Le trojan 'Silentbanker' s'intéresse à votre argent

Ce nouveau code malveillant surnommé « Silentbanker » par Symantec a la capacité de récupérer des données sensibles, en l'occurrence des informations bancaires qui sont normalement protégées par un double processus d'authentification.

Concrètement, lors d'une transaction en ligne, Silentbanker va changer les détails permettant l'identification d'un client.

Du côté de l'utilisateur, le fonctionnement du site est le même, après utilisation de son second mot de passe, l'internaute se croit en sécurité, mais en réalité, il va sans le savoir, envoyer de l'argent sur le compte du hacker.

Symantec estime que le risque associé à ce trojan est faible, cependant, un chercheur de l'éditeur, Liam O'Murchu indique de son coté que *« Silentbanker reste dangereux dans la mesure où les utilisateurs ne peuvent pas en détecter les effets. «*

*« L'échelle et la sophistication de cette attaque sont inquiétantes. Même pour quelqu'un comme moi, qui a l'occasion d'étudier des tentatives de phishing tous les jours. »*indique O'Murchu sur le blog de Symantec.

« Ce cheval de Troie télécharge un fichier de configuration qui contient les noms de domaine de plus de 400 banques. Tous les pays sont représentés dans cette liste, la Turquie la France, l'Espagne, l'Irlande, la Grande-Bretagne, les USA, des pays d'Asie… » précise le chercheur.

Pour arriver sur une machine cible, ce code malveillant utilise les exploits Web. Une fois sur la machine il va explorer les API présentes dans les dossiers d'IE et de Firefox.

Si un programme faillible est lancé avec le navigateur, le hacker peut commercer son activité, par exemple rediriger l'internaute vers un faux site, altérer des pages HTML, récupérer des mots de passe, réaliser des captures d'écrans des pages visitées… bref tout l'arsenal classique du cybercriminel moderne. Ce trojan a également la capacité de se mettre à jour tout seul et de façon quasi indétectable pour un utilisateur lambda…