

Le logiciel Malwarebytes (XP, Vista, Win7)

Un des outils les plus efficaces pour lutter contre les logiciels malicieux installés sur votre ordinateur

Télécharger à partir de ce lien

<http://fileforum.betanews.com/detail/Malwarebytes-AntiMalware/1186760019/1>

Le site du logiciel : www.malwarebytes.org

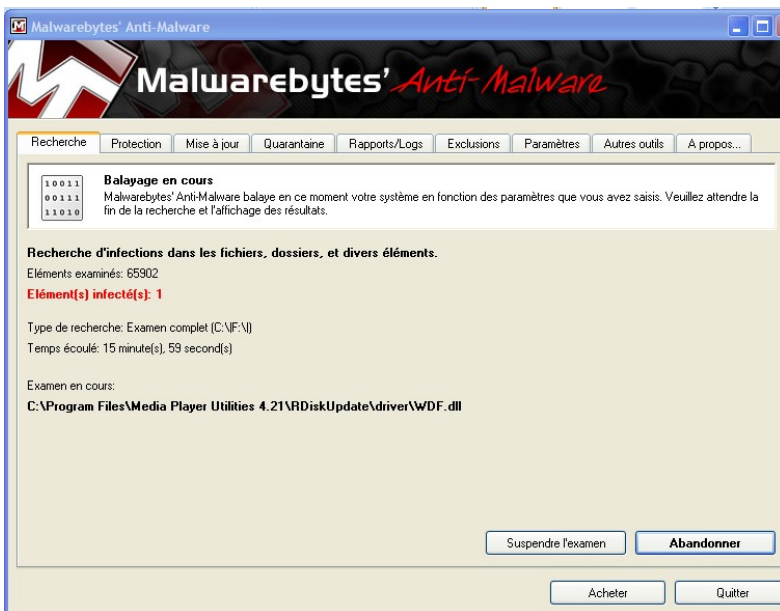
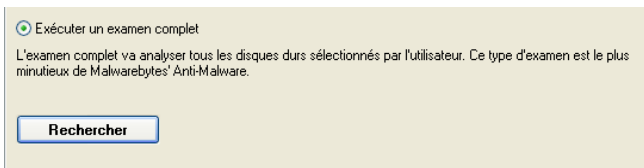
Une fois téléchargé l'installer de la façon usuelle

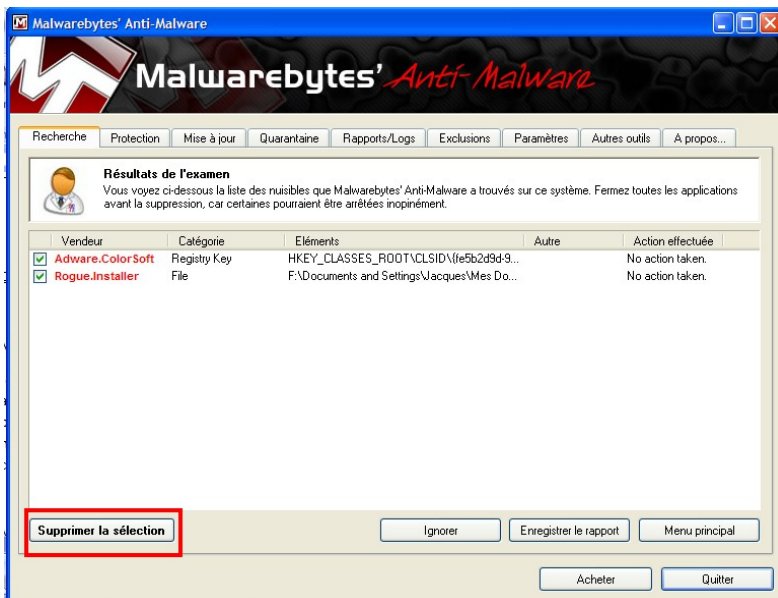
Une fois installé, le mettre à jour



...et ensuite procéder à un examen complet de l'ordinateur

NB : Ce programme ne doit pas être utilisé en [mode sans échec](#), car cela diminue son efficacité.





