Ver: Opanki se la joue iTunes sur AOL IM

Toujours la même histoire: un faux message alléchant reçu sur sa messagerie instantanée et c'est votre PC qui se transforme en moulin La nouvelle mode des vers et autres malwares est de se diffuser via les messageries instantanées en se dissimulant derrière des messages alléchants. Les utilisateurs, souvent des ados, cliquent sans trop savoir et infectent leurs machines. La vigilance qui existe aujourd'hui autour des mails n'est pas encore une habitude pour l'IM, l'instant messaging.

Bref, le dernier ver en date qui utilise ce vecteur est Opanki qui selon F-Secure aime à se propager sur la messagerie instantanée d'AOL. Conçu pour Windows 95, 98, Me, NT, 2000, XP et Server 2003 ce ver propose se présente sous ce message cliquable: *« this picture never gets old »*. Le naïf qui clique observe avec joie l'apparition de l'exécutable itunes.exe. L'erreur est bien sûr de penser qu'il s'agit de la célèbre plate-forme d'Apple. En fait, une fois exécuté, itunes.exe ouvre les ports qui ont téléchargé, puis ouvert le fichier infecté. Et c'est comme cela qu'un PC se transforme en moulin grâce à l'ouverture de cette back door. Les machines infectées peuvent ainsi être contrôlées à distance par des pirates à travers des commandes en IRC. Opanki modifiera également la base des registres pour s'exécuter à chaque démarrage et vous offrira au passage quelques spywares. Enfin, il se dupliquera à travers la base de contact de la messagerie