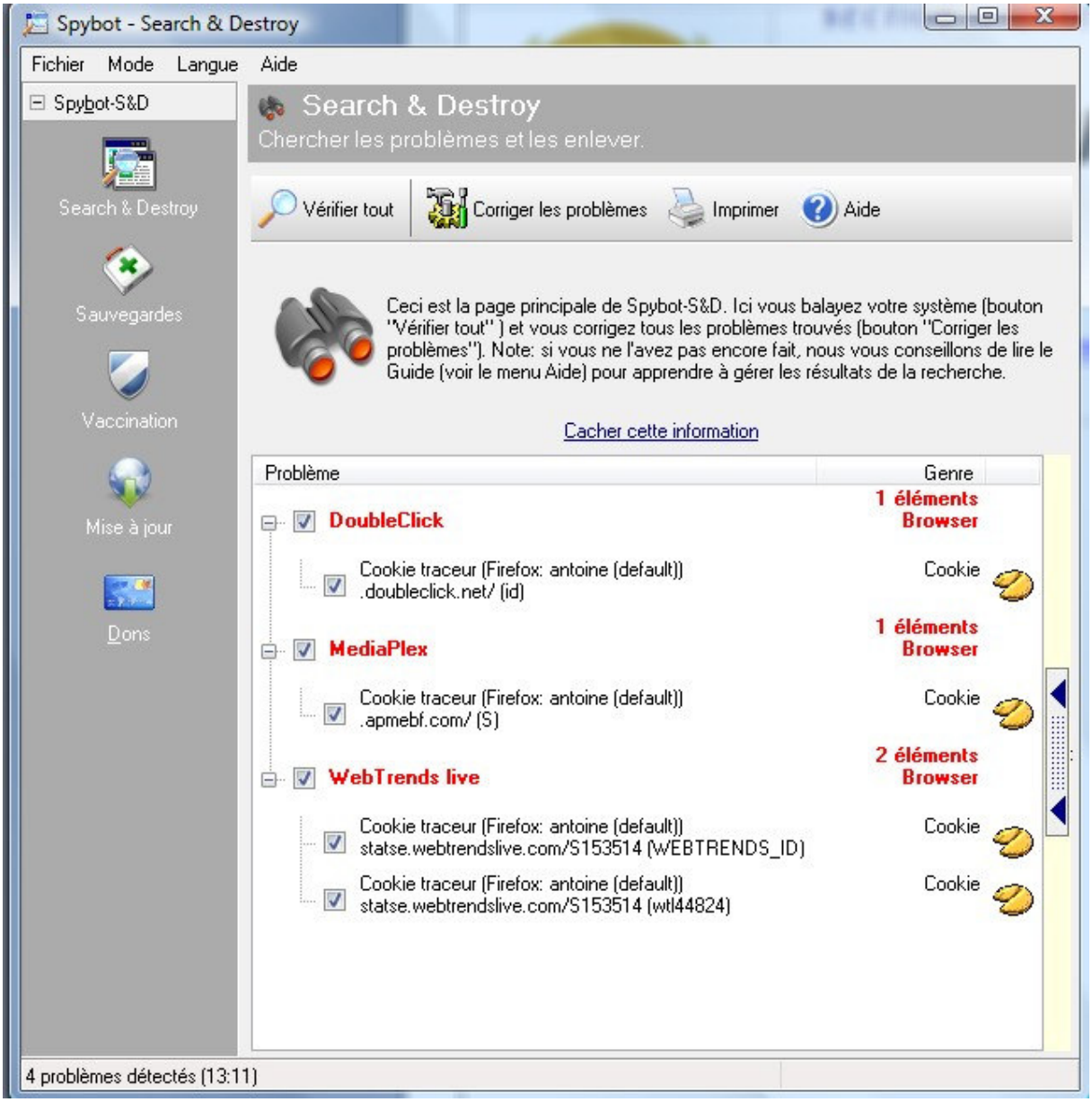
Bloqueur permanent de téléchargements nuisibles pour Internet Explorer

Ceci est une nouvelle couche de protection pour IE. Alors que l'Immunité permanente bloque les installeurs par leur ID ActiveX (IDentificateur ActiveX), ceci bloque tout ce qui pourrait passer au travers sous d'autres formes.
Vous pouvez voir un journal (log) d'installeurs bloqués dans la section Outils / Résident.

