



PLUS DE VIRUS QUE JAMAIS

ATTENTION! Tous les producteurs de logiciels semblent être d'accord pour dire qu'il n'y a jamais eu autant de logiciels malveillants. Les laboratoires de F-Secure, par exemple, recevraient une moyenne de 25 000 échantillons de nouveaux logiciels malveillants par jour, sept jours sur sept. Selon cette compagnie, si cela continue ainsi, on devrait dépasser le cap du million de virus et chevaux de Troie d'ici la fin de l'année 2008. De même, F-Secure signale que les criminels utilisent de moins en moins les fichiers attachés à des courriels mais donnent plutôt, dans des messages, un hyperlien vers un logiciel infecté en utilisant des arguments qui incitent les internautes à cliquer sur cet hyperlien comme « *There is a video of you on YouTube* » ou « *You have received a greeting card* ». Ce type d'infection peut aussi se produire directement sur un site Web qu'on visite si on n'a pas pris la précaution d'installer tous les correctifs fournis pour le navigateur qu'on utilise. Le pire, c'est que, dans la plupart des cas, celui qui est infecté ne s'en rend pas compte. Il est donc recommandé de faire toutes les mises à jour du logiciel de navigation utilisé et d'éviter de visiter des sites douteux et, surtout, d'éviter de cliquer sur des liens sans réfléchir. Mais la meilleure recommandation de toutes reste d'avoir sur son ordinateur un bon logiciel antivirus mis à jour régulièrement. Ce n'est que comme cela qu'on peut éviter des virus comme **Mebroot**, un programme qui infecte l'enregistrement d'amorçage maître de Windows, comme cela se faisait sous DOS il y a une quinzaine d'années, ce qui peut faire de gros dégâts, permettre la prise en main de l'ordinateur à distance aussi bien que rendre un ordinateur inopérable. Le virus **Win32.Ntldrbot** (alias **Rus-tock.C**) de type *rootkit* est présent sur tellement d'ordinateurs qu'on estime à plus de 90 milliards le nombre de messages de spam qu'il peut envoyer par jour à travers ces ordinateurs sans que leur utilisateur n'en sache rien. On pourrait aussi mentionner les virus avec demande de rançon, pour ordinateurs aussi bien que pour téléphones intelligents, de même que les virus qui se déploient par MMS ou par lien Bluetooth. Les criminels profitent en effet de la généralisation des oreillettes Bluetooth pour s'infiltrer dans les téléphones sous Windows ou Symbian. En bref, disons que les virus sont de plus en plus vicieux, qu'ils s'attrapent de plus en plus souvent par les liens HTTP et FTP, sur PC aussi bien que sur Mac. Les entreprises, les banques et les médias sont visés autant que les utilisateurs ordinaires parce que les criminels le font surtout pour rentabiliser au maximum leur investissement auprès des programmeurs qu'ils ont engagés, sans scrupules mais parmi les meilleurs au monde.

DES CLÉS DE MÉMOIRE ULTRA SÉCURISÉES ET POUR CAUSE...

Après le vol d'ordinateurs portatifs et d'ordinateurs de poche vient celui des clés USB avec des données importantes, privées ou personnelles, non sécurisées. Juste aux États-Unis, pour 2007, on estime à plus de deux millions de dollars la valeur des informations perdues à cause du vol de clés USB et, semble-t-il, plus de 40% des pertes et vols de clés USB se sont passés dans le secteur gouvernemental. Un sondage fait par Sandisk a permis de déterminer que 77% des utilisateurs de clés USB en entreprise avaient déjà amené de leurs données personnelles sur une clé ou qu'ils avaient copié des fichiers de l'entreprise sur leur clé personnelle. 25% d'entre eux avaient copié des dossiers de clients, 17% des données financières, 15% des plans d'affaires... 12% des personnes interrogées avaient déjà trouvé une clé de mémoire dans un lieu public et 55% de ces personnes ont admis qu'elles auraient essayé de lire les données qui s'y trouvaient si cela leur était arrivé. Pourtant, dans le même sondage, Sandisk apprenait que près de la moitié des entreprises n'ont aucune politique face au transport de données sur des clés USB par leurs employés et à la sécurisation de ces données. On comprend donc pourquoi les producteurs de clés USB ne les vendent plus sans logiciels permettant de sécuriser les données qui y sont sauvegardées mais encore faut-il qu'ils soient utilisés.



Certains fabricants ont aussi poussé cette sécurité au maximum. Ainsi, SanDisk (www.sandisk.com) a mis sur le marché la **clé USB Cruzer Enterprise FIPS Edition** avec un niveau de sécurité de classe *gouvernement* certifié FIPS 140-2 niveau 2. Cette clé vise surtout les personnes qui travaillent dans des organismes gouvernementaux, militaires, financiers ou de santé. Toutes les entreprises peuvent aussi en profiter. La clé ne peut être utilisée sans qu'un logiciel vérifie en permanence si les fonctions de cryptage ont été altérées et il est impossible d'accéder au contenu sans mot de passe ni clé de cryptage. Prix: de 87\$ pour 1 Go à 385\$ pour 8 Go. De son côté, la firme MXI Security (www.mxisecurity.com) propose maintenant des clés de 512 Mo, 1 Go, 2 Go, 4 Go et 8 Go dans ses séries **Stealth MXP** et **Stealth MXP Passport** avec des logiciels de cryptage des données. Ces clés sont aussi certifiées FIPS 140-2 niveau 2. Leur prix n'était pas encore disponible au moment d'écrire cet article.

