Nettoyer Virus

Un article de ChtilandWiki.

Sommaire

- 1 Avant Propos
- 2 Les symptômes
- 3 Préparatifs
  - 3.1 Le matériel
  - 3.2 Sur le PC sain
  - 3.3 Les logiciels
    - 3.3.1 Utilitaire de compression/decompression
    - 3.3.2 Nettoyeurs Virus, Trojan
    - 3.3.3 Anti Spyware
    - 3.3.4 Anti Root-kit
    - 3.3.5 Toolbar
    - 3.3.6 Antivirus en ligne
  - 3.4 Sur le PC Infecté
    - 3.4.1 IE PrivacyKeeper
      - 3.4.1.1 Installation
      - 3.4.1.2 Paramétrage
- 4 Nettoyage
  - 4.1 Nettoyage Virus
    - 4.1.1 Avast Cleaner
    - 4.1.2 Multi Virus Cleaner
  - 4.2 Nettoyage Rootkit
    - 4.2.1 AVG Anti-Rootkit
    - 4.2.2 Sophos
    - 4.2.3 F-Secure Blacklight
    - 4.2.4 Gmer
  - 4.3 Ultimate BootCD
- 5 Se prémunir
  - 5.1 Son comportement
    - 5.1.1 Eviter de
  - 5.2 Les logiciels
    - 5.2.1 Mises à jour
    - 5.2.2 Antivirus
    - 5.2.3 Tests
    - 5.2.4 Surfez sur Internet avec Firefox
- 6 Conclusion
- 7 Service
- 8 Autres

Avant Propos

En cours de réalisation

03-08-2007 : Remplacement de VMWare par une autre application Open Source, VirtualBox.

01-06-2008 : Pas beacoup de temps, toute aide sera la bienvenue.

Cette méthode s'applique aux systèmes sous Windows. La version utilisée pour cet article est Windows XP Pro SP2 mis à jour complètement au
Cette méthode fonctionnera aussi sur les PC équipés de Windows XP Home (Familiale) et il y a 99% de chances que cela fonctionne aussi sous '
versions de Windows envoyez moi vos retours. Pour les autres, hummmm ça existe les virus ? LOL, je plaisante, c'est beaucoup plus rare de renc
MacOS. Personellement, sous Linux, je n'ai encore rien eu :)

Cette première méthode est une méthode simple utilisant des outils gratuits. Il existe une méthode experte qui sera vue plus tard, mais réservé

LICENCE : Certains programmes sont uniquement utilisables à des fins personnelles, et ne sont donc pas à utiliser professionnellement. Ils ser
mesure.

Les symptômes

- Votre PC ralenti sans raison apparente
- Vos contacts MSN reçoivent des messages de votre part leur demandant de télécharger un fichier alors que vous n'avez rien fait.
- Vous commencez à recevoir beaucoup plus de spams (et vous les recevrez toujours, car cette procédure ne supprime pas votre email des lis
  il en existe aucune réellement efficace)

- En faisant une recherche sur Google avec votre navigateur sur le mot "Virus" ou "Anti VIrus", une nouvelle page s'ouvre pour vous proposer (dans ce cas précis il s'agit d'un Rootkit)
- (...)

Préparatifs

Point important, le nettoyage se fera en **mode sans échec**, il ne faut donc pas compter sur une connexion réseau ou internet.

Le nettoyage des virus ne se fait pas à la légère une petite phase de préparation est nécessaire.

Il existe plusieurs sortent de virus, vers etc. Une variante qui commence actuellement à s'accroître, ce sont les Rootkits.

Le matériel

En fonction de vos possibilités et de vos moyens, voici une petite liste de ce qui pourrait (donc facultatif) servir :

- Un PC Sain connecté à internet : chez un ami, au boulot (pendant les heures de pause et avec accord de son supérieur hiérarchique !), cafés. Gardez quand même à l'esprit que ce PC pourrait ne pas être aussi sain que vous le pensez ;)
- Un graveur et des CD Vierges
- Une clef USB (si possible verrouillable en écriture - un petit interrupteur avec un cadena)

Sur le PC sain

Si vous n'avez pas de PC sain, vous pouvez également effectuer ces manipulations sur le PC infecté, soit directement avec le système infec d'un CD Bootable d'une distribution Linux.

Les logiciels

Pour simplifier et évitez de chercher, créez un dossier "Nettoyage" sur le bureau et téléchargez-y l'ensemble des logiciels cités sur cette pa

N'enregistrez pas directement les fichiers sur la clef USB, une fois que vous aurez tout téléchargé copiez le dossier sur la clef, comme ça e vous n'aurez pas à tout recommencer.

Utilitaire de compression/decompression

Je suppose que vous avez déjà un utilitaire pour gérer vos archives **.zip** ou autre, mais si tel n'est pas le cas, ou même si c'est le cas, je vou (http://www.7-zip.org/fr/) le meilleur et le plus performant à mon humble avis. Notez également qu'il est entièrement gratuit !!!

Nettoyeurs Virus, Trojan

- Avast Cleaner (http://files.avast.com/files/eng/aswclnr.exe)
- Multi Virus Cleaner (http://www.viruskeeper.com/fr/mvc.zip)
- AVG Cleaner (http://www.grisoft.cz/filedir/util/avg_rem_sup.dir/vcleaner.exe)
- SmitFraudFix (http://siri.urz.free.fr/Fix/SmitfraudFix.exe)
- Ultimate Boot CD (http://www.ultimatebootcd.com/)
  CD Bootable Linux indépendant du système d'exploitation installé

Anti Spyware

Voici trois anti-spywares, pourquoi 3 ? Simplement parce qu'ils se complètent, l'un va détecter un spyware que l'autre de détectera pas et i

Cependant, en couplant simplement Windows Defender avec l'un des deux autre, ça suffit amplement.

