# La promiscuité sans fil des réseaux WiFi publics

Se connecter à un Wifi public dans un parc, une gare ou un café [1] pour accéder à Internet, c'est un peu comme passer par la salle d'attente du médecin avant une consultation. Dans les deux cas, vous avez confiance en votre destination [2], mais vous êtes au préalable enfermé dans un espace avec des étrangers, tous plus ou moins malades.

En effet, le WiFi d'un café vous connecte, comme la salle d'attente, avec votre entourage direct, sans que vous ayez rien demandé. Or, si votre dossier médical est confidentiel, il suffit de faire tomber ses papiers dans une salle d'attente pour que toutes les personnes présentes puissent les lire, et il suffit de se connecter (via un WiFi public) à un service qui n'utilise pas le protocole HTTPS pour que votre entourage connecté puisse s'immiscer dans votre session et votre intimité.

Les coupables ? Les sites conservant à votre place des éléments de votre vie privée d'une part, et proposant d'autre part et sans la protection du petit cadenas qui dénote de l'utilisation du protocole HTTPS, de « garder votre session ouverte » grâce à un cookie. Si vous y prenez garde, ce n'est pas le cas des services en ligne de votre banque.

Toutefois, si l'auteur est assez pessimiste dans son petit billet complémentaire (reproduit ici à la suite du premier) face aux moyens de protection à notre disposition, il existe plusieurs extensions Firefox pour limiter les risques sans trop se compliquer la vie, citons (sur les bons conseils de Goofy) HTTPS Everywhere, et Force-TSL. De plus, il me semble également assez simple de se connecter, où qu'on soit, d'abord à un VPN personnel, ou directement en SSH sur son serveur à soit (voir l'extension Foxyproxy de Firefox), pour surfer ensuite l'esprit tranquille et sans laisser de traces locales, comme si on était à la maison. D'ailleurs, votre WiFi chez vous, il est protégé comment ?

# Quand le berger prévient les moutons à New York City

**Herding Firesheep in New York City**

*Gary LosHuertos – 27 octobre 2010 – TechnologySufficientlyAdvanced.blogspot.com*
*Traduction Framalang : Goofy, Pablo, cheval_boiteux*

On a beaucoup parlé de Firesheep ces derniers jours. Cette extension gratuite pour Firefox récolte pour vous les cookies qui sont envoyés depuis un réseau WiFi non protégé n'utilisant pas le protocole SSL. Vous la mettez en route, elle collecte les cookies de Facebook, Twitter et de 24 autres sites (par défaut). Ensuite, vous pouvez voler l'identité d'un compte et obtenir l'accès sous cette identité.

L'extension n'a rien de scandaleux en elle-même. Si vous êtes un développeur un peu compétent, vous savez depuis longtemps que cette faille existait, n'est-ce pas ? Mais quid du reste du monde ? Tous ces gens qui n'ont jamais entendu parler de cette nouvelle menace si facile d'accès, qui n'ont pas été alertés par leurs amis, qui ne regardent pas Engadget, ni Slashdot, ni ABC Pronews7 à Amarillo ?

Je me suis dit que j'allais faire passer le message et aider les béotiens après leur travail, puisqu'il y a un grand Starbucks tout près de chez moi. J'y suis allé, j'ai acheté un peu de nourriture malsaine, j'ai ouvert mon portable et lancé Firesheep. Moins d'une minute plus tard, j'avais cinq ou six identités disponibles dans le panneau latéral. Trois d'entre elles étaient sur Facebook.

Absolument rien de surprenant ; Firesheep n'est pas magique, et tous ceux qui vont au Starbucks savent qu'un tas de gens y mettent à jour leur statut Facebook sans faire attention, tout en sirotant leur café au lait. J'ai pensé que j'allais y passer un peu plus de temps, j'ai donc écouté un peu de musique, parlé à quelques amis, et le plus important (mais pas le plus simple) je n'ai navigué sur aucun site avec le protocole standard HTTP (et surtout pas sur Facebook évidemment).

