Le cheval de Troie Bagle fait des petits

Sophos, l'éditeur britannique de solutions de sécurité professionnelles pour réseaux, a détecté de nombreux exemplaires d'un cheval de Troie qui se diffuse par mass mailing, sous la forme d'un spam sur les messageries.

Ce cheval de Troie, BagleD1-L, appartient à la famille des virus Bagle de sinistre mémoire. Il se diffuse dans le monde entier, et comporte une pièce jointe de type '*doc_01.exe*' ou '*prs_03.exe*'. A l'ouverture du fichier attaché, BagleD1-L tente de se connecter à un des sites web de la liste qu'il possède pour télécharger un autre code malicieux. En revanche, selon Sophos, il semblerait qu'aucun de ces sites ne contienne à cette heure quoi que ce soit de malfaisant. Parallèlement, BagleD1-L tente de désactiver les applications de sécurité, anti-virus et pare-feu, en renommant certains de leurs fichiers afin de les rendre inactifs. Et en modifiant le fichier HOST de Windows, le virus bloque l'accès de sites Web liés à la sécurité. BagleD1-L ne semble pas particulièrement actif, mais il est fortement recommandé aux utilisateurs de s'assurer que leur antivirus est parfaitement à jour. **Les conseils de Sophos**

»

Tout cheval de Troie capable de désactiver votre antivirus ou votre pare-feu ouvre la porte à d'autres attaques, y compris par des virus très anciens« , met en garde Annie Gay, directeur général de Sophos France et Europe du Sud. « *La meilleure protection reste de disposer d'une mise à jour automatique de son antivirus et, bien sûr, d'être toujours extrêmement prudent vis-à-vis de tout fichier joint à un courriel non sollicité*« . Sophos recommande également aux entreprises de mettre en ?uvre des règles de filtrage au niveau de leur passerelle de messagerie, de manière à se protéger des nouvelles menaces avant même que les mises à jours antivirales correspondantes soient disponibles. « *Les entreprises doivent envisager sérieusement d'interdire systématiquement la réception de programmes exécutables par courriel. Les utilisateurs désirant installer un logiciel sur leur ordinateur ne doivent le recevoir que du service informatique, et jamais par des amis travaillant dans d'autres sociétés ou via des messages de spam potentiellement dangereux*« .