EVALUER

25 févr. 2015

Pirater un réseau Wi-Fi public ? Un jeu d'enfant

Il a suffi d'une dizaine de minutes à Betsy Davies, une fillette britannique de 7 ans, pour pirater les connexions d'utilisateurs utilisant un point d'accès Wi-Fi public. Si la fragilité du Wi-Fi public n'est plus à démontrer, restent les précautions d'usage à suivre.

Betsy Davies n'a que 7 ans, mais il lui a suffit de **10 minutes pour pirater un hotspot Wi-Fi public, dans un café**. L'histoire, qui a créé le buzz au Royaume-Uni, était en réalité une opération de communication montée par Hide my Ass, une société spécialisée dans les **VPN** et le chiffrement de données.

Mais elle reste révélatrice de l'extrême dangerosité d'un usage sans filet des réseaux Wi-Fi publics. Hide my Ass a fourni à Betsy Davies une vidéo explicative (un tutoriel), qui a permis à la jeune fille d'apprendre à pirater un hotspot, comme s'il s'agissait d'un jeu… "A une époque où les enfants baignent dans les nouvelles technologies et le codage, le piratage est littéralement devenu un jeu d'enfant, et n'importe quel profane peut aujourd'hui pirater un hotspot WiFi", indique le spécialiste en sécurité, Marcus Dempsey, au site Information Age.

Pour pirater le réseau, Betsy a simplement créé un faux point d'accès, se faisant passer pour celui du café. Les clients se sont ensuite connectés à son hotspot, ce qui a permis à la jeune fille de réaliser une attaque "man in the middle". Avec un analyseur de réseau sans fil ("packet sniffer"), un logiciel qui permet de "sniffer" les paquets de données, elle était alors en mesure de récupérer des données personnelles (mots de passe, e-mails, documents). Sessions reniflées, comptes détournés Au delà de ce test mené par Hide my Ass, un expert en sécurité (adulte) a fait une expérience similaire, mais plus en profondeur, en 2013. Eric Geier, fondateur de NoWiresSecurity (une société de conseils à destination des entreprises souhaitant sécuriser leur Wi-Fi), s'est lui aussi installé dans un café. Parce que "les réseaux Wi-Fi sont semblables aux ondes publiques, que n'importe qui peut capter", il a réussi, lui aussi via un "packet sniffer", à "capturer" des signaux Wi-Fi.

Sur son écran d'ordinateur, il pouvait ainsi voir les pages web visitées par des internautes connectés au réseau Wi-Fi, mais aussi récupérer les idenfiants d'un compte Webmail, des adresses e-mail, des mots de passe, et même des messages instantanés passant par Yahoo! Messenger (non chiffrés). Eric Geier a aussi utilisé une application Android, DroidSheep, qui lui a permis de "renifler" toutes les sessions ouvertes par d'autres internautes connectés au réseau, et de "se rendre sur ces sessions à leur place : Facebook, Twitter, Yahoo, Live, Flickr", afin de détourner leurs comptes. DroidSheep cherche et répertorie toutes les connexions non sécurisées à des sites Web populaires, et permet d'ouvrir les sites en utilisant la session de quelqu'un d'autre, en exploitant des vulnérabilités.

Les VPN et Tor à la rescousse Les réseaux Wi-Fi publics sont bel et bien de véritables passoires. D'où la nécessité, soit de s'en passer, soit d'utiliser un VPN. Ce réseau privé virtuel vous permettra de surfer anonymement, et chiffrera votre connexion, en modifiant votre adresse IP via des serveurs proxys situés à l'étranger. Hyde my Ass a fait le buzz, mais il existe d'autres VPN, plus fiables, bien que payants, comme Toonux VPN ou Strong VPN. En matière de VPN gratuits, Freedom-IP s'avère une solide alternative. Enfin, il n'est pas inutile d'utiliser le réseau Tor, qui vous permettra de surfer anonymement, derrière des serveurs relais qui cacheront votre adresse IP. Pour cela, rendez-vous dans notre article sur l'anonymisation en ligne, où des solutions pour PC et smartphones vous serons proposées.

Par Fabien Soyez

ET AUSSI DANS L'ACTUALITÉ :

Comment anonymiser tout ce que vous faites en ligne

Sécurité de vos comptes : un seul mot de passe pour les protéger tous