



# Freecorder

## Freecorder

MAJ le30/03/2011

### Présentation du problème

Ce logiciel est bien pour écouter de la musique mais il contient au moins un malware Conduit Lcd Pricegong.

Il faut donc essayer de supprimer le maximum d'éléments nuisibles :

1. Au moment de l'installation
2. Après l'installation

### A voir

Pour Windows 7, voir la fiche 142 qui concerne les fichiers inutiles sur le disque système.

[http://aivm.free.fr/BI/JT/JT142\\_FichiersInutilesSurDisqueC.pdf](http://aivm.free.fr/BI/JT/JT142_FichiersInutilesSurDisqueC.pdf)

### Téléchargement

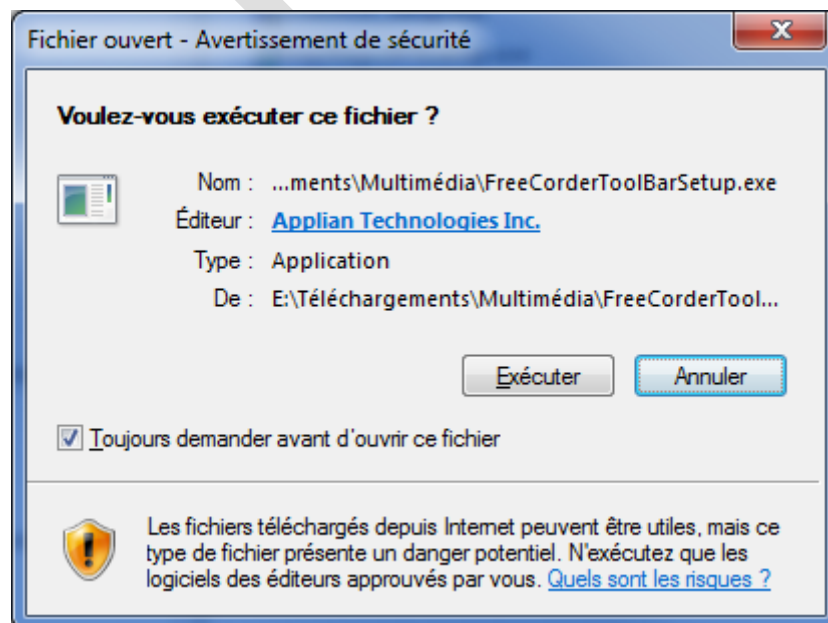
Voici les sites possibles pour le téléchargement du setup de la Toolbar

<http://www.01net.com/telecharger/windows/Internet/plugins/fiches/49590.html>

[http://www.01net.com/telecharger/windows/Multimedia/edition\\_audio/fiches/29515.html](http://www.01net.com/telecharger/windows/Multimedia/edition_audio/fiches/29515.html)

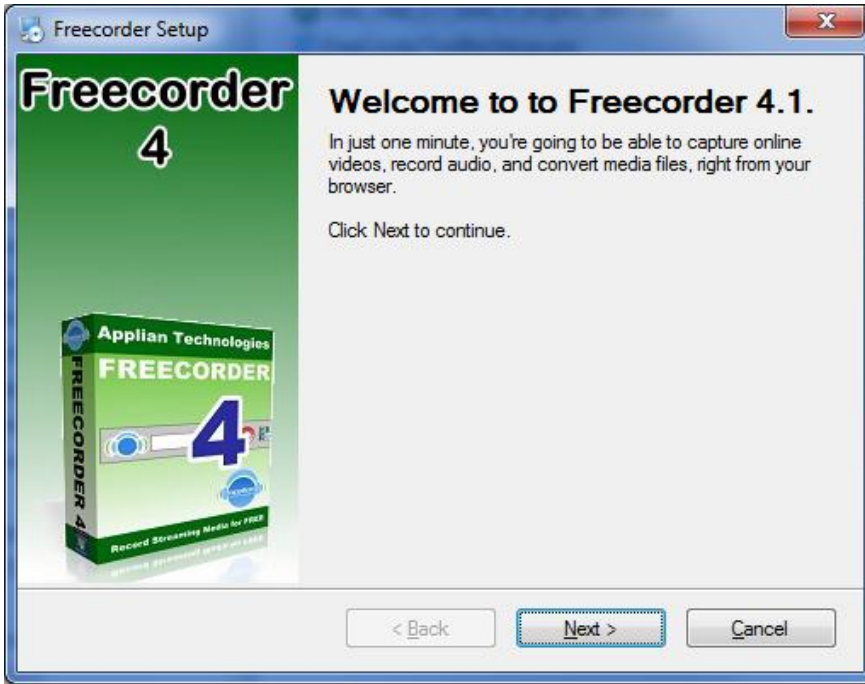
<http://www.commentcamarche.net/download/telecharger-34057249-freecorder-toolbar>

### Installation

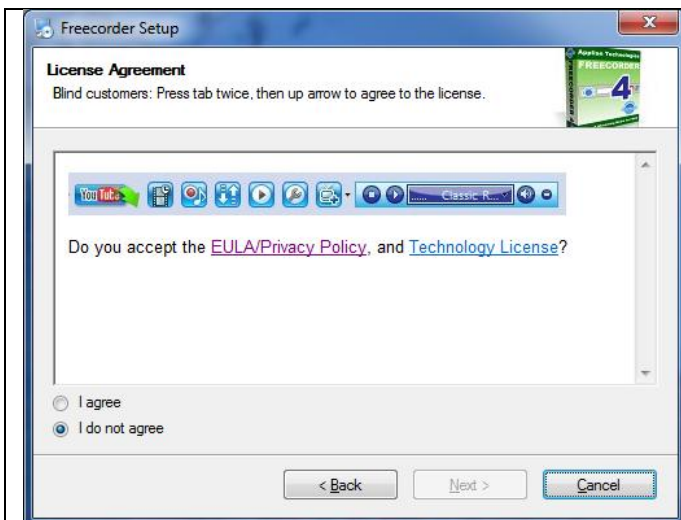


Vous devez cliquer sur Exécuter, vous n'avez pas le choix.

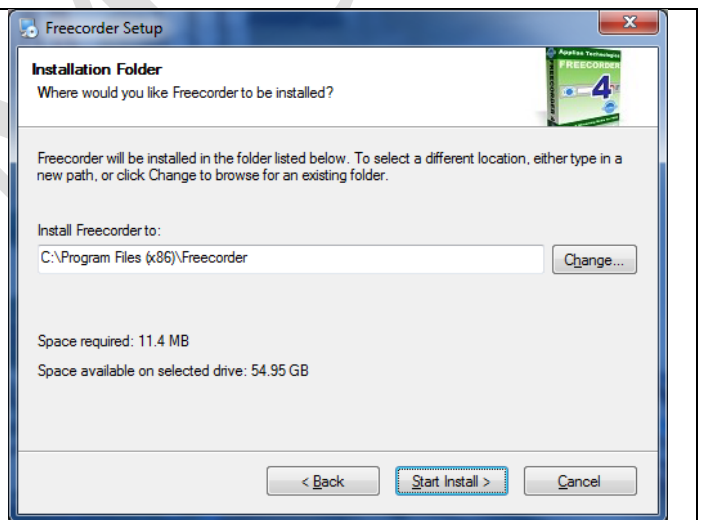
# Fiche Technique



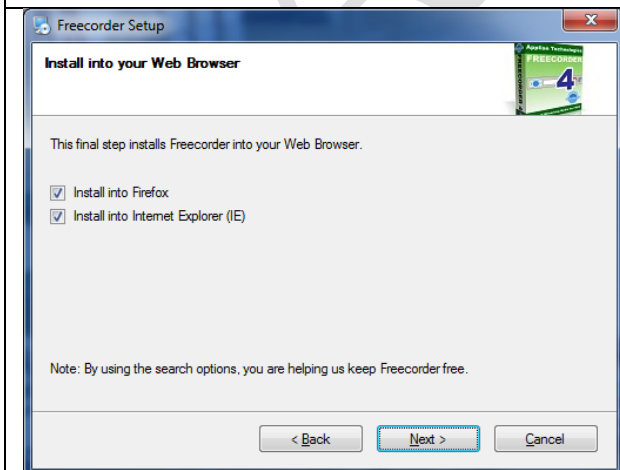
Là encore, sur cet écran, pas de choix. Cliquez Next



