


# Indétectable et envahissant : le successeur des cookies est là, le fingerprinting

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p><b>vous informe...</b></p>	<p>Indétectable et envahissant le successeur des cookies est là, le fingerprinting</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

**Devilé par le tracking publicitaire des sites marchands, vous protestez contre les cookies ? Le fingerprinting ou « empreinte » s'ajoute à leur succion. Combien en avez-vous, vous n'êtes pas sûr de le savoir.**

Où ne s'en sont jamais dérangés de nombreux publicitaires. Certains publicitaires peuvent même vous regarder instantanément, quel que soit le site sur lequel vous venez de tomber, la liste des produits que vous avez consultés sur un site marchand. Le recensement publicitaire consiste en réalité à suivre l'activité des internautes via les cookies. Des plug-ins tels que Lightbulb de Cédric de la Colonne permettent de se faire une idée de l'intensité du tracking réalisé par une multitude d'agences et de prestataires divers, que l'on s'aperçoit lorsque l'on surfe sur un site. Depuis quelques mois, tous les sites de contenus et autres sites marchands sont contraints par la Loi d'afficher un bandeau pour vous avertir de l'utilisation de cookies, incitant les internautes à activer l'option de non-trace de Firefox, à installer des bloqueurs de cookies pour Firefox ou à accepter les cookies sur le site. Depuis quelques mois, les sites marchands ont commencé à utiliser le fingerprinting pour vous reconnaître et vous suivre.

**Fingerprinting, l'âge sombre, est déjà là**

Pour l'instant, seuls les chiffres comptent par AF Internet, la base d'acquisition des cookies en Europe atteint encore 92%. Une proportion respectable pour les publicitaires, mais qui ne les empêche pas d'anticiper l'après cookies. Le futur, c'est le fingerprinting, une solution qui est, sur le papier, imparable. Le service conserve sur ses serveurs les principales caractéristiques de son poste de travail de chacun des internautes, des caractéristiques qui permettent l'identification numérique de son poste, l'adresse d'installation, le navigateur, le matériel d'écran, une vidéo sur le site Facebook et l'ID d'une adresse IP. L'ensemble des informations que votre ordinateur peut transmettre au serveur, sur simple coup de souris.

Elles sont très largement suffisantes pour identifier à coup sûr un internaute qui revient sur le site. Pour un cookie sur le poste devient inutile, il suffit de vérifier cette configuration à chaque connexion.

L'après cookies peut sembler extrêmement obscur et incertain, puisque toutes les données doivent être analysées et stockées sur le serveur, mais les technologies Big Data rendent aujourd'hui cette approche centralisée totalement possible. En France, des acteurs tels que Criteo ou AF Internet affirment ne pas utiliser cette solution technique.

« Une piste de non-trace, le fingerprinting est une alternative sur laquelle nous sommes prêts à reconnaître Melisa Classe, chef de produit chez AF Internet. Elle souligne néanmoins : « Il reste aujourd'hui malgré tout des zones d'ombre sur des aspects fondamentaux du respect de la vie privée, comme la transparence vis-à-vis des internautes, et surtout, sur leur capacité à accepter ou non la collecte d'informations en continu, mais anonymes selon la loi. De ce fait, il est un technique qui AF Internet d'utiliser pas tout ce que nous avons dit pas besoin. »

Une promesse qui n'est pas de mise chez un certain nombre d'acteurs du Web. Des chercheurs de HP Labs et de Princeton ont ainsi démontré en cas de fingerprinting sur 5 200 des 100 000 sites qu'ils ont analysés. Des services tels que Admix, ligatus exploitent les 92 JavaScripts connus, initialement destinés à mesurer des graphiques sur une page HTML, afin de générer une empreinte unique.

**Une approche possible, mais pas tout à fait**

Pour ceux qui souhaitent de la stabilité des techniques de fingerprinting, les chercheurs de l'EMIS, du Laboratoire IRISA et de l'INRIA-Rennes viennent de mettre en ligne le site du 100% Unique ? Celui-ci réalise un calcul de votre signature, votre empreinte et vous dit si celle-ci est véritablement unique et donc s'il vous expose au tracking. Les résultats sont étonnants. Même avec une configuration de type PC sans Windows 7 avec Google Chrome, un serveur ne peut pas reconnaître votre ordinateur sans sur le site, sans qu'aucun cookie n'ait été posé sur le poste. Sur le site de 100% Unique, un chercheur de l'EMIS, Benoît Beaudry, détaille les résultats de son projet unique, qui vise à garantir la diversité logicielle.

Les chercheurs visent à diversifier les logiciels afin d'améliorer leur résistance aux bugs et aux attaques.

Application de cette recherche, Benoît Beaudry cherche comment déjouer le fingerprinting grâce à votre diversité dans le projet 100% Unique. « Globalement, il y a deux stratégies possibles pour déjouer le fingerprinting : soit on va modifier le serveur, soit chercher à le tromper. Modifier le serveur, c'est très simple, on lui renvoie de fausses informations. Le problème, c'est : d'une part, vous risquez d'entraîner des problèmes d'affichage du site car ces informations sont liées à l'affichage des pages, d'autre part, si l'on renvoie des informations fausses pour ne pas être identifié comme un tracker par le serveur, on ne s'agit pas de faire de la recherche, on ne s'agit pas de faire de la recherche. »

Autre approche possible, ne pas modifier le serveur, mais le prendre à son propre jeu. La première stratégie c'est de présenter strictement la même signature pour l'ensemble des internautes. C'est ce que fait le Tor Browser, une version spécifique de Firefox qui surfe via le réseau Tor. Absolument tous les utilisateurs ont un seul et même fingerprint. De fait, un serveur n'est pas capable de distinguer un individu unique dans la masse.

« La recherche s'appuie notamment sur des machines virtuelles pour générer cet environnement automatisé avec une liste de configurations disponibles. Mais, il pourrait être possible de créer une solution plus légère pour générer ces configurations. C'est aussi la vocation de 100% Unique ? que de collecter des configurations « réelles » afin d'élaborer un stock de fingerprint (enorme, bien entendu) et générer ces configurations. Une stratégie de fait contre la loi pour lutter contre le fingerprinting. »

Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire.

Sources : <http://www.100percentunique.com/behavioral-fingerprinting-en-ligne.html> - 100% Unique - fingerprinting cookies alert par Alain Chapard