

FireSheep, une extension Firefox pour pirater les réseaux Wifi

Les outils permettant de réaliser des actions malveillantes se démocratisent. Ils deviennent même de plus en plus simples à exploiter. Dernière illustration en date, Firesheep, une extension pour le navigateur Firefox, facile à installer, donc, et à utiliser. Démonstration faite par Eric Butler, un développeur Web de Seattle lors de la conférence Toorcon (du 22 au 24 octobre à San Diego), souligne ITespresso.fr.

En pratique, cet outil permet d'intercepter des données qui transitent sur un réseau Wifi ouvert. Les cookies servant à identifier un utilisateur sur des sites tels que Facebook, Google, Yahoo ou encore Twitter sont ainsi vulnérables car, une fois interceptés, ils peuvent servir à l'attaquant pour se connecter illégalement aux comptes d'internautes qui se sont identifiés auparavant à partir du même réseau. Avec cette méthode, les mécanismes d'authentification des sites pensent reconnaître un cookie de connexion valide alors qu'il n'en est rien.

Eric Butler a précisé qu'il avait créé Firesheep pour montrer le danger de l'accès «en clair» à partir de points d'accès Wi-Fi accessibles sans authentification (ouverts). Dans une contribution diffusée sur [son blog](#), l'expert milite pour un chiffrement des connexions (HTTPS), à l'instar des sites de banques, ce qui permettrait d'éviter l'interception de sessions. Cela reste toutefois à mettre en place sur de nombreux sites.

Depuis la mise en ligne de l'extension Firefox Firesheep, celle-ci a été téléchargée près de 50.000 fois. Un carton!