Le logiciel Super Anti Spyware (XP Vista Win7)

A utiliser idéalement en **mode sans échec**

Logiciel gratuit très efficace également

Téléchargeable à cette adresse :

<http://www.commentcamarche.net/telecharger/telecharger-34055294-superantispyware>

Tutoriel détaillé : http://www.malekal.com/tutorial_SUPERAntiSpyware.php

SUPERAntiSpyware 4.35.1000



4,6/5 (29 votes)

☆☆☆☆☆
Donnez votre avis

Description

Avis des utilisateurs

Editeur: SUPERAntiSpyware.com
Versión: 4.35.1000 (dernière version)
MD5: 92109c68c52a26d44a65a4d36afbc9c5
Langue: Français
Système: 98/Me/2000/XP/Vista/Win7
Licence: Freeware/gratuit (free)

 **Télécharger**
SUPERAntiSpyware4.35.1000exe
(8 Mo)

Comme son nom nous l'indique déjà, SuperAntiSpyware est un programme conçu par SUPERAntiSpyware.com afin de stopper et d'éliminer les processus ou les logiciels espions susceptibles de se trouver sur votre ordinateur.

Il élimine des éléments de spyware, adware, trojans, vers, keylogger, hijacker, dialer et toutes autres menaces destinées au vol d'informations confidentielles.

Allons le voir concrètement

Pour les utilisateurs **avancés**, deux programmes qui gagnent à être connus : **Hi-Jack This** et **Combo Fix**

Hijack This (XP-Vista-win7)

C'est quoi Hi-Jack-This ? : Hi-Jack-This est un programme spécialisé, fourni gratuitement par Trend Micro. Il sert à détecter et à neutraliser les « pirates » de navigateur qui s'installent par la navigation (Java) ou l'installation d'un programme et ne sont pas détectés ni nettoyés par les anti-virus habituels.

Il sert également à détecter les programmes espions et non légitimes qui s'installent au démarrage du système.

Et n'oubliez pas qu'avant d'utiliser HijackThis, il est fortement conseillé de faire un premier nettoyage avec ces logiciels :

Votre anti-virus
Malwarebytes
SuperAntiSpyware
Spybot S&D

*Toutes ces analyses sont à effectuer **en mode sans échec** et en **désactivant la restauration système**.
(Cliquez de la droite sur Poste de travail, Propriétés, Restauration système et mettre le crochet)
Ne pas oublier d'aller enlever le crochet quand l'ordinateur fonctionnera bien à nouveau*

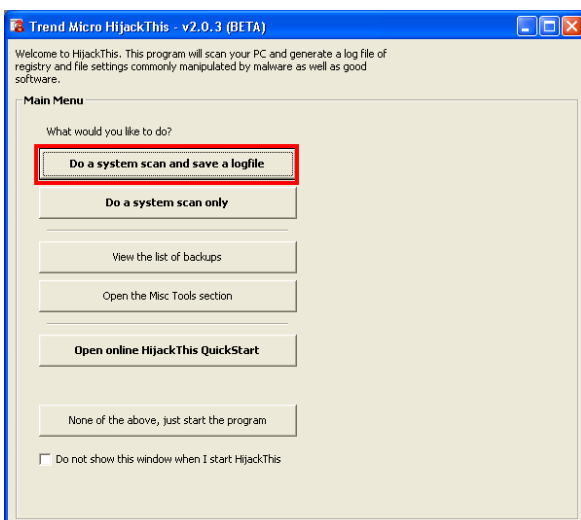
Quand vous avez déjà utilisé ces trois là, une très grande partie des cochonneries sont dépistées. HijackThis est à utiliser en dernier recours quand les précités ne vous ont pas débarrassé d'un spyware (Ou autre.) quelconque.

A ce moment vous pouvez utiliser HijackThis pour vérifier ce qui reste.

ET ATTENTION : exécutez-le sans aucune application ouverte !

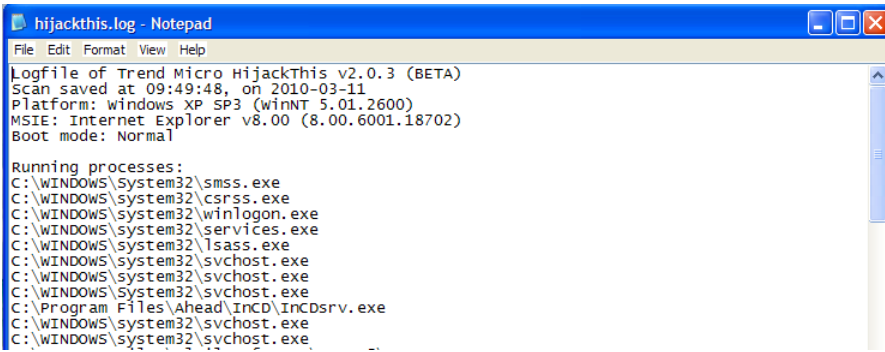
Téléchargement : http://www.trendsecure.com/portal/fr/tools/security_tools/hijackthis