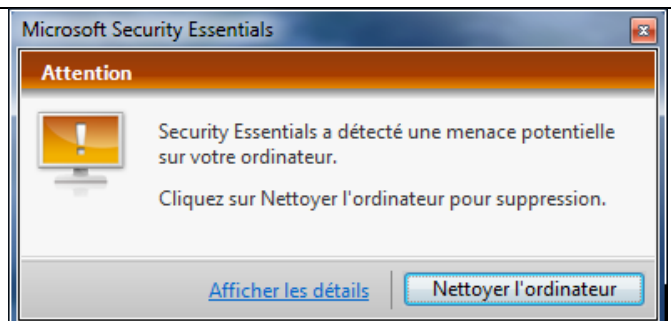
Pas le choix là non plus. Cliquez I Agree puis Next



Gardez le répertoire par défaut et cliquez Start Install

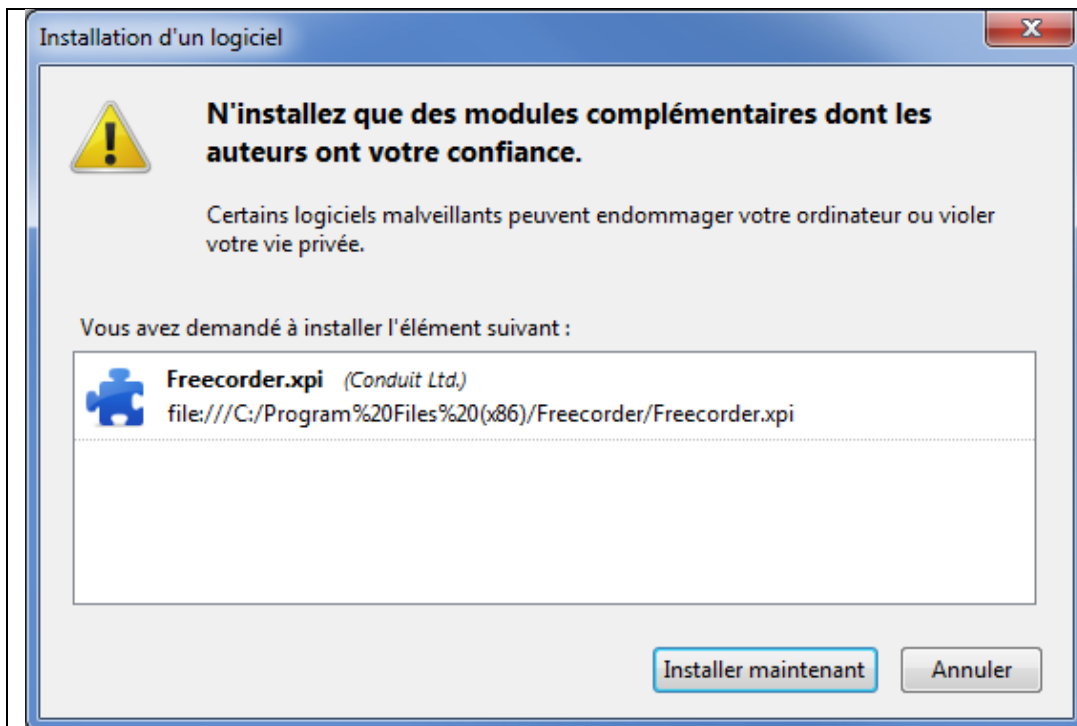


Gardez les deux choix, et cliquez sur Next



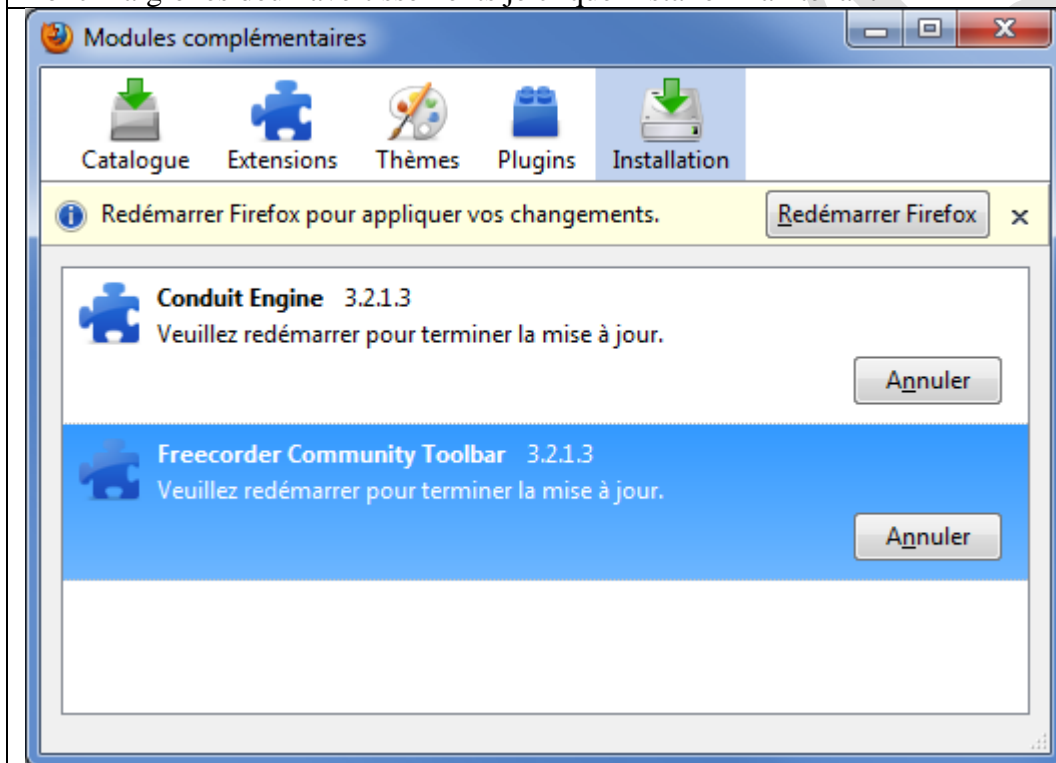
Mais comme vous pouvez le constater une menace est détectée par Microsoft Security Essentials, que vous laissez en attente, sans répondre.