Certains diront qu'Adaware est plus efficace que Spybot, mais bon, Spybot reste mon préféré.

- Adware Home (http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10045910.html?part=dl-ad-aware&subj=dl&tag=
- Spybot Search and Destroy (http://www.spybot.info/fr/mirrors/index.html)
- Windows Defender (http://www.microsoft.com/athome/security/spyware/software/default.mspx)
  Requiert la validation de votre licence Windows.

Anti Root-kit

- AVG Anti Root-Kit *sur ZDNet* (http://www.zdnet.fr/telecharger/windows/fiche/0,39021313,39238198s,00.htm)
- Sophos Anti Root-Kit (http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html) ou via Clubic (http://www.clubic.com/telechar anti-rootkit.html) (sans le formulaire)
  La version sur Clubic n'est pas à jour mais celle sur le site de Sophos est quasi impossible à obtenir...

- GMER (http://www.gmer.net/) ou via Chtiland (http://www.chtiland.com/download/gmer.zip) si le site est inaccessible.
  Excellent outil, permet également d'y intégrer des anti-virus en ligne]
- F-Secure Blacklight (http://www.f-secure.com/blacklight/) ou Téléchargement direct de la dernière version (ftp://ftp.f-secure.com/anti-v
  N'est pas gratuit
- SmartScan (http://www.simplytech.it/SmartScan/index.htm)
  Petit nouveau que je viens de découvrir (30-09-2007), je vous donnerai mon avis dès que possible ;)

Toolbar

Certaines Toolbar se désinstallent simplement, mais d'autres ont la peau dure.

EliteToolbar Remover (http://www.simplytech.it/ETRemover/index.htm)

Look2Me Remover (http://www.simplytech.it/L2MRemover/index.htm)

Antivirus en ligne

Une solution complémentaire consiste aussi à effectuer un scan online de votre PC.

Attention la plupart de ces outils ne fonctionnent qu'avec Internet Explorer.

Vous pouvez lancer ces différents scans en ligne avant ou après toute autre manipulation, voire avant et après si vous êtes paranoïaque cor

Voici une liste restreinte d'antivirus en ligne en qui j'ai le plus confiance.

[Nod32 (http://www.eset.eu/online-scanner)]

[Kaspersky (http://webscanner.kaspersky.fr/)]

[Avast (http://onlinescan.avast.com/)]

Sur le PC Infecté

Avant le nettoyage, pour accélérer les traitements :

- Vider la Corbeille
- Nettoyer le cache d'Internet Explorer
- Nettoyer les fichiers temporaires

Pour faire tout ça nous allons utiliser un autre freeware très pratique : IEPrivacyKeeper :(télécharger (http://www.unhsolutions.net/downloa
)

Vous pouvez également en profiter pour désinstaller des programmes que vous n'utilisez plus en passant par le **Panneau de Configuration**
programmes, pas obligatoire mais tant qu'on y est ;)

IE PrivacyKeeper

Après avoir téléchargé cet outils depuis le lien ci-dessus, lancez l'installation en double cliquant sur le fichier téléchargé.

Installation

Il est possible qu'un message d'avertissement apparaisse lors du lancement de programme d'installation, vous demandant si vous voulez vr
"Exécuter" bien entendu ;)

- Choisissez la langue dans lequel se déroulera l'installation (il ne s'agit pas de définir la langue du programme), puis **OK**
- Faites **Suivant**
- Acceptez le contrat de licence (après l'avoir lu), puis faites **Suivant** jusqu'à ce que vous deviez cliquer sur **Installer**
- Une fois l'installation terminée, laissez la case "Démarrer IE Privacy Keeper" cochée, et cliquez sur **Terminer**

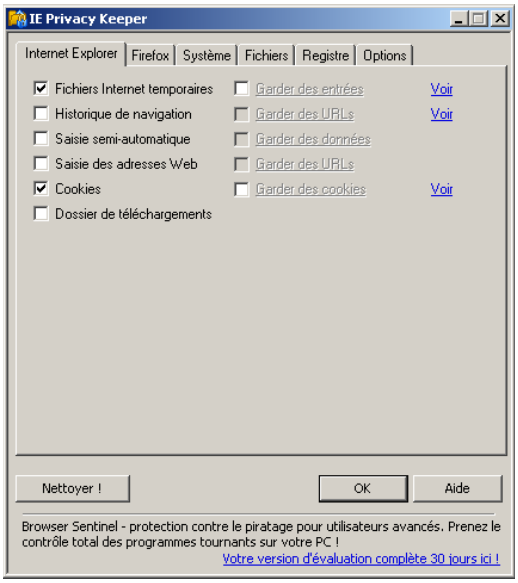
Si tout c'est bien déroulé, le programme se lance et sera en français.

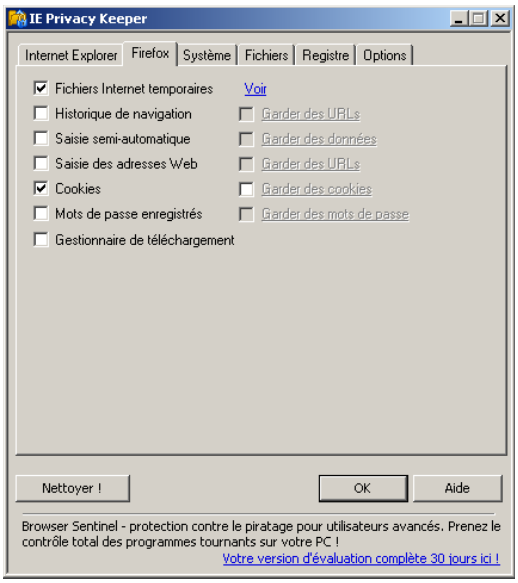
Pour les paramètres, basez-vous sur les captures écran ci-dessous (vous êtes libre de sélectionner ce que vous voulez)

