

## 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. <u>http://aivm.free.fr/BI/JT/JT142\_FichiersInutilesSurDisqueC.pdf</u>

#### **Téléchargement**

Voici les sites possibles pour le téléchargement du setup de la Toolbar <u>http://www.01net.com/telecharger/windows/Internet/plugins/fiches/49590.html</u> <u>http://www.01net.com/telecharger/windows/Multimedia/edition\_audio/fiches/29515.html</u> <u>http://www.commentcamarche.net/download/telecharger-34057249-freecorder-toolbar</u>

## Installation

Fichier ouvert - Avertissement de sécurité
Voulez-vous exécuter ce fichier ?
Nom :ments\Multimédia\FreeCorderToolBarSetup.exe Éditeur : <u>Applian Technologies Inc.</u> Type : Application
De : E:\Téléchargements\Multimédia\FreeCorderTool
☑ <u>T</u> oujours demander avant d'ouvrir ce fichier
Les fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier présente un danger potentiel. N'exécutez que les logiciels des éditeurs approuvés par vous. <u>Quels sont les risques ?</u>
ous devez cliquez sur Exécuter, vous n'avez pas le choix.

sociation loi 1901

er Informatique

Siège Jallan-Miré



Gardez les deux choix, et cliquez sur Next

Installation d'un logiciel	Avec Internet Explorer
N'installez que des modules complémentaires dont les auteurs ont votre confiance.           Certains logiciels malveillants peuvent endommager votre ordinateur ou violer votre vie privée.	9 vous recevez un deuxième avertisse- ment. Le logiciel peut être malveillant ou porter atteinte à votre vie privée. Les choses sont claires Mais je vais
Freecorder.xpi       (Conduit Ltd.)         file:///C:/Program%20Files%20(x86)/Freecorder/Freecorder.xpi         Installer maintenant	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	
Modules complémentaires Catalogue Extensions Thèmes Plugins Installation Catalogue Extensions Thèmes Plugins Installation Redémarrer Firefox x Veuillez redémarrer pour terminer la mise à jour. Annuler Annuler Sur la fenêtre suivant il est prudent de tout annuler	Firefox vient d'ouvrir cette fenêtre où je constate le module Conduit Engine qui est lui aussi lié à Freecor- der. Je fais donc la mise à jour. Firefox demande à être redémarré. J'exécute cette mani- pulation, puis je ferme Firefox.

Freecorder Community Toolbar Installation
Stream it. Record it. Keep it.
Freecorder Community Toolbar Installation
You are about to install the Freecorder Community Toolbar and Conduit Engine. Conduit Engine let you instantly add apps from all over the Web with no additional installation.
Please configure these additional settings. You will be able to change them at any time.
🔍 🔲 Set the Freecorder customized Web Search as my default in Internet Explorer
👩 🔲 Set my home page to the Freecorder customized Web Search page
🦪 🔲 Send me community news alerts from Freecorder
🔍 🔲 Show an alternate Search page when web pages are not found
To continue the installation, you must agree to the following License Agreement.
Conduit End-User License Agreement Welcome PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT (THE "EULA") BEFORE DOWNLOADING, INSTALLING OR USING THE CONDUIT
< <u>Back</u> <u>Disagree</u>
conseille de tout annuler puis de cliquer sur Agree. J'ai droit à cette fenêtre d'accueil. Depuis IE9
Image: http://www.applian.com/freecorder4/welcome.php     P - 20 C × 10 Freecorder 4 - Welcome! ×       Fichier Edition Affichage Favoris Outils ?
x Google 🔄 🔄 Saisie automatique * 🤌 👘 😨 Partager * 🔊 * 💷 * 💋 Sidewiki * 🎪 Orthographe * 🖓 Traduire * 🍠 Saisie automatique * 🥜 🦴 🦤 + 🖉 🔌 Seisi
Image: Search the Web     Image: Search the Web <th< th=""></th<>
applian technologies       Since 1997         Stream & Record & Keep &       Incention of the second of the s

À 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)



der seul en ne gardant que la Tool bar, avec les dernières versions.