## Fiche Technique



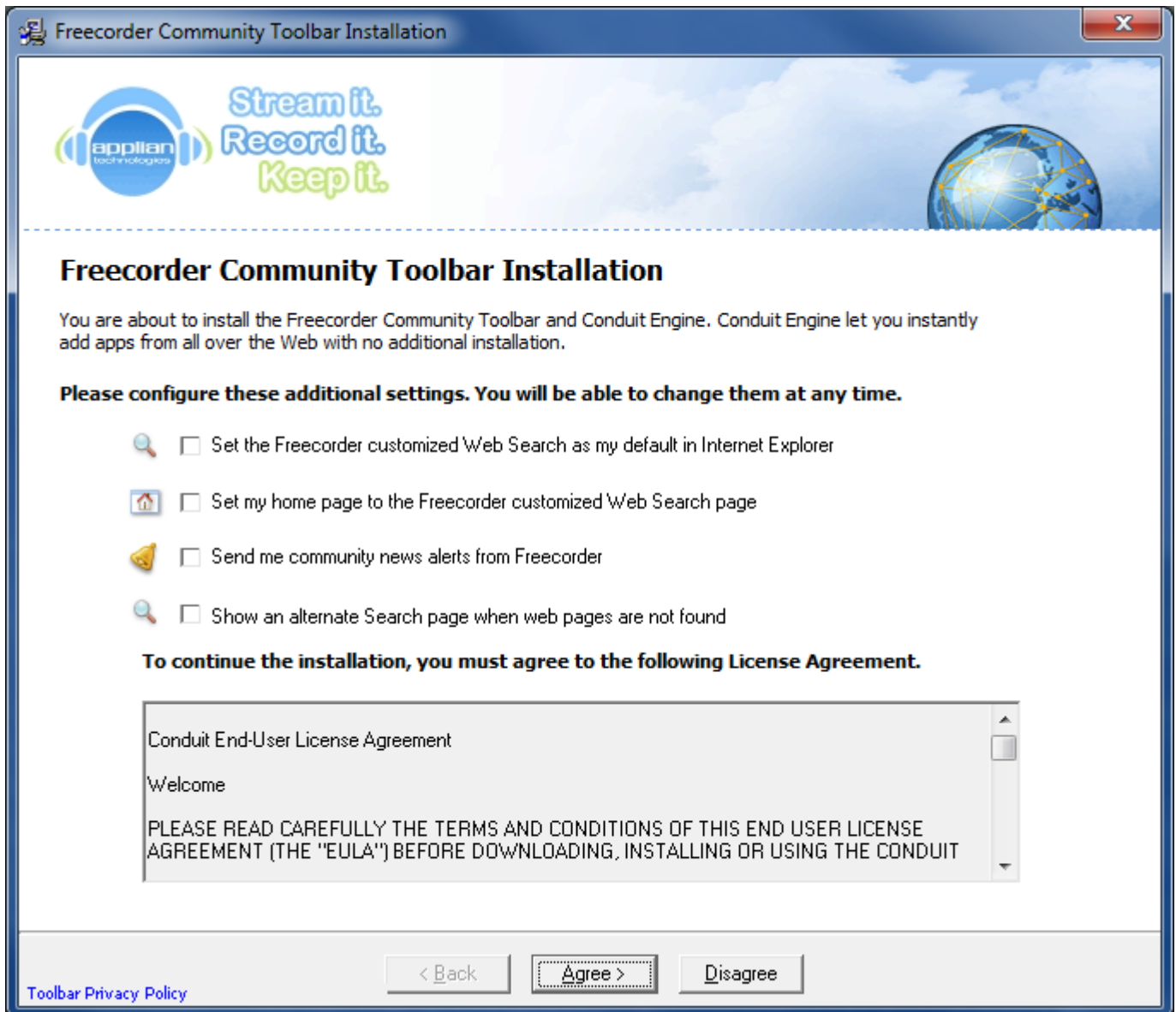
Avec Internet Explorer 9 vous recevez un deuxième avertissement. Le logiciel peut être malveillant ou porter atteinte à votre vie privée. Les choses sont claires. Mais je vais tout de même insister, car toutes les barres mouchardent, que ce soit celle de Microsoft (Bing) ou celle de Google, c'est la même chose. Ici, il semble que ce soit commercial avec indexation de produits.

Donc malgré les deux avertissements je clique Installer maintenant



Firefox vient d'ouvrir cette fenêtre où je constate le module Conduit Engine qui est lui aussi lié à Freecorder. Je fais donc la mise à jour. Firefox demande à être redémarré. J'exécute cette manipulation, puis je ferme Firefox.

Sur la fenêtre suivant il est prudent de tout annuler



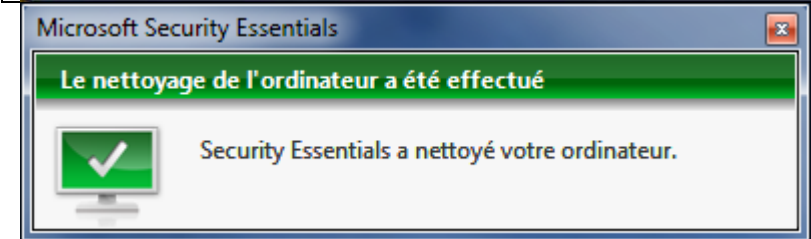


Je conseille de tout annuler puis de cliquer sur Agree. J'ai droit à cette fenêtre d'accueil. Depuis IE9



A ce niveau, testez si La Toolbar fonctionne en récupérant un streaming quelconque, radio, musique... Tester le fichier MP3 créé.

S'ouvre alors une autre fenêtre que je refuse.(page suivante)

	<p>Pas question d'installer ce logiciel associé. Décochez la case correspondante. On ne sait absolument pas à quoi peut servir ce logiciel. Des logiciels sérieux s'occupent très bien de la BDR. Cliquez sur Continue et vous aboutissez au dernier écran</p>
	<p>Cliquez sur Finished et lance Nettoyer l'ordinateur depuis la fenêtre de l'antivirus Essentials, qui est restée ouverte. Intervenir plus tôt n'aurait pas permis d'installer Freecorder.</p>
	<p>Cette fenêtre de l'antivirus apparaît. Elle ne veut rien dire car il est trop tard. Si mal il y a, il est déjà fait. Il nous reste maintenant à faire le ménage. Deux logiciels ont été installés (Freecorder et Freecorder Toolbar. <b>Il est malheureusement impossible de désinstaller Freecorder seul en ne gardant que la Tool bar, avec les dernières versions.</b></p>

