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

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

Excédé par le tracking publicitaire des sites marchands, vous pestez contre les cookies ? Le Fingerprinting ou « empreinte » s'apprête à leur succéder. Cookies ou pas, vous n'échapperez donc pas au traçage.

Qui ne s'est jamais érigé en défenseur des bandeaux publicitaires. Certaines publicités peuvent même vous rappeler intassablement, quel que soit le site sur lequel vous vous rendez, la liste des produits que vous avez consultés sur un site marchand. Le ciblage publicitaire connaît un succès foudroyant auprès des annonceurs, mais il suscite aussi l'agacement car il révèle l'efficacité du traçage systématique des internautes via les cookies.
Des plugins tels que Lightbeam ou Collusion permettent de se faire une idée de l'intense pistage réalisé par une multitude d'agences et de prestataires divers, que l'on subit lorsque l'on surfe sur un site. Depuis quelques mois, tous les sites de contenus et autres sites marchands sont contraints par la Cnil d'afficher un bandeau pour vous avertir de l'utilisation de cookies, incitant les internautes à activer l'option Do not Track de Firefox, à installer des plugins tels que Ghostery, BetterPrivacy ou NoScriptSecurity Suite, afin de se démettre de l'emprise des publicités.
L'extension Lightbeam pour Firefox identifie 245 sites tiers impliqués pour la visite de 21 sites Web seulement. Chaque site Web pose un cookie pour son fonctionnement interne, mais bien davantage pour tous ses partenaires commerciaux

Fingerprinting, l'après cookies, est déjà là
Pour l'instant, selon les chiffres compilés par AT Internet, le taux d'acceptation des cookies en Europe atteint encore 92%. Une proportion négligeable pour les publicitaires, mais qui ne les empêche pas d'envisager l'après cookie. 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 constituent l'empreinte numérique de son poste. Système d'exploitation, navigateur, résolution d'écran, une visite sur le site Panopticlick de l'EFF donne une petite idée de l'étendue des informations que votre ordinateur peut transmettre au serveur, sur simple requête.

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

L'approche peut sembler extrêmement coûteuse en ressources, 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 AT Internet affirment ne pas utiliser cette solution technique.

« D'un point de vue technique, le fingerprinting est une alternative sur laquelle nous nous sommes penchés » reconnaît Mélanie Claisse, chef de produit chez AT 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 es concernant, aussi anonymes soient-elles. De ce fait c'est une technique qu'AT Internet n'utilisera pas tant que ces zones d'ombre ne sont pas levées. »

Une prudence qui n'est pas de mise chez un certain nombre d'acteurs du Web. Des chercheurs de Kü Leuven et de Princeton ont ainsi débusqué un code Javascript de fingerprinting sur 5 282 des 100 000 sites qu'ils ont expertisés. Des services tels que Addthis, Ligatus exploitent les API JavaScript Canvas, initialement destinées à dessiner des graphiques sur une page HTLM, afin de générer une empreinte unique.

Votre ordinateur vous trahit
Pour ceux qui douteraient de la fiabilité des techniques de fingerprinting, les chercheurs de l'INRIA, du laboratoire IRISA et de l'INSA-Rennes viennent de mettre en ligne le site Am I 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 traçage.
Les résultats sont étonnants. Même avec une configuration de type PC sous Windows 7 avec Google Chrome, un serveur va facilement pouvoir vous repérer à votre prochaine venue sur le site, sans qu'aucun cookie n'ait été posé sur le poste.
Derrière le site Am I Unique ?, un chercheur de l'INRIA, Benoit Baudry. Celui-ci participe au projet européen Diversify, qui étudie la problématique de la diversité logicielle.

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

Application de cette recherche, Benoit Baudry cherche comment déjouer le fingerprinting grâce à cette diversité dans le projet Blink : « Globalement, il y a deux stratégies possibles pour déjouer le fingerprinting : soit on va mentir au serveur, soit chercher à le tromper. Mentir au serveur, c'est très simple, on lui renvoie de fausses informations. Le problème, c'est : d'une part, vous risquez d'avoir des problèmes d'affichage du site car ces informations sont utiles à l'affichage des pages, d'autre part, il faut envoyer des informations cohérentes pour ne pas être identifié comme un tricheur par le serveur qui va alors mettre en place d'autres stratégies pour vous reconnaître. »

Autre approche possible, ne pas mentir au 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 ses utilisateurs ont un seul et même fingerprint. De fait, un serveur n'est pas capable de distinguer un individu unique dans la masse.

Autre piste possible, et c'est l'objet de la recherche de Benoit Baudry, c'est tout simplement de changer de configuration à chaque visite. Cet expert de la diversité logicielle travaille sur une solution qui génère automatiquement une configuration qui fonctionne réellement, avec un comportement le plus proche possible de ce qu'attend l'internaute, mais qui, du point de vue du serveur, est différente et donc, impossible à tracer. « Le fingerprint est unique et stable dans le temps » ajoute le chercheur. « Notre recherche porte sur la stabilité dans le temps. On veut faire évoluer le fingerprint de l'utilisateur dans le temps, mais sans renvoyer de fausses informations. On doit donc faire varier sa configuration pour faire évoluer son fingerprint. » Automatiquement, les paramètres du navigateur, les polices de caractère installées, la liste des plugins et même l'OS vont varier.

Le chercheur s'appuie notamment sur des machines virtuelles pour générer cet environnement automatiquement parmi une liste de configurations disponibles. Demain, il pourrait avoir recours à Docker, une solution plus légère pour générer ces configurations. C'est aussi le rôle de Am I Unique ? que de collecter des configurations « réelles » afin d'amasser un stock de fingerprint (anonymes, bien entendu) et générer ces configurations. Une stratégie du mal contre le mal pour lutter contre le fingerprinting.

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

Source : http://pro.clubic.com/webmarketing/publicite-en-ligne/actualite-742853-fingerprinting-cookies.html
par Alain Clapaud