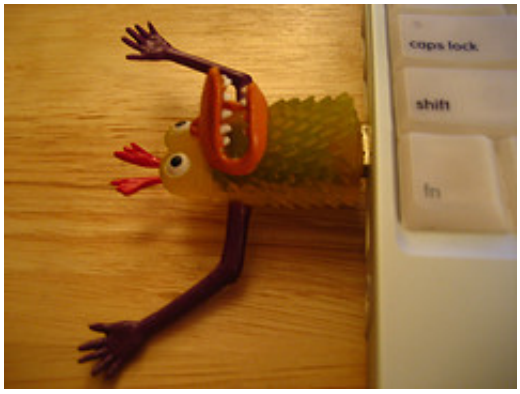
Désinfecter une clé USB ou un disque amovible

De plus en plus, les lieux publics (cyber café, lycées, bibliothèques...) deviennent de vrais nids à infection. Ces PC infectés par inadvertance ou malveillance propagent entre autres des infections s'attaquant aux disques amovibles que l'on peut y brancher !



Ce sont donc des infections qui se propagent par supports amovibles : clé USB (cas le plus fréquent), disque dur externe, carte flash, ipod, lecteur MP3, appareil photo, etc...
Tout disque amovible inséré dans un ordinateur infecté sera infecté à son tour si l'infection est active. Autrement dit, l'infection se fera automatiquement par simple connexion si l'exécution automatique est activée pour les lecteurs amovibles.
Le simple fait d'ouvrir le poste de travail et de double-cliquer sur la clé usb / disque dur externe (ré)infectera le système d'exploitation ! La clé infectera à son tour un PC sain. Et ainsi de suite ...

Symptômes

- Le double-clic pour ouvrir vos supports amovibles infectés ne fonctionne plus.
- Si vous rendez visible les fichiers et dossiers cachés, vous vous rendrez compte que la clé contiendra plusieurs fichiers et processus inconnus et donc infectés ; ne surtout pas double-cliquer dessus pour les ouvrir car ils rendront active l'infection, si ce n'est déjà fait !
- L'élément clé pour que l'infection se propage automatiquement de clé en PC et de PC en clé est l'activation de fichier par l'autorun.inf, en faisant un double-clic pour accéder aux fichiers d'une clé !

Méthode de désinfection

Avant de passer l'un de ces outils, assurez-vous d'avoir fermé tous les programmes en cours d'exécution et connectez au PC tous les périphériques externes qui auraient pu être contaminés (disques durs externes, clé USB, iPod...), répétez l'opération de

désinfection s'il y a plusieurs disques amovibles susceptibles d'avoir été infectés.

UsbFix

A- Option Scanner d' Usbfix (recherche)

- Télécharger UsbFix *(de El Desaparecido)* sur le Bureau.

Autre lien de téléchargement : >> Cliquez Ici<<

- **Important** : brancher les sources de données externes au PC (clé USB, disque dur externe, carte SD, etc...) sans les ouvrir.
- Double-cliquer sur le programme *UsbFix.exe* sur le Bureau, l'installation se fera automatiquement.
- **/!** Désactiver la garde de l'antivirus pour éviter tout conflit lors de l'utilisation de l'outil.
- Cliquer sur le bouton **Recherche**.
- Laisser travailler l'outil.
- Poster le rapport *UsbFix.txt* obtenu si vous avez créé un sujet sur le forum Virus/Sécurité.
- Note : le rapport *UsbFix.txt* est sauvegardé à la racine du disque (C:*UsbFix.txt*).

B- Option Suppression d' Usbfix (nettoyage)

/!\ Avant de passer l'option Suppression, il est recommandé de demander conseil

sur le forum Virus/Sécurité. /!