Lorsque la vaccination est terminée on a la fenêtre suivante



- passez maintenant votre ordinateur à la vérification, cliquez sur Vérifier tout et patienter



Interpréter les résultats

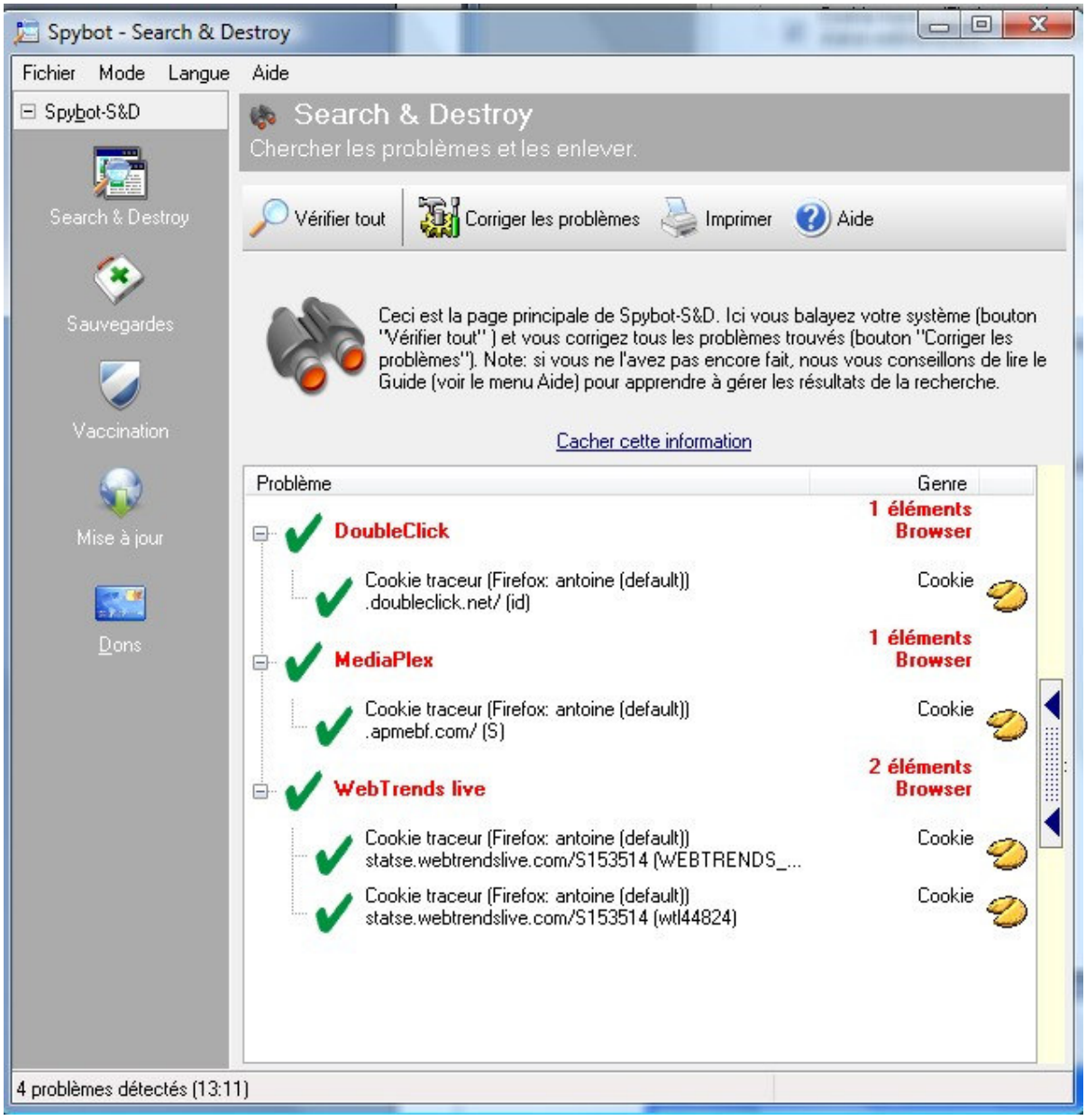
Arrivé là, vous pourriez sauter au dernier point, et supprimer les résultats. Au lieu de cela, nous vous conseillons de jeter un œil sur tous les trucs que Spybot-S&D a détectés. La première chose est de faire la distinction entre les lignes en rouge, qui représentent le spyware et les menaces similaires, 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 coté 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 par vous-même. Si vous faites un clic sur un produit puis sur le bouton gris à droite, vous pourrez lire les informations produit qui s'affichent dans une nouvelle fenêtre en pop-up.

