N°265

INFO-AIVM 37

MAJ le 05/05/2013

Les malwares
Les barres pour navigateur

Présentation du problème

Suite à l'installation d'un freeware

- une barre toxique est venue se mettre dans vos navigateurs Internet
- votre page d'accueil a été modifiée sans votre consentement
- Un malware invisible est venu s'installer

Citation

PUP est l'acronyme de Potentially Unwanted Program soit donc logiciels potentiellement indésirables (LPI). Ce sont des programmes qui peuvent être non désirés mais qui peuvent tout de même être installé par l'utilisateur. Dans ces détections sont classées les adwares commerciaux ou barre d'outils qui sont bundles avec des programmes : souvent ces derniers modifient la page de démarrage et recherche afin d'augmenter le tracking, voir pour certains ouvrir des popups de publicités pour rémunérer l'éditeur.

Le schéma général est de proposer un programme gratuit et en contre-partie une barre d'outils ou un adware. Le fond du problème est que ces éditeurs ont en général des politiques assez aggressives voir trompeuses afin d'installer le plus possibles ces programmes (et donc gagner plus d'argent), l'utilisateur se laissent berner et installent ces programmes sans trop savoir ce qu'il en retourne, soit ils gagnent des popups de publicité, soit ils gagnent un packs complet de logiciels (barre d'outils, comparateur d'achats) qui a terme concours à ralentir l'ordinateur.

Ces programmes potentiellement indésirables ne sont pas à sous-estimer – Microsoft, via son rapport SIR, positionnant la France, fin 2011, comme championne des PUPs/Adwares.

Les plus communs et les logiciels utiles et dangereux.

Les logiciels où l'on ne peut pas éviter les saloperies même en prenant des précautions : Free-corder, Super, Freemake. Tous les autres freewares, ou presque, doivent être surveillés au moment de leur installation. (Cases à décocher ou bouton radio avec le bon choix). Même Java de chez Oracle, cCleaner et Photofiltre essaient de vous mettre en place la barre ASK, lors d'une **première installation** (pas pour les MAJ).

Liste des logiciels toxiques les plus courants :

Snap.do, Ask, Conduit, Pricegong sont les plus anciens.
Babylon, Iminent sont les plus pervers et les plus dangereux. Ils sont présents à plusieurs endroits, pour pouvoir reprendre la main si la désinstallation de ces saloperies n'est pas complète. Ils polluent tous vos navigateurs (IE, Firefox et Chrome). Ils prennent la main sur la page d'accueil pour vous envoyer leur pub.
Que font les institutions chargées des libertés informatiques pour intervenir ? Au lieu de jeter l'argent par les fenêtres avec la stupide loi Hadopi qui ne peut rien contre le steaming, intervenons sur les vrais dangers.
Si vous trouvez Iminent, vous devez le désinstaller avec Iobit Uninstaller ou Uninstaller Pro 11, car il faut supprimer tous les liens, ce que ne font pas le désinstalleur du panneau de configuration ou cCleaner.

Comment éliminer ces logiciels crapuleux ?

Comme toujours, la meilleure solution consiste à passer AdwCleaner. Mais dans le cas de snap do, je n'ai réussi à éliminer que les barres mais pas le logiciel.

Dans tous les cas

Avant de commencer.

Préparez un document texte, avec le bloc- notes, contenant toutes les URL que vous avez l'habitude d'utiliser pour vos pages d'accueil.
Voici un exemple, nommé MAJNavigateurs.txt

CHROME
------
https://www.google.fr/
http://aivm.free.fr/
https://accounts.google.com/ServiceLogin? Etc… (pour mon agenda gmail personnel)

FIREFOX
----
https://google.fr | http://aivm.free.fr | http://fr.search.yahoo.com?type=198484&fr=spigot-yhp-ff

IE
---
https://www.google.fr/
http://aivm.free.fr/
http://fr.search.yahoo.com/?type=198484&fr=spigot-yhp-ie

Etape 1.