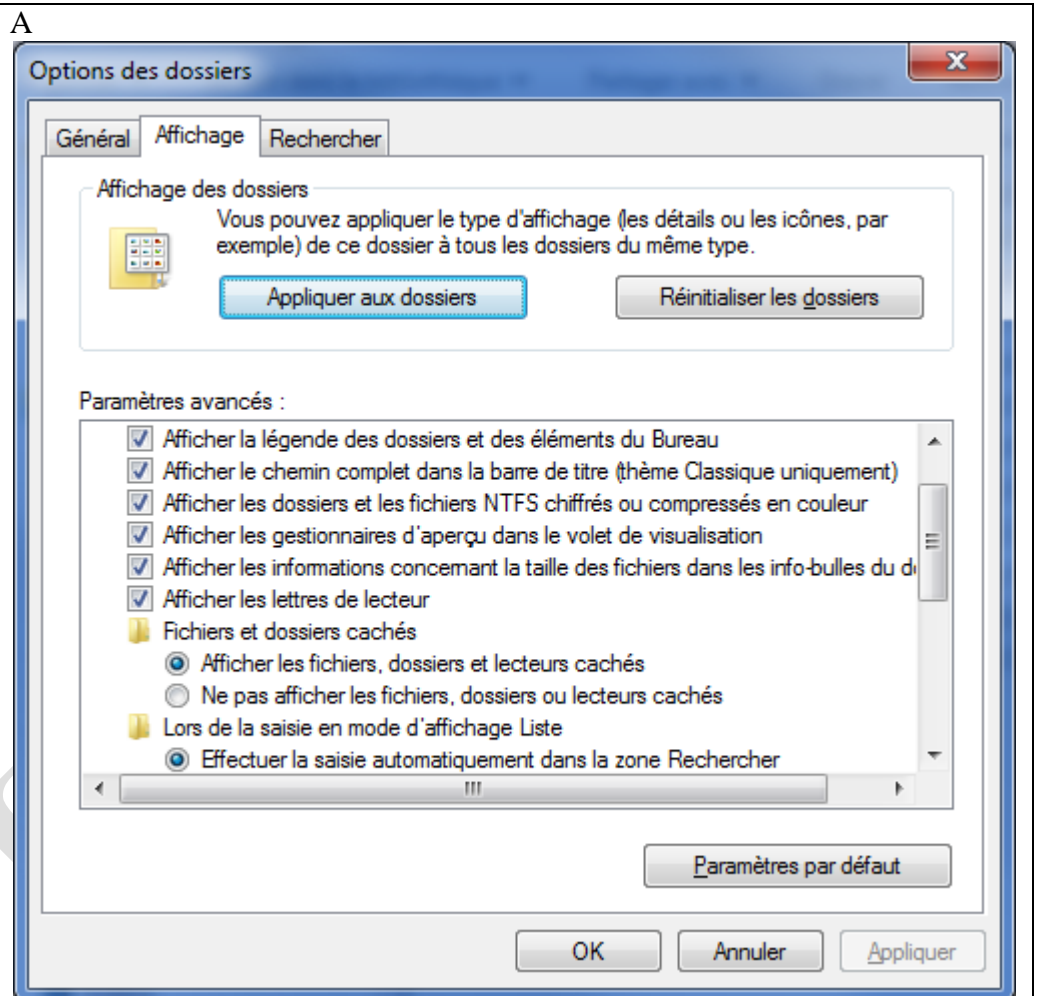
## Comment procéder

### Suppression pure et dure de PriceGong

**Avant de commencer, faite fonctionner Freecorder pour constater que tout va bien et pour qu'il termine de mettre les répertoires en place. Puis relancez votre PC (reboot).**

#### Etape 1

Comme la désinstallation est impossible nous allons procéder en force. Vous devez rendre visibles, tous les fichiers et dossiers cachés. Pour cela dans une fenêtre quelconque de l'explorer de Windows, afficher le menu. Commande Outils → Options des dossiers → Onglet Affichage → et cocher « Afficher les fichiers et dossiers cachés ». Figure ci-jointe de la fenêtre correspondante. Il faudra redémarrer votre machine sans relancer votre navigateur IE9 ou Firefox.



#### Etape 2 : Avec Vista et Windows 7

Fermez Internet Explorer et Firefox afin que la toolbar Freecorder ne soit pas active.

Ouvrez Ordinateur → C:\ → Utilisateurs → Votre nom de connexion → AppData → LocalLow

1. Supprimer purement et simplement le répertoire PriceGong.
2. Ouvrez maintenant le répertoire Freecorder et supprimer de même le sous répertoire plugins qui contient la même DLL que PriceGong. Validez avec oui sur la fenêtre de confirmation.

Avec XP, remplacer Utilisateur par documents and settings et Appdata par Applications Data, vous trouvez tout de suite les répertoires correspondants. Faites les mêmes suppressions.

#### Etape 3 : Avec Vista et Windows 7 version 64 bits

Internet Explorer et Firefox doivent être fermés. Avec XP essayer de trouver quelque chose de semblable.. Vous pouvez aussi faire une recherche de PriceGong.dll pour détecter les répertoires.

Ouvrez Ordinateur → C:\ → Windows → SysWOW64 → Config → systemprofile → AppData → LocalLow .

Si vous trouvez le répertoire PriceGong, supprimez le (possible si la dll n'est pas en mémoire).

## Fiche Technique

Entrez dans le répertoire Freecorder et supprimez, là aussi plugins, s'il existe.

Si vous avez trouvé les deux répertoires et que vous les avez supprimés, vous serez tranquille. Dans le cas contraire, ils réapparaîtront systématiquement au démarrage de la toolbar dans le répertoire de l'étape 2.

### Etape 4 : recherche de la DLL pricegongIE.dll

Faites une sauvegarde de votre système pour restauration éventuelle.

Faites la recherche sur tout le disque C. Lorsque vous avez trouvé, cliquez bouton droit sur le fichier pour trouver son emplacement et supprimer le répertoire qui le contient, y compris dans le système (sous répertoire SysWoW64 du répertoire Windows, pour la version 64 bits)

### Etape 5 : Nettoyage base de registre

Remarque : La base de registre est souvent nommée BDR. Faites une sauvegarde de la BDR avant de commencer, au cas où vous feriez une grave erreur. Lancer Regedit (éditeur de registre) et cherchez PriceGong. Supprimez toutes les clés que vous trouvez (en principe 2 clés trouvées, correspondant aux deux répertoires précédents).

Rechercher la clé {5E1360DC-8FA8-40df-A8CD-FC3831B3634B} en faisant ici un copier coller et supprimer toutes ces occurrences dans la BDR avec la clé plugins qui la contient (venant de freecorder)

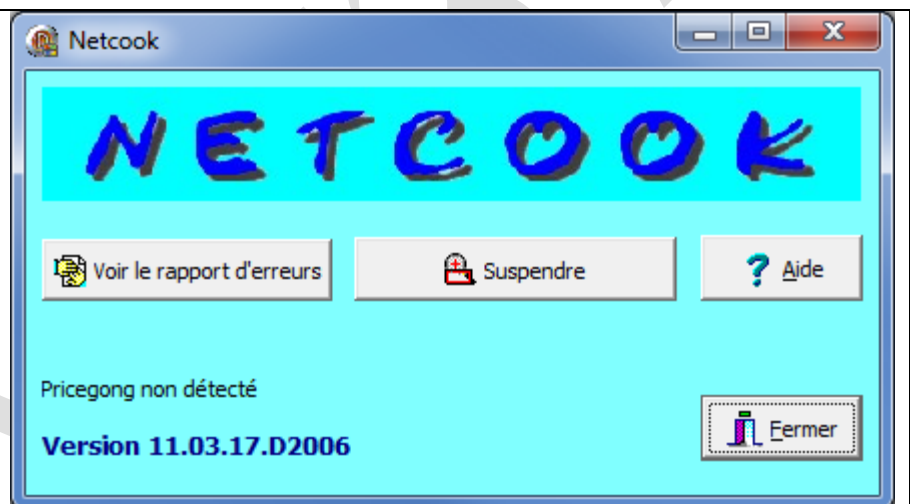
## Ultime solution

Si Pricegong réapparaît, à chaque démarrage de freecorder, ce qui semble être le cas dans la dernière version, utilisez le logiciel que j'ai créé JT\_Util, bouton Nettoyage des cookies.

Ce logiciel, si vous le lancez, avant d'ouvrir le navigateur contenant freecorder, va « flinguer » les répertoires temp, cookies toutes les dix secondes ainsi que PriceGong et les plugins de Freecorder Toolbar.

Vous évitez le mouchardage tout en conservant Freecorder actif.

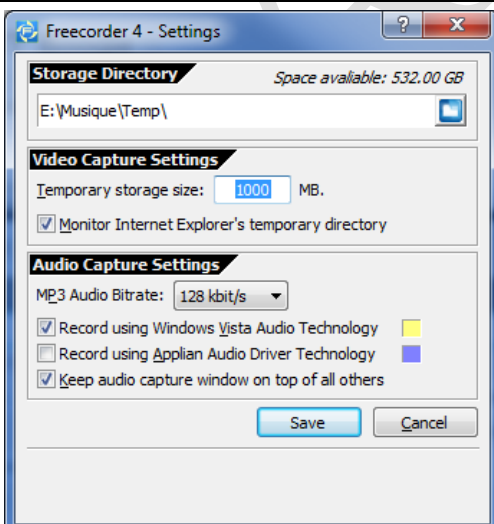
Refermez IE ou Firefox au moins 10 secondes avant Netcook. Ainsi les fichiers de PriceGong seront supprimables car la dll ne sera plus en mémoire



Pour le télécharger directement (vous pouvez y accéder depuis les pages d'accueil de mes sites aivm.free.fr ou jean.thiou.free.fr) ou directement depuis la page suivante.