- **Important** : brancher les sources de données externes au PC (clé USB, disque dur externe, carte SD, etc...) sans les ouvrir.
- Double-cliquer sur le programme *UsbFix* sur le Bureau.
- Cliquer sur le bouton **Suppression**.
- Le Bureau disparaîtra et réapparaîtra à le fin de la désinfection.
- Ensuite, poster le rapport *UsbFix.txt* qui apparaîtra avec le Bureau si vous avez créé un sujet.
- Note : le rapport *UsbFix.txt* est sauvegardé à la racine du disque (C:*UsbFix.txt*).

Site de l'auteur - Tutoriel

Flash_Disinfector

- Télécharger Flash_Disinfector (de sUBs) sur le Bureau :
  - Flash_Disinfector
  - Note : Ce programme risque de déclencher une alerte de l'antivirus : si c'est le cas, il faut le désactiver temporairement, c'est une fausse alerte.
  - Double-cliquer sur Flash_Disinfector.exe pour le lancer.
  - Si la clé n'est pas introduite, il sera demandé de la connecter.
  - Quand le message : "Plug in your flash drive & clic Ok to begin disinfection" apparaîtra :
  - connecter les clés USB et/ou périphériques USB externes susceptibles d'avoir été infectés.
  - Puis cliquer sur OK
  - Les icônes sur le bureau vont disparaître jusqu'à l'apparition du message: "Finish"
  - Appuyer ensuite sur "OK", pour faire réapparaître le bureau.

RAV d'Evosla

RAV est un soft qui traite les virus et vers qui se trouvent dans les racines des lecteurs fixes et amovibles.
Pour le télécharger, cliquez ici
Désinfecter une clé usb/disque amovible :

- Télécharger Rav
- Brancher les disques amovibles sans les ouvrir avant de lancer le Fix
- Décompresser l'archive sur le bureau
- Double-cliquer sur RAV.exe pour lancer l'outil
- Une fois RAV lancé, il scannera automatiquement tous les lecteurs susceptibles d'être infectés
- S'il y a infection un rapport s'établira, sinon le soft affichera le message : « Votre Ordinateur est sain »
- Retirer les disques amovibles et redémarrer l'ordinateur.

Autres outils

Voici trois autres outils que vous pouvez utiliser pour compléter la désinfection :

- L'outil Symantec
  - Sur le bureau, double-cliquer sur le fichier FxRajump.exe
  - Puis cliquer sur Start pour lancer le nettoyage.
  - En fin de nettoyage, une fenêtre s'ouvrira pour signaler la fin de la recherche.

    - Le fichier FxRajump.log sera créé sur le bureau, avec le listing des suppressions de fichiers/clés registre.
- L'outil McAfee
    - Cliquer sur "Download v3.x.x" pour télécharger le fichier, puis le lancer.
    - Si les lettres correspondant aux périphériques externes n'apparaissent pas automatiquement dans la liste des lecteurs à scanner, les rajouter manuellement en se servant du bouton "Browse" pour les sélectionner.
    - Puis lancer le nettoyage en cliquant sur le bouton "Scan Now".
- L'outil Autorun Plasma : Télécharger Autorun Plasma
    - Télécharger le fichier ZIP.
    - Placer son contenu à la racine de votre clé USB.

Important : Tant que vous ne serez pas sûr(e) d'avoir éradiqué l'infection, n'ouvrez aucun des disques ou périphériques externes, sous peine de relancer l'infection !

Cas des ordinateurs en réseau

- Par exemple, le ver Rjump (AdobeR.exe, Ravmonlog...) en plus de se copier sur les périphériques externes, se propage aussi en utilisant les dossiers partagés sur les postes en réseau et ouvre une backdoor (= « porte dérobée ») en configurant à l'insu de la personne, une exception dans le pare-feu de Windows. Il y a donc de fortes chances pour que le ver se soit propagé dans les fichiers partages réseau.
- Si un PC est en réseau, il faut l'isoler du réseau et vérifier que les dossiers/disques partagés sont propres, ne pas les reconnecter tant que vous n'êtes pas sûr(e) que les autres machines sont propres ou désinfectées elles aussi, sinon vous risquez de voir l'infection se propager de nouveau !