Téléchargement de AdwCleaner et de Eraser

Télécharger la toute dernière version de **AdwCleaner** depuis
http://www.pcastuces.com/logitheque/adwcleaner.htm
http://www.01net.com/telecharger/windows/Utilitaire/nettoyeurs_et_installeurs/fiches/118605.html
http://telecharger.tomsguide.fr/AdwCleaner,0301-48079.html
puis le logiciel **Eraser** à télécharger par exemple ici :
http://www.clubic.com/telecharger-fiche11144-eraser.html
http://www.01net.com/telecharger/windows/Utilitaire/nettoyeurs_et_installeurs/fiches/6615.html
http://sourceforge.net/projects/eraser/

Etape 2

Exécutez AdwCleaner (ce logiciel ne s'installe pas).
Passez directement la commande du bouton Supprimer (gigure page suivante).
En fermant AdwCleaner, il va vous demander de redémarrer la machine.
Vous pouvez par la suite, effacer le rapport qui se trouve dans la racine du disque C.

En principe, les barres sont éradiquées des navigateurs, mais il faut remettre les pages d'accueil dont vous avez l'habitude. L'idéal est de copier ces adresses URL dans un fichier texte, pour pouvoir faire du Copier/Coller à chaque fois que vous avez besoin de réinitialiser vos pages d'accueil.

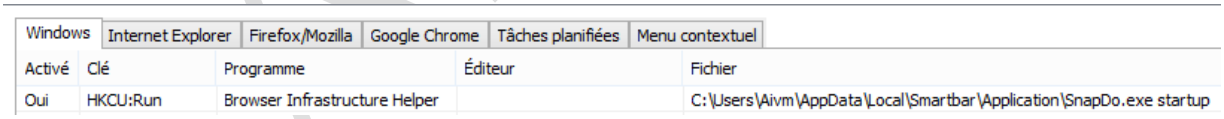
Généralement le passage de AdwCleaner suffit à tout nettoyer.

Smartbar et Snap.do

Présentation du problème

Ce malware se présente sous deux formes :

1. Des barres d'outils dans chaque navigateur avec prise en main des pages d'accueil sur IE, Chrome et Firefox.
2. Un logiciel qui se télécharge à l'ouverture de votre OC comme le montre la figure ci-dessous obtenu depuis cCleaner.



D'une façon générale qu'est-ce que c'est ?

SNAP.do	Cette saloperie est pudiquement appelé LPIs, c'est-à-dire « Logiciels potentiellement Indésirables ». Il faut retirer cette « merde » le plus rapidement possible.

Etape 3

Faites en sorte de voir les répertoires cachés.
Si le répertoire suivant existe toujours après le passage de AdwCleaner, il faut le détruire.

