

Les clés USB (Universal Serial Bus) représentent aujourd'hui un support privilégié pour le stockage des données, elles permettent une utilisation beaucoup plus souple et un espace disponible beaucoup plus important que les autres supports amovibles utilisés aussi bien dans le cadre professionnel que personnel

Dans ce petit guide nous essayerons de présenter les différents risques relatifs à l'utilisation de ces clés, ainsi que les différentes mesures préventives afin de les protéger.

Risques et menaces associés aux clés USB:

Vols d'informations

Exécution automatique d'applications ou de codes malicieux contenus dans la clé

Mesures préventives

1. Bloquer la clé en écriture
2. Nettoyer proprement le contenu de la clé
3. Attribuer des comptes et droits utilisateurs adéquats
4. Bloquer la Fonction Autorun
5. Verrouiller vos postes
6. Affecter une clé par usage
7. Chiffrement et intégrité des informations contenues dans la clé
8. Autres mesures

Risques et menaces associés aux clés USB:

Vols d'informations

Le contenu de la clé USB peut être copié intégralement au moment où la clé est branchée sur un poste étranger. Le risque est qu'une clé peut être utilisée par n'importe qui dans le but de dérober ou voler les données du propriétaire de la clé, dans un intervalle de temps très court, et de la manière la plus simple possible.

Un processus généralement dissimulé au niveau de la liste des processus, tâches, des appels système, comme la plupart des codes malveillants actuels, peut très bien attendre que la clé soit branchée pour lancer la lecture et la copie de son contenu. Un tel processus, ne sera pas facilement détectable sur le poste hôte.

Certains outils permettent même de faire une image complète de la clé. Outre le vol de documents présents, ces outils permettraient également de faciliter la récupération de documents effacés sur la clé USB et qui ne sont pas affichés lors de l'exploration ordinaire de la clé.

L'action décrite dans le paragraphe ci dessus est perpétrée par la machine d'accueil. Une autre approche, se nomme podslurping (podslurping fait référence au produit iPod d'Apple) et s'effectue depuis le périphérique. Elle consiste à brancher sur un système un support de stockage, ou aussi un lecteur MP3, afin d'en dérober l'information de façon furtive.

Il suffit ainsi de brancher le lecteur de musique sur un ordinateur cible, sur le port USB, en prétendant que ses batteries sont déchargées et pendant quelques minutes, une partie du disque est copiée sur le lecteur, qui dispose d'un espace de stockage important (de l'ordre de quelques Go à plusieurs dizaines de Go).. Ceci est aussi valable pour un appareil photo numérique.

Ce problème n'est pas récent. Il existait déjà dès l'apparition des disquettes. Cependant, ces nouveaux "supports de stockage" ont une capacité et un débit de transfert beaucoup plus importants, ce qui augmente la quantité de données pouvant être copiées facilement et rapidement.

Exécution automatique d'applications ou de codes malicieux contenus dans la clé

Le deuxième cas correspond lorsque la clé est utilisée pour attaquer le poste sur le quel elle est branchée

Il suffit de placer sur la clé un fichier infecté manuellement par une personne malveillante, ou automatiquement par un virus, puis d'attendre que la clé soit branchée sur un nouveau poste et d'exécuter le fichier infecté

Il est aussi possible de rendre l'attaque plus efficace en déclenchant automatiquement l'exécution du fichier malicieux dès l'insertion de la clé USB, sur les ordinateurs n'ayant pas désactivé la fonction "Autorun" (qui permet le lancement automatique des CD-ROM dès leur insertion).

La fonction "Autorun" ne fonctionne pas normalement pour une clé USB puisqu'elle est reconnue par Windows comme un disque amovible, et donc jugée comme source non sûre. Cependant, il est possible de faire passer certaines clés USB pour un CD-ROM : lorsque la clé est insérée, Windows voit alors cette clé comme étant un CD-ROM (au lieu d'un disque amovible) et exécute automatiquement le fichier "autorun.inf" présent sur la clé.

