

Mocnex : un virus pour cadres numériques

Un cheval de Troie, arrivant directement de Chine s'attaque aux cadres numériques. Il serait capable lors de la connexion de l'équipement sur un PC de voler des données.

Selon les premières informations, les cadres numériques contenant des codes malveillants ont été vendus durant les vacances de Noël sur les sites suivants : Sam's Club, Best Buy, mais aussi des magasins : comme Target et Costco.

L'information, rapportée par le *San Francisco Chronicle*, a de quoi surprendre. Pourtant tous les gadgets high-tech, sont des cibles potentielles pour les cybercriminels.

Selon *SFGates*, ce maudit canasson a été conçu pour voler les mots de passe des joueurs en ligne, et selon les spécialistes de la sécurité, il a été élaboré pour réaliser des attaques encore plus performantes.

« Il s'agit d'un trojan très bien ficelé et qui dispose d'une certaine forme d'intelligence » explique dans les colonnes du journal californien, Brian Grayek, responsable du développement produit de Computer Associates (CA).

Baptisé Mocmex par CA, ce cheval de Troie a la particularité de reconnaître et de bloquer les protections antivirus de plus de 100 éditeurs de solutions de sécurité. Il est également en mesure de mettre hors service le pare-feu intégré dans le dernier système d'exploitation de Microsoft.

Il se propage dans les cadres numériques et tous les équipements portables qui se connectent à un PC déjà infecté. Il télécharge puis dissimule des fichiers depuis des sources distantes. Ces fichiers sont nommés aléatoirement. Ce qui fait qu'il est très difficile à identifier sur un poste d'autant que selon SFGate, Mocnex dispose déjà de près de **67.500 variantes**.

Grayek compare d'ailleurs cette nouvelle menace chinoise à une « bombe nucléaire » élaborée par des professionnels du monde de la cybercriminalité, « elle a été spécifiquement élaborée pour voler des données sans laisser de traces. » Le gang à l'origine de cette menace est connu et a été signalé aux autorités, mais Grayek se refuse à communiquer son nom.

L'émergence de cette nouvelle menace, apporte une fois de plus la preuve que les cybercriminels ciblent des produits très populaires. Rappelons que selon la Consumer Electronics Association (CEA) plus de **2,26 millions de cadres numériques** ont été vendus en 2007 (lire notre [article](#) qui traite de l'évolution de ce marché).

Le CEA estime qu'en 2008, ce chiffre déjà important va encore progresser pour atteindre les **3,26 millions d'unités**.

Pour conclure, signalons que ce nouveau trojan a déjà identifié sur les réseaux de Singapour et de Russie.