[http://jean.thiou.free.fr/JT\\_Util/Aide\\_JTUtil.htm](http://jean.thiou.free.fr/JT_Util/Aide_JTUtil.htm)

Netcook est un composant de JT\_Util



Dans tous les cas ce module Netcook (Nettoyage des cookies) est indispensable à un semblant de vie privée sur Internet en supprimant les mouchards toutes les 10 secondes. Il interrompt tout espionnage. Fermez l'explorer (IE ou Firefox) avant netcook. Une fois l'explorer Internet fermé, Netcook ne mettra pas plus de 10 secondes à supprimer tous les fichiers de PriceGong. Fermez alors netcook. Ce logiciel tient peu de place en mémoire. Il peut rester ouvert en permanence, tout en refermant JT\_Util qui n'est qu'un lanceur.

## Réglage de Freecorder

Depuis la barre le bouton avec la clé plate.

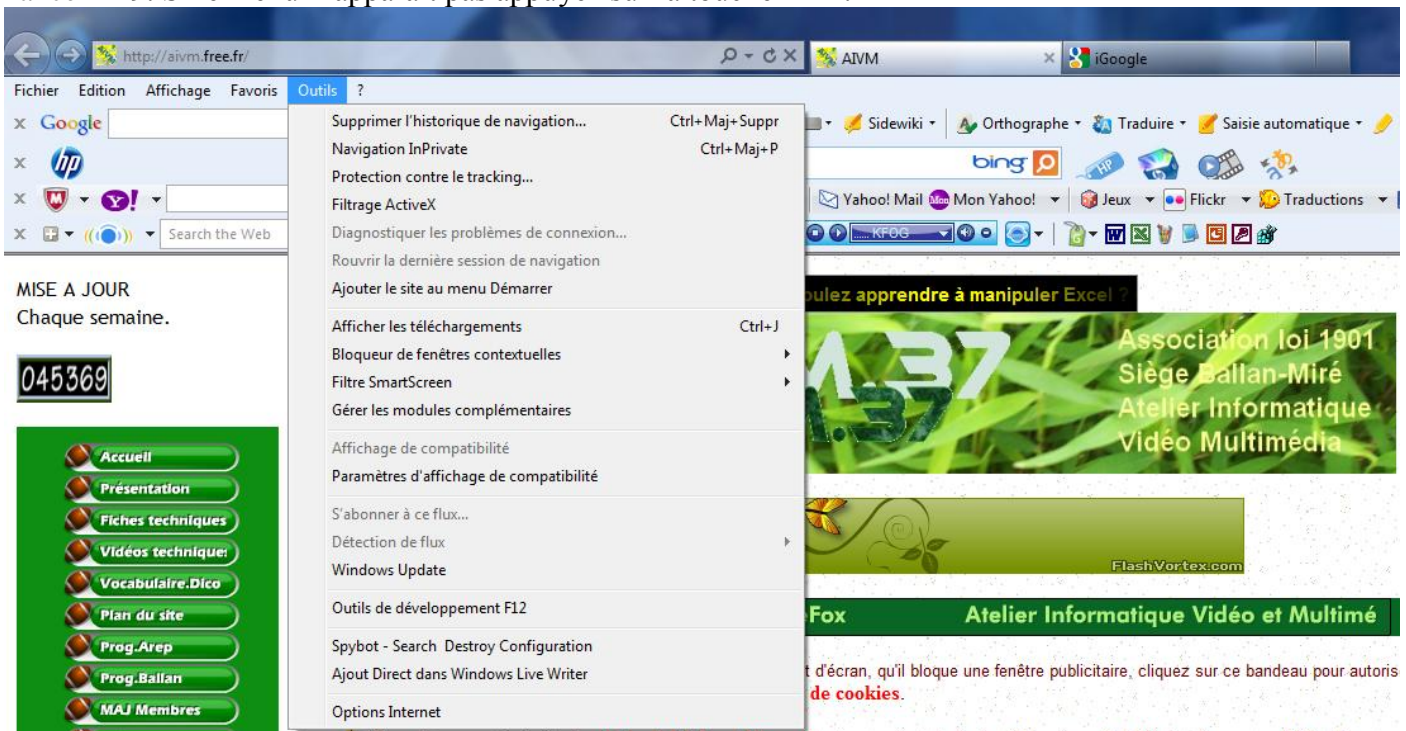
Donnez le répertoire où vous souhaitez récupérer les enregistrements du streaming en MP3 et choisissez en bas le format de votre MP3 (jaune ou bleu, à vous de voir).

# Fiche Technique

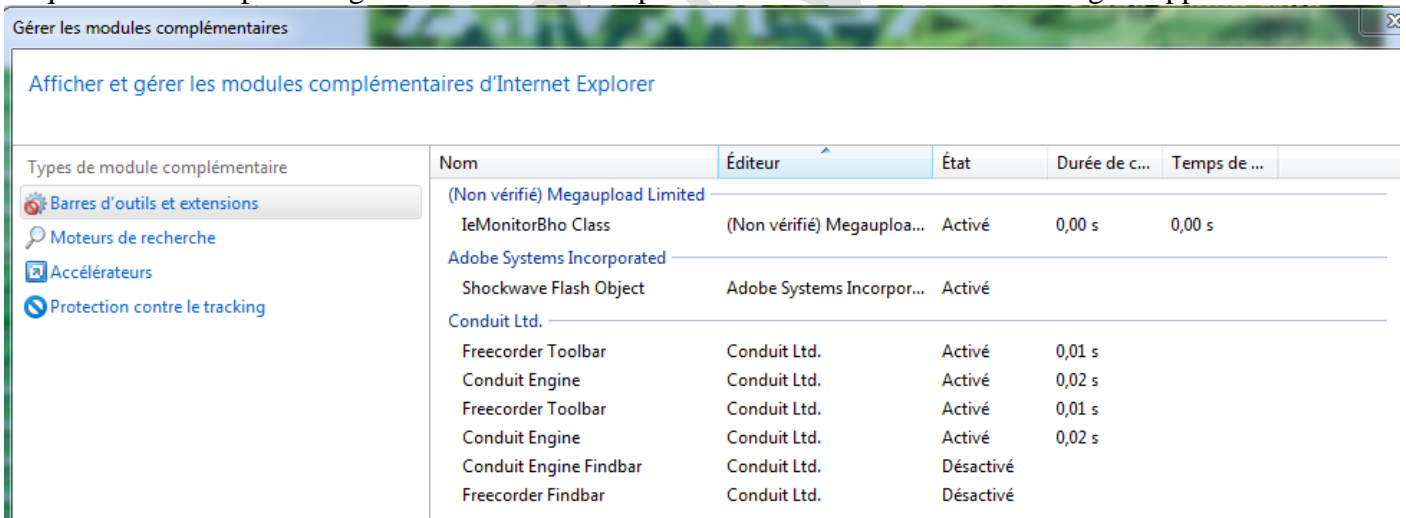
Laissez la dernière coche qui permet de toujours voir la fenêtre de freecorder .

## Une solution qui semble possible avec IE9.

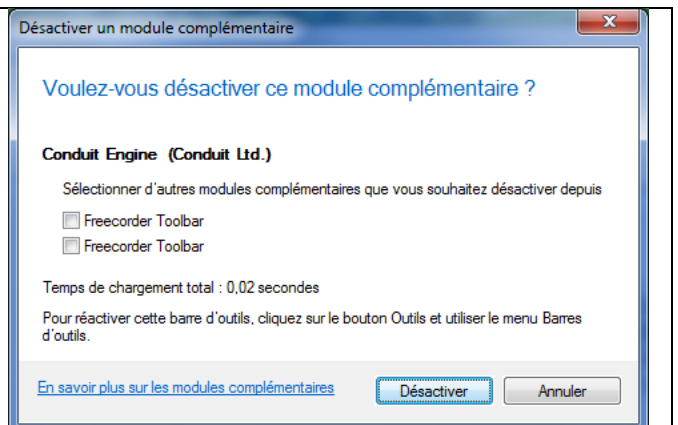
Lancez IE9. Si le menu n'apparaît pas appuyez sur la touche ALT.