Une fois l'installation terminée, ouvrez HijackThis en cliquant sur Démarrer > Programmes > HijackThis et cliquez sur le bouton « Do a system scan and save a logfile » (Effectuer un balayage du système et sauvegarder le journal).



Le résultat apparaît en deux parties :

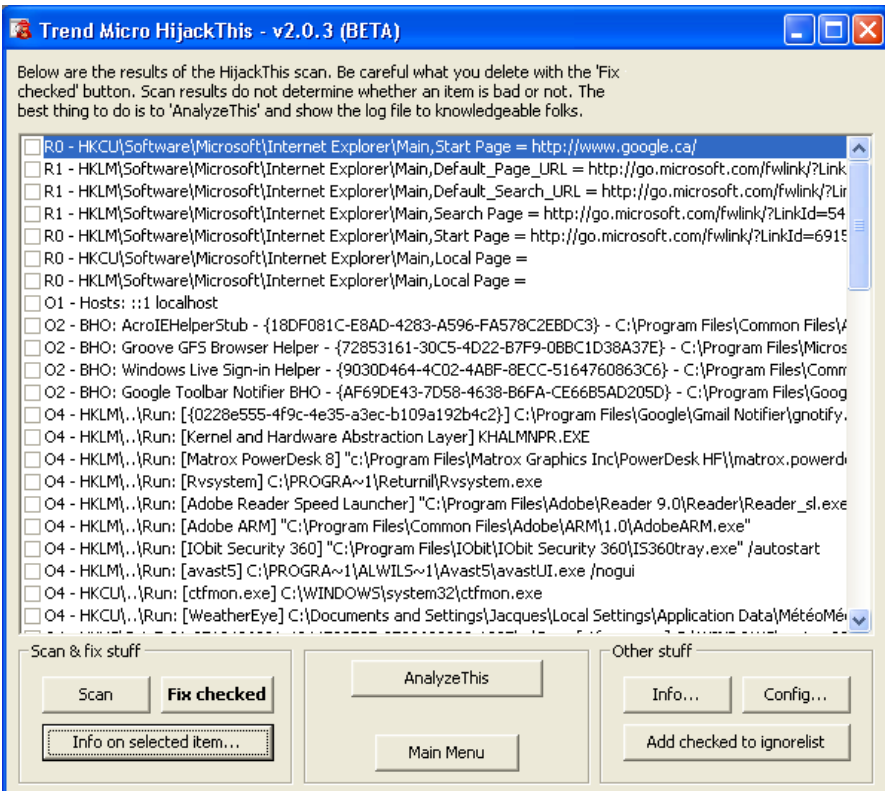
1- Rapport écrit



```
hijackthis.log - Notepad
File Edit Format View Help
Logfile of Trend Micro HijackThis v2.0.3 (BETA)
Scan saved at 09:49:48, on 2010-03-11
Platform: windows XP SP3 (winNT 5.01.2600)
MSIE: Internet Explorer v8.00 (8.00.6001.18702)
Boot mode: Normal

Running processes:
C:\WINDOWS\system32\smss.exe
C:\WINDOWS\system32\csrss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\Program Files\Ahead\InCD\InCDsrv.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
```

2- Console de travail



Maintenant que le balayage est terminé. Allons voir ensemble ce que le rapport enregistré contient

Le rapport s'enregistre habituellement dans le dossier du programme Hijack This

Pour l'ouvrir on utilise le bloc notes (note pad)

Vue d'ensemble

Chaque ligne d'un log d'HijackThis démarre avec un nom de section. (Pour plus d'informations techniques, cliquez sur 'Info' dans la fenêtre principale et descendre. Sélectionnez une ligne et cliquez sur 'More info on this item'.)

