# Virus de clés USB

- Découvrir, s'informer - Découvrir et connaître -

Date de mise en ligne : dimanche 10 janvier 2016

De plus en plus d'établissements sont victimes d'infections virales. Ce n'est pas (ce n'est plus seulement) Internet le principal vecteur de propagation mais les disques amovibles usb.

Voici quelques conseils et précautions pour lutter contre ce fléau.

# Principe de propagation

## Scénario 1

Vous branchez votre clé usb sur un pc où l'infection est active. Le virus va automatiquement copier/coller sur celle-ci des fichiers relatifs à l'infection, aux attributs "cachés" et "Systèmes". En effet, le virus désactive généralement l'affichage des fichiers et dossiers cachés, dans le cas où vous l'auriez activé, afin de se masquer sur le pc infecté et sur la clé.

## Scénario 2

Une clé infectée est branchée sur une machine saine. Le virus va automatiquement copier/coller sur celle-ci des fichiers relatifs à l'infection, aux attributs "cachés" et "Systèmes".

Suivant les variantes, ces fichiers ne sont pas les mêmes, mais il y aura presque systématiquement un fichier Autorun.inf qui permettra au virus de se propager quand la clé sera branchée sur un autre pc.

Pas la peine de continuer la démonstration : vous avez compris qu'un réseau de collège ou de lycée est un terrain particulièrement favorable à la propagation de ce type virus. Un indicateur de leurs présences sur des machines du réseau ou sur des supports amovibles est la présence d'un fichier autorun.inf - en fichier caché - à la racine des unités de disque : disques amovibles, lecteurs réseaux, disques locaux... en fait, toutes racines de disques où un utilisateur à des droits d'écriture.

# Précautions et conseils

# Avoir un antivirus à jour

La première des précautions est, bien sûr, d'avoir un antivirus à jour sur l'ensemble des machines de l'établissement.

# Avoir un système d'exploitation à jour

La majorité des virus exploitent des failles du systèmes d'exploitation. Les mises à jour automatiques de Windows doivent être activées sur tous les postes. Il faut régulièrement mettre à jour les images de sauvegarde. Pour cela, OSCAR vous facilitera grandement la tâche.

Malheureusement ces deux précautions de base ne sont pas forcément suffisantes.

- Certaines variantes ne sont pas détectées même avec un antivirus à jour
- Vous ne maîtrisez pas la situation des machines en dehors de l'établissement sur lesquelles les clés USB sont régulièrement branchées.
  Il est donc également conseillé de :

# Désactiver les modes AUTORUN pour les clés USB

Pour ce faire, le plus simple est d'utiliser les modèles académiques ESU qui bloquent les autorun sur tous les lecteurs.

# Informer les utilisateurs

De nombreux utilisateurs véhiculent des virus via leurs clés USB sans le savoir. Informez-les (par une affiche en salle des profs, par exemple) des précautions à prendre comme indiqué sur cette page. Pour un ordinateur à usage personnel, pas la peine d'investir dans un antivirus coûteux. Plusieurs solutions gratuites, assurent une protection tout à fait satisfaisante.
Mais le plus performant doit rester la solution offerte par le Ministère que vous trouverez sur cette page.

# Quelques utilitaires

- UsbFix : http://www.usbfix.net/
- Outil de suppression des logiciels malveillants Microsoft® Windows®