500.000 internautes infectés par l'outil MPack

MPack est véritablement le cauchemar de tous ceux qui luttent de près ou de loin contre la propagation des '*malwares*'. Cet outil cheval de Troie, également appelé *Rootkit*, permet en effet de simplifier et d'automatiser le piratage informatique et selon Finjan il est actuellement très à la mode.

Au cours de ce mois de juillet, Finjan a identifié 58 cybercriminels utilisant sans modération ce maudit MPack.

Ces voyous du Net auraient déjà infecté 500.000 utilisateurs. Le niveau d'infection est élevé et le taux de réussite de l'attaque est de 16%.

Selon les outils statistiques utilisés par les sites Web frauduleux, avec seulement 16% des attaques réussies sur un total de 3,1 millions de tentatives, la propagation de ce code malveillant s'avère donc rapide et inquiètante.

Les experts de Finjan indiquent que les cybercriminels utilisent MPack pour dérober des données confidentielles et sensibles comme des numéros de compte, des codes secrets ou des mots de passe, des numéros de sécurité sociale… L'objectif de ces mafieux du clavier reste donc le même : l'argent.

Les données volées sont renvoyées aux cybercriminels via des sessions SSL (encryptage: *Secure Communication Channel*) de façon à éviter les systèmes de défense ou de détection des éditeurs de sécurité.

Côté utilisateur, il est pratiquement impossible de remarquer la présence de MPack sur son poste! les indicateurs habituels, la bande passante ou les processeurs sont trompés par ce '*trojan*' (cheval de Troie).

La force de ce *malware* « invisible » est justement de rester dans l'ombre et de ne pas impacter ce que l'on nomme « l'expérience utilisateur ».

Finjan indique dans son rapport que la majorité des solutions du marché sont incapables de le détecter. Un rapport disponible sur le site de cet éditeur montre l'ensemble des banques touchées par cette colossale arnaque de l'été.

« Ce type d'attaque est encore plus dangereux que le 'phishing' *(ou hameçonnage) traditionnel. Elle se produit directement sur la machine de l'utilisateur et elle est particulièrement difficile à constater. Elle repose sur une grande réactivité et créativité des pirates qui doivent déplacer et créer de nouveaux sites frauduleux presque quotidiennement »* précise Uval Ben-Itzhak, directeur technique de Finjan.

?Une fois que l'utilisateur a donné ses identifiants sur le faux site et que ces communications ont été interceptées par les pirates la situation est critique. Toutes les données sont envoyées sur le serveur du pirate et non sur celui de la banque. »