Trojan.Peskyspy met Skype sur écoute

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 31 août 2009

Spyworld Actu

Ce cheval de Troie enregistre les conversations vocales des utilisateurs de Skype, à leur insu. Reste au pirate à récupérer les fichiers enregistrés au format MP3.

Cela risque de donner des idées aux services de police français, bientôt autorisés à installer des mouchards sur les PC des suspects. Trojan.Peskyspy est un nouveau cheval de Troie capable de mettre sur écoute les utilisateurs de Skype et d'enregistrer leurs conversations à leur insu. L'éditeur de sécurité Symantec a donné l'alerte le 27 août dernier, soulignant cependant que le risque d'infection est faible, le malware étant incapable de se propager par lui-même.

Trojan.Peskyspy (ou Troj_Spaykr.C pour Trend Micro) serait le premier de son genre. Ce cheval de Troie cible pour l'instant Skype, mais il pourrait tout aussi bien fonctionner avec d'autres logiciels de voix sur IP, souligne Symantec, qui précise que toutes les versions de Windows sont affectées.

Des conversations enregistrées en MP3

Le programme ne s'appuie pas sur une faille quelconque mais intercepte directement le flux audio à la sortie du micro en détournant les interfaces logicielles audio de Windows. La technique permet au passage de se jouer des dispositifs d'encryptage utilisés par des logiciels comme Skype pour préserver la confidentialité des échanges. Une fois la conversation interceptée, Trojan.Peskyspy l'enregistre sur le disque dur de l'ordinateur, au format MP3. Reste au pirate à la récupérer sans se faire remarquer.

Pour cela, Trojan.Peskyspy ouvre une « back door » dans le PC compromis. Autrement dit, il permet à un utilisateur de s'introduire à distance dans la machine pour télécharger le fichier MP3 ou effectuer d'autres actions malveillantes. Symantec précise que le malware est capable de contourner les barrières de certains pare-feu afin de transférer les données sans éveiller aucun soupçon.

Pour l'instant, les éditeurs de sécurité n'agitent pas le chiffon rouge. Trojan.Peskyspy ne serait qu'une « proof of concept », autrement dit une démonstration de savoir-faire. Mais le code du malware a été rendu public, ce qui va immanquablement susciter la créativité de petits malins malintentionnés.

Post-scriptum :

http://www.01net.com/editorial/5056...