Le Cheval de Troie racketteur enfin craqué

Des experts en sécurité viennent de trouver le mot de passe nécessaire pour récupérer les fichiers encryptés par un cheval de Troie dénommé Arhiveus-A.

Un fichier malicieux particulièrement efficace qui a fait plusieurs victimes sur la Toile depuis son apparition qui remonte seulement à une semaine. Une fois activé, le code malicieux rafle des fichiers dans le dossier « Mes Documents » et puis les transforme en un fichier nommé : EncryptedFiles.als. Ensuite, les utilisateurs sont informés qu'ils ne peuvent plus accéder à ses documents. Et c'est là que le chantage intervient. L'auteur du ver indique que si l'utilisateur souhaite récupérer ses données il doit effectuer au moins un achat sur un magasin en ligne plus que suspect. Une fois l'achat effectué, le pirate promet, de fournir la clé composée de 30 chiffres permettant de décrypter les fichiers. Seulement, le procédé vient de tomber à l'eau puisque des spécialistes de la lutte antivirus de l'éditeur Sophos viennent de trouver la parade et ils ont retrouvé le mot de passe nécessaire pour la récupération des données. Ce dernier est le : »mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw ». Ce cheval de Troie qui repose sur le chantage n'est pas le premier du genre. Déjà en mars 2006, un code malicieux dénommé le Troyen Zippo (lire notre article), réclamait 300 dollars à ses victimes contre la 'libération' de leurs fichiers. Reste que ces menaces sont de plus en plus utilisées par les « voyous de la Toile », et les éditeurs de logiciels de sécurité estiment qu'elles vont proliférer en 2007.