09 juillet 2018
Minute tech

# Attention espionnage : l'extension Stylish du navigateur Chrome enregistre secrètement tout ce que ses utilisateurs font sur le Web, au nez et à la barbe de Google et Mozilla


Stylish, une extension de navigateur web, vient d'être supprimée de Mozilla et de Google. Téléchargée par plus de deux millions d'internautes, elle collectait leur historique de navigation.

Avec Franck DeCloquement

**Atlantico : Comment cette nouvelle affaire a-t-elle été découverte, et comment une extension telle que 'Stylish' parvenait-elle à récolter nos données personnelles ? Cette récolte sauvage se limitait-elle aux historiques de recherche utilisateurs, ou cela allait-il beaucoup plus loin encore ?**

**Franck DeCloquement :** Les affaires de captations sauvages de données personnelles se suivent et ne se ressemblent pas toujours… Mais revenons-en aux faits concernant ce dernier épisode original en date, issue en droite ligne d'une longue série. Cette nouvelle révélation est à porter au crédit de Robert Theaton, un ingénieur logiciel basé à San Francisco en Californie, qui a mis au jour le fait que l'extension baptisée 'Stylish', pouvait théoriquement enregistrer depuis janvier 2017, l'historique utilisateur des navigateurs Google Chrome et Firefox. Date à laquelle l'extension considérée avait justement été acquise par son nouveau propriétaire : la société 'SimilarWeb'.

Sur son blog, Robert Theaton a ainsi déclaré: « Il suffit d'une requête de suivi contenant un cookie de session pour associer définitivement un compte d'utilisateur à un identifiant de suivi de Stylish ». En conséquence, cette extension de navigateur était donc bien en capacité « théorique » de suivre les moindres faits et gestes utilisateurs sur la toile. Et Robert Theaton d'enfoncer le clou : « cela permet à son nouveau propriétaire, SimilarWeb, de relier toutes les actions d'un individu dans un profil unique. Et pour les utilisateurs comme moi qui ont créé un compte Stylish sur userstyles.org, cet identifiant unique peut facilement être associé à un cookie. Cela signifie que non seulement SimilarWeb possède une copie complète de nos historiques de navigation, mais détient également suffisamment d'autres données pour lier théoriquement ces historiques aux adresses email et aux identités réelles. »

En d'autres termes, le script caché dans le code de Stylish renvoie l'historique de navigation complet d'un utilisateur lambda à un serveur central adjoint d'un identifiant unique. Pour celui qui aurait aussi un compte Stylish sur 'userstyles.org' pour télécharger de nouveaux skins de navigateurs, l'identifiant unique SimilarWeb vous permet d'être lié à votre cookie de connexion, comme le suggère clairement Robert Theaton. Ainsi, l'extension Stylish est donc en capacité manifeste de pouvoir renvoyer une activité de navigation complète à ses serveurs, avec un identifiant unique. Et cela inclut bien entendu les résultats des recherches effectuées sur Google ou Firefox. Conséquence immédiate : Google et Mozilla ont conjointement éjecté cette semaine l'extension Stylish de leurs catalogues respectifs, suite à un dépôt de plainte : « Nous avons décidé de la bloquer en raison de la violation des pratiques de données inscrites dans la politique d'examen », a en substance indiqué Andreas Wagner, l'ingénieur logiciel Mozilla. Si Stylish a bien été désactivé, l'extension n'a pour autant pas été supprimé des navigateurs. Cependant, tous les utilisateurs ont reçu un avertissement pour redémarrer leur navigateur Chrome. Google n'a pas commenté cette subite « disparition ». Et de son côté, la page Stylish sur le

**Quel usage aurait pu faire ‘Similar Web’ de ces données personnelles récoltées ? Était-ce pour eux une façon d’envisager de mieux cibler nos envies, dans le but de nous proposer des publicités adaptées, ou cela allait-il plus loin encore (possibilité de nous identifier physiquement, et donc ouvrant sur des risques de demandes de rançon, et de hacking) ?**

