Attention à vos clés USB et Disques externes

La clé USB est un petit périphérique bien pratique. Cet accessoire permet d'emmener avec soi fichiers, musiques, photos, vidéos… Elle peut être utilisée comme solution de copie de secours de documents, comme moyen d'échange avec des amis, ou encore pour finir de travailler sur un dossier à la maison. Véritable accessoire de mode dans certains cas, elle est devenue un objet de notre quotidien. Mais qui se douterait que derrière ce petit bout de plastique peut se cacher une petite bombe numérique ?

LA PERTE DE VOTRE CLÉ USB

Qui n'a pas perdu un jour sa clé USB ? Si ce n'est pas le cas, ça risque d'arriver. C'est toujours au mauvais moment qu'on ne la trouve plus. Tantôt on la cherche pour y stocker les photos prises par ses amis, tantôt c'est pour retrouver son document travaillé à la maison, mais impossible de mettre la main dessus.

C'est toujours contrariant, mais est-on sûr de tout ce qu'il y avait sur sa clé ? Quelles sont les informations qui s'y trouvent ? Fin 2011 une société de sécurité informatique a acheté aux enchères un lot de clés USB perdues dans le métro de Sydney et les a analysées.

La très grande majorité des documents qui s'y trouvent sont des photos, mais il y avait aussi des documents fiscaux, des documents d'entreprises, des devoirs scolaires... Et s'il s'agissait de photos intimes que vous avez perdues ? Ou encore des rapports confidentiels de votre entreprise ? Ou encore, une lettre d'amour... Plutôt gênant, surtout si on les retrouve ensuite sur les réseaux sociaux.

Alors que faire *?* ***Voici quelques conseils simples*** *:*

1. Ne pas mettre sur une clé USB des fichiers qui ne doivent pas circuler dans le public. C'est une solution radicale, mais pas toujours possible à mettre en œuvre.

2. Chiffrer sa clé. Solution simple et très efficace. Il existe plusieurs outils gratuits qui le font bien et qui sont assez faciles à utiliser. Sans le mot de passe de déchiffrement, impossible d'accéder aux données de la clé. Elles sont totalement illisibles. Évidemment, il ne faut pas perdre le mot de passe.

3. Régulièrement purger sa clé de ce qui ne doit plus s'y trouver. Un peu de "ménage" régulièrement permet de limiter le risque de voir trop d'informations perdues et aussi de gagner de l'espace sur la clé.

LA CLÉ USB MALICIEUSE …

Nous sommes dans le cas d'une clé qui contient, le plus souvent à l'insu de son propriétaire, un logiciel qui va chercher à s'introduire sur un ordinateur. Ce sont ce que l'on appelle des malwares. Leur objectif peut être multiple. Un virus qui détruit vos données, un cheval de Troie qui permet à une personne tierce de pénétrer votre ordinateur, des keyloggers qui espionnent ce que vous tapez au clavier pour récupérer vos mots de passe, etc. Les deux-tiers des clés analysées par la société de sécurité informatique Sophos contenaient un virus (Sophos Naked Security December 2011).

Ces logiciels malveillants procèdent de trois façons pour s'introduire dans votre ordinateur :
1. L'autorun, qui ne fonctionne plus que sur les anciens systèmes. Dès que la clé est introduite, un logiciel s'exécute automatiquement sans vous demander votre avis. C'est extrêmement dangereux et désactivé sur les systèmes récents.
2. Le boot sur la clé. Un microprogramme est caché au tout début de la clé et s'exécute si celle-ci est introduite avant le démarrage de l'ordinateur. Le PC cherchera à s'initialiser à partir de la clé et exécutera le logiciel malveillant.
3. En vous incitant à cliquer sur un fichier. Une expérience a été menée dans une entreprise. Des clés contenant un document nommé "photo coquine de xxx" ont été éparpillées.

Pour une grande majorité, les personnes qui ont trouvées les clés ont cliqué sur le fichier. Une photo s'affichait bien, mais le document était en fait un programme expérimental destiné à compter les gens qui cliqueraient sur le fichier. Un malware, lui, aurait silencieusement infecté les ordinateurs.

Comment se prémunir de la clé malicieuse ?
1. Disposer d'un antivirus à jour qui analyse les clés lors de leur introduction.
2. Désactiver l'autorun sur un ordinateur ancien.
3. Ne pas démarrer son ordinateur avec une clé déjà insérée.
4. Prendre moult précautions avant d'ouvrir un fichier inconnu.

LA CLÉ ASPIRÉE

Que se passe-t-il lorsque l'on connecte sa clé sur l'ordinateur des autres ? Bien évidemment, il faut qu'il y ait un antivirus qui soit à jour. Mais d'une façon générale, il ne faut jamais brancher une clé qui contient des données personnelles sur un ordinateur autre que le sien. Pourquoi ? Parce qu'il existe des "aspirateurs" de clé. Dès que vous branchez votre clé sur l'ordinateur, un programme que vous ne voyez pas se déclenche et fait une copie de toute votre clé dans un dossier caché de l'ordinateur.

Ne connectez que des clés dont le contenu peut être diffusé sur des ordinateurs inconnus.

LA CLÉ QUE L'ON CROIT EFFACÉE

Vous venez d'acheter une nouvelle clé USB, plus belle, plus grosse, et l'ancienne ne sert plus à rien. Vous effacez son contenu et la donnez à une connaissance. Erreur ! Il existe des logiciels qui permettent de récupérer le contenu d'une clé USB, même si cette dernière vient d'être formatée.

Avec Windows, il existe des programmes pour sécuriser vos informations,

Par exemple … Chiffrement de clé : Veracrypt

Et les smartphones et disques durs externes ?

Smartphones et disques durs externes se comportent de la même façon qu'une clé USB lorsque vous les connectez à un ordinateur, il faut donc leur appliquer les mêmes précautions. Il faut même être encore plus prudent avec un smartphone puisque son contenu peut difficilement être totalement effacé. De plus, si on branche son smartphone à charger sur la prise USB d'un ordinateur inconnu, rien ne dit qu'un "aspirateur" de données ne vas pas essayer de récupérer tout son contenu.