

Tutoriel USBFix

 malekal.com/tutoriel-usbfix/

malekalmorte

12/11/2010

A Lire :

Les personnes qui posteront leurs rapports USBfix en commentaire de ce tutorial se verront leurs commentaires supprimés sans sommation.

Si vous avez besoin d'aide à désinfecter votre PC, merci de créer un sujet dans la partie Virus du forum :

[Aide désinfection virale forum malekal.com](#)

Il est important de bien comprendre le fonctionnement de ces infections sous peine d'être à nouveau infecté.

USBfix est un outil développé par El Desaparecido qui supprime certaines infections USB et nettoye les périphériques amovibles. Le simple fait d'ouvrir le poste de travail et de double-cliquer sur une clef USB/disque dur infecté installe l'infection sur votre système. Tous les médias amovibles insérés seront alors infectés à leur tour afin de propager l'infection dans votre entourage.

Je vous conseille vivement de lire le contenu des liens suivants afin de mieux comprendre leur fonctionnement et donc de pouvoir les éviter:

- [Les infections par disques amovibles](#)
- [Les infections par disques amovibles 2](#)

Enfin USBfix vise aussi [les infections MSN](#).



Table des matières [[masquer](#)]

- [1 Utilisation de USBFix](#)
 - [1.1 Rechercher sur USBFix](#)
 - [1.2 Nettoyage USBFix](#)
- [2 Supprimer la vaccination USBFix](#)
- [3 Après le nettoyage... Sécuriser son ordinateur contre les menaces par médias amovibles](#)

Utilisation de USBFix

- Vous pouvez télécharger USBFix depuis ce lien : [Télécharger USBFix](#)
- Une nouvelle icône est alors créée sur le bureau qui permet de démarrer le programme. Double-cliquez dessus.
- Le programme se lance...
- Vous arrivez alors sur le menu principal de USBFix
 - Recherche : Recherche permet de rechercher d'éventuelle infection
 - Nettoyage : Supprimer les infections amovibles détectées et nettoyer vos médias amovibles
 - Listing : permet de lister les éléments présents sur la clef sans devoir l'ouvrir et donc éventuellement infecter son PC.

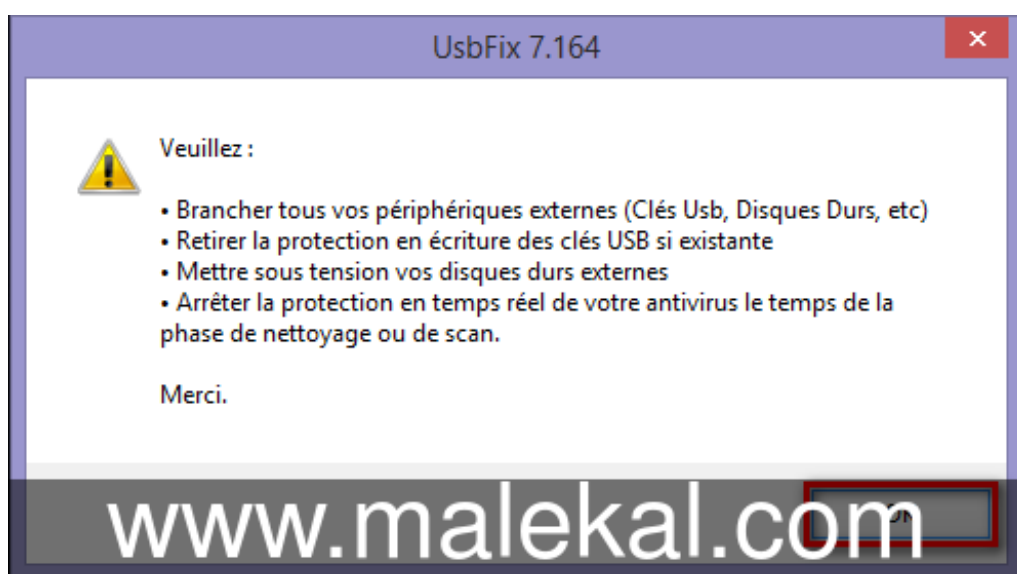


- Vacciner : Vaccine vos disques amovibles pour empêcher leurs infections
- Option : permet d'activer des fonctionnalités du programme.
- Désinstaller : Supprimer USBFix de votre ordinateur
- Quitter : Quitte USBFix

Rechercher sur USBFix

La recherche permet de générer un rapport – Aucune modification sur le système n'est effectuée et aucune suppression de l'infection n'est effectuée à l'issue de l'option 1.

- Sur le menu principal, cliquez sur Rechercher.
- Un message vous indique alors de brancher tous vos medias amovibles, insérez les puis appuyez sur une touche pour lancer le scan.



- La recherche s'effectue, cela peut prendre plusieurs minutes, le % sur l'avancement de la recherche s'affiche en bas à gauche. Ne touchez à rien. Le texte sur fond noir peut passer en rouge ou vert, c'est normal.



Elément(s) infecté(s) : 0

Recherche générique ...

Une fois l'analyse terminée, un rapport de scan vous est proposé... appuyez sur une touche pour ouvrir ce rapport.