## **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



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

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

Ouvrez Ordinateur  $\rightarrow$  C:\  $\rightarrow$  Utilisateurs  $\rightarrow$  Votre nom de connexion  $\rightarrow$  AppData  $\rightarrow$ 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  $\rightarrow$  C:\  $\rightarrow$  Windows  $\rightarrow$ SysWOW64  $\rightarrow$  Config  $\rightarrow$  systemprofile  $\rightarrow$  AppData  $\rightarrow$  Local-Low.

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

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 réapparaitront 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 ou 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 dé-X 👰 Netcook marrage de freecorder, ce qui semble être le cas dans la dernière version, utili-NETCOO sez 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 🙀 Voir le rapport d'erreurs 📇 Suspendre <u>A</u>ide temp, cookies toutes les dix secondes ainsi que PriceGong et les plugins de Freecorder Toolbar. Pricegong non détecté Vous évitez le mouchardage tout en <u>Fermer</u> conservant Freecorder actif. Version 11.03.17.D2006 Refermez IE ou Firefox au moins 10 secondes avant Netcook. Ainsi les fi-Pour le télécharger directement (vous pouvez y accéder depuis les pages chiers de PriceGong seront supprid'accueil de mes sites aivm.free.fr ou jean.thiou.free.fr) ou directement mables car la dll ne sera plus en médepuis la page suivante. moire 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 ? × 😔 Freecorder 4 - Settings indispensable à un semblant de vie privée sur Internet en supprimant Storage Directory Space avaliable: 532.00 GB les mouchards toutes les 10 secondes. Il interrompt tout espionnage. E: \Musique \Temp \ Fermez l'explorer (IE ou Firefox) avant netcook. Une fois l'explorer Video Capture Settings Internet fermé, Netcook ne mettra pas plus de 10 secondes à sup-Temporary storage size: 1000 MB. primer tous les fichiers de PriceGong. Fermez alors netcook. Ce Monitor Internet Explorer's temporary directory logiciel tient peu de place en mémoire. Il peut rester ouvert en per-Audio Capture Settings manence, tout en refermant JT Util qui n'est qu'un lanceur. MP3 Audio Bitrate: 128 kbit/s 🔻 Record using Windows Vista Audio Technology

### 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).

Record using Applian Audio Driver Technology

Save

Cancel

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'apparait pas appuyez sur la touche ALT.



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

Gérer les modules complémentaires

#### Afficher et gérer les modules complémentaires d'Internet Explorer

Types de module complémentaire	Nom	Éditeur	État	Durée de c	Temps de
& Barres d'outils et extensions	(Non vérifié) Megaupload Limited				
O Moteurs de recherche	IeMonitorBho Class	(Non vérifié) Megauploa	Activé	0,00 s	0,00 s
Accélérateurs	Adobe Systems Incorporated Shockwave Flash Object	Adobe Systems Incorpor	Activé		
O Protection contre le tracking	Conduit Ltd.				
	Freecorder Toolbar	Conduit Ltd.	Activé	0,01 s	
	Conduit Engine	Conduit Ltd.	Activé	0,02 s	
	Freecorder Toolbar	Conduit Ltd.	Activé	0,01 s	
	Conduit Engine	Conduit Ltd.	Activé	0,02 s	
	Conduit Engine Findbar	Conduit Ltd.	Désactivé		
	Freecorder Findbar	Conduit Ltd.	Désactivé		

Cliquez sur le premier Conduit Engine, puis cliquez en bas sur le bouton Désactiver, La nouvelle fenêtre cijointe 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.

#### Désactiver un module complémentaire

#### Voulez-vous désactiver ce module complémentaire ?

#### Conduit Engine (Conduit Ltd.)

Sélectionner d'autres modules complémentaires que vous souhaitez désactiver depuis

- Freecorder Toolbar
- Freecorder Toolbar

Temps de chargement total : 0,02 secondes

Pour réactiver cette barre d'outils, cliquez sur le bouton Outils et utiliser le menu Barres d'outils.