Après nettoyage

- Pour vérifier qu'il ne reste rien sur l'ordinateur et les supports externes, il est préférable de passer un antivirus en ligne ou son antivirus

Comment s'informer sur ce type d'infection ?

- El Desaparecido (Auteur de UsbFix) à mis à disposition deux articles intéressant, que nous vous invitons à lire :
- Les infections par supports amovibles
- Infection Houdini - Dinihou : On vous explique son fonctionnement

Comment se prémunir au quotidien sur des PC publics ?

- La plupart des ordinateurs publics, et beaucoup d'ordinateurs privés sont touchés par des infections se transmettant par disques amovibles. Pour éviter ça, une précaution très simple à prendre est de vacciner vos disques amovibles.
- Il suffit de créer des répertoires portant le nom des fichiers infectieux les plus courants, et surtout des répertoires portant le nom autorun.inf pour bloquer le mécanisme de propagation de ce type d'infection. Une fois ces répertoires verrouillés en lecture seule, l'infection ne pourra écraser un fichier/dossier existant et ne pourra donc pas se propager ! (Merci à Gof pour cette astuce ;-))
- Pour faire ces vaccinations, vous pouvez utiliser les programmes suivant :

Panda USB and AutoRun Vaccine

- Téléchargez Panda USB and AutoRun Vaccine.
- Installez le logiciel en choisissant les options désirées ("auto-vaccin" de chaque clé dès son branchement, démarrage automatique de l'application, activation du support NTFS ...).
- Lancez l'application.
- Vaccinez vos supports USB et votre PC.

VaccinUSB

VaccinUSB.exe. Il vous suffit de le lancer pour créer des répertoires de vaccination, et vous pourrez ensuite supprimer le fichier VaccinUSB.exe.

- Cette astuce très pratique vous permettra de garder votre clé USB propre même en la connectant à un pc infecté !
- **/!** Lors du téléchargement de ce programme, votre antivirus va se déclencher. Pas de panique, c'est juste une partie du code de VaccinUSB qui est détecté à

tord par les antivirus , donc Faux Positif.

Usbfix

Usbfix déjà présenté permet de vacciner : il suffit de le lancer et de choisir l'option 3 (l'option 2 de suppression vaccine en même temps les périphériques connectés)

Rav d'Evosla

Rav d'Evosla déjà présenté permet de vacciner: il suffit de le lancer et de choisir de vacciner son pc puis de redemarrer son pc.

Flash Disinfector

Flash Disinfector déjà présenté permet aussi de vacciner sont pc : si vous l'avez lancé il se charge de virer les infections trouvées et de vacciner son pc en créant un fichier autorun à la base du disque.

MKV

MKV permet de vacciner ses supports externes
A télécharger ici: MKV
Il suffit ensuite de brancher tous les supports à proteger et lancer le logiciel

Usb-set

Usb-set est un outil utilisable pour protéger ses supports externes: tutoriel ici: http://forum.zebulon.fr/usb-set-ver-10-t173063.html

Bitdefender Usb Immunizer

- Tout comme les logiciels précedent, Bitdefender Usb Immunizer permet de proteger des infections ses supports externes.
- http://labs.bitdefender.com/?page_id=108

EliPen

- http://www.zonavirus.com/descargas/elipen.asp

USB Doctor

USB Doctor permet de vacciner : voir ici:
http://usb-doctor.fr.malavida.com/d7087-telechargement-gratuit-windows

Désactiver l'autorun des supports amovibles en gardant le support pour les CD/DVD

- Lien d'astuce CCM: http://www.commentcamarche.net/faq/29048-desactiver-l-autorun-usb
- Microsoft met à disposition une mise à jour permettant cette fonction : mise à jour KB 971029.

Pour en savoir plus, consultez la page suivant : http://support.microsoft.com/kb/971029
Choisir le fichier de maj en fonction de vôtre version de Windows.

Réalisé sous la direction de Jean-François PILLOU, fondateur de CommentCaMarche.net.

Publié par **green day** - Dernière mise à jour par **¡El Desaparecido!**