Danger : le virus Grum n'est pas une bêta d'IE

Alerte de Sophos, éditeur de solutions de sécurité et de contrôle des réseaux : une attaque malveillante largement diffusée se fait passer pour une incitation à télécharger une version beta du logiciel Internet Explorer 7.0.

Les messages, qui prétendent être envoyés par Microsoft via l'adresse admin@microsft.com sous la ligne d'objet « *Internet Explorer 7 Downloads*« , comportent une image qui invite le destinataire à télécharger la version beta 2 d'Internet Explorer 7. Derrière se cache un fichier nommé ie7.0.exe, infecté par le ver Grum-A.

Le ver Grum est un virus qui infecte les fichiers exécutables référencés par les clés Run de la base de registres Windows. Lorsqu'il est exécuté, il se recopie vers winlogon.exe et effectue des changements dans le registre. Il édite également le fichier HOSTS, injectant une instruction (thread) dans system.dll, et tente de modifier les fichiers système ntdll.dll et kernel32.dll.

« *Ce type de ver ne réussit à se propager que parce trop de gens n'ont pas encore appris à se méfier de tout message non sollicité, même s'il semble provenir d'une entreprise aussi connue que Microsoft*« , commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud.

« *Dans ce cas, le problème est que pour un observateur inattentif le message paraît authentique, avec une image presque identique à celle que Microsoft utilise sur son site pour promouvoir Internet Explorer 7.0.* »

Ce n'est pas la première fois que des auteurs de virus dissimulent leurs attaques derrière une soi-disant communication de Microsoft. En 2003, par exemple, le ver Gibe-F, alias Swen, s'était fait passer pour une mise à jour de sécurité critique émise par la société. Il y a deux ans, par ailleurs, des pirates renvoyaient les utilisateurs vers un site Web imitant la page de mise à jour de Microsoft.