Désactiver

En savoir plus sur les modules complémentaires

Annule

X

					X
Gerer les modules complementaires				100 M	
Afficher et gérer les modules comp	lémentaires d'Internet Explorer				
Towns do no dada a constituio anteiro	Nom	Éditeur	État	Durée de c	Temps de
Types de module complementaire	(Non vérifié) Megaunload Limite	d	LUUT	Durce de em	remps de
Sarres d'outils et extensions	IeMonitorBho Class	(Non vérifié) Megauploa	Activé	0 00 s	0.00 s
P Moteurs de recherche	Adobe Systems Incorporated	(Non Venne) megaapioani	Active	0,00 3	0,00 3
🔁 Acc <u>é</u> lérateurs	Shockwave Flash Object	Adobe Systems Incorpor	Activé		
SProtection contre le tracking	Conduit Ltd	Adobe of sterns meorpoint	, and the second s		
	Erecorder Toolbar	Conduit Ltd.	Activé	0.01 s	
	Conduit Engine	Conduit Ltd.	Désactivé	(0,02 s)	
	Freecorder Toolbar	Conduit Ltd.	Activé	0,01 s	
	Conduit Engine	Conduit Ltd.	Désactivé	(0,02 s)	
	Conduit Engine Findbar	Conduit Ltd.	Désactivé		
	Freecorder Findbar	Conduit Ltd.	Désactivé		
Afficher :	Google Inc				
Modules complémentaires actuellement cha	rgés 🔻 Google Toolbar	Google Inc	Activé	0,00 s	0,00 s
Constants Francisco					
Londuit Engine Conduit Etd					
Varsian : 6220	Tur	Parro d'autile			
Date du fichier :	Typ Rec	hercher le module complémen	taire à l'aide d	u moteur de rec	herche par défaut
Plus d'informations					
					Activer
Rechercher d'autres barres d'outils et extensi	ons				Former
E <u>n</u> savoir plus sur les barres d'outils et les ext	ensions				rermer
and an a atta aita ati an diffin					
ardez cette situation, defin	nuvement.				
isuite dans IE9, barre Free	corder, cliquez sur le bou	ton de fenêtre dé	roulante	c1-dessou	18:
-) (-) 😤 http://www.pcastuces.com/logithequ	ue/telechargement.asp?num=1354		0 - 🛛 C X	🐥 PC Astuces :	ici
chier Edition Affichage Favoris Outils ?				_ /	
🗄 👻 (( )) 👻 Search the Web	💌 💽 Search 💌 🕂 🔟 🌆 💽 🚺 💽	🖉 🚉 🔻 🖸 🛈 🛌 KFOG 🛶	◙ ם 💽 -  [	👌 🕶 💽 👿 🛯	I 🖸 🗑 🖻 🖪 🌌
Google	💌 🛃 Rechercher 🕶 🏢 👻 📲 🔹 🐼 Parta	ger • 🔊 • 💷 • 🅖 Sidewiki • 🖞	Mes favoris	About	🝇 Traduire 🔹 🍠 Saisie automati
🧟 🗸 🛐 🗸 🖸 Yahoo! Search	SEARCH + Bookmarks +	🗖 Mail 🔹 🔎 🏭 Weather 🔹 🔳	Facebook -	Home Page	eBay 🔹 🧰 Shopping 🔹
				💢 Disable	
bing	🔛 🦢	) 📣 🕇 📃			- 🛛 💭 🐝
Dan	s la barre free-	tcook			- O X
	er cliquez sur la				
	tre dénoulant		-	~ ~	
About	tre deroulante	NET	C	CC	
i cont	enant une lettre 🛛 🚺 🧧				
🔤 Home Page 🛛 🖸 à 1	peine visible.				