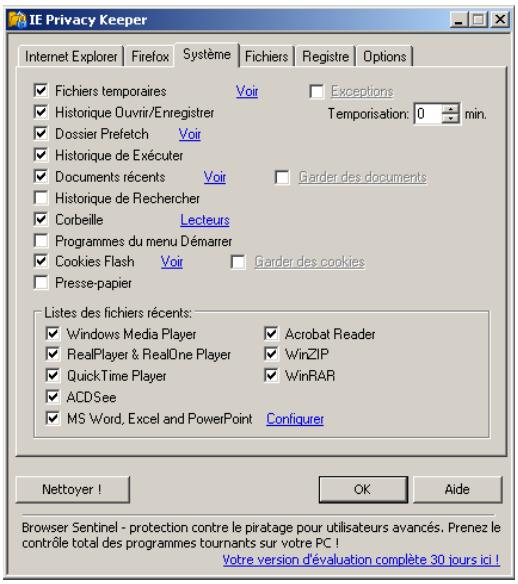
Notez que dans les paramètres définis ci-dessous, les Cookies seront supprimés et les connexions automatiques à vos sites favoris (les foru
perdues.

Paramétrage

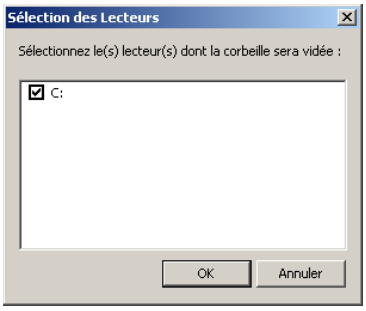
Le paramétrage proposé ci-dessous est celui que je recommande. Seuls les onglets demandant une modification sont ici, pour les autres on
par défaut.
Vous restez libre de paramétrer comme il vous semble, amis gardez à l'esprit que certains virus, trojan qui se sont installés via Internet Ex
(beaucoup plus rare), peuvent rester dans les différents caches.
Dans l'absolu vous pouvez cocher d'autres cases, mais évitez d'en décocher par rapport aux recommandations ci-dessous.


IE Privacy Keeper
Internet Explorer
Firefox
Système
Fichiers
Registre
Options
Fichiers Internet temporaires
Historique de navigation
Saisie semi-automatique
Saisie des adresses Web
Cookies
Dossier de téléchargements
Garder des entrées
Garder des URLs
Garder des données
Garder des URLs
Garder des cookies
Voir
Voir
Voir
Nettoyer !
OK
Aide
Browser Sentinel - protection contre le piratage pour utilisateurs avancés. Prenez le contrôle total des programmes tournants sur votre PC !
Votre version d'évaluation complète 30 jours ici !


IE Privacy Keeper
Internet Explorer
Firefox
Système
Fichiers
Registre
Options
Fichiers Internet temporaires
Historique de navigation
Saisie semi-automatique
Saisie des adresses Web
Cookies
Mots de passe enregistrés
Gestionnaire de téléchargement
Voir
Garder des URLs
Garder des données
Garder des URLs
Garder des cookies
Garder des mots de passe
Nettoyer !
OK
Aide
Browser Sentinel - protection contre le piratage pour utilisateurs avancés. Prenez le contrôle total des programmes tournants sur votre PC !
Votre version d'évaluation complète 30 jours ici !

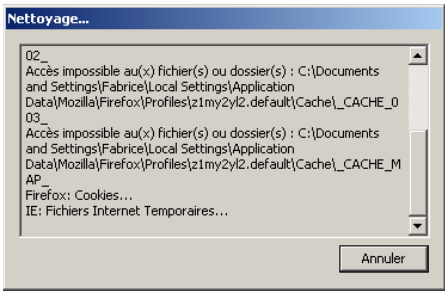


En face de **Corbeille**, cliquez sur le lien **Lecteurs** et vérifiez que tous les lecteurs soient cochés (Capture ci dessous)



Une fois les paramétrages effectués, cliquez sur le bouton **Nettoyer !**

Cliquez sur OK, une fenêtre comme ci-dessous va apparaître puis disparaître plus ou moins rapidement. Une fois qu'elle a disparu, le netto



Remarque Firefox : Si vous utilisez Firefox, il faudra aussi passer par le menu **Outils -> Effacer mes traces** cochez tout (sauf ***mots de p*** désirez les conserver, cela n'a pas d'importance pour la suite)

Nettoyage

Il n'est pas réellement nécessaire de redémarrer Windows, mais redémarrer en mode sans échec est une bonne idée.

Cependant, certains logiciels peuvent mal fonctionner ou pas du tout en mode sans échec. L'accès aux clef USB peut également poser problème.

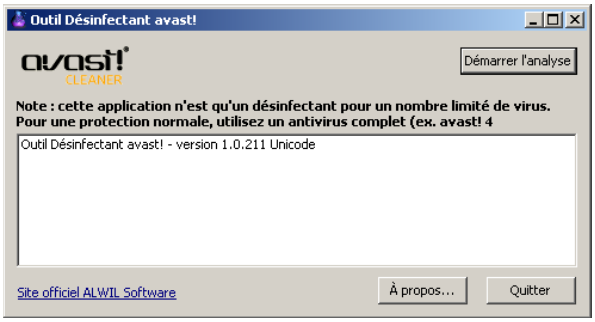
Notez cependant qu'il est indispensable que vous ayez les droits Administrateur sur votre compte, ce qui est le cas dans le cadre d'une installati acheté votre PC avec Windows déjà installé. Le plus souvent, si vous n'avez pas un accès Administrateur sur votre ordinateur, c'est que quelqu'u membre de votre famille ou la personne gérant l'informatique dans votre société s'il s'agit d'un poste de travail).