Cliquez sur Outils puis sur gérer les modules complémentaires. Le fautif Conduct Engine apparait alors.

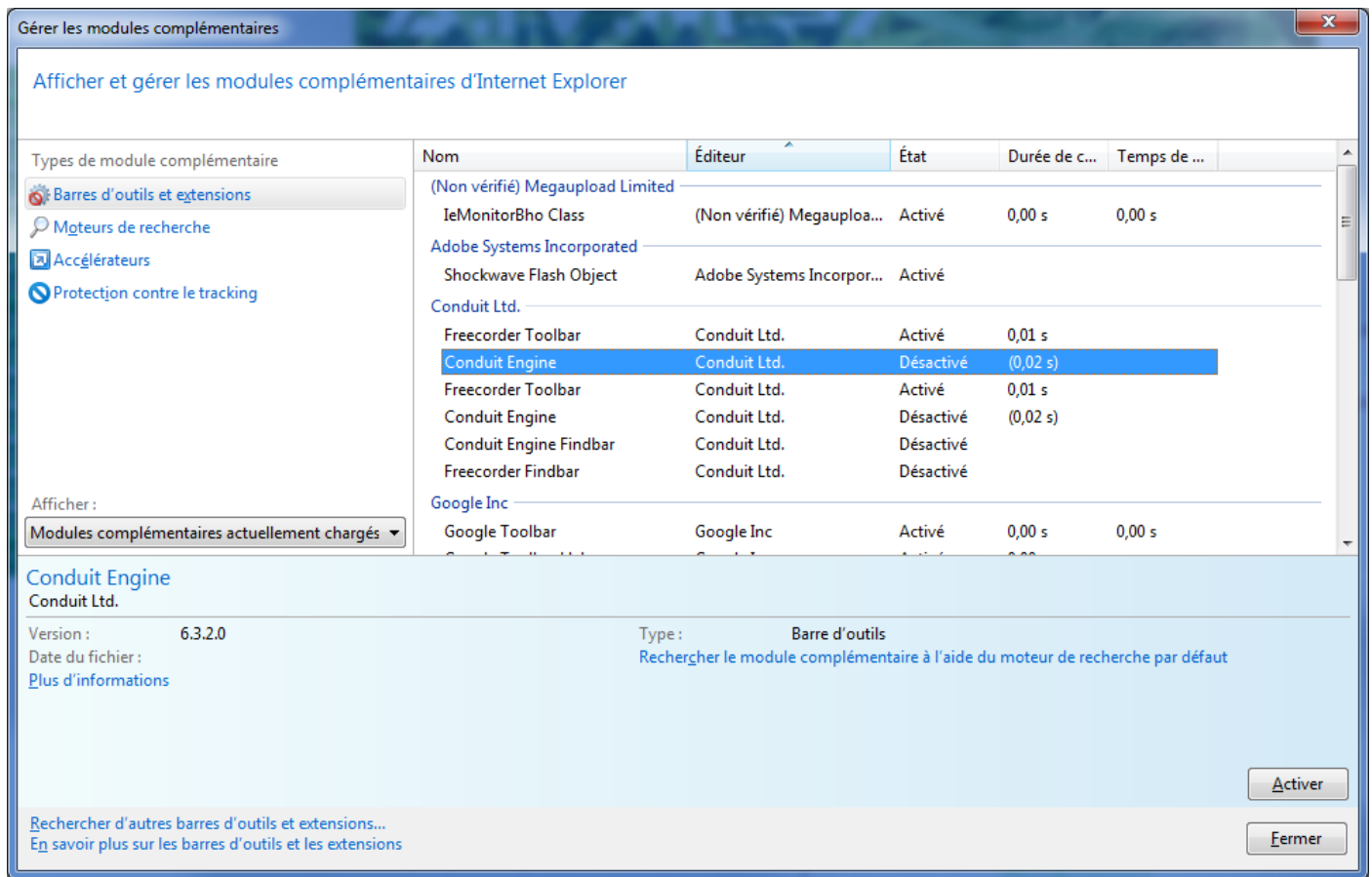


Cliquez sur le premier Conduit Engine, puis cliquez en bas sur le bouton **Désactiver**. La nouvelle fenêtre ci-jointe apparaît. Ne cochez pas Freecorder Toolbar, mais cliquez à nouveau en bas sur **Désactiver**. Vous allez alors arriver à la situation suivante, qui ne bloque pas le fonctionnement de la Toolbar, mais semble faire en sorte qu'après fermeture de IE on puisse supprimer PriceGong (plus de dll en mémoire). Page suivante, ce que vous obtenez.



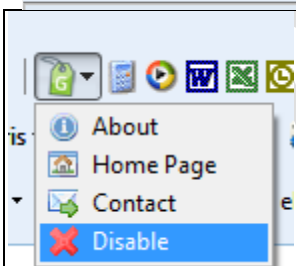


# Fiche Technique



Gardez cette situation, définitivement.

Ensuite dans IE9, barre Freecorder, cliquez sur le bouton de fenêtre déroulante ci-dessous :



Ce bouton désactive complètement PriceGong dans le supprimer.

Dans la barre free-corder, cliquez sur la fenêtre déroulante contenant une lettre G à peine visible. Cliquez sur Disable qui doit désactiver PriceGong. En effet Netcook semble indiquer, malgré IE9 ouvert que maintenant PriceGong est supprimé. Fermer IE9.



Netcook indique alors « Pricegong temporairement supprimé ». Il semble qu'il ne reviendra pas en ouvrant IE9. **Mais comme « désactivé » ne signifie pas « supprimé »**, Netcook est nécessaire pour retirer tous les répertoires correspondants à PriceGong et la dll correspondante

## Fiche Technique

Fermez IE9, puis fermez Netcook lorsqu'il affiche « PriceGong temporairement supprimé »  
Relancez Netcook, il doit afficher « PriceGong non détecté ». Même si PriceGong réapparaît, sa base de données n'existe plus, ce qui est essentiel.

### Étape ultime

Malheureusement, je n'y crois pas, car là non plus, rien n'est définitif. Un simple faux moyen de se débarrasser pour ce site dont le seul but est de vous installer ce malware. Essayez quand même..

Télécharger le fichier uninstall.exe sur le site de PriceGong.

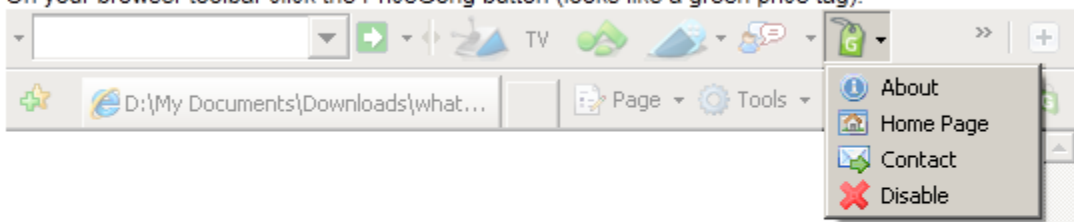
[http://www.pricegong.com/Removing\\_PriceGong.aspx](http://www.pricegong.com/Removing_PriceGong.aspx)

Voici le bas de la page qui s'ouvre :

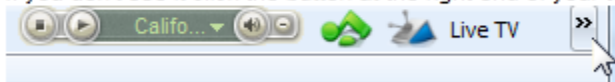
#### **Disable PriceGong on a browser toolbar**

In case you have installed a browser toolbar that includes PriceGong as an additional service, all you need to do is disable it as follows:

1. On your browser toolbar click the PriceGong button (looks like a green price tag).



If you don't see it click the button at the right end of your toolbar, this will expose the PriceGong button.



