


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

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</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'en comptez donc pas en traquant.

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 associer des données, mais il nécessite aussi l'appui car il réalise l'efficacité du travail systématique des internautes via les cookies. Des plug-ins tels que Lightbulb de Cédric Dubois 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'active 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 (NoScript) ou de s'activer les paramètres de confidentialité de leur navigateur. Chaque site web passe un certain temps à vérifier son fonctionnement interne, mais bien sûr, pas pour tous les partenaires commerciaux.

Fingerprinting, l'après cookies, est-ce déjà là ?

Pour l'instant, seuls les chiffres comptent par AF Internet, la base d'acquisition des cookies en Europe atteint encore 90%. 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, imparfaite. Le service conserve sur ses serveurs les principales caractéristiques de son poste de travail de chacun des internautes, des caractéristiques qui caractérisent l'ordinateur matériel de son poste, l'adresse d'installation, le navigateur, le système d'exploitation, une adresse sur le site publicitaire et l'ID unique de l'internaute qui vous identifie pour l'ensemble de vos interactions avec le serveur, sur simple coup de main.

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

L'après cookies peut sembler extrêmement complexe en réalité, 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 son technique, le fingerprinting est une alternative sur laquelle nous nous sommes penchés », reconnaît Mélanie 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 surtout anonymes. »

« Une promesse qui n'est pas de mise chez un certain nombre d'acteurs du Web. Des chercheurs de K2 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 AdBrite, Ligatus exploitent les 92 JavaScript Cookies, initialement destinés à mesurer des groupes sur une page HTML, afin de générer une empreinte unique. »

Une approche possible, est-ce déjà là ?

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 de l'EMIS ? Celui-ci réalise un calcul de votre signature, votre empreinte et vous dit si celui-ci est véritablement unique et donc s'il vous expose au tracking.

Les chercheurs ont démontré, mais avec une configuration de type PC sans Windows 7 avec Google Chrome, un serveur ne permettant pas de revenir à votre adresse unique sur le site, sans qu'une cookie n'ait été posé sur le poste. Sur le site de l'EMIS, un chercheur de l'EMIS, Benoît Beaudry, détaille ici les principes de 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 RIUK : « Concrètement, il y a deux stratégies possibles pour déjouer le fingerprinting : soit on va tenter de se connecter au serveur, soit chercher à le tromper. Tenter de se connecter au serveur, c'est très simple, on lui renvoie de fausses informations. Le problème, c'est : d'une part, vous risquez d'activer 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'en rend pas compte et donc n'est pas possible. »

Autre approche possible, ne pas tenter de se connecter 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 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 automatiquement après une liste de configurations disponibles. Mais, il pourrait être possible de générer une signature unique pour chaque configuration. C'est aussi la règle de l'EMIS ? que de collecter des configurations « réelles » afin d'élaborer un stock de fingerprint (enorme, bien entendu) et générer une configuration. Une stratégie de fait contre le tracking pour lutter contre le fingerprinting. »

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

Source : <http://www.citilab.com/behavioral-tracking-en-ligne/actualites-74083-fingerprinting-cookies.html> par Alain Clément