Le Trojan Zippo encrypte vos fichiers bureautiques

Le rançonnage est toujours à la mode chez les pirates informatiques. Pratique largement utilisée contre les entreprises, elle vise désormais le pauvre utilisateur lambda.

L'éditeur de sécurité Sophos a ainsi repéré un cheval de Troie baptisé Zippo-A (ou CryZip) qui crypte les fichiers bureautiques présents dans le disque dur et exige par la suite une rançon pour les rendre à nouveau lisibles. Sophos explique que Zippo-A recherche les fichiers de type documents Word, bases de données ou feuilles de calcul Excel et les transforme en fichiers ZIP (fichiers compressés avec WinZip) dont l'ouverture est protégée par un mot de passe. Il crée ensuite un nouveau fichier, dans lequel il explique à l'utilisateur la marche à suivre pour payer **300 dollars** sur un compte eGold s'il veut récupérer ses données. La formule peut s'avérer payante, notamment avec les victimes novices prises de panique. Mais Sophos, qui a *« analysé en profondeur le code de ce cheval de Troie »* est en mesure de fournir le fameux mot de libérateur: « C:Program FilesMicrosoft Visual StudioVC98 ».