Nettoyage Virus

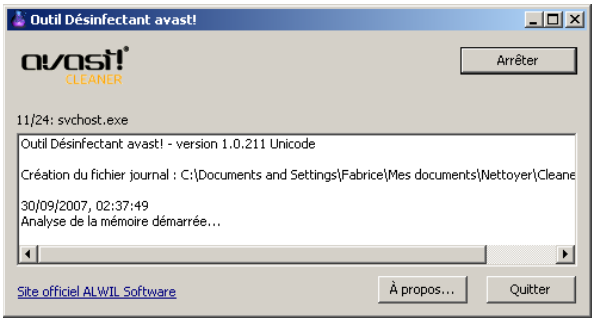
Pour cette section nous allons utiliser 2 nettoyeurs de virus, Avast Cleaner et Multi Virus Cleaner (MVC), libreà vous d'utiliser les autres outils, l'utilisation de **gmer** et l'installation de l'antivirus Avast Home Edition permet de ramener le risque d'être infecté à presque Zéro (On est à l'abı

Avast Cleaner

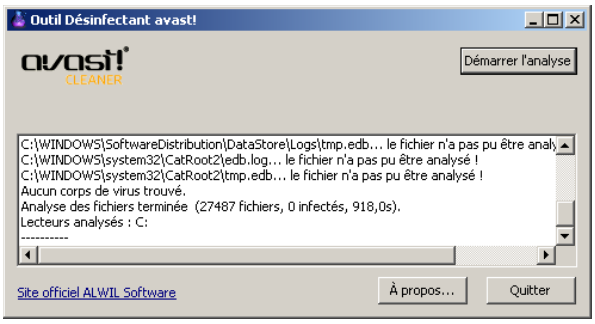
Lancez Avast Cleaner en double cliquant sur son icône :



Cliquez sur le bouton **Démarrer l'analyse**



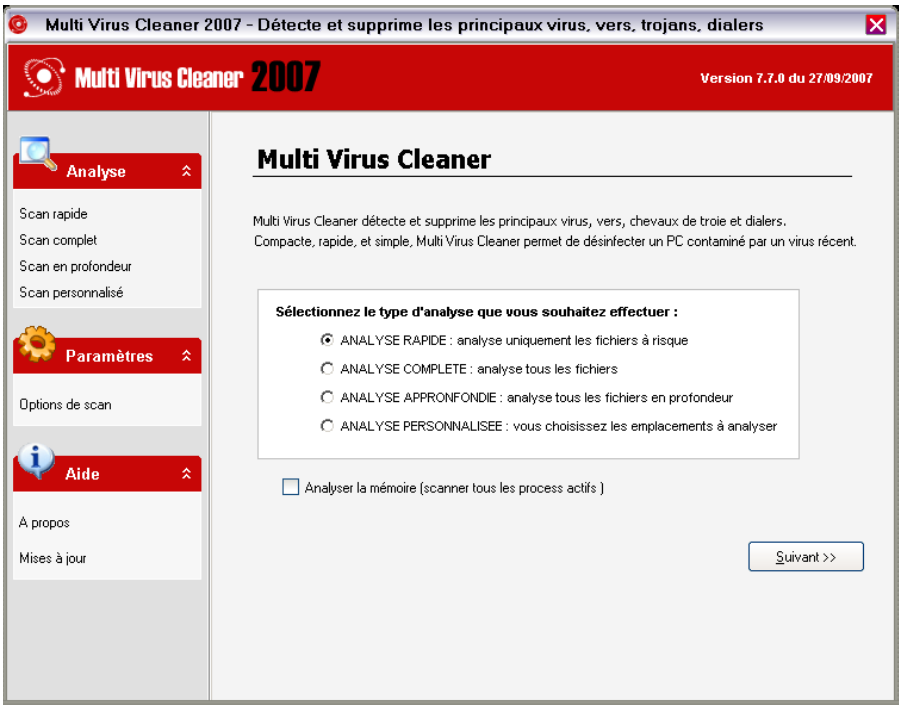
L'analyse peut durer un certain temps.
Si un virus est détecté, il sera supprimé.



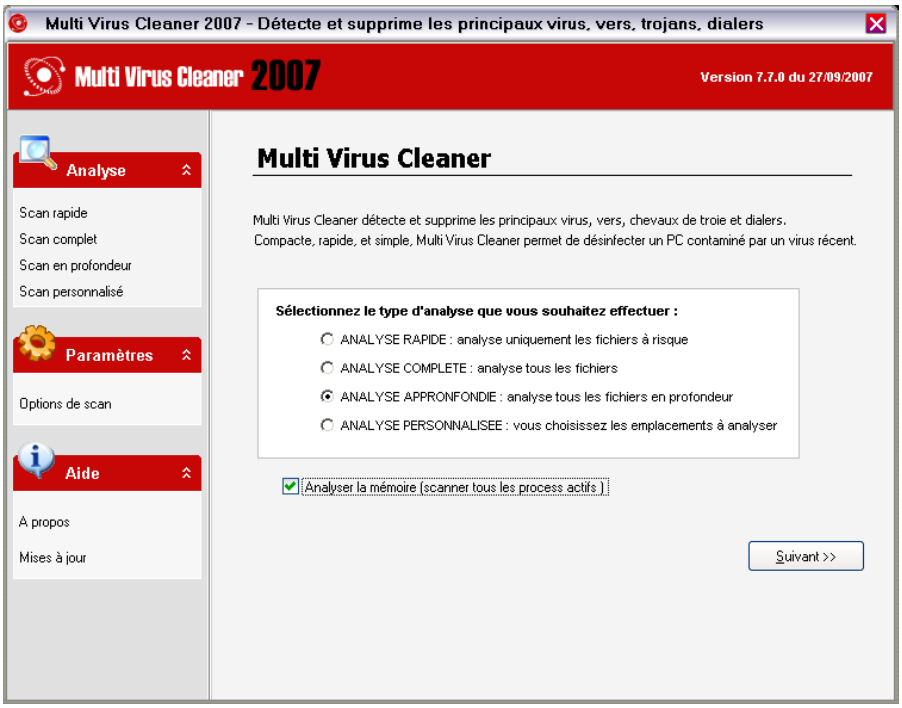
Une fois l'analyse terminée vous obtiendrez les résultats de l'analyse, ceux-ci seront également copiés dans un fichier **aswclnr.log** dans le Cleaner. Sauf si Avast Cleaner est sur un support non inscriptible (CD ou Clef vérouillée).
Vous pouvez converser ce rapport, au cas où, pour une analyse ultérieure.

