Alerte MPack: l'outil de développement de 'malwares' menace la Toile

160.000 ordinateurs infectés par une seule version de MPack, l'analyseur en ligne *NanoScan*de Panda Software a repéré plusieurs versions de ce programme qui permet de créer des *malwares* exploitant plusieurs vulnérabilités.

Les menaces sont diffusées via des pages web vérolées. Dans sa version de base, MPack permet de télécharger des *malwares* sur des ordinateurs distants.

Les méthodes de diffusions restent classiques : code malicieux glissé dans des pages web rendues invisibles par une balise '*iframe*' placée sur un serveur ? ces pages sont d'ailleurs souvent indexées dans les bases des moteurs de recherche -, domaines pirates, postes zombies, spam…

Une fois installé, le programme MPack recueille les données de l'ordinateur hôte (identité, OS, navigateur, etc.) qu'il expédie sur un serveur pirate.

La particularité de cette menace provient de sa vente en ligne. En effet, le 'kit MPack' est proposé sur les forums au prix de 700 dollars environ. Et ses auteurs poussent même leur 'professionnalisme' jusqu'à proposer un an de support gratuit sur chaque version !

« *Les mises à jour de MPack sont de nouvelles versions de l'application comprenant de nouveaux exploits pour profiter des dernières vulnérabilités découvertes. Une nouvelle mise à jour est disponible tous les mois en moyenne et coûte entre 50 et 150 dollars.*« , explique Luis Corrons, le directeur technique de PandaLabs.

Le programme dispose même d'une extension, *DreamDownloader*, qui crée un exécutable pour télécharger d'autres menaces – virus, vers, chevaux de Troie, etc. Celle-ci est proposée au prix de 300 dollars.

Panda Software propose sur son blog une étude complète de MPAck au format PDF.