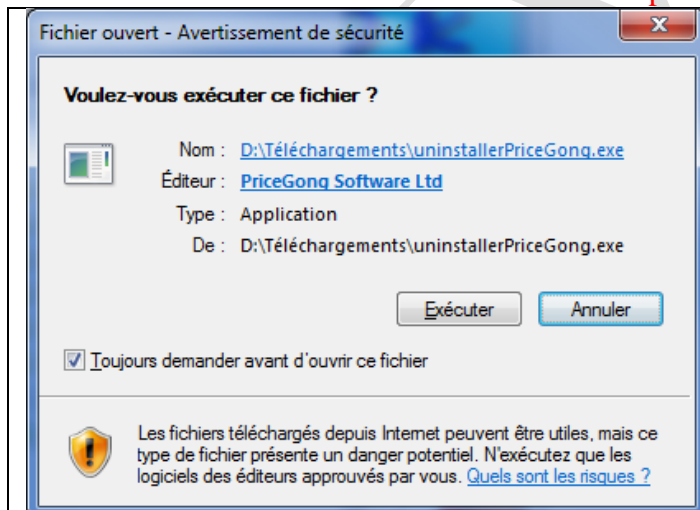
2. From the menu opened select "Disable".

You can also download our removal tool that will help you uninstall PriceGong by running it.

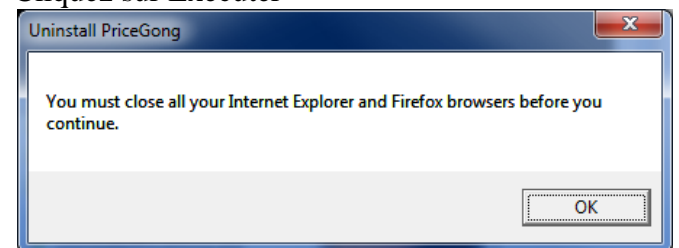
[Click here](#) to download PriceGong Removal Tool.

En cliquant sur « Click here » vous allez télécharger un fichier nommé Uninstaller.exe

Redémarrer votre machine. **Ne démarrez surtout pas de navigateur Internet.** Lancez ce fichier Uninstaller



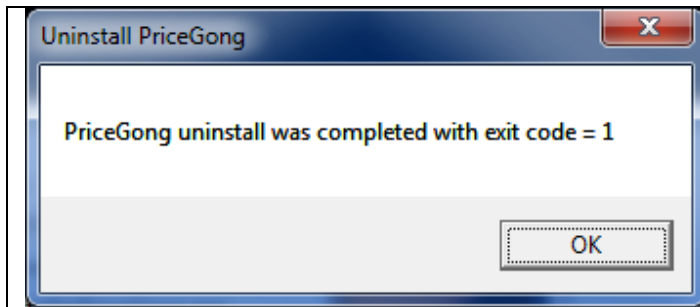
Cliquez sur Exécuter



La fenêtre ci-dessus vous prévient que tous les navigateurs doivent être fermés.

Remarque :

S'ils ont été ouverts après votre redémarrage, puis refermés, c'est fichu, car la dll de pricegong est toujours en mémoire.



Il doit se terminer **avec le code=0**. Lorsqu'il se termine avec le code 1 il semble que cela ne soit pas bon. Windows vous demande alors en général si le logiciel c'est bien installé (terme impropre car il s'agit d'uninstaller) et vous propose une solution adaptée que vous devez accepter.

## Constat

Nom	Modifié le	Type
Adobe	09/12/2009 14:52	Dossier de fichiers
Apple Computer	25/04/2010 08:02	Dossier de fichiers
Conduit	08/04/2010 16:37	Dossier de fichiers
ConduitEngine	23/03/2011 19:18	Dossier de fichiers
Freecorder	25/03/2011 07:06	Dossier de fichiers
Google	03/02/2010 17:01	Dossier de fichiers
Microsoft	06/03/2011 08:00	Dossier de fichiers
Sun	25/11/2009 19:22	Dossier de fichiers
Yahoo!	29/04/2010 12:12	Dossier de fichiers
Yahoo! Companion	29/04/2010 12:13	Dossier de fichiers

PriceGong a disparu. Je vais analyser la situation des répertoires Conduit et ConduitEngine pour voir ce qui peut être retiré. Promis c'est pour la prochaine version.

Sur un PC 64 bits, faites aussi le ménage en supprimant manuellement :

C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Conduit

## En résumé :

1. Si vous n'avez pas besoin de freecorder, ouvrez IE9 en mode Private. Il est possible de créer un raccourci pour cela, du type "**C:\Program Files (x86)\Internet Explorer\iexplore.exe**" -private en 64 bits ou bien "**C:\Program Files\Internet Explorer\iexplore.exe**" -private en 32 bits (voir la fiche sur IE8)
2. Si vous avez besoin de freecorder, ouvrez d'abord Netcook, puis IE9. Tous les cookies y compris ceux de Conduit Ltd PriceGong seront supprimés toutes les 10 secondes.
3. Utilisez Freecorder.
4. Fermer IE9.
5. Attendez que Netcook vous indique « PriceGong temporairement supprimé » ou vérifiez que Netcook indique « PriceGong non détecté »
6. Fermer IE9. Votre disque C est propre, Tous les répertoires, clés, bibliothèques dll et fichiers xml ont disparu. Théoriquement c'est définitif mais je préfère que Netcook vérifie à chaque fois. Dans tous les cas de figure, par sa façon de fonctionner, il rend tout espionnage par cookies impossible. Mais Conduit Lcd est très intrusif. Si IE9 vous demande de rétablir le module complémentaire Conduit, refusez absolument.

Vous pouvez, évidemment, mettre netcook.exe dans votre menu de démarrage, vous n'aurez plus à y penser et il n'est pas très gourmand en mémoire.

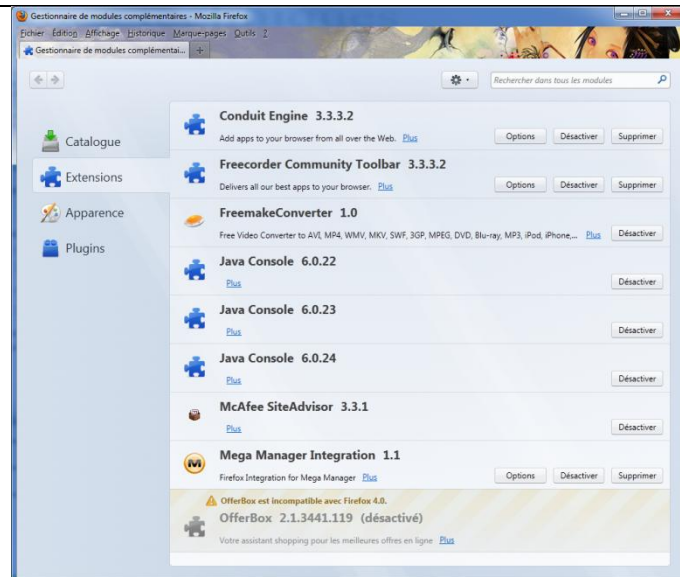
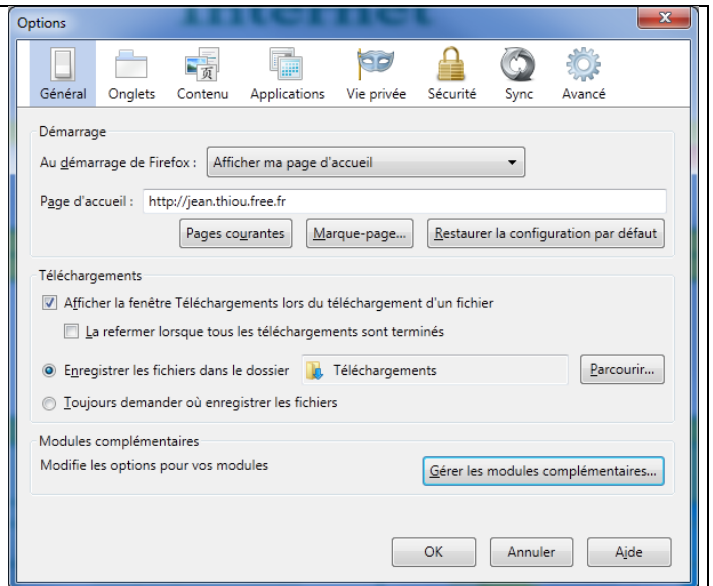
## Avec Firefox version 4