Dans le cas où vous effectuez une désinfection via un forum, vous pouvez copier/coller ce rapport pour cela :

- Cliquez sur le menu Edition puis Sélectionner tout.
- Cliquez à nouveau sur le menu Edition puis coller.
- Dans votre sujet sur le forum, créez un nouveau message puis clic droit / coller dans le message afin de coller le rapport.

```

UsbFix.txt - Notepad
File Edit Format View Help

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\logonui.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\userinit.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\VMware\VMware Tools\VMwareService.exe
C:\WINDOWS\system32\wbem\wmiprvse.exe

##### [ Fichiers # Dossiers infectieux ]

Deleted ! C:\WINDOWS\system32\nmdfgds0.dll
Deleted ! C:\WINDOWS\system32\olhrwef.exe
C:\autorun.inf # -> fichier appelé : "C:\logf.exe" ( présent ! )
Deleted ! -> C:\logf.exe
Deleted ! C:\autorun.inf

##### [ Registre # Clés infectieuses ]

Deleted ! HKCU\SOFTWARE\Microsoft\windows\CurrentVersion\Run "cdoosoft"

##### [ Registre # Mountpoint2 ]

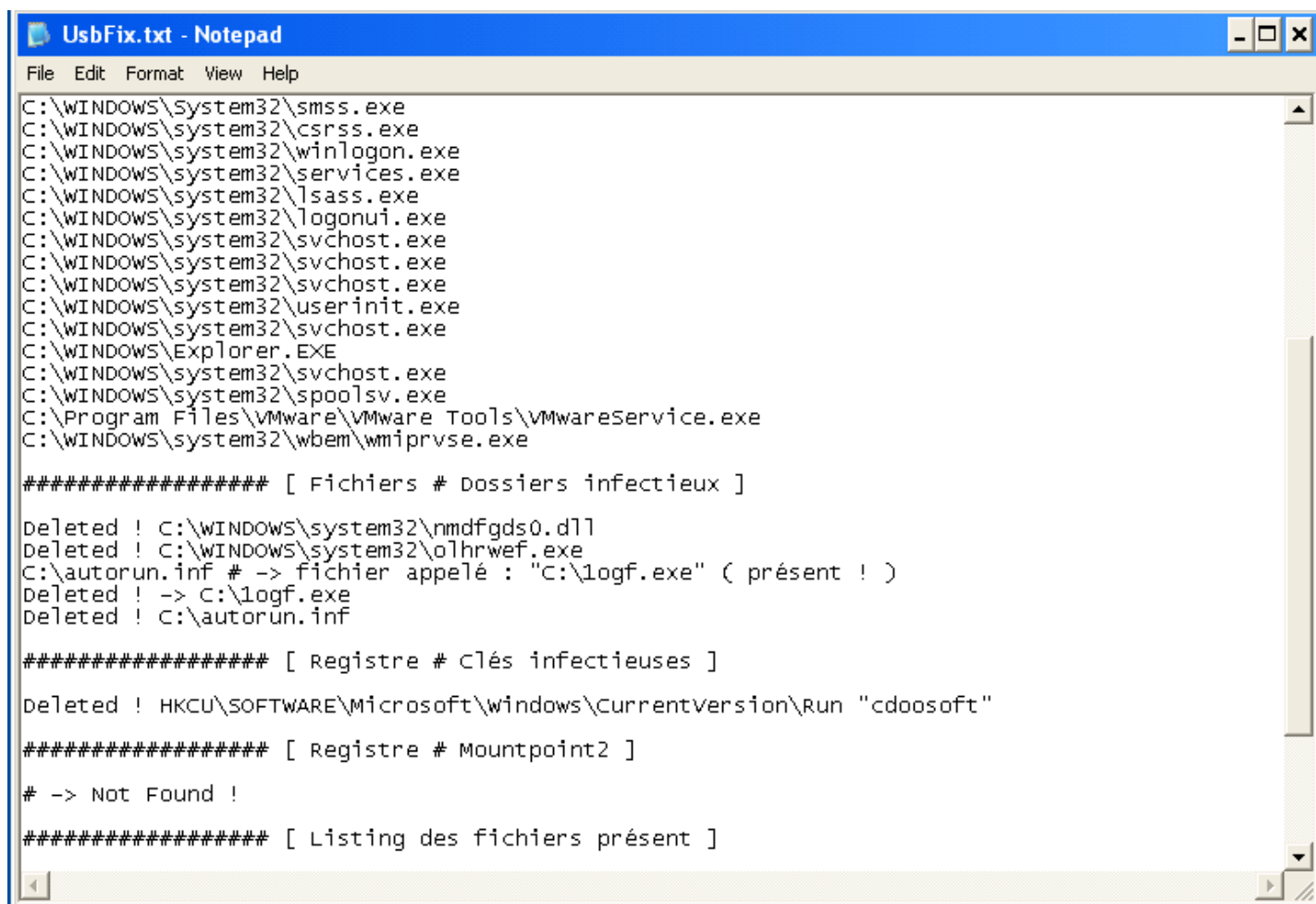
# -> Not Found !

##### [ Listing des fichiers présent ]
    
```

Nettoyage USBFix

Le nettoyage supprime les infections amovibles détectées et nettoie vos médias amovibles.