Environ une demi-heure plus tard, j'avais récolté entre 20 et 40 identités. Puisque Facebook était de loin le service le plus représenté (et qu'il détient plus

d'informations personnelles que Twitter) j'ai décidé d'envoyer aux utilisateurs des messages depuis leur propre compte, pour les avertir des risques auxquels ils s'exposaient. J'ai fait un modèle de message sympa qui précisait la localisation du Starbucks, la nature de la vulnérabilité, et comment y remédier. J'ai envoyé des messages aux 20 personnes autour de moi.

J'ai nettoyé le panneau latéral, retiré mes écouteurs, et j'ai attendu. J'ai entendu quelqu'un marmonner un juron pas très loin, et me suis demandé si mon message en était la cause. Pendant le quart d'heure suivant, je n'ai entendu strictement personne parler de ce qui venait se passer (pourtant ceux qui fréquentent les Starbucks ne sont le plus souvent pas du genre à tenir des conversations discrètes). Pourtant, j'ai pu vraiment constater une nette chute du nombre d'identités que je pouvais récolter quand j'ai relancé Firesheep.

C'était un soulagement — en voilà qui avaient compris le message. Avec un peu de chance, ils allaient alerter leurs amis, mettre à l'abri leur femme et leurs enfants. J'ai de nouveau nettoyé le panneau latéral, et après une vingtaine de minutes de conversations impromptues j'ai vu que cinq identités que j'avais déjà croisées étaient revenues dans mon troupeau.

C'était assez surprenant. Avaient-ils reçu le premier message ? Je me suis mis sur leur compte avec leurs identifiants, et en effet ils l'avaient reçu. L'un d'entre eux était même sur Amazon.com, site contre lequel j'avais mis en garde dans mon premier message. Je l'ai choisi pour première cible : j'ai ouvert sa page perso sur Amazon, j'ai repéré un truc sur lequel il avait récemment jeté un coup d'œil et lui ai envoyé un mot : « non, c'est pas sérieux » sur Facebook depuis son propre compte, avec un clin d'œil sur ses goûts musicaux.

J'ai encore une fois effacé les identités, attendu dix minutes, et lorsque j'ai à nouveau rassemblé mon troupeau avec Firesheep, il était parti. Mais il y en avait encore quatre qui restaient là. Peut-être, me suis-je dit, qu'ils ont cru que c'était un message d'avertissement automatique les ciblant au hasard (bien que j'aie mentionné leur localisation dans un rayon d'une trentaine de mètres). Donc, un dernier message était nécessaire.

J'ai bricolé un très court message (le premier était peut-être trop long ?) et je l'ai envoyé aux quatre, une fois encore avec leur propre compte :

> *« C'était vraiment pas une blague l'avertissement sur la sécurité. Je n'enverrai*

> *plus d'autre message après celui-ci –– à vous de prendre sérieusement en main votre propre sécurité. Vous êtes au Starbucks XYZ connecté de façon non sécurisée, et absolument n'importe qui peut accéder à votre compte avec l'outil approprié nécessaire (et disponible à tous). »*

Vingt minutes ont passé, et tous les quatre utilisaient encore Facebook frénétiquement. Encore une fois, j'ai envisagé qu'ils auraient pu ne pas recevoir le message, mais en vérifiant leur compte j'ai vu qu'ils l'avaient bel et bien reçu.

Voilà ce qu'il y a de plus choquant à propos de la sécurité sur Internet : ce n'est pas que nous soyons tous scotchés sur un réseau global qui tient avec des bouts de sparadrap et laisse béants d'horribles failles de sécurité ; ce n'est pas non plus qu'un outil librement disponible puisse récolter des cookies d'authentification ; et ce n'est toujours pas qu'il y ait des gens pas du tout au courant de l'un ni de l'autre. Ce qui est absolument incompréhensible, c'est qu'après avoir été averti d'un danger (et sur son propre compte !) on puisse tranquillement ignorer l'avertissement, et reprendre le fil de ses activités.

Mais enfin j'ai tenu parole et n'ai pas envoyé d'autre message. J'ai rangé mon matériel, fait un petit tour dans le café, et reconnu plusieurs personnes auxquelles j'avais montré leur vulnérabilité. Je n'avais pas laissé d'indices sur ma propre identité, moins par crainte de rétorsion que parce que l'intrusion dans la vie privée est encore plus traumatisante quand elle est commise par un étranger complet, dont on n'a pas la moindre chance de découvrir l'identité.

