

# Panoptinet

Gardez un œil sur votre réseau

## Une Android App vole les cookies par Wi-Fi

admin · Tuesday, June 21st, 2011



**On savait la sécurité du Wi-Fi fragile et les technologies de cracking évolutives. Une nouvelle application Android appelée FaceNiff permet aujourd'hui d'intercepter automatiquement des cookies de réseaux sociaux via les ondes Wi-Fi. Si l'on n'y prend pas garde, l'usurpation d'identité pourrait devenir un jeu d'enfant.**

En avril 2009, le hacker éthique et PDG de [First Base Technologies](#) Peter Wood révélait déjà une **faille de sécurité dans les navigateurs internet**, lorsqu'ils passent d'une connexion standard (HTTP) à une connexion sécurisée (HTTPS) : **l'interception de cookies devient possible en Wi-Fi.**

Cette faille est aujourd'hui exploitée par l'**application Android FaceNiff**. Si le nom de l'application est dérivé de la contraction de "**Facebook**" et de "**Sniff**" (renifler, flairer), c'est pour une bonne raison : elle est capable de **capturer en Wi-Fi certains cookies** d'utilisateurs, pour ensuite se connecter à leur place à leurs réseaux sociaux préférés, comme en atteste cette vidéo :

En théorie, il est donc possible de **prendre le contrôle d'une session IP "sécurisée"** dès qu'un utilisateur valide des **informations personnelles ou bancaires** ! FaceNiff permet d'automatiser ce processus.

Selon toute vraisemblance, FaceNiff permettrait d'intercepter des sessions web de sites très populaires, tels que **Facebook, Twitter, Youtube, Amazon** ou Nasza-Klasa (Pologne). Et d'après la chercheuse spécialisée en sécurité informatique "Ms Smith", qui s'est exprimée sur [NetworkWorld](#), "*même un débutant écervelé pourrait hacker un compte Facebook via le Wi-Fi grâce à FaceNiff*".

Si la nouvelle application fait un peu penser à [Firesheep](#), FaceNiff ne se contente pas de contourner le simple chiffrement WEP : en quelques secondes, il est possible de cracker la session d'un utilisateur, même si celui-ci utilise un **cryptage WPA ou WPA2**, pourtant réputés sécurisés.

Seule - mais faible - consolation pour l'instant : FaceNiff est limité à trois

interceptions de profils, sur un bouquet de sites encore restreint. Toutefois, l'auteur de l'application, Bartosz Ponurkiewicz, a déjà annoncé qu'une version payante serait développée, et qu'elle offrirait **beaucoup plus de latitudes...**

Après manipulation logicielle, l'application fonctionnerait sous ces différents smartphones : HTC Desire CM7, original Droid/Milestone CM7, SE Xperia X10, Samsung Galaxy S, Nexus 1 CM7, HTC HD2, LG Swift 2X, LG Optimus black (original ROM), LG Optimus 3D (original ROM), and Samsung Infuse.

FaceNiff confirme finalement l'intérêt de l'**usage permanent du HTTPS**. Si vous ne l'avez pas encore fait, vous pouvez activer cette sécurisation sur vos comptes Facebook et Twitter. Quant aux utilisateurs du navigateur Firefox, ils peuvent installer l'extension [HTTPS Everywhere](#) (Electronic Frontier Foundation), pour forcer l'utilisation du [SSL](#) dès que cela est possible.

Source : [InfoSecurity](#)

This entry was posted on Tuesday, June 21st, 2011 at 2:27 pm and is filed under [Autres actualités](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.