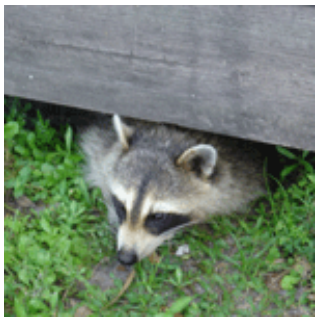
Panoptinet

Gardez un oeil sur votre réseau

Penetrate, le passe-partout Wi-Fi sous Android

admin · Thursday, September 15th, 2011

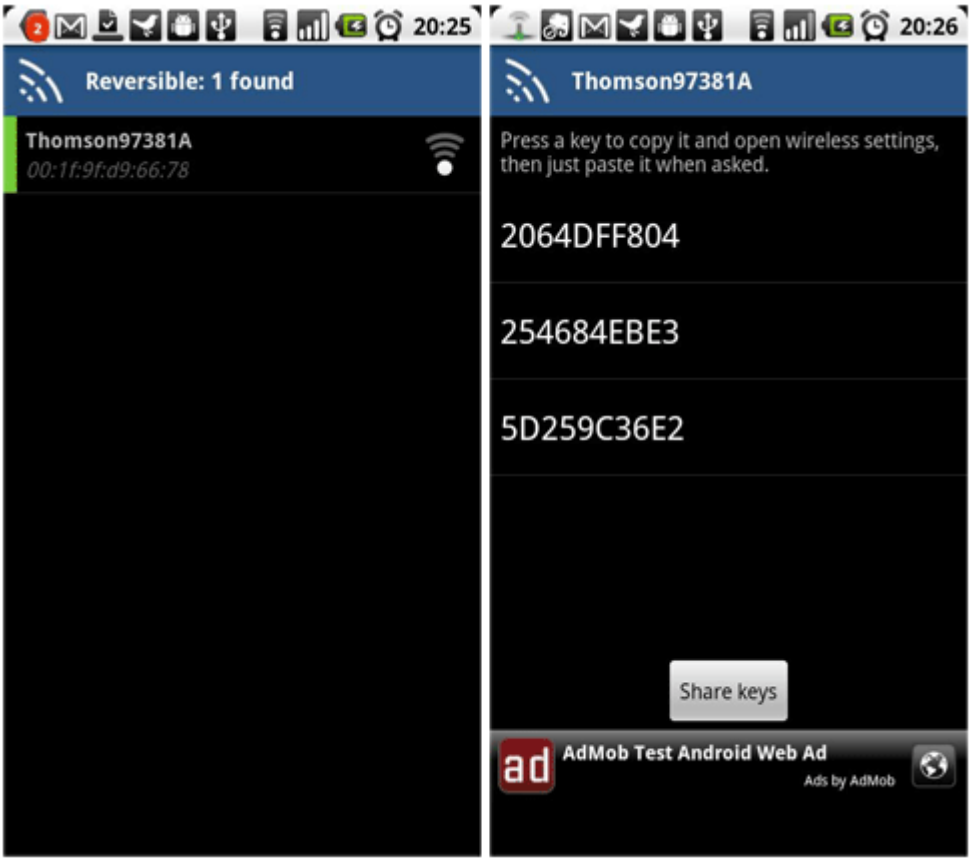


Il est de plus en plus facile de cracker un réseau Wi-Fi, notamment s'il est peu ou pas protégé : les logiciels spécialisés deviennent très simples à utiliser, et les cours (tutoriaux) se multiplient sur Internet. Le crack d'une connexion Wi-Fi se fait généralement à l'aide d'un ordinateur, mais de plus en plus d'applications permettent de faire la même chose à partir de smartphones. C'est le cas par exemple de Penetrate, une application Android très populaire ces derniers mois.

Les chasseurs de réseaux Wi-Fi adorent déjà cette application : elle leur permet de **se connecter rapidement (moins de 10 secondes) à certains réseaux Wi-Fi**, même protégés par mot de passe (cryptage WEP, WPA, WPA2). A l'inverse, pas sûr que les abonnés Internet – juridiquement responsables de toutes les activités transitant par leur box – acceptent qu'on squatte leur connexion de la sorte. On ne risque cependant pas de les entendre beaucoup, puisque dans 99% des cas, ces abonnés **ne se rendront absolument pas compte** que leur Wi-Fi est occupé par un tiers (à moins qu'ils utilisent un logiciel de monitoring).

Comment Penetrate fonctionne ?

