‘Trojan’ : Cimuz.EZ en veut à nos mots de passe

Une nouvelle saleté se propage actuellement massivement sur la Toile. Cimuz.EZ est particulièrement menaçant car il dérobe les mots de passe stockés dans les ordinateurs ou tapés directement sur Internet.

Selon l’éditeur Panda, ce cheval de Troie est très actif puisqu’il aurait représenté jusqu’à 57 des menaces détectées au cours des dernières heures. Dès que Cimuz.EZ est installé entièrement sur le système, il commence à récupérer des informations sur l’ordinateur infecté : adresses email, mots de passe des programmes, matériel et logiciels installés, adresse IP…, précise Panda. Et de préciser : ce cheval de Troie est également programmé pour surveiller l’activité des utilisateurs sur Internet. Pour cela, il injecte une DLL dans le navigateur web Internet Explorer. Cela lui permet de dérober toutes les données saisies par les utilisateurs dans les formulaires en ligne, notamment les numéros de cartes bancaires, les mots de passe, etc. Toutes ces informations sont ensuite envoyées, à intervalles réguliers, à l’auteur du malware via un serveur. « *Les caractéristiques de ce malware et la vitesse à laquelle il se propage en font une des variantes les plus dangereuses de la famille Cimuz »,*explique Luis Corrons, le directeur technique de PandaLabs. « *Ce cheval de Troie ne peut pas se propager de lui-même mais il utilise une grande variété de moyens de propagation : téléchargements sur Internet, CD, clés USB, emails, etc. Pour cette raison, il est fortement déconseillé d’exécuter des fichiers en provenance de sources non fiables.* » ajoute le directeur technique.