- Relancez le programme.
- Dans le menu principal, cliquez sur le bouton **Nettoyage**.
- Le menu démarrer et les icônes vont à nouveau disparaître.. c'est normal.
- Le nettoyage va prendre quelques minutes... Appuyez sur OK sur la fenêtre d'informations
- Le fix peut avoir besoin de redémarrer l'ordinateur, un message vous en avertit, vous devez appuyer sur une touche.
- Au redémarrage, le fix se relance... laissez l'opération s'effectuer.
- Un rapport de nettoyage vous est proposé... appuyez sur une touche pour ouvrir ce rapport.



```
UsbFix.txt - Notepad
File Edit Format View Help
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\logonui.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\userinit.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\VMware\VMware Tools\VMwareService.exe
C:\WINDOWS\system32\wbem\wmiprvse.exe

##### [ Fichiers # Dossiers infectieux ]

Deleted ! C:\WINDOWS\system32\nmdfgds0.dll
Deleted ! C:\WINDOWS\system32\olhrwef.exe
C:\autorun.inf # -> fichier appelé : "C:\logf.exe" ( présent ! )
Deleted ! -> C:\logf.exe
Deleted ! C:\autorun.inf

##### [ Registre # Clés infectieuses ]

Deleted ! HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "cdoosoft"

##### [ Registre # Mountpoint2 ]

# -> Not Found !

##### [ Listing des fichiers présent ]
```

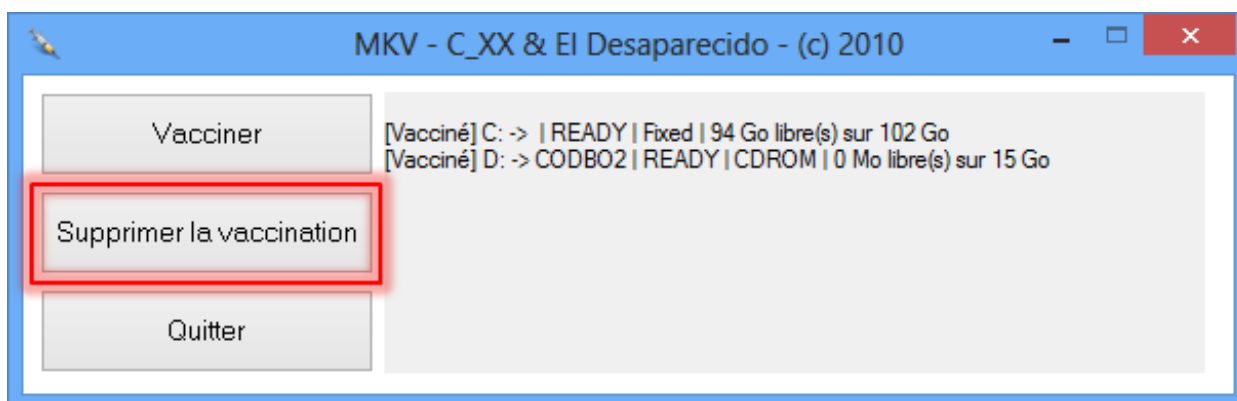
Encore une fois, au cas où vous effectuez une désinfection via un forum, vous pouvez copier/coller ce rapport pour cela :

- Cliquez sur le menu Edition puis Sélectionner tout.
- Cliquez à nouveau sur le menu Edition puis coller.
- Dans votre sujet sur le forum, créez un nouveau message puis clic droit / coller dans le message afin de coller le rapport.
- Vous pouvez aussi utiliser <http://pjjoint.malekal.com> pour transmettre le rapport.

Supprimer la vaccination USBFix

Si vous désirez supprimer la vaccination USBFix, il faudra passer par le programme [MKV](#)

=> [Télécharger MKV](#)



Après le nettoyage... Sécuriser son ordinateur contre les menaces par médias amovibles

Scannez éventuellement votre disque avec votre antivirus afin de supprimer les restes.

Eventuellement faire un nettoyage [Malwarebytes Anti-Malware](#) qui est assez efficace : [Tutorial Malwarebytes Anti-Malware](#)

Une fois les infections supprimées, il convient de sécuriser votre ordinateur afin de ne plus être infecté à nouveau par ces médias, se reporter à la page : [Maîtriser ses médias amovibles](#) et plus globalement voir le sujet : [Sécuriser son ordinateur \(version courte\)](#) notamment, [vous pouvez désactiver les scripts \(WSH etc\)](#) afin de protéger votre ordinateur et limiter ce type d'infection.

Le programme [Marmiton](#) permettant justement de bloquer ce type de menaces :



Si vous avez prêté des clefs USB à vos amis ou si ces derniers ont inséré une clef USB dans votre ordinateur quand celui-ci était infecté, vous devez les prévenir car ils ont certainement infecté leur ordinateur à leur tour.

Ces derniers peuvent suivre ce tutorial et prévenir à leur tour leurs amis.