Vacciner une clé USB contre les infections virales

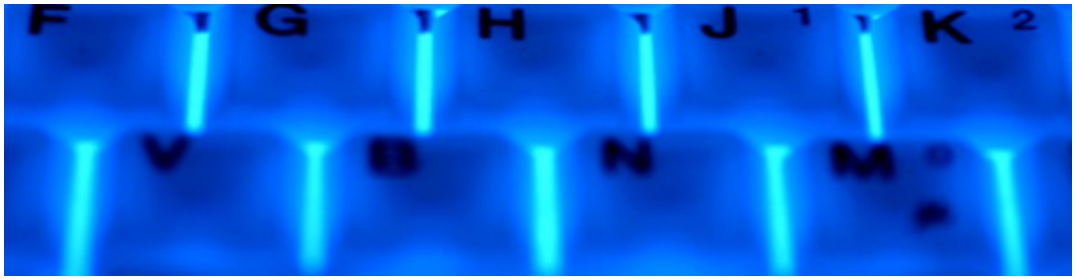
« KGen : scanner la sémantique d'un site / blog
(modifié le 20 octobre 2013 à 16:38)

Avant-propos : ce billet **n'est pas sponsorisé** par Roseline.

La **clé USB** fait partie des périphériques mobiles qui sont connectés sur de très nombreuses machines au cours de leur vie. De la même façon que sur les disquettes de l'époque, **les virus n'hésitent pas à s'installer dessus**.

L'arrivée des disques (CD et DVD) avait permis de limiter ce phénomène par la lecture seule du média, rendant l'écriture impossible et de façon intrinsèque l'infection de ces types de supports.

Certaines clés disposent d'un interrupteur permettant d'interdire la lecture, ce qui s'avère très pratique lorsque vous connaissez le niveau d'infection d'une machine pour éviter les dégâts. Pour éradiquer les virus présents **il arrive parfois de ne pas avoir d'autre recours que de passer par une clé USB**, sans parler de l'aspect pratique.



En effet, connecter une machine infectée sur le réseau risquerait de **contaminer d'autres machines**, graver un CD/DVD pour y déposer les programmes de désinfection se révèle couteux (ou fastidieux s'il s'agit d'un ré-inscriptible).

Voici deux logiciels qui vont vous permettre de vacciner une clé USB pour vous protéger par exemple du récent Conficker qui a beaucoup fait parlé de lui.

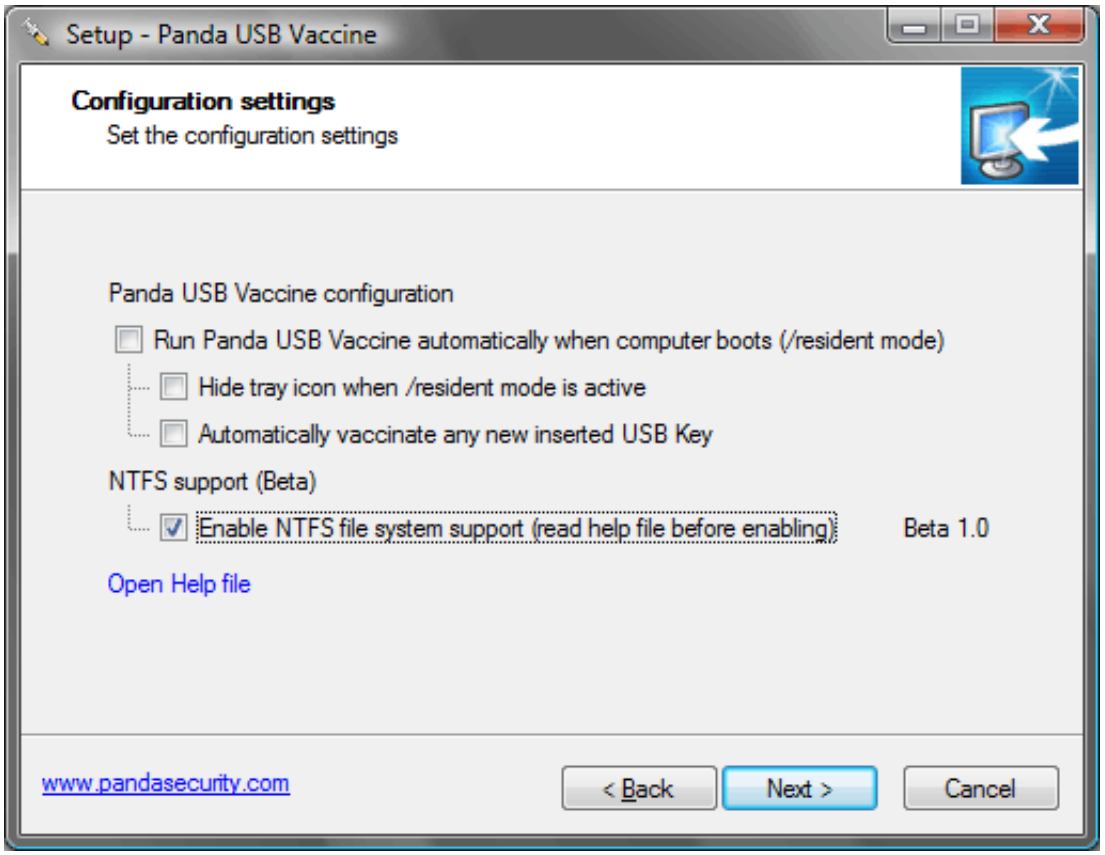
Panda USB Vaccine

Panda USB Vaccine est un logiciel gratuit de l'éditeur antivirus Panda Security qui permet de **désactiver l'exécution automatique** (autorun.inf) sur une clé USB.

Avant toute chose, sachez qu'une clé USB vaccinée par ce logiciel **le restera** tant que

vous ne formaterez pas de nouveau la clé.

J'attire votre attention sur les options proposées lors de l'installation :



Cocher ***Enable NTFS file system support*** si certaines de vos clés disposent de partitions **NTFS** (utile sur les clés de plus de 2Go mais). Je vous déconseille l'option "*Automatically vaccinate any new insterted USB Key*" pour éviter de vacciner vos cartes flash d'appareils photos, PSP, téléphone portable, etc.

Pour vacciner une clé insérez-là puis sélectionnez la lettre de lecteur correspondante (vérifier dans le poste de travail si besoin) et cliquez sur ***Vaccinate USB*** :

Le bouton ***Vaccinate computer*** permet de désactiver l'exécution automatique sur **tous** les périphériques (CD, DVD, USB, SmartFlash, etc.).

Si vous ne connaissez pas l'impact d'une telle manipulation ne le faites pas car vous devrez par la suite explorer les médias manuellement afin de lancer le programme habituellement exécuté via l'autorun.

En entreprise cette fonctionnalité est généralement implémentée au travers d'une stratégie de groupe par votre administrateur système.

Pour conclure, Panda USB Vaccine **fait parfaitement ce qu'on lui demande, et gratuitement**. Il dispose également d'un accès via ligne de commande (cf. documentation).

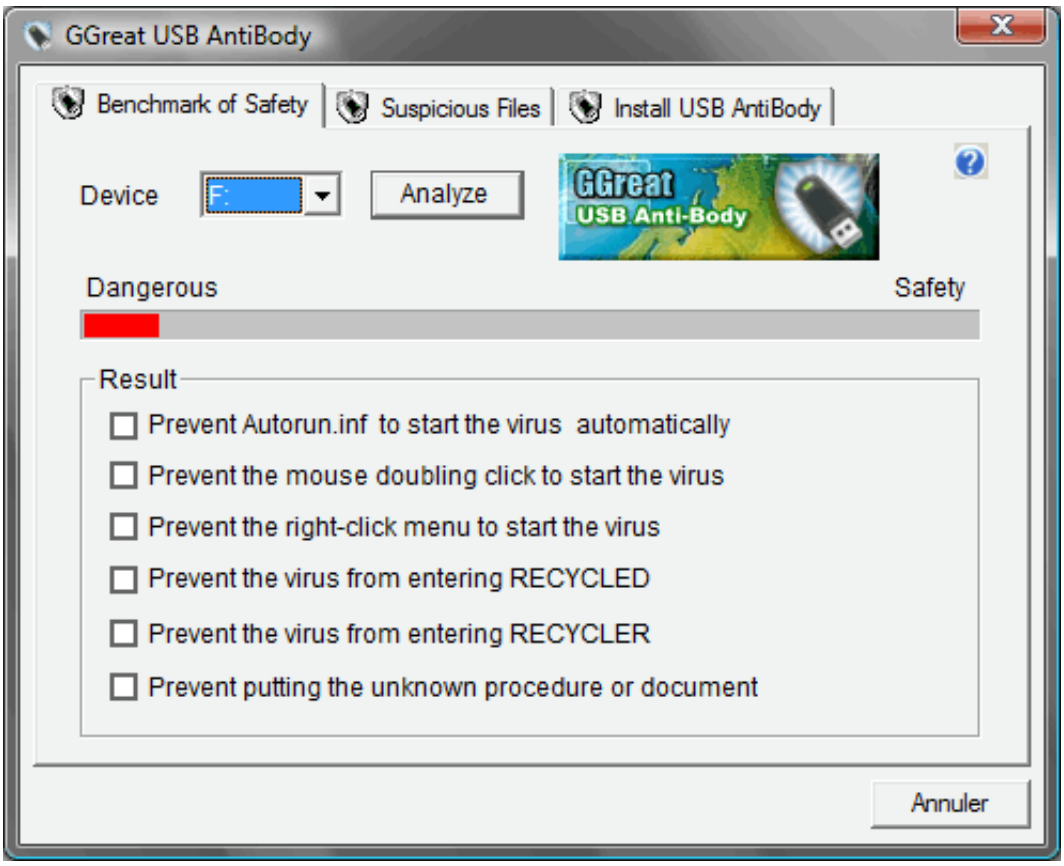
Compatibilité : Windows 2000, XP, 2003, Vista.

Panda USB Vaccine

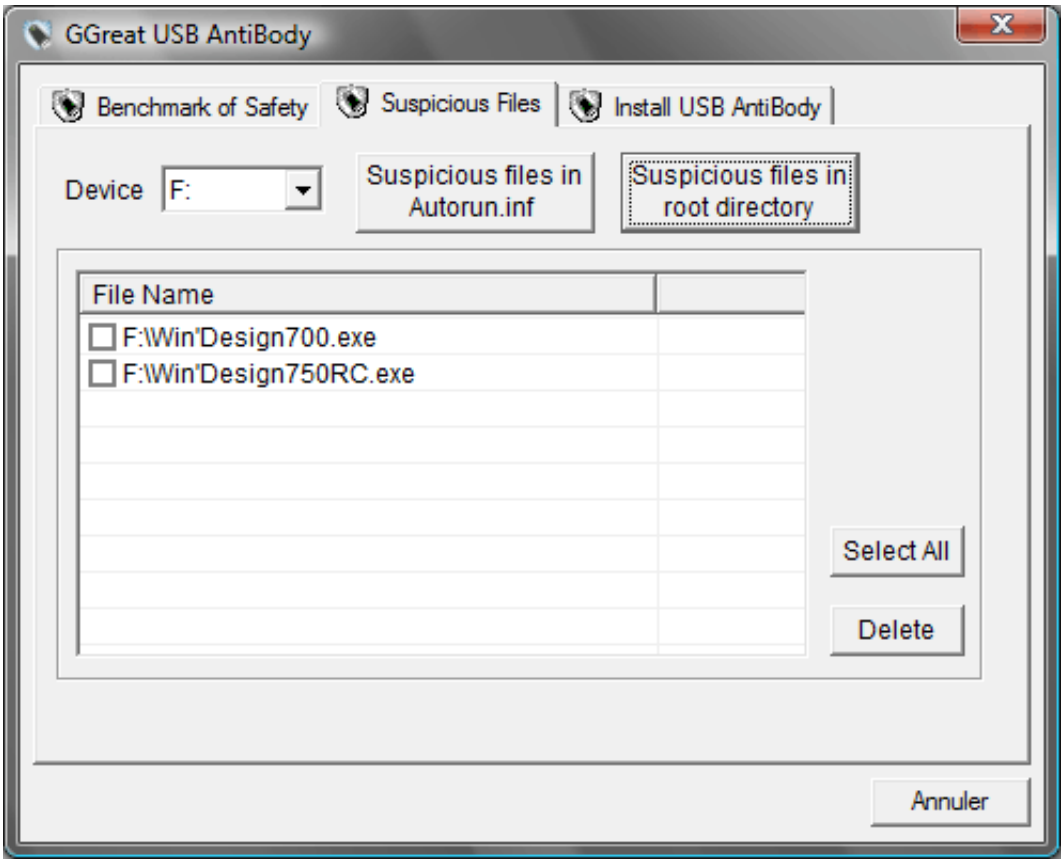
GGreat USB AntiBody (USBAB)

GGreat USB Antibody est un utilitaire gratuit qui ne se limite pas à la protection de l'autorun. Il va plus loin en proposant une **analyse (benchmark) du niveau de vulnérabilité aux virus de la clé**.

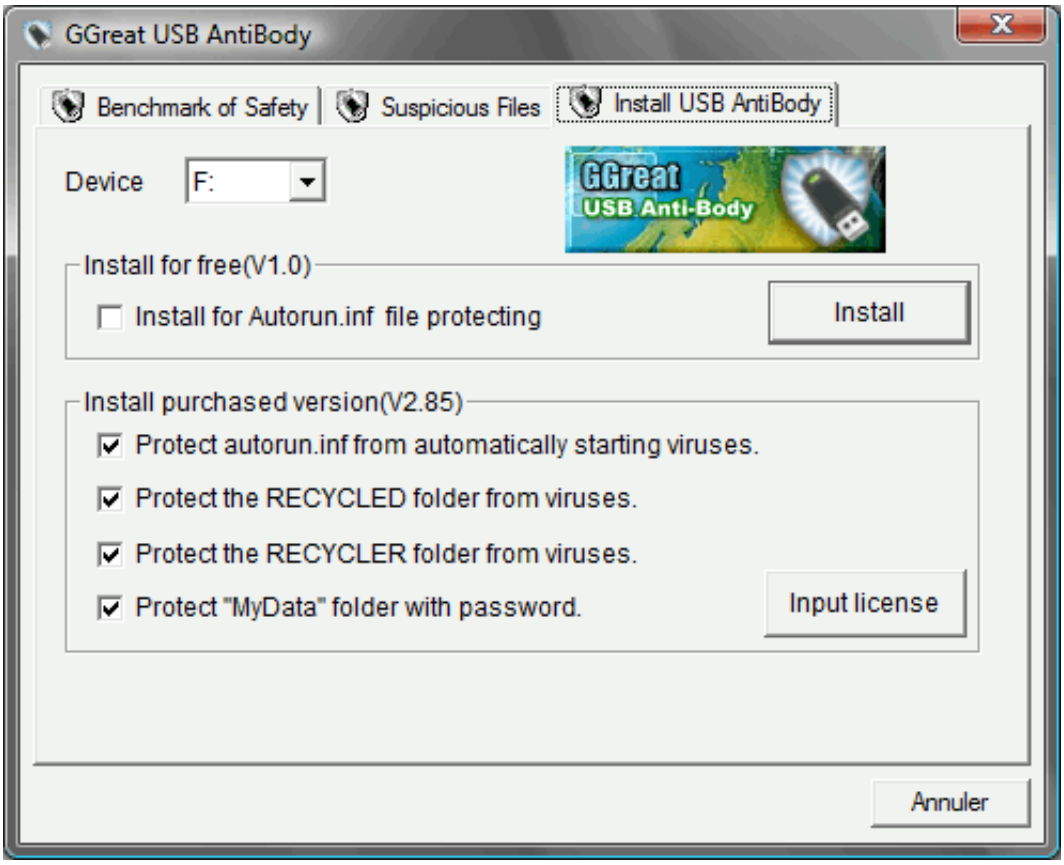
Sélectionnez la lettre de lecteur puis cliquez sur ***Analyze*** :



Le deuxième onglet permet de **lister les programmes potentiellement dangereux** et présents dans l'autorun ainsi qu'à la racine de la clé (uniquement basé sur l'extension des fichiers) :



Le dernier onglet permet de **protéger le fichier autorun.inf** de façon similaire à Panda USB Vaccine :



On regrette toutefois que les options de protections avancées ne soient disponibles que dans la version payante de GGreat USB Antibody.

Compatibilité : Windows 2000, XP, 2003, Vista.

GGreat USB Antibody

Conclusion

Les créateurs de virus et de malware le savent, les clés USB sont une cible privilégiée pour contaminer des machines qui sont parfois déconnectées du web. Pour éviter de rendre votre clé inutilisable suite à une infection de type autorun mais également de contaminer une machine saine **je vous recommande de vacciner vos clés**.

En complémenter, je vous invite à lire cet excellent article sur les infections chez Zebulon ainsi que quelques moyens de désinfection chez CCM s'il est déjà trop tard pour votre clé. Enfin, vous pouvez interdire l'écriture sur une clé USB au moyen d'une modification du registre.

http://research.pandasecurity.com/archive/Panda-USB-and-AutoRun-Vaccine.aspxPandsa

Retour sur l'évènement WebInAlps #5 »