ZDNet.fr
Business et Technologies

Sécurité et Menaces

Les cookies, maillons faibles des réseaux Wi-Fi

Estelle Dumout, publié le 3 août 2007

Sécurité - Les internautes qui se connectent à un réseau Wi-Fi non sécurisé ont des soucis à se faire : un expert en sécurité a développé des outils qui permettent de récupérer les cookies transitant sur ces réseaux et d'usurper l'identité de leur victime.

Les utilisateurs des réseaux Wi-Fi non sécurisés peuvent être la proie d'un nouveau type d'attaque. Robert Graham, un expert qui travaille pour la société Errata Security en a fait la démonstration cette semaine pendant la Convention Black Hat de Las Vegas (28 juillet au 2 août), dédiée à la sécurité informatique. Lors d'une présentation, il est parvenu à détourner en direct le compte Gmail, le service de courrier électronique de Google, d'un des membres de l'assistance.

L'expert a utilisé deux outils mis au point par ses soins et baptisés « Ferret » et « Hamster » : le premier lui permet de surveiller le trafic d'un hot-spot Wi-Fi public, puis de récupérer les cookies non chiffrés et les identifiants de sessions utilisés par un navigateur web, lorsqu'un utilisateur se connecte à son interface webmail ou bien à un service communautaire de type MySpace ou Facebook.

Utiliser une connexion sécurisée SSL

Le second lui permet de réutiliser ces informations pour se connecter aux applications en se faisant passer pour sa victime. Car les cookies sont de petits fichiers de texte stockés par un navigateur, pour éviter à l'internaute d'avoir à saisir de nouveau ses identifiants ou à repréciser ses préférences chaque fois qu'il revient sur un même service.

Lors de sa démonstration, Robert Graham a ainsi pu envoyer des messages avec le compte Gmail détourné, lire tous les messages dans la boîte de réception et même modifier les préférences. En revanche, il n'est pas possible, par ce biais, de changer le mot de passe de l'utilisateur légitime, puisque la plupart des services réclament la saisie de l'ancien avant de pouvoir en activer un nouveau (voir le descriptif de la procédure, en anglais, sur *ZDNet.com*).

Une technique permet toutefois de se prémunir contre ce type de vol de données : utiliser une connexion sécurisée SSL. C'est le protocole retenu par de nombreux e-commerçants pour sécuriser les transactions sur internet. Google permet aux utilisateurs de Gmail d'activer ce mode, mais ce n'est pas dans la configuration par défaut du webmail. Selon Robert Graham, très peu d'autres sites de la sphère web 2.0 proposent cette sécurisation. Une autre solution serait l'utilisation d'un VPN (réseau privé virtuel), ce que ne feront quasiment jamais des utilisateurs non experts. La seule protection véritablement efficace pour l'instant est de se méfier des hot-spots Wi-Fi publics non sécurisés.