Dr.Web CureIt :

Outil de désinfection très puissant, Dr.Web CureIt est un utilitaire freeware dont la particularité est la capacité à désinfecter des fichiers exécutables (*.exe), ou très sensibles du système d'exploitation de Windows, touchés par le très redoutable virus nommé VIRUT. Un antivirus « ordinaire » actuel est capable de nettoyer ces infections mais en les supprimant ou en les mettant en quarantaine ; or ces fichiers, s'ils sont éliminés ou mis en quarantaine sont tout simplement inutilisables et un format du disque deviendrait inévitable !

Téléchargement et tutoriel d'utilisation rédigé en équipe par les conseillers en sécurité du forum de sécurité du site http://forum.zebulon.fr/index.php?showforum=51

Télécharge **Dr.Web CureIt** sur ton Bureau:

ftp://ftp.drweb.com/pub/drweb/cureit/drweb-cureit.exe ou

http://www.freedrweb.com/cureit/ Lien ajouté par Apollo.

- Double clique **drweb-cureit.exe** et ensuite clique sur **Analyse** ;
- Clique **Ok** à l'invite de l'analyse rapide. Ce scan permet l'analyse des processus chargés en mémoire ; s'il trouve des processus infectés, clique le bouton **Oui pour tout** à l'invite.

Note : une fenêtre s'ouvrira avec options pour "Commander**" ou "**50% de réduction**" ; vous pouvez quitter en cliquant le "X"

- Lorsque le scan rapide est terminé, Clique sur le menu **Options** >> **Changer la configuration**;
- Choisis l'onglet "Scanner", et **décoche** "Analyse heuristique". Clique "Ok"
- De retour à la fenêtre principale : clique pour activer "**Analyse complète**";
- Clique le bouton avec **flèche verte** sur la droite, et le scan débutera.
- Clique **Oui pour tout** à l'invite "Désinfecter ?" lorsqu'un fichier est détecté, et ensuite clique "**Désinfecter**".
- Lorsque le scan sera complété, regarde si tu peux cliquer sur cet icône, adjacent aux fichiers détectés : 
- Si oui, alors clique dessus et ensuite clique sur l'icône "Suivant", au dessous, et choisis **Déplacer en quarantaine l'objet indésirable**
- Du menu principal de l'outil, au haut à gauche, clique sur le menu **Fichier** et choisis **Enregistrer le rapport**
- Sauvegarde le rapport sur ton Bureau. Ce dernier se nommera **DrWeb.csv**
- Ferme Dr.Web Cureit
- **Redémarre** ton ordi (*très important*), car certains fichiers peuvent être déplacés/réparés au redémarrage.
- Suite au redémarrage, poste (Copie/Colle) le contenu du rapport de l'outil Dr.Web dans ta prochaine réponse.

- (***Prototype encore à améliorer dans un futur proche)***
- ***Nec plus ultra :***
- ***Ajout par Apollo le 10-11-2007.***

Le plug-in est disponible :
Pour Mozilla Firefox/Thunderbird : http://www.freedrweb.com/browser/mozilla+firefox/
Pour Internet Explorer : http://www.freedrweb.com/browser/internet+explorer/
Pour Opera : http://www.freedrweb.com/browser/opera/

- **Le plug-in pour navigateurs servent à scanner directement un lien (url ou raccourci de téléchargements ou vers des sites afin de vous assurer que le lien est « clean » (propre /sûr)**
- **Attention ! Il est vivement recommandé de pratiquer une sauvegarde de la base de registres avant d'effectuer toute fusion avec n'importe lequel des fichiers *.reg !**
- **Le fichier *.reg ressemble à ceci :** 
-
- **Comment sauvegarder sa base de registres ?**
- **Allez dans le menu Démarrer/Exécuter et taper REGEDIT → presser la touche Entrée ou cliquez sur le bouton Ok.**
- **Au-dessus de la fenêtre de l'éditeur de registre, cliquez sur Fichier/Exporter et choisissez un répertoire de destination que vous aurez préalablement créé spécialement (par exemple : sauvegarde registre du DATE) ; cette opération peut durer plusieurs minutes, alors patientez le temps qu'il faut.**
- **Enregistrez alors le plug-in convenant à votre navigateur et si vous en utilisez plusieurs, faites les fusions dans le registre une à une afin de ne pas vous tromper !**

***C'est seulement à cet instant que vous pouvez double-cliquer sur le fichier*.reg : acceptez la fusion au registre, le changement est immédiat !**

Résultat de la fusion du fichier plug-in.reg pour Internet Explorer

Ci-dessous.

- 

- ***Apollo. http://theknitter-apollo.xooit.com/index.php***
- ***Fait ce samedi 10 novembre 2007.***

- 

-