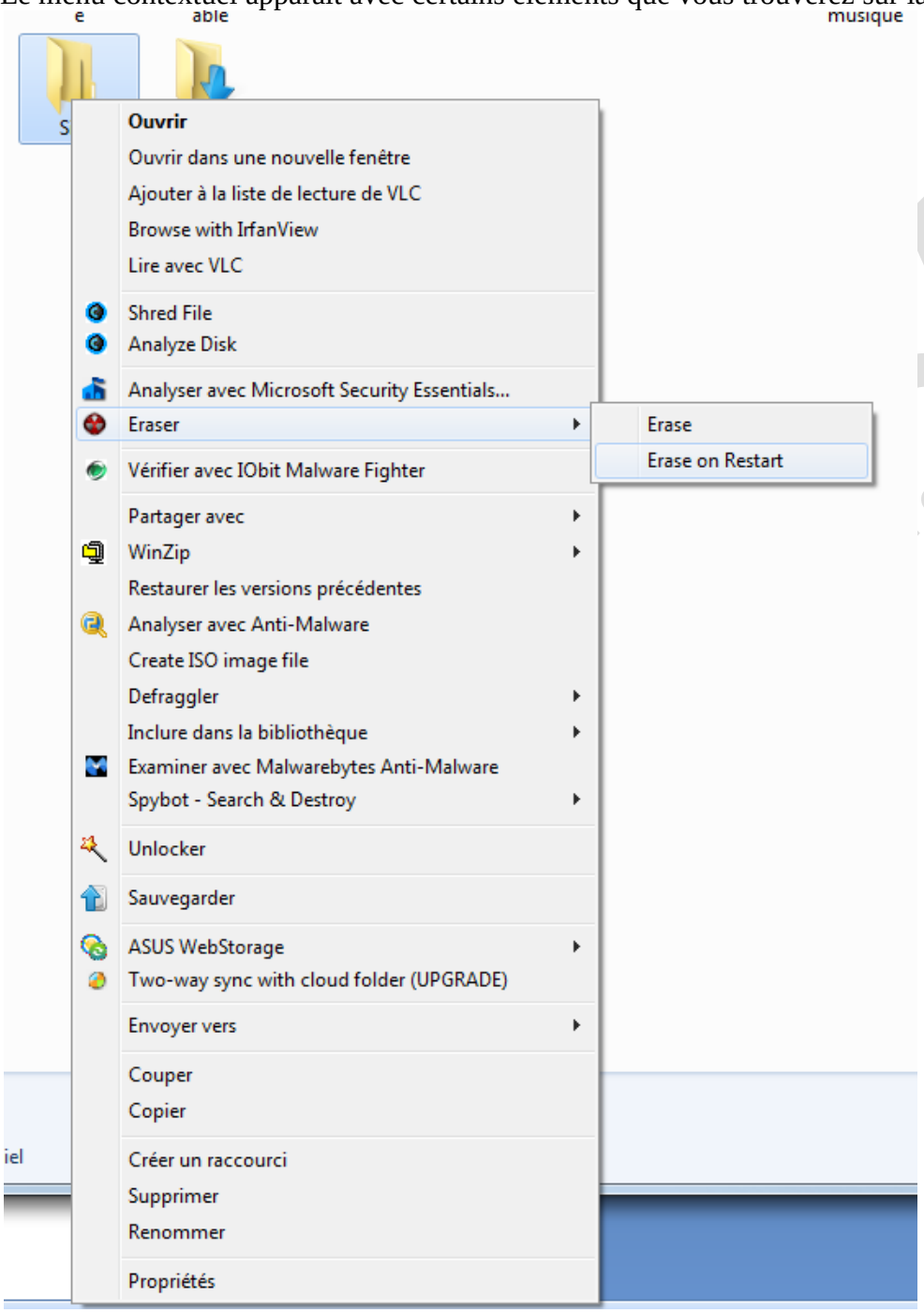
C:\Users\<Votre nom>\AppData\Local\Smartbar

C'est alors le moment de livrer l'assaut final, en utilisant le logiciel **Eraser.**

Installez Eraser. Pas de problème à ma connaissance au moment de l'installation avec toutes les options par défaut.

Cliquez du bouton droit sur le répertoire en question Smartbar.

Le menu contextuel apparaît avec certains éléments que vous trouverez sur la figure ci-dessous/



Vous trouvez Eraser. Comme l'un des fichiers des dossiers Contenu dans Smartbar est ouvert, il est impossible de supprimer le dossier. Cliquez en conséquence sur **Erase on Restart**, qui signifie « Supprimer au redémarrage ».

Il vous suffit alors de relancer votre PC et dès le démarrage le dossier sera supprimé.

OUF…

Du même genre

Vous trouvez aussi **Babylon** et **Conduit** qui sont aussi des malwares puissants et dont il faut se débarrasser absolument.

Remarque

Le site de xplode qui a crée AdwCleaner, est considéré comme dangereux par site advisor et je n'en connais pas la r
aison. Voilà pourquoi je préfère vous donner des adresses sur des sites plus sûr.