- Une fois le balayage terminé, Spybot affichera tous les mouchards, dialers et autres indésirables en rouge
- Assurez-vous qu'ils soient tous cochés
- Puis cliquez sur Corriger les problèmes
- Cliquez maintenant sur le bouton Corriger les problèmes



- Cliquez sur Oui pour autoriser Spybot à nettoyer les mouchards

- Un crochet vert précèdera chacun des mouchards nettoyés
- Il se peut que certains mouchards récalcitrants et actifs ne puissent pas être supprimés lors de la première tentative
- Spybot vous demandera l'autorisation de se lancer avant Windows au prochain démarrage pour les neutralisés avant qu'ils ne s'activent.
- Cochez l'option Oui pour autoriser Spybot de faire le nettoyage au prochain démarrage.
- Maintenant cliquez sur Ok pour refermer la boîte de dialogue des problèmes corrigés.

Supprimer les menaces trouvées

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 commencez à penser à 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 savez ce que vous voulez faire, il existe un bouton caché *Cocher tous les problèmes* disponible sur la page des *Réglages* (seulement en mode avancé).

En bas à droite dans la barre des tâches vous avez probablement remarqué la présence de ce petit cadenas  Il appartient à Spybot, il protège en temps réel Internet Explorer et les réglages fondamentaux du système. Si vous souhaitez le fermer, faites un clic droit sur celui-ci et cliquez sur Quitter Résident. Si vous souhaitez le désactiver totalement, fermez-le avant tout, cliquez ensuite sur Démarrer, Exécuter, tapez : msconfig Allez dans l'onglet Démarrage, décochez la case TeaTimer, cliquez sur Appliquer puis Ok. Au redémarrage du PC, une fenêtre s'ouvrira : cochez la case Ne plus me demander et cliquez sur Ok.

• Spybot et son outil TeaTimer vous protègent de toute modification étrangère qui pourrait affecter Windows et/ou Internet Explorer.
Il se peut que des modifications voulant être faites sur le système ne soient pas nuisibles, par exemple après une désinfection ou une mise à jour Windows. Si vous ne savez pas comment interpréter le contenu de la petite boîte de dialogue, demandez de l'aide sur un forum.

• Vous souhaitez avoir le rapport de la dernière vérification ou tout simplement parce qu'on vous l'a demandé ? Pour cela, cliquez sur Mode sélectionnez Mode avancé, en bas à gauche, cliquez sur Outils, puis Voir le rapport, cliquez sur Voir le rapport précédent, sélectionnez le dernier fichier ayant pour nom Fixes et cliquez sur Ouvrir.

• Spybot est un logiciel anti-spywares relativement efficace pour un programme gratuit, éxécutez-le logiciel deux fois par mois cela sera raisonnable. N'oubliez pas qu'un seul anti-spywares ne suffit pas. Téléchargez un antivirus et un pare-feu (pas celui d'XP/Vista, car inefficaces).

• Spybot contient un mode avancé à découvrir éventuellement. Pour l'activer, cliquez en haut sur Mode et choisissez Avancé, cela vous donnera accès à plus d'informations et de paramétrages.

F.A.Q. (foire aux questions) de Spybot

Ad-Aware 2008

Protection de processus en temps réel : Ad-Watch suspend les fichiers suspects et bloque les processus malveillants qui essaient de se lancer ou de s'exécuter sur votre système (pour empêcher leur intégration dans votre système), vous donnant la liberté d'autoriser ou de bloquer le processus.