Multi Virus Cleaner

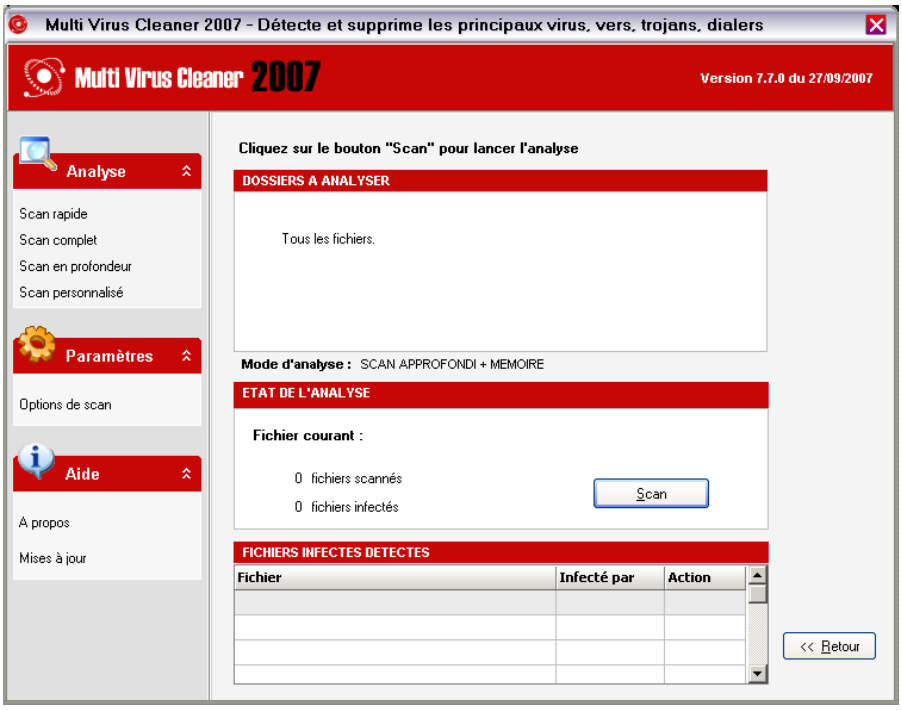
Lancez l'installation de MVC, à la fin de l'installation, cochez la case pour lancer MVC. Vous arrivez sur cet écran (**ne cliquez pas** encore s



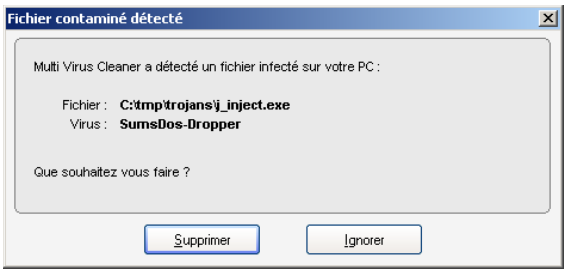
Configurez comme ci-dessous, puis cliquez sur **"Suivant"**



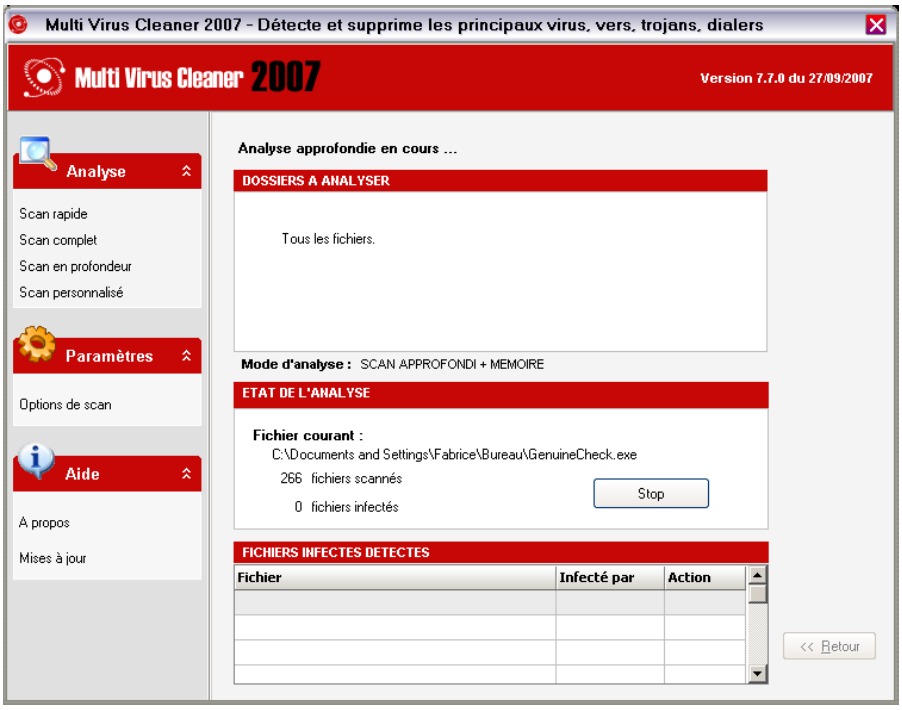
Cliquez sur le bouton **"Scan"**



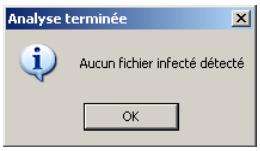
Si un virus est détecté vous obtiendrez cet fenêtre, cliquez sur **"Suprimer"**



Si aucun virus n'a été détecté vous obtiendrez ceci



Une fois le Scan terminé, vous obtiendrez un récapitulatif comme celui-ci :



Vous pouvez maintenant quitter MVC.