En revenant chez moi, j'ai réfléchi à ce que cette expérience révélait de notre société. Peu importe le nombre de mesures de sécurité que nous procurons au monde entier, il y aura toujours des gens qui laisseront la porte ouverte, même s'ils ont été victimes d'une intrusion. **Le maillon le plus faible de la sécurité c'est et ce sera toujours la décision de l'utilisateur.**

De retour dans mon appartement, j'ai commencé à m'installer — et c'est le moment où je me suis rendu compte que pendant toute la soirée j'avais eu la braguette grande ouverte. La preuve par neuf finalement : nous nous baladons tous avec des vulnérabilités qu'il nous reste à découvrir.

# Addendum

**Herding Firesheep Addendum**

*Gary LosHuertos – 04 novembre 2010 – TechnologySufficientlyAdvanced.blogspot.com*
*Traduction Framalang : Siltaar, RaphaelH, Goofy*

À la suite du billet précédent, je me suis dit qu'en voulant faire court j'avais omis quelques informations. Ceci sert donc d'addendum à mon précédent billet, et a été rédigé de la manière la plus courte possible.

Le message original envoyés aux clients était le suivant :

> *Comme vous utilisez Facebook sans chiffrement dans un Starbucks, votre compte a été compromis. Je ne suis qu'un amical client du Starbucks qui a souhaité vous prévenir de cette vulnérabilité.*
>
> *Vous pouvez en apprendre davantage en cherchant des informations sur « Firesheep ». Il n'y a pas vraiment de solutions disponibles pour protéger votre compte Facebook lorsque vous êtes connectés à un réseau public, et je vous recommande donc simplement de ne pas vous y connecter lorsque vous êtes dans un Starbucks. Cette faille affecte également Twitter, Amazon.com, Google (mais pas Gmail), et quantité d'autres services.*
>
> *Votre mot de passe n'a pas été compromis. Vous déconnecter de Facebook est tout ce que vous avez besoin de faire.*

Pour préciser mes motivations, laisser un compte Facebook sans protection ne signifie pas seulement que quelqu'un peut regarder vos photos, vos coups de cœurs et messages. Un compte Facebook compromis donne à quelqu'un d'autre l'accès à votre identité, lui permettant de se faire passer pour vous auprès de vos amis, ruinant potentiellement des relations. S'il est possible de rattraper les choses ensuite, le temps et l'énergie que ça demande sont importants, surtout pour quelqu'un qui a beaucoup d'amis. Quelqu'un envoyant un faux message à l'un de vos amis n'est peut être pas un gros problème, mais un faux message envoyé à 500 de vos amis est déjà plus gênant. D'autant plus qu'il peut y avoir des collègues de travail, des membres de votre famille, ou des clients dans ces 500

personnes.

Concernant la légalité de mes actions : ça n'était pas l'objet de mon article. On peut toujours spéculer sur fait que je finisse en prison, mais c'est hors sujet par rapport à ce dont je parle dans mon billet : les sites non protégés comme Facebook et Twitter sont dangereux pour leurs utilisateurs. Il semble plus intéressant de consacrer son énergie à faire passer le mot plutôt que de troller sur mon éventuelle incarcération.

Enfin concernant ce que les utilisateurs peuvent faire, la meilleure réponse à l'heure actuelle est : rien. Ne vous connectez pas aux réseaux non protégés pour utiliser ces sites web, ou bien utilisez une application qui n'utilise pas d'authentification par cookie non protégée (pour ce que j'en sais, l'application Facebook pour iPhone ne le ferait pas). Assurez-vous que votre réseau WiFi domestique est chiffré en WPA, voire en WPA2 (le WEP est trivialement déchiffrable). Si vous utilisez Facebook au travail sur une connection sans-fil, vérifiez le chiffrement du réseau. **La faille de sécurité ne vient pas seulement de Firesheep, elle vient du manque de protection des connexions**. La menace la plus grande vient des outils automatisés qui existent depuis des années [3].

## Notes

[1] Crédit : CarbonNYC *David Goehring* Creative Commons By

[2] Et le sujet ici, n'est pas savoir si cette confiance est bien placée…

[3] Voir la magie des Google Cars expliquées par PCINpact ou ZDNet par exemple…