Ceci peut être réalisé très facilement avec les clés USB de type "U3". La norme "U3" permet d'embarquer sur des clés USB des applications autonomes qui s'exécutent sur la clé. Les clés conformes "U3" sont disponibles couramment depuis l'automne 2005, et depuis l'été 2006 la méthode pour configurer une clé U3 en clé d'attaque a été largement diffusée sur Internet.

Les clés "U3" sont susceptibles de contenir plusieurs informations personnelles ou confidentielles. Le vol de celles-ci peut avoir des conséquences importantes:

- la configuration du client de messagerie
- les contacts stockés par le client de messagerie
- les pages en cache du navigateur Internet
- les sites favoris installés sur le navigateur
- des mots de passe gérés par une application dédiée (application fréquemment offerte par défaut avec la clé).

Les clés U3 sont généralement fournies avec un lanceur. Une fois la clé insérée ce lanceur donne accès aux applications. Certains lanceurs malveillants permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant de récupérer les tables de mots de passe, d'installer une capture de clavier ou un rootkit.

Mesures préventives :

1. Bloquer la clé en écriture

Certaines clés présentent un interrupteur physique, qui permet de bloquer l'accès en écriture à la clé, cela empêcherait de modifier le contenu de la clé, de l'effacer ou certains codes malicieux de l'utiliser comme moyen de propagation.

2. Nettoyer proprement le contenu de la clé

La suppression n'est souvent pas suffisante pour détruire complètement toute trace d'un document. Certains outils permettent de faire un nettoyage beaucoup plus complet.

Sous Windows, il existe par exemple :

- eraser <http://www.bugbrother.com/eraser>
- BCWipe <http://www.jetico.com/bcwipe.htm>

Sous Linux ou MacOS, il existe entre autres la commande shred (ShredIt sous Mac OS) ou l'application :

- wipe <http://wipe.sourceforge.net/>

3. Attribuer des comptes et droits utilisateurs adéquats

La clé dispose exactement des mêmes droits que ceux de l'utilisateur courant sous Windows. Il serait donc nécessaire de n'autoriser la connexion de clés que sur des sessions avec des droits limités. Les droits administrateur ne doivent être réservés que dans des cas étudiés, afin de limiter les actions qui pourraient être effectuées sur le système.

4. Bloquer la Fonction Autorun

Pour désactiver la fonction autorun sous Windows, il suffit de modifier la clé suivante dans la base de registres HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/CDRom

- Pour la désactivation de l'autorun : attribuer la valeur Autorun = 0
- Pour l'activation de l'autorun : attribuer la valeur Autorun = 1

5. Verrouiller vos postes

Un poste sans contrôle est sujet à tout type de malversation entre autre physique. Ainsi et afin d'éviter des incidents liés à l'insertion de clés USB sur son système, il est important de verrouiller son poste de travail lorsque ce dernier n'est pas utilisé

6. Affecter une clé par usage

Il faudrait considérer une clé par usage, et d'interdire son déplacement hors des lieux de son utilisation. Si une clé doit être insérée dans un système critique, il est nécessaire de vérifier son origine. Une solution serait de conserver une clé propre, régulièrement formatée, et d'en réserver l'usage de l'USB.

7. Chiffrement et intégrité des informations contenues dans la clé

Il existe plusieurs solutions assurant l'intégrité et le chiffrement des données contenues sur les clés USB, mais nous nous contenterons à ce niveau de présenter seulement des solutions simples. Notons que les informations relatives à l'intégrité ou au chiffrement ne doivent pas être placées sur la clé elle-même :

- Vérifier en cas de soupçon tout fichier inconnu trouvé sur une clé USB

- Besoin de protéger les données sous une forme chiffrée placées sur une clé USB avant que l'utilisateur les extraire. Cette solution est simple il suffit de stocker toute information sensible dans un fichier "**ZIP**" (qui effectue respectivement la compression et la décompression des fichiers) protégé par mot de passe.

8. Autres mesures

D'autres mesures non directement liées à l'utilisation des clés USB peuvent être dans notre cas très utiles. Un guide présentant les précautions de base pour sécuriser efficacement son PC, et se prémunir contre tous types de danger cybernétique est disponible sur notre site web :

http://www.ansi.tn/fr/Guides_et_ressources/brochures/brochure_guide_internaute.pdf