Nettoyage Rootkit

Pour le nettoyage des Rootkits nous allons utiliser presque toutes les solutions énoncées au début de cet article. En fait, seul SmartScan ne ser j'écris ces lignes il en est encore à la version 1.0 et en me semble pas encore tout à fait au point.

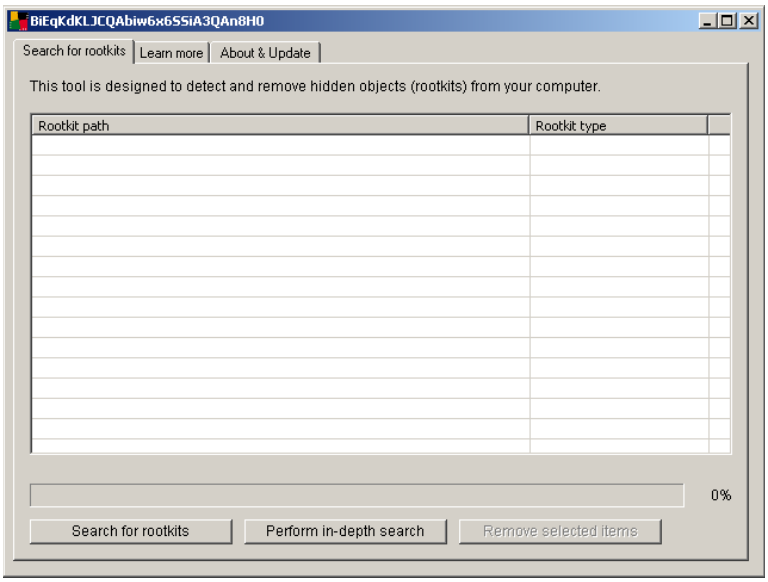
AVG Anti-Rootkit

Lors de l'installation on vous demande de sélectionner "Normal Interface" ou "Low Graphics Interface". La première est la plus jolie, mais f pas à un Anti-Rootkit d'être joli, mais rapide et efficace, c'est pour cela que je vous recommande l'interface "Low Graphics Interface".

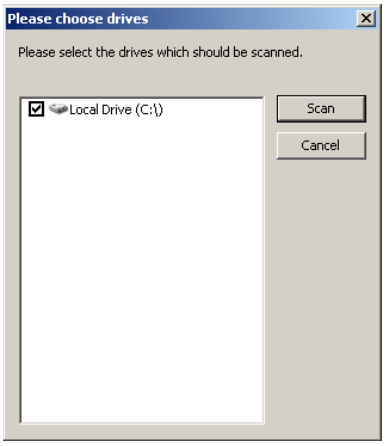
Suivez la procédure d'installation qui est typique à toute installation, si ce n'est qu'un redémarrage de votre PC sera requis (immédiateme finaliser l'installation et pouvoir utiliser AVGARK.

Une fois votre PC redémarré, lancez AVG Anti-Rootkit à l'aide du raccourci se trouvant sur le bureau.

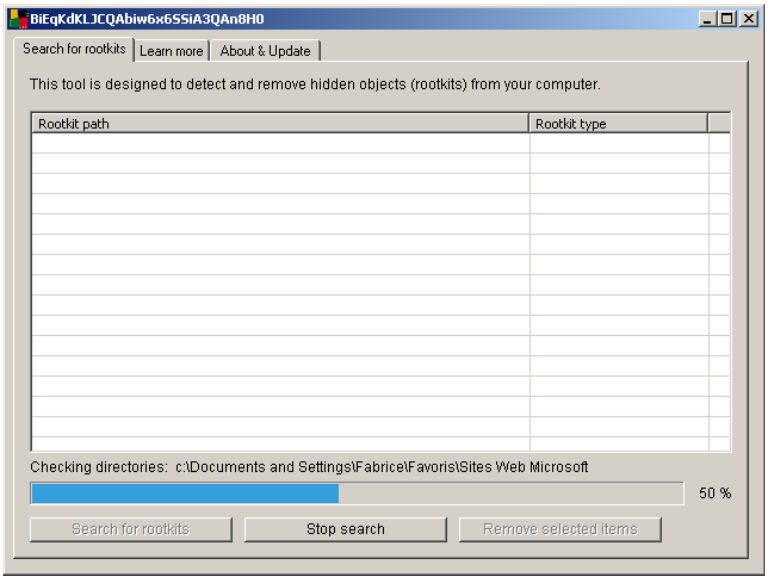
Vous obtenez cet écran :



Cliquez sur **Perform In-depth search**, sélectionnez tous les disques dans l'écran ci-dessous (exceptés les disques réseaux s'il y en a, cela ı plus de temps)



Le Scan se déroule.



Si des éléments sont détectés, vous les verrez apparaître dans la fenêtre après le scan.
Les Rootkits ont des fichiers assez typiques, ayant le même nom dont un a une extension .dat et un autre se trouvant dans le dossier de res
me souviens plus de l'endroit mais si vous avez un doute n'hésitez pas à me contacter)
S'ils ne sont pas encore cochés, cochez-lez et cliquez sur le bouton **Remove Selected Items**.