Appuyez sur ALT pour afficher le menu si nécessaire.

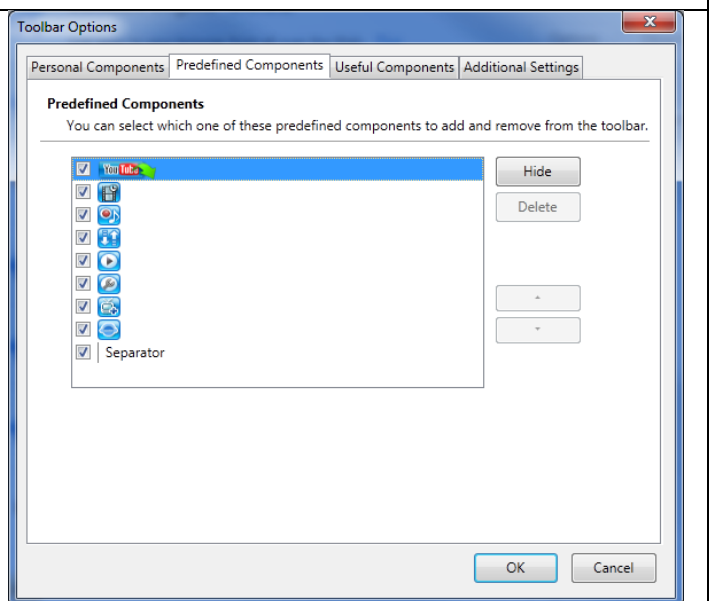
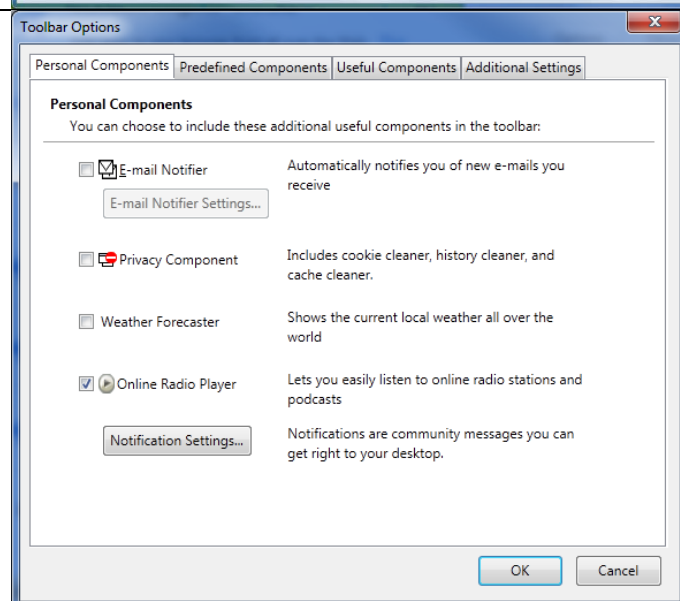
Allez dans Outils Options. La fenêtre ci-jointe à droite va s'ouvrir.

Depuis l'onglet général, cliquez alors sur le bouton Gérer les modules complémentaires.

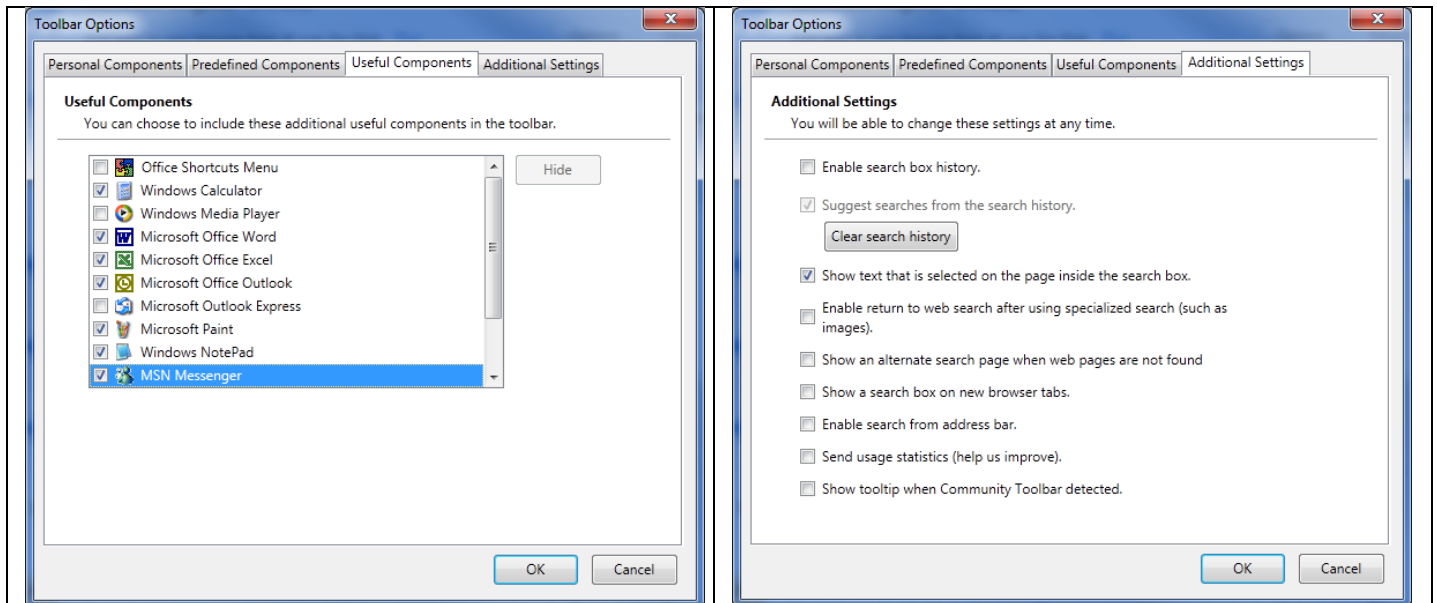
La fenêtre ci-dessous va s'ouvrir.



Cliquez alors sur le bouton « Options » correspondant à Freecorder Community Toolbar. La fenêtre ci-dessous avec 4 onglets va s'ouvrir. Nous allons les analyser, puis nous allons cliquer sur le bouton « Notification Settings » Choisissez les réglages afin d'éviter les problèmes. Vous pouvez cocher les boutons pour ouvrir des modules de Microsoft Office comme Word, Excel etc...



## Fiche Technique



En cliquant sur le bouton Notification Settings de l'onglet Personal Components, désactivez tout, puis cliquez OK  
Refermez toutes les fenêtres en validant avec OK si nécessaire.

