# Un ver « basique » s'attaque aux clés USB

Les experts en sécurité alertent sur l'arrivée d'un nouveau ver qui se propage par les clés USB en s'inspirant des premières techniques de propagation virale. SillyFD-AA s'auto installe sur les systèmes Windows en tentant de créer un fichier autorun.inf sur tous les périphériques de stockage comme les clés USB et les disquettes.

*« Les clés USB deviennent tellement économiques que les professionnels du marketing n'hésitent pas à en distribuer sans compter dans le but de renforcer les ventes »*, déclare Graham Cluley, consultant technologique chez Sophos. *« Les utilisateurs devraient être particulièrement méfiants quand ils connectent un périphérique d'origine inconnu sur leur PC parce qu'un code malveillant pourrait s'y trouver. »*

*« Avec la croissance significative des attaques à caractère financier, ce pourrait évidemment être une porte dérobée permettant aux criminels l'accès au réseau d'une entreprise. »*

Une fois le périphérique connecté à un autre ordinateur, le ver s'installe automatiquement sur le nouveau PC et répète l'exercice afin de se propager plus amplement. Les utilisateurs sont invités à arrêter la fonction de démarrage automatique [Autorun] dans Windows.

La technique imite les toutes premières méthodes de propagation virale quand les virus se propageaient seulement à travers les disquettes. La protection antivirale était alors simple; les utilisateurs avait juste besoin de recouvrir l'encoche propre aux disquettes 5,25 pouces avec de la bande adhésive, également baptisé 'le préservatif à virus' – cette encoche, une fois obturée, interdisait toute nouvelle écriture disque.