Reference State St

PriceGong temporairement supprimé

Version 11.03.20.D2006

A Suspendre

Netcook indique alors « Pricegong temporairement suppri-

mé ». Il semble qu'il ne reviendra pas en ouvrant IE9. Mais

comme « désactivé » ne signifie pas « supprimé », Net-

cook est nécessaire pour retirer tous les répertoires corres-

pondants à PriceGong et la dll correspondante

7 Aide

Eermer

🕁 Contact

Ce bouton désactive

complètement Pri-

ceGong dsans le

supprimer.

Cliquez sur Disable

qui doit désactiver PriceGong. En effet

Netcook semble in-

diquer, malgré IE9 ouvert que mainte-

nan PriceGong est

supprimé. Fermer

IE9.

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 dédouaner pour ce site dont le seul but et de vous installer ce malware. Essayez quand même.. Télécharger le fichier uninstall.exe sur le site de PriceGong.

Telecharger le fichier uninstall.exe sur le site de PficeGon

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).



2. From the menu opened select "Disable".

🗈 🕞 🛛 Califo... 🗕 🔞 🕒

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

👠 Live TV

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

»

Fichier ouvert - Avertissement de sécurité	Cliquez sur Exécuter
Voulez-vous exécuter ce fichier ?	Uninstall PriceGong
Nom :         D:\Téléchargements\uninstallerPriceGong           Éditeur :         PriceGong Software Ltd	g.exe You must close all your Internet Explorer and Firefox browsers before you continue.
lype : Application De : D:\Téléchargements\uninstallerPriceGong	g.exe
<u>E</u> xécuter Ar	La fenêtre ci-dessus vous prévient que tous les navi-
☑ <u>T</u> oujours demander avant d'ouvrir ce fichier	gateurs doivent être fermés.
	Remarque :
Les fichiers téléchargés depuis Internet peuvent être utiles type de fichier présente un danger potentiel. N'exécutez q logiciels des éditeurs approuvés par vous. <u>Quels sont les r</u>	S'ils ont été ouverts après votre redémarrage, puis refermés, c'est fichu, car la dll de pricegong est tou- jours en mémoire.



#### Constat

Ordinateur 🕨 System	n (C:) 🕨 Utilisateurs 🕨 JT 🕨 AppData 🕨 Loo	calLow 🕨	
Affichage Outils	?		
Inclure dans la bibliot	hèque ▼ Partager avec ▼ Graver	Nouveau dossier	
F	Nom	Modifié le	Туре
ma	🎍 Adobe	09/12/2009 14:52	Dossier de fichiers
	\mu Apple Computer	25/04/2010 08:02	Dossier de fichiers
nts	🕕 Conduit	08/04/2010 16:37	Dossier de fichiers
Keleves	🌗 ConduitEngine	23/03/2011 19:18	Dossier de fichiers
	January 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
in	📔 Sun	25/11/2009 19:22	Dossier de fichiers
errPureau	🔰 Vahoo!	29/04/2010 12:12	Dossier de fichiers
esibureau	¥ahoo! 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 :

 $C: \label{eq:config} would w$ 

#### En résumé :

- 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**



Toolbar Options	Toolbar Options
Personal Components Predefined Components Useful Components Additional Settings	Personal Components Predefined Components Useful Components Additional Settings
Useful Components You can choose to include these additional useful components in the toolbar.	Additional Settings You will be able to change these settings at any time.
Image: Solution of the second seco	<ul> <li>Enable search box history.</li> <li>Suggest searches from the search history.</li> <li>Clear search history</li> <li>Show text that is selected on the page inside the search box.</li> <li>Enable return to web search after using specialized search (such as images).</li> <li>Show an alternate search page when web pages are not found</li> <li>Show a search box on new browser tabs.</li> <li>Enable search from address bar.</li> <li>Send usage statistics (help us improve).</li> <li>Show tooltip when Community Toolbar detected.</li> </ul>
OK Cancel	OK Cancel
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.	Notification Settings       Image: Conduit Engine Notifications         Image: Conduit Engine Notifications       Image: Conduit Engine Notifications         Image: Freecorder Special Offer       Image: Conduct Engine Notifications