Il n'en reste pas moins, que si une nouvelle version vous est signalée et qu'elle n'est pas encore à jour chez Clubic, PcAstuces ou 01Net, vous pouvez télécharger sur le site de Xplode, sans rien faire d'autre, et en vous sauvant le plus vite possible après le téléchargement. Personnellement je n'ai jamais eu d'ennui.

Quelques précautions

Le grand nettoyage par Adwcleaner, Iobit Uninstall Care, Spybot, Glary Utilities se tremine parfois avec un profil endommagé dans Chrome/ Votre barre de favoris devient alors inaccessible. J'ai fait une fiche pour anticiper ou résoudre ce problème : http://aivm37.free.fr/BI/JT/JT270_ReparerProfilChrome.pdf

Analyse par AdwCleaner

Voici une liste après l'installation de la bande de lancement d'un film avec un exécutable pourri. J'ai coupé, il y en a quatre pages, à cause d'un seul logiciel :

AdwCleaner v2.300 - Rapport créé le 04/05/2013 à 22:24:53
Mis à jour le 28/04/2013 par Xplode
Système d'exploitation : Windows 8 Pro with Media Center (64 bits)
Nom d'utilisateur : Aivm - PCAIVM
Mode de démarrage : Normal
Exécuté depuis : D:\Téléchargements\adwcleaner.exe
Option [Suppression]

***** [Services] *****

Arrêté & Supprimé : SProtection

***** [Fichiers / Dossiers] *****

Dossier Supprimé : C:\Program Files (x86)\Common Files\Umbrella
Dossier Supprimé : C:\Program Files (x86)\Iminent
Dossier Supprimé : C:\Program Files (x86)\IMinent toolbar
Dossier Supprimé : C:\Program Files (x86)\IObit Apps Toolbar
Dossier Supprimé : C:\Program Files (x86)\TornTV.com
Dossier Supprimé : C:\Program Files (x86)\Yontoo
Dossier Supprimé : C:\ProgramData\Iminent
Dossier Supprimé : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Iminent
Dossier Supprimé : C:\Users\Aivm\AppData\Local\Google\Chrome\User Da-
ta\Default\Extensions\igdhbblpcellaljokkpfhcjlagemhgjl
Dossier Supprimé : C:\Users\Aivm\AppData\Local\Temp\Iminent
Dossier Supprimé : C:\Users\Aivm\AppData\Roaming\Iminent
Dossier Supprimé : C:\Users\Aivm\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\TornTV.com
Dossier Supprimé :
C:\Users\Aivm\AppData\Roaming\Mozilla\Firefox\Profiles\pk272ymt.default\extensions\{C9B68337-
E93A-44EA-94DC-CB300EC06444}
Dossier Supprimé :
C:\Users\Aivm\AppData\Roaming\Mozilla\Firefox\Profiles\pk272ymt.default\extensions\plugin@yontoo.co
m
Fichier Supprimé : C:\Program Files (x86)\Mozilla Firefox\defaults\pref\all-iminent.js
Fichier Supprimé : C:\Program Files (x86)\Mozilla Firefox\searchplugins\StartWeb.xml
Fichier Supprimé : C:\Users\Aivm\Desktop\TornTV.lnk

***** [Registre] *****

Clé Supprimée : HKCU\Software\1ClickDownload
Clé Supprimée : HKCU\Software\APN PIP
Clé Supprimée : HKCU\Software\Iminent
Clé Supprimée : HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{03EB0E9C-7A91-4381-A220-9B52B641CDB1}
Clé Supprimée : HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{03EB0E9C-7A91-4381-A220-9B52B641CDB1}
Clé Supprimée : HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\grusskartencenter.com
Clé Supprimée : HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\EscDomains\grusskartencenter.com
Clé Supprimée : HKCU\Software\PIP
Clé Supprimée : HKCU\Software\Microsoft\Internet Explorer\SearchScopes\{BFFED5CA-8BDF-47CC-AED0-23F4E6D77732}
Clé Supprimée : HKLM\SOFTWARE\Classes\AppID\{01994268-3C10-4044-A1EA-7A9C1B739A11}