Le processus évoqué plus haut permet en effet à un technicien spécialisé - ou à un pirate averti - de relier « en théorie » les données d’historique à un individu spécifique. Cependant, rien ne vient démontrer à ce jour que SimilarWeb a délibérément cherché à établir l’identité des internautes via ce procédé. Son modèle économique repose évidemment sur des données utilisateur agrégées. Et cela permet aussi « théoriquement » à un technicien de SimilarWeb ou à un employé malveillant, de relier des individus à l'ensemble de leurs activités réelles... Ainsi, tous ceux qui ont créé un compte Stylish sur ‘userstyles.org’ auront un identifiant unique qui peut aussi être facilement lié à un cookie de connexion, et à des fichiers texte destinés à aider chaque utilisateur à accéder plus rapidement et plus efficacement à un site Web.

Selon une déclaration de SimilarWeb relevée en 2017, et d’ailleurs rapportée à l’époque par « ghacks.net » (au moment même ou cette société avait justement mis à jour sa politique de confidentialité des données personnelles), ce suivi spécifique aurait été ajouté par elle pour améliorer l'extension du navigateur. On pouvait ainsi lire à l’époque cette déclaration faite en ligne : « en ce qui concerne le suivi, les informations anonymes telles que les styles installés ou les sites visités sont collectés […] cette information alimente certaines fonctionnalités de l'extension telle que la possibilité de proposer des suggestions aux utilisateurs, lorsqu'ils visitent des sites dans le navigateur. »

Cependant, cette découverte de l’ingénieur Robert Theaton suggère aujourd’hui que Stylish pouvait également suivre bien plus que des informations nécessaires utilisés par ailleurs sur certains d’autres sites concurrents, dont la vocation est également de proposer des suggestions en la circonstance. Il semble en effet que SimilarWeb pouvait effectuer aussi le suivi URL de pages entières - en lieu et place du simple suivi de domaine habituel - mais également la collecte des requêtes HTTP, les adresses IP anonymisées, et de toute une gamme d’autres données des moteurs de recherche. Et notamment les mots-clés, les résultats de recherche sur les liens et les pubs affichées.

**Mozilla puis Google ont supprimé ‘Stylish’ de leur catalogue d'extensions. Est-ce possible qu'ils n'étaient pas au courant de la "fonction" réelle de Stylish ? A l'échelle nationale comment peut-on encadrer ces pratiques afin qu’elles ne se répètent plus ?**

Cette application populaire compte environ 1,8 million d'utilisateur à travers le monde. Elle était justement devenue un succès commercial jusqu’alors, en permettant aux internautes d’appliquer en outre des couches successives sur des sites Web visités, et de masquer ainsi les fonctionnalités qu'ils ne veulent pas voir. De son côté, la politique de Google consiste à autoriser l’ouverture des données de ‘Gmail’ à des tiers, mais pas la navigation Web. Conséquence immédiate dans l’interstice de cette découverte de tracking intempestive : l’extension ‘Stylish’ a été bannie de ‘Google Chrome’ et de ‘Firefox’ (appartenant à Mozilla). Naturellement, cette nouvelle affaire ouvre sur des possibilités intrusives aux conséquences potentiellement vertigineuses. Et ceci d’autant plus, quand on réalise qu'une part de la stratégie marketing de ‘SimilarWeb’ consiste en réalité à « commercialiser des solutions pour voir le trafic de tous vos concurrents ». Nous le répétons, il est fort peu probable que ‘SimilarWeb’ ait eu l'intention délibérée d'utiliser ces historiques de navigation personnelle de manière malveillante. Toutefois, sa collecte de données était apparemment beaucoup plus étendue et profonde, que ce qui est vraiment nécessaire. Aussi, rester en sécurité en ligne devient aujourd’hui de plus en plus difficile pour le vulgum pecus, surtout quand 500 sites Web enregistrent en permanence tout ce que nous frappons sur nos claviers. Fort heureusement, ‘Stylish’ offrait également une option « par défaut » qui permettait en outre de désactiver ce suivi intempestif, et d’utiliser comme avant l’extension.