En réalité, Penetrate ne peut pas calculer n'importe quelle clé de protection, certaines demanderaient beaucoup trop de temps. L'application embarque néanmoins quelques **algorithmes et dictionnaires** qui permettent de **déduire les clés de chiffrement originales** de certains modems-routeurs, en fonction des modèles. En effet, le programme exploite les **failles de certains firmwares**, qui génèrent de façon mathématique les mots de passe de la clé de cryptage (souvenez-vous en 2009 du scandale de la Bbox, qui de la même façon était devenue facilement piratable). Reste à l'application le soin de définir le modèle du routeur détecté par Wi-Fi, de vérifier si un de ses algorithmes correspond, et si c'est le cas, de **générer la clé valide par défaut**.



Tous les routeurs et box ne sont pas sujets à cette faille, seuls quelques-uns sont donc concernés par l'application Penetrate :

- Thomson-based routers : Thomson, Infinitum, BBox, DMax, Orange, SpeedTouch, BigPond, O2Wireless, Otenet
- Pirelli Discus
- Eircom
- DLink
- Verizon FiOS (seulement certains routeurs)
- Fastweb (Pirelli & Telsey)
- Jazztel_XXXX and WLAN_XXXX

Comment protéger mon Wi-Fi de cette application ?

Si votre box ou votre routeur n'est pas cité dans la liste précédente, Penetrate n'est pas actuellement en mesure de cracker votre Wi-Fi. Les conseils de sécurité suivants sont néanmoins importants pour tous.

1. **Modifier la clé de cryptage d'origine**

L'application Penetrate déduit les clés de cryptage par rapport à la **configuration usine** de ces routeurs, qui possèdent par défaut une clé de chiffrement (WEP, WPA ou WPA2). C'est cette clé par défaut qu'il faut **modifier**, afin d'en instaurer une plus personnelle, qui ne correspondra donc à aucun algorithme de l'application. Si le Wi-Fi de votre box/routeur est protégé par une **clé WEP**, vous pouvez aussi profiter de l'occasion pour activer un **cryptage plus sécurisé comme le WPA2** : tout se

configure au même endroit !

Pour ce faire, il faut **accéder à l'interface de paramétrage de votre routeur/box**. Si vous ne connaissez pas l'adresse de cette interface, utilisez **Amabox** (gratuit), qui le fera pour vous. Sinon, voici la procédure à suivre en fonction de la box de votre FAI : Livebox, Neufbox, Freebox, Dartybox, Bbox, Numericable.

Une fois connecté à cette interface de configuration de la box, il faut aller jeter un œil du côté du **paramétrage Wi-Fi**. En fonction de votre box, voici comment choisir un type de **cryptage plus sécurisé (WPA2)** et surtout **modifier le mot de passe** qui l'accompagne : Livebox, Neufbox, Freebox, Dartybox, Bbox, Numericable.

2. Modifier les identifiants de connexion à la box

Si vous avez suivi la procédure précédente, vous avez du vous connecter à la box. Avant d'apparaître, la box affiche sur votre écran une **fenêtre de connexion**, où vous avez du saisir votre **identifiant** et votre **mot de passe**. Ces informations sont fournies par défaut à la livraison de la box, sont signifiées sur un courrier envoyé par le FAI, mais sont **rarement personnalisées**.

Or, ces identifiants sont souvent largement répandus, voire publics (ex : "**admin / admin**" ou "**admin / password**"). Si un jour **un pirate cracke votre réseau Wi-Fi**, il pourra aussi se connecter à l'interface d'administration de la box grâce à ces identifiants communs, et ainsi configurer votre box comme il l'entend (ex : paramétrage des ports pour permettre le peer-to-peer). Il pourra même **modifier la clé de cryptage** ou **instaurer un filtrage MAC** pour bénéficier de l'accès web, tout **en vous empêchant de vous y connecter** !

Le plus simple reste encore de **changer ces identifiants**, ou en tout cas le mot de passe, et de les personnaliser. En fonction de votre box, voici comment modifier ce mot de passe : Livebox, Neufbox, Freebox, Dartybox, Bbox, Numericable.

Voilà, vous êtes désormais prémunis contre toute **intrusion Wi-Fi provoquée par l'application Penetrate** ! Vous êtes également davantage protégé contre les intrusions Wi-Fi en général. Mais souvenez-vous que **le risque zéro n'existe pas**, pensez aussi à **surveiller votre connexion** !

Source : korben.info

Image : By Poivrier (Own work) [Public domain], via Wikimedia Commons

This entry was posted on Thursday, September 15th, 2011 at 3:30 pm and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.