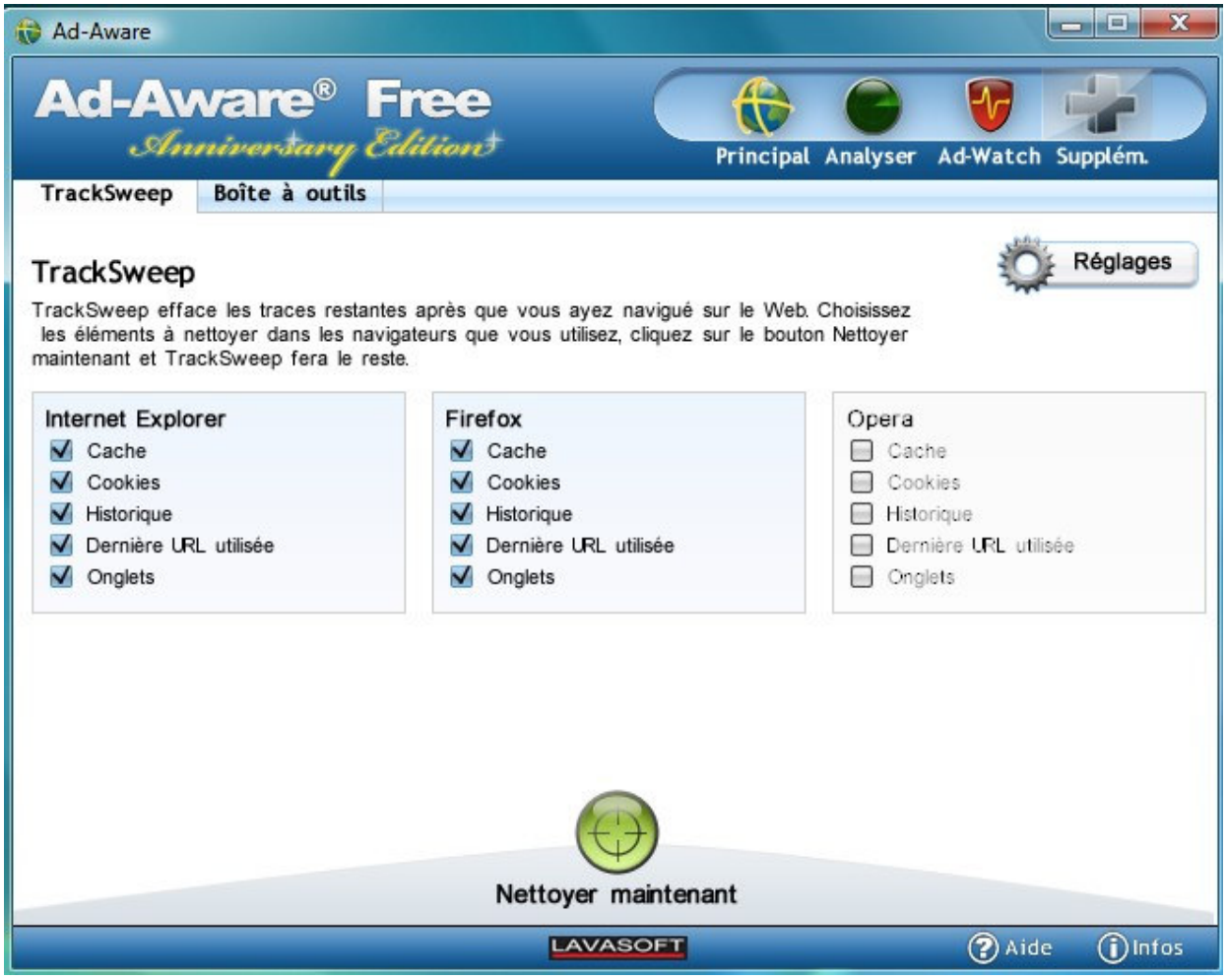
Protection exhaustive contre les programmes malveillants. Protection contre les logiciels espions, chevaux de Troie, rootkits, détournements informatiques, enregistreurs de frappe, etc.

Système de suppression des rootkits. Technologie anti-rootkits évoluée pour vous protéger contre les menaces cachées et les attaques furtives visant à obtenir l'accès à votre système en évitant la détection

Détection, suppression ET nettoyage. Outre la simple détection et suppression des programmes malveillants, Ad-Aware nettoie votre système de manière intelligente en effaçant toutes les traces de l'infection.

ThreatWork. Envoyez les fichiers suspects pour analyse aux chercheurs de Lavasoft d'un seul clic. ThreatWork est une communauté bénévole rassemblant des spécialistes du monde entier dans la sécurité et la lutte contre les programmes malveillants dans le but de combattre activement les menaces en ligne.

TrackSweep. Contrôlez vos informations privées en effaçant les traces que vous avez laissées en navigant sur internet avec de multiples navigateurs, dont Internet Explorer, Firefox et Opera, d'un simple clic.



Point de restauration du système. Définissez un point de restauration du système de manière à pouvoir nettoyer votre ordinateur sans crainte d'endommager le système d'exploitation. En cas de problème, vous pouvez ainsi revenir à un état précédent.

Analyse précise. Déterminez facilement si des fichiers suspects sont sûrs ou malveillants : cliquez avec le bouton droit de la souris sur un fichier ou un dossier pour effectuer immédiatement une analyse Ad-Aware.

Fichiers journaux détaillés. Exportez les rapports d'analyse sous forme de fichiers textes.

Intégration complète au centre de sécurité Windows. Obtenez des notifications d'état et de protection Ad-Aware par l'intermédiaire du centre de sécurité Windows.

Télécharger Ad-aware:

L'installation est terminée, cliquez sur le bouton Terminer et redémarrer l'ordinateur.

Fermer la fenêtre concernant la licence de la version payante

Réglages : ne rien changer

Mise à jour des définitions de malwares sur le Web

Analyse astucieuse

Analyse complète

Résultats de l'analyse

Cocher la case faire un point de restauration