Forum: Sécurité

Topic: Se protéger du «Canvas fingerprinting»

Subject: Se protéger du «Canvas fingerprinting»

Publié par: tignothe

Contribution le : 31/10/2017 02:07:14

Bonjour,

C'est «quoi t'esse» que cette nouveauté?

Pour qualifier très vite ce «canvas fingerprinting» on pourrait le comparer à un cookie d'un nouveau genre; un «super cookie» si vous préférez, même si au final il n'a rien à voir avec les cookies habituels.

Personnellement je fais la chasse à tout ce qui tente de me marquer à la culotte, et j'élimine systématiquement tout ce qui s'incruster dans mon navigateur sans mon consentement explicite. Pour cela différent moyens peuvent être utilisés;

Un module (compatible FF57) Cookie Autodelete qui élimine les cookies à la fermeture des onglets (avec un paramétrage à la demande).

Un autre module (compatible FF57)umatrix par l'activation dans le tableau de bord de;

«Supprimer les cookies bloqués»

«Supprimer les cookies de session non-bloqués et inutilisés depuis plus de ... minutes»

«Supprimer les données locales des noms d'hôtes bloqués »

«Nettoyer le cache du navigateur toutes les ..... minutes»

Pour ce qui concerne Canvas fingerprinting cela ne ressemble pas à une trace qui vient s'implémenter dans le navigateur, car c'est une méthode de traçage des visiteurs qui utilise une technique bien particulière, le canvas HTML5. Cette technique génère au moyen d'un script java une empreinte digitale individuelle sur la base du système de configuration du visiteur. Un flash en quelque sorte, une photo du système utilisé, du navigateur, de la carte graphique, du pilote de la carte graphique, des polices installées.

Rien de très personnel si ce n'est que cela peut permettre de pister le couple Michu/Pignon en visite sur le site avec une efficacité redoutable (pas à 100% quand même) pouvant permettre de suivre les comportements de navigation du dit couple (vous avez dit parano?).

Pour contrer cette technique silencieuse (rien ne vient vous avertir que vous avez étés «radarisés») impossible à postériori car aucune information se glisse dans le navigateur. Il faut donc agir en amont;

Le module (compatible FF57)Canvas Blocker avec le paramétrage liste blanche/noire, autoriser/interