INFECTION CLEF USB

Date de l'infection : 29 mars 2013

Documentations : http://fspsa.free.fr/contamination-lecteurs-amovibles.htm

Un fichier autorun.inf a été créé sur la clef par la machine sur laquelle elle a été connectée.
Un fichier autorun.inf est un fichier texte contenant une série d'instructions exécutées par Windows lors de l'ouverture de la clé. Il suffit de renommer autorun.inf en autorun.inf.txt pour le neutraliser.
En éditant le fichier on trouve, pour le cas cité, les commandes suivantes :

```
[autorun]
Shellexecute=SHDAR.EXE
Open=SHDAR.EXE
SHELL\LV=To My (LV) -please-
SHELL\LV\COMMAND=LOVE.EXE
SHELL\SH=BY THE SHA@DE
```

Les exécutables SHDAR.EXE et LOVE.EXE sont présents à la racine de la clé. Leur exécution infeste la machine sur laquelle la clé est connectée. Les trois fichiers sont recopiés sur la racine de tous les volumes ; les exécutables sont également copiés dans c:\Windows. Le registre est modifié de façon à ce que le PC hôte continue d'infecter les volumes qui seront reliés à l'ordinateur. On trouvera quelques infos sur le web : http://www.google.com/search?q=SHDAR.EXE

En examinant les exécutables on voit apparaître des adresses comme :
http://www.sex.net
http://onec.dz
http://www.linux.com
http://www.arabeyes.com

DÉSINFECTION DE LA CLEF

Pour désinfecter la clé il suffit de renommer ou supprimer les fichiers cités. Si on opère depuis un autre ordinateur on prendra des mesures pour éviter de se faite inutilement infecter. Les précautions et protections à adopter sont explicitées dans le document de référence dont le lien est donné plus haut ; on peut opérer tranquillement depuis le mode sans échec de Windows, une console de réparation winre, ou un système Linux. Avec Linux cliquer sur un exécutable prévu pour Windows ne donnera rien, on est tout-à-fait tranquille.

DÉSINFECTION DU PC

Afficher les Processus (CTL+MAJ+Esc) et supprimer les [Processus] LOVE.EXE et SHDAR.EXE
Revenir à un point de restauration afin de supprimer toute inscription du malware dans le registre.
Redémarrer la machine et supprimer toutes les occurrences des trois hostiles : AUTORUN.INF LOVE.EXE et SHDAR.EXE
Pousser plus avant avec un scan complet avec l'antivirus à jour. On trouve toujours des choses. Soyez

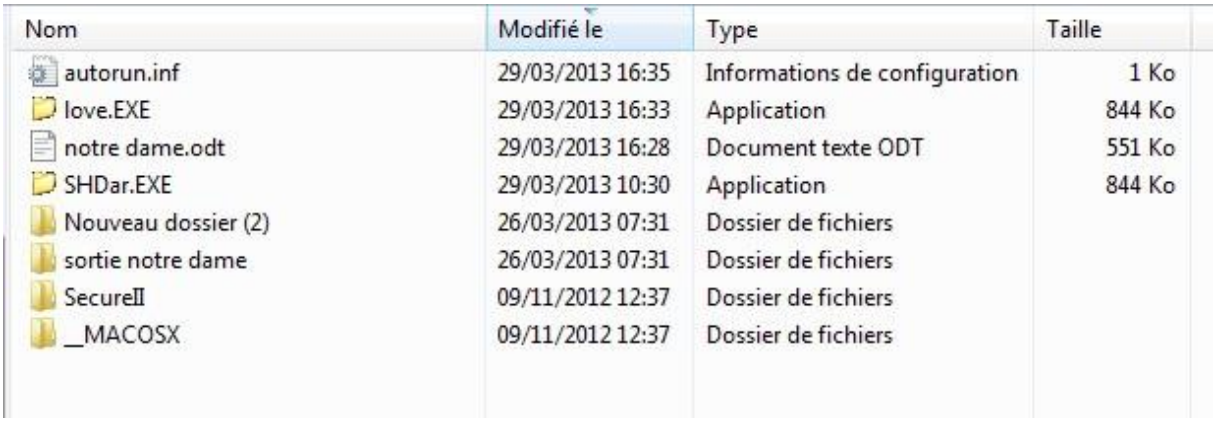
circonspect dans vos mises en quarantaine et ne videz pas l'historique, il peut servir. Poussez plus avant avec un outil spécialisé avec l'aide de la communauté du forum zebulon. Voici une présentation d'un outil très apprécié : ZHP ; faites-vous assister par le forum.
Autres outils d'aide au nettoyage : http://telechargement.zebulon.fr/7/securite/
J'ajoute l'excellent **MalwareBytes Anti-Malware**, de son petit nom **MBAM** dont voici un tutoriel par le non moins excellent Malekal :
http://www.malekal.com/
http://www.malekal.com/2010/11/12/tutorial-malwarebyte-anti-malware/

VACCINATION

Pour protéger la clé contre d'autres attaques il suffit de créer un dossier autorun.inf sur la racine de la clé. En occupant le terrain ce dossier s'oppose à la création du fichier autorun.inf contenant le script hostile. Un fichier spécial est ensuite créé dans ce dossier. Il a la particularité de comporter un mot réservé dans son appellation. La présence de ce mot réservé interdit son effacement et empêche son remplacement un autorun.inf hostile.
Pour terminer on donne au dossier et au fichier les attributs System, Hide, et Read only à l'aide de la commande ATTRIB.
Je n'ai pas utilisé **USB-set** ➔ http://telechargement.zebulon.fr/7/securite/

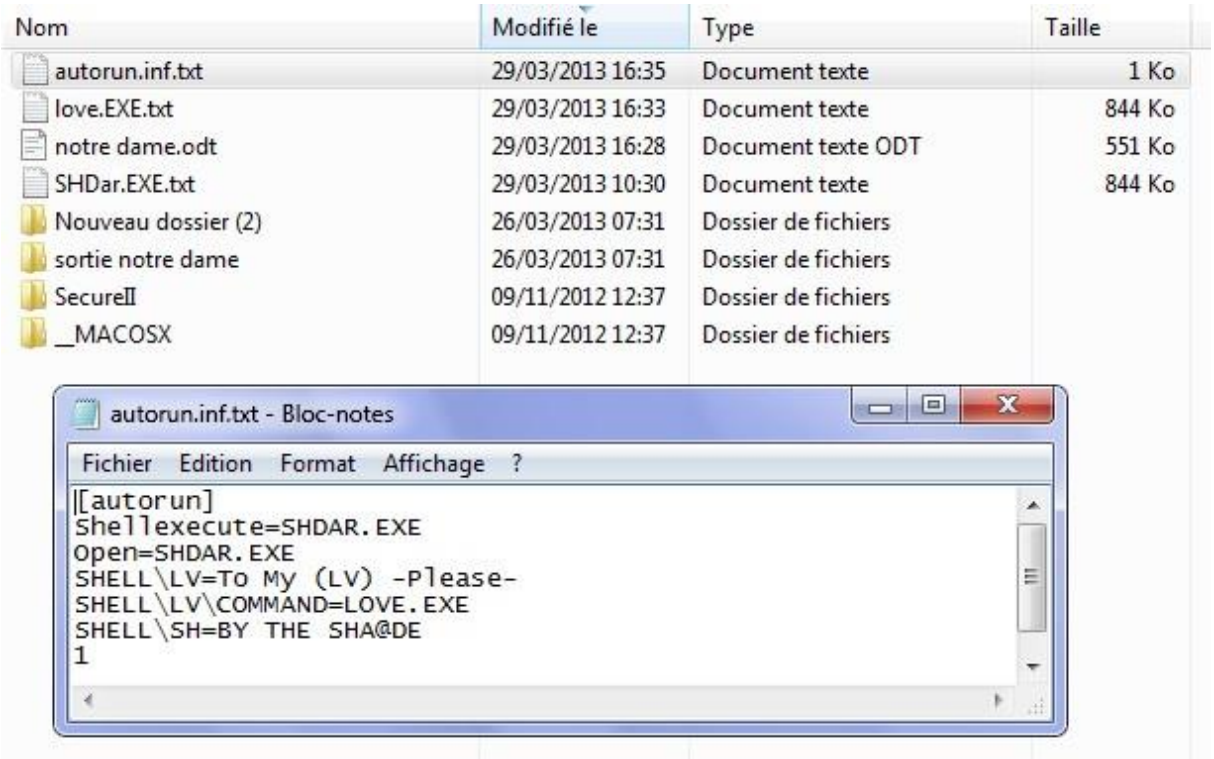
CAPTURES

La capture ci-après montre le contenu de la clef classé par dates. On constate que l'exécutable SHDAR.EXE a été placé à 10h30 alors que love.EXE et autorun.inf ont été créés à 16h33 et 16h35. Les exécutables ont une icône de dossier (désuète) destinée à tromper l'utilisateur qui, malheureusement, n'affiche en général pas les extensions des fichiers (option par défaut). Le but est qu'en croyant ouvrir un dossier **love** ou **SHDar** l'utilisateur active de lui-même l'exécutable :

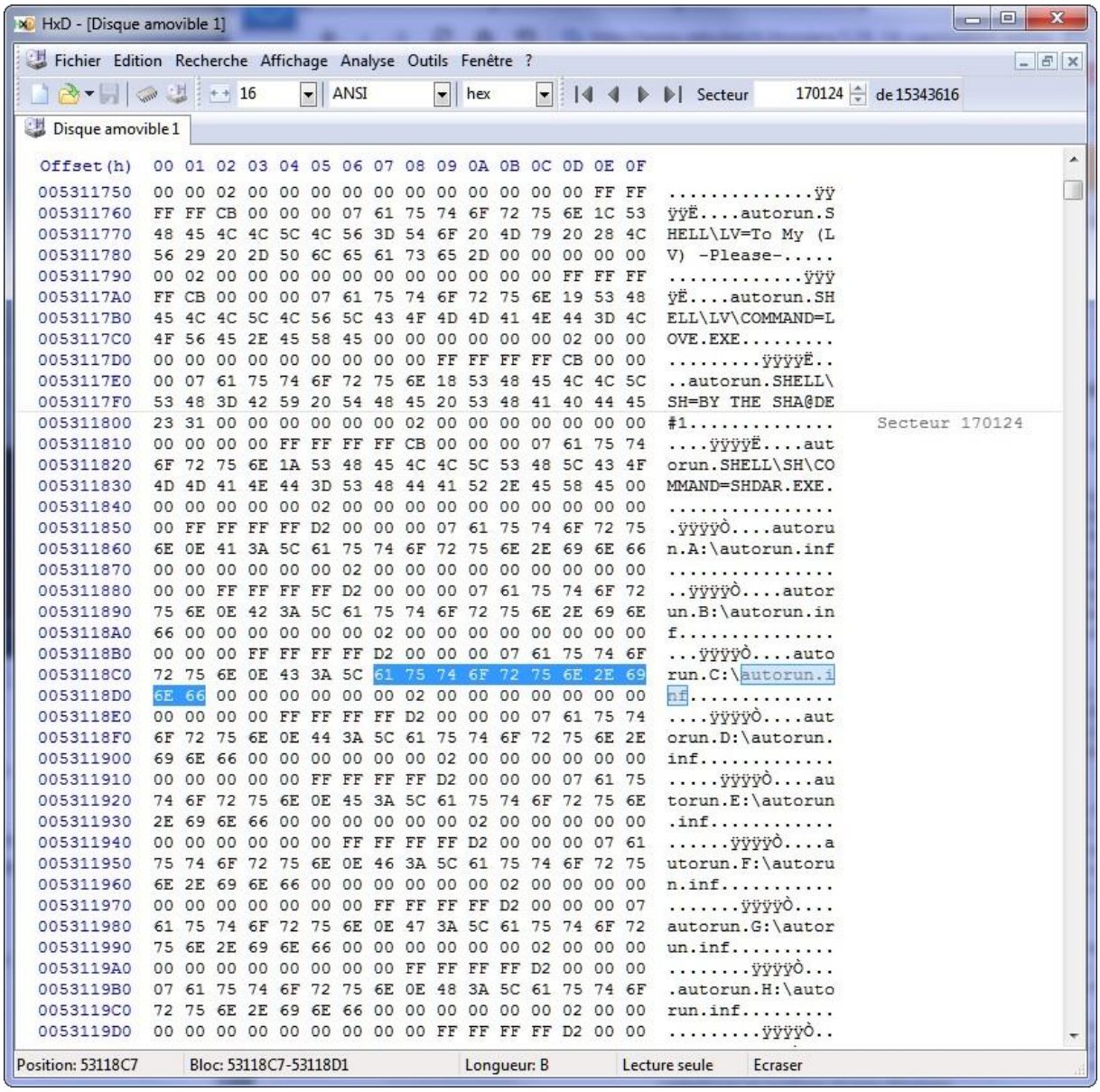


Nom	Modifié le	Type	Taille
autorun.inf	29/03/2013 16:35	Informations de configuration	1 Ko
love.EXE	29/03/2013 16:33	Application	844 Ko
notre dame.odt	29/03/2013 16:28	Document texte ODT	551 Ko
SHDar.EXE	29/03/2013 10:30	Application	844 Ko
Nouveau dossier (2)	26/03/2013 07:31	Dossier de fichiers	
sortie notre dame	26/03/2013 07:31	Dossier de fichiers	
SecureII	09/11/2012 12:37	Dossier de fichiers	
__MACOSX	09/11/2012 12:37	Dossier de fichiers	

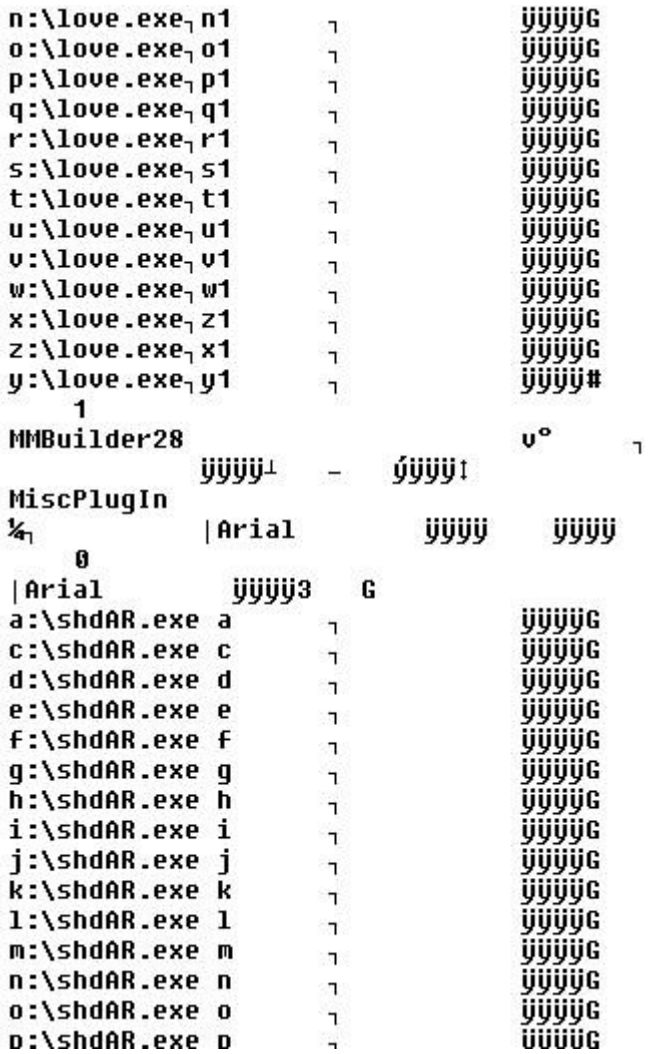
La vue suivante montre que j'ai désactivé les trois fichiers hostiles en leur ajoutant une extension txt ; le contenu de autorun.inf.txt est affiché dans Bloc-notes :



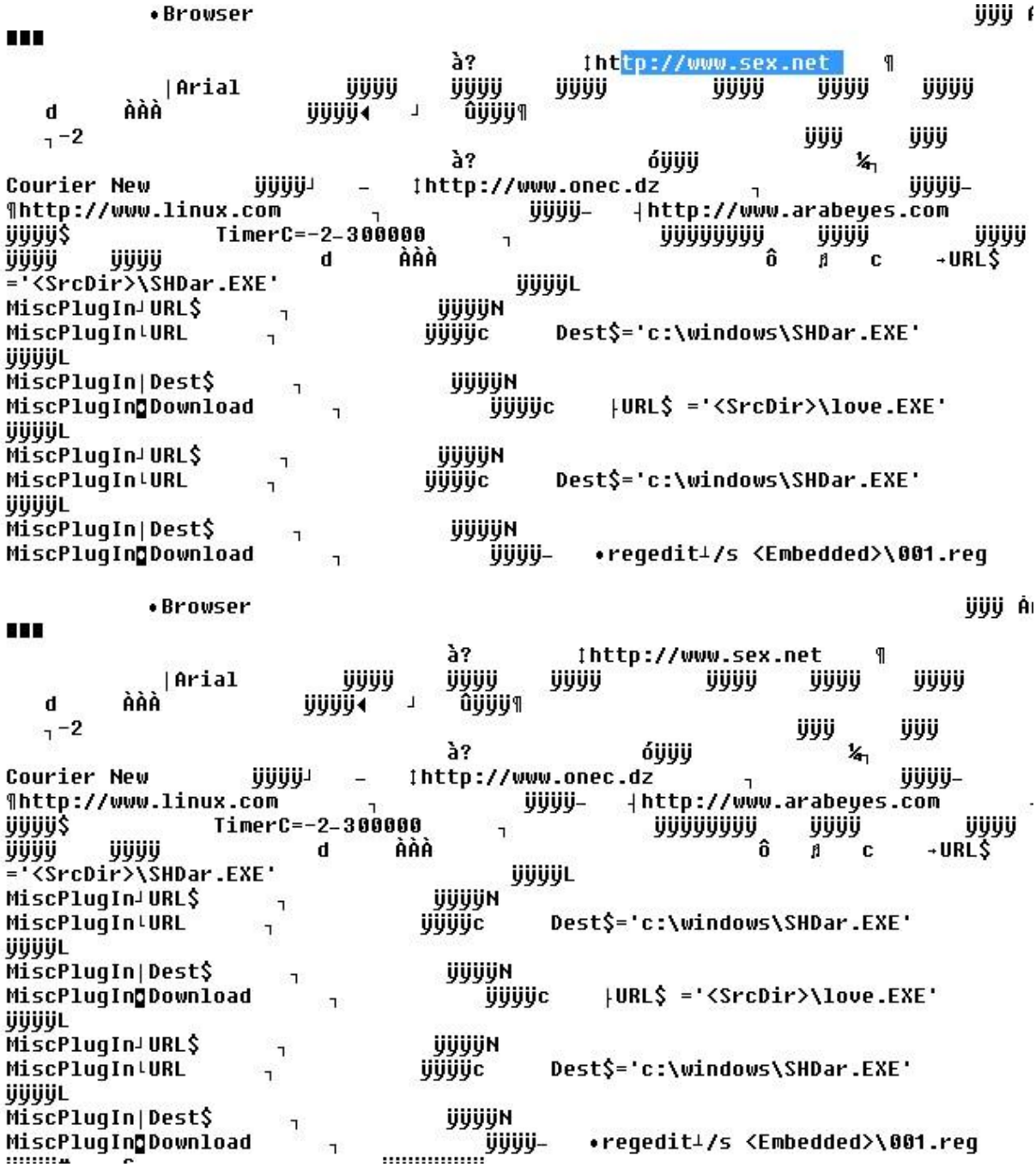
À l'aide d'un éditeur hexadécimal on examine le contenu de la clé. Une recherche du terme autorun.inf montre qu'il apparaît souvent. On devine que les exécutables copient ce fichier sur tous les disques et volumes (il faudra donc les nettoyer, ainsi que les autres clés et disques amovibles) :



En affichant les contenus des exécutables dans Bloc-Notes et en faisant dérouler rapidement les pages de caractères on identifie des passages qui montrent que le double malware tente de se reproduire sur les racines des volumes présents :



On trouve de la même façon les adresses des sites vers lesquels la victime sera dirigée.
On voit également que SHDar.EXE est recopié dans c:\windows
La commande regedit /s sert à fusionner silencieusement au registre le contenu de 001.reg :



•Browser
http://www.sex.net
Courier New
http://www.onec.dz
http://www.linux.com
http://www.arabeyes.com
TimerC=-2-300000
='<SrcDir>\SHDar.EXE'
MiscPlugIn URL$
MiscPlugIn URL
Dest$='c:\windows\SHDar.EXE'
MiscPlugIn Dest$
MiscPlugIn Download
URL$ ='<SrcDir>\love.EXE'
•regedit /s <Embedded>\001.reg

CONCLUSION

La clé est à présent **protégée contre les autorun.inf** (ne pas chercher à supprimer le dossier de vaccination caché et protégé autorun.inf).

On n'est pas protégé des attaques simples qui consistent à écrire sur la clé un exécutable, le nom et l'icône de cet exécutable étant choisis de façon à piéger l'utilisateur.

Pour se protéger plus avant il faut utiliser d'autres formatages que le FAT32. Le **NTFS**, le format par défaut des disques durs, **permet de régler finement les droits d'écriture**. C'est le format à retenir pour une clé de travail de bureau, qui n'est pas destinée à être accessible par les lecteurs de salon (films, images, musique). Créez vos dossiers de travail puis **interdisez toute écriture sur la racine uniquement (sans propagation de la stratégie aux sous-dossiers)**.

On peut acheter des clés possédant un système de verrouillage contre l'écriture. Efficace seulement si on s'en préoccupe activement et qu'on décide de ne jamais lever cette interdiction lorsque la clé est connectée à un PC douteux (tous ou presque).

En ce qui concerne les PC, outre le nettoyage à faire suite à une infection (recherches internet sur l'infection, retour à un point de restauration, recherche de restes éventuels de fichiers, recherches dans le registre, mise à jour de Windows et de l'antivirus, scans du système avec divers outils, demande d'aide personnalisée sur le forum Zebulon), on peut faire quelques réglages de façon à supprimer l'utilisation de l'autorun.inf, ou même interdire l'utilisation de clefs USB. On peut également faire en sorte qu'une clé connectée soit systématiquement vaccinée, voir le document de GOF dans les liens ci-après.

LIENS

http://forum.zebulon.fr/ le forum Sécurité est apprécié :
http://forum.zebulon.fr/securite-f40.html http://telechargement.zebulon.fr/7/securite/
http://www.gratilog.net source fiable de freewares commentés.
Freewares en français de lutte contre les malwares :
http://www.gratilog.net/xoops/modules/mydownloads/viewcat.php?cid=243&show=99
ZHP, Zeb Help Process : Présentation, Conseils, Commentaires, Tutos, Téléchargement =>
http://www.gratilog.net/xoops/modules/mydownloads/singlefile.php?lid=2085

Le document exhaustif de GOF au format PDF :
Sécurisation des Windows face aux menaces des périphériques amovibles :
http://forum.zebulon.fr/guide-securisation-windows-face-aux-menaces-infectieuses-usb-t170848.html
Version web (avec beaucoup de pubs) :
http://www.zebulon.fr/actualites/5151-proteger-infection-virus-malware-cles-usb.html

http://fspsa.free.fr *quelques petites notes perso sur Windows…*
http://fspsa.free.fr/contamination-lecteurs-amovibles.htm le danger des clés USB.
http://fspsa.free.fr/infection-du-29-mars-2013.pdf ce document.

Amicalement, JF => contact *2005fspsajf* (ajouter *@free.fr*)