Première partie : Running processes : (Processus activés au démarrage)

Exemples :

C:\WINDOWS\System32\smss.exe

C:\Program Files\Alwil Software\Avast5\AvastSvc.exe

C:\WINDOWS\Explorer.EXE

C:\Program Files\TrendMicro\HiJackThis\HiJackThis.exe

C:\WINDOWS\system32\mspaint.exe

Vous pouvez « Googouler » les processus inconnus comme **smss.exe** et aller voir ce qu'on en dit.

Voici le résultat sur www.commentcamarche.net

Le processus **smss.exe** (*smss* signifiant *Session Management Subsystem*) est un processus générique de Windows NT/2000/XP servant à créer, gérer et supprimer les sessions utilisateurs. Il s'agit du premier processus exécuté au démarrage en mode utilisateur.

Le processus smss n'est en aucun cas un [Virus résident](#), un [ver](#), un [cheval de Troie](#), un [spyware](#), ni un [AdWare](#).

Il s'agit d'un processus système critique ne pouvant pas être arrêté par le gestionnaire des tâches.

Seconde partie

R0,R1,R2,R3 – URL des pages de Démarrage/Recherche d'Internet Explorer

F0,F1 – Programmes chargés automatiquement –fichiers .INI

N1,N2,N3,N4- URL des pages de Démarrage/Recherche de Netscape/Mozilla

O1- Redirections dans le fichier Hosts

O2- Browser Helper Objects

O3- Barres d'outils d'Internet Explorer

O4 – Programmes chargés automatiquement –Base de Registre et dossier Démarrage

O5 – Icônes d'options IE non visibles dans le Panneau de Configuration

O6- Accès aux options IE restreints par l'Administrateur

O7 – Accès à Regedit restreints par l'Administrateur

O8 – Eléments additionnels du menu contextuel d'IE

O9 – Boutons additionnels de la barre d'outils principale d'IE ou éléments additionnels du menu 'Outils' IE

O10 – Pirates de Winsock

O11 – Groupes additionnels de la fenêtre 'Avancé' des Options d'IE

O12 – Plugins d'IE

O13 – Piratage des DefaultPrefix d'IE (préfixes par défaut)

O14 – Piratage de 'Reset Web Settings' (réinitialisation de la configuration Web)

O15 – Sites indésirables de la Zone de confiance

O16 – Objets ActiveX (alias Downloaded Program Files – Fichiers programmes téléchargés)

O17 – Pirates du domaine Lop.com

O18 – Pirates de protocole et de protocoles additionnels

O19 – Piratage de la feuille de style utilisateur

O20 – Valeur de Registre AppInit_DLLs en démarrage automatique

O21 – Clé de Registre ShellServiceObjectDelayLoad en démarrage automatique

O22 – Clé de Registre SharedTaskScheduler en démarrage automatique

O23 – Services NT

URL (*Anglais* : *Uniform Resource Locator*). Adresse **Internet** exploitée par les **navigateurs** (Internet Explorer ou Firefox par exemple). C'est l'adressage standard de n'importe quel document, sur n'importe quel ordinateur en local ou sur Internet.

Structure de base d'une URL : protocole ://serveur/répertoire/document.extension

Un outil spécial pour interpréter les rapports Hijack this : <http://www.hijackthis.de/fr>

Il s'agit d'y coller notre log et d'attendre la réponse.

Ensuite il faut décider de ce que l'on garde ou supprime .

Le logiciel Combo fix (XP) (Vista et Win7-32 bits)

ComboFix est un outil qui nettoie certaines infections spécifiques telles SurfSideKick, QooLogic, Look2Me et Vundo.

De plus, il permet également de déterminer les fichiers récemment créés (indiqués dans le rapport du scan), ce qui peut donner des informations sur d'autres éventuelles infections de votre PC.

Autre fait important, ComboFix détecte et supprime un nombre important de rootkits tels des infections chinoises ou pe386, lzx32...

Attention de bien suivre les étapes de désinfection. Pour ce faire, imprimer et suivre pas à pas les instructions

Il est essentiel de désactiver l'anti virus, Windows defender et les anti-spywares. Mode sans échec pour Vista et Win7 (F8 au démarrage)

Combo Fix est un logiciel qui désinfecte Windows à sa source sur le disque dur.

Téléchargement : <http://download.bleepingcomputer.com/sUBs/ComboFix.exe>

Instructions de fonctionnement : <http://www.bleepingcomputer.com/combofix/fr/comment-utiliser-combofix>

Merci

Jacques Laliberté

Cimbcc 2010-04-07

aidecimbcc@gmail.com