La messagerie instantanée d'AOL est victime d'un ver/ virus

Voilà qu'un nouveau code malveillant essaye de pénétrer le service d'IM d'AOL. Ce dernier se fait passer pour un fichier image.

Le ver ouvre une porte dérobée pour les 'rootkits' et les chevaux de Troie, leur permettant de se propager d'un poste à l'autre et de contaminer un maximum d'utilisateurs du service.

L'information provient du laboratoire FaceTime Security.

Selon le rapport publié par les experts antivirus de ce labo, le niveau de dangerosité de ce code est important, dans la mesure où, lorsqu'il est activé, il contamine l'ensemble de la liste de contacts de la cible.

Dénommé **W32.pipeline**, ce fichier est extrêmement virulent et très à la mode chez les pirates qui ciblent de plus en plus les utilisateurs de ce type de service.

L'arnaque est bien ficelée. Pour contaminer un maximum de postes les pirates ont trouvé là le bon truc, semble-t-il. W32.pipeline apparaît comme un message instantané, qui demande à l'utilisateur d'envoyer une photo de lui vers un faux lien.

Au lieu de cela, un fichier qui se fait passer pour du .jpg est téléchargé discrètement sur le poste cible. SI le fichier est activé, l'application csts.exe est créée et s'installe dans le dossier system32.

Une fois qu'un poste est infecté, la machine devient un des nombreux ordinateurs d'un réseau de 'botnet', dont le but et la propagation de codes malveillants.

Le plus original dans cette attaque n'est pas le ver utilisé ou son résultat, mais bien la façon dont les pirates le diffusent. Les internautes vont donc avoir à se méfier encore et toujours des programmes de messageries instantanées.