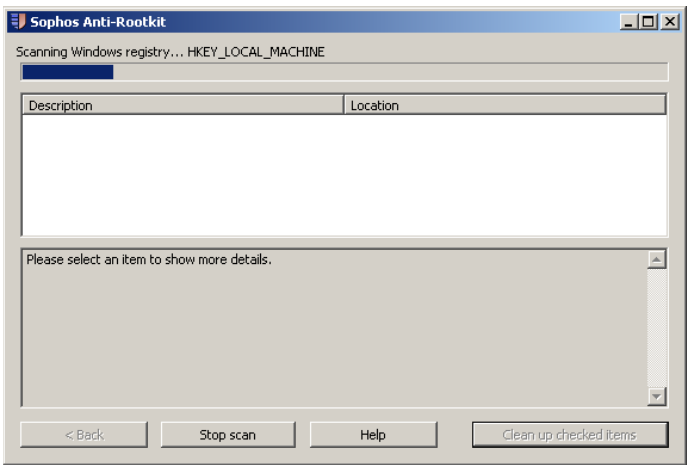
Si aucun Rootkit n'est détecté, vous obtiendrez l'écran suivant :

Cliquez sur **Close**.

Sophos

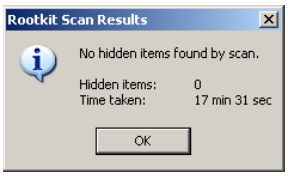
Après l'installation, vous avez la possibilité de lancer directement Sphos Anti-Rootkit.
Vous obtenez l'écran suivant :

Par défaut toutes les cases sont cochées, si ce n'est pas le cas, cochez-lez toutes et cliquez sur **Scan**.
Le scan démarre, tout comme les autres soyez patients...



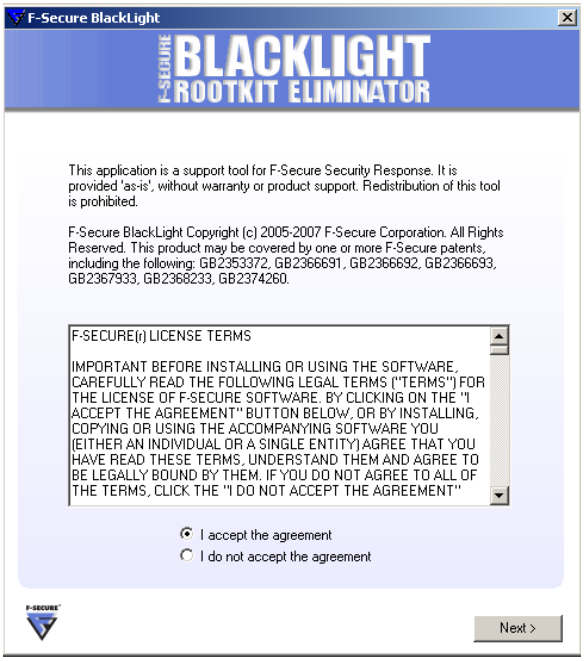
Si des Rootkits sotn détectés, sélectionnez les et cliquez sur **Clean up selected Items**

Si aucun Rootkit n'est détecté vous obtenez ceci :

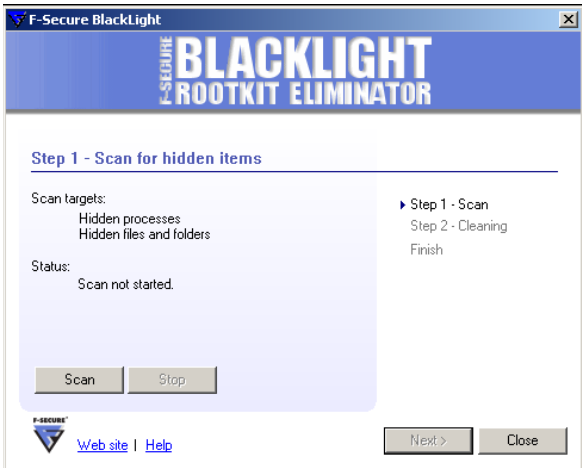


F-Secure Blacklight

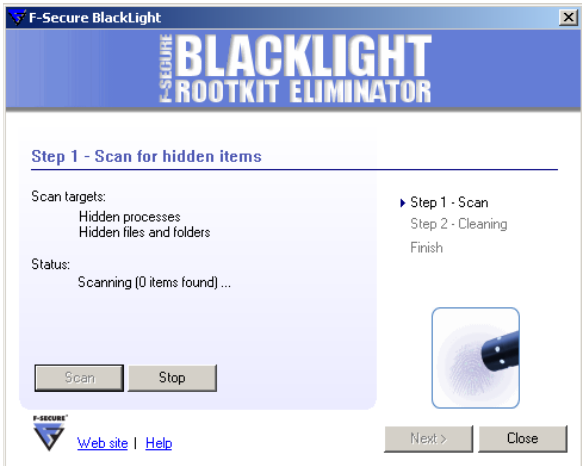
Bien que payant cette version fonctionne parfaitement.
Il n'y a pas d'installation, juste lancer l'application.



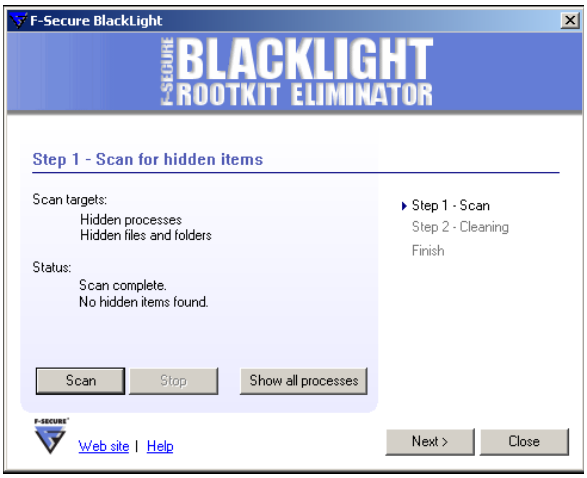
Acceptez la licence et cliquez sur Next.



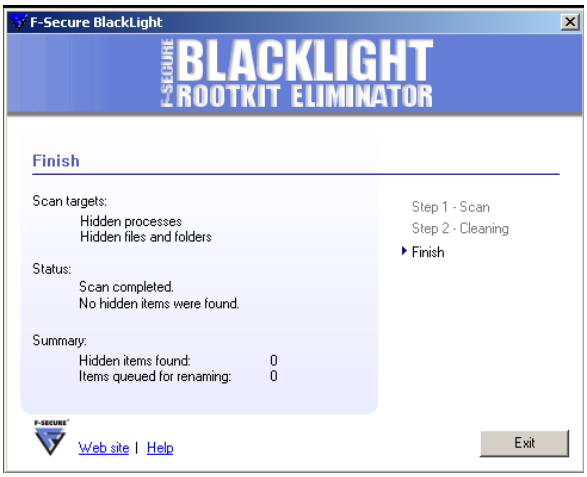
Cliquez sur le bouton **Scan**.



Laissez le scan tourner, cela peut prendre beaucoup de temps.



Ici rien n'a été détecté, on peut cliquer sur Next



Si rien n'a été détecté, vous n'aurez rien à faire. Par contre, dans l'affirmative, n'hésitez pas à supprimer les fichiers éventuellement détec

Gmer

S'il y a bien un logiciel qu'il ne faut pas contourner dans cet article, c'est bien celui-ci.

Ultimate BootCD

Se prémunir

Son comportement

Eviter de

Surfer n'importe ou sans anti-virus

Récupérer et utiliser des cracks pour des antivirus commerciaux

Ouvrir une pièce jointe sans avoir vérifié sa provenance et confirmé par l'expéditeur

Les logiciels

Mises à jour

Les mises à jour n'apportent pas uniquement des nouvelles fonctionnalités ou des corrections de Bugs, mais aussi des corrections de failles

Il est donc important de maintenir son Système d'exploitation à jour en utilisant les outils de mise à jour fournis comme Windows Update s

Une petite astuce pour Windows, pensez à lancer la mise à jour manuellement de temps en temps, car certaines mises à jour ne peuvent pa notamment à l'outil Windows Installer utilisé par Windows Update, et de ce fait plus aucune mise à jour n'est détectée...

N'oubliez pas également de faire les mises à jour régulières de vos anti-virus etc...

Antivirus

Avast (http://www.avast.com)

Très complet il s'agit certainement du meilleur logiciel anti-virus gratuit dans le cadre d'une utilisation personelle.

Comodo (http://www.antivirus.comodo.com/)

Gratuit Perso & Pro à vie !!! (s'enregistrer avec la beta pour bénéficier de cette offre qui ne durera pas je pense, mais la licence acquise se
Le seul soucis est que ce logicile prend de plus en plus de ressources avec le temps, et votre PC fini par ramer. Il n'est pas recommandé pc

Antivirus à éviter

- Norton : Trop lourd et efficacité relative...
- Les tout en un, Antivirus, Firewall, etc : Car si une faille est découverte elle peut mettre en déroute toute la sécurité

Tests

PC Security Test (http://www.pc-st.com/fr/index.htm)

MicroWorld Free AntiVirus Toolkit Utility (MWAV) (http://www.mwti.net/products/mwav/mwav.asp)

Surfez sur Internet avec Firefox

Téléchargez et installez Firefox (http://pagead2.googlesyndication.com/pagead/iclk?sa=l&num=0&client=ca-ref-pub-9438421278873118&ad
/firefox/toolbar/bundle/intl/fr/%3Fai%3DB4wW0xUy2RvuaHofK0wS_--yPBtGe8hfdsZSXAsWNtwEAEAEgtcC0BDgBUK6qm935____wFg--
GFg5wKoAG1lcj9A7IBEHd3dy5jaHRpbGFuZC5jb23lAQLaARhodHRwOi8vd3d3LmNodGlsYW5kLmNvbS-AAgGoAwM&ai=BbqDPxUy2RvuaHofK
yPBtGe8hfdsZSXAsWNtwEAEAEgtcC0BDgBUP6pmYMEYPvhhYOcCqABtZXI_QOyARB3d3cuY2h0aWxhbmQuY29tyAEC2gEYaHR0cDovL3d3dy5j
et utilisez le comme navigateur par défaut, vous aurez déjà gagné en sécurité !

Une fois Firefox installé, ajoutez l'extension NoScript ainsi vous pourrez activer le Javascript et autres scripts uniquement pour les sites au
confiance.

Consultez également la page Firefox de ce WIKI pour plus d'infos

Conclusion

Service

Cette méthode semble trop complexe pour vous ? Vous n'arrivez pas à vous en sortir seul, ou vous n'osez pas par crainte de tout perdre ?
Contactez-moi (http://www.chtiland.com/modules/click/fclick.php?Contact) pour discuter d'une solution ensemble .

Autres

Cet article demeure la propriété de Chtiland.com et ne peut être diffusé sur un autre site (ou autre support) sans mon accord. Seuls les liens ve

Les captures d'écran ont été réalisées à l'aide de XnView (http://www.xnview.com/) sur l'hôte Windows.

Certaines images ont été retouchée à l'aide de Paint.net (http://www.getpaint.net) ou Gimp.

Afin de faire certains tests, j'ai également utilisé des packs de virus (574 + variantes) et trojans (68 + variantes). Inutile de me demander comm
permis. Pour les captures écran ces virus n'étaient pas résidents en mémoire, simplement copiés sur le disque dur. Tous n'ont pas été utilisés c
un test des différents anti-virus.

Récupérée de « http://www.chtiland.com/wiki/index.php/Nettoyer_Virus »

Catégories de la page: Informatique | En Cours

- Dernière modification de cette page le 1 juin 2008 à 23:15.
- Cette page a été consultée 7474 fois.
- Privacy policy
- À propos de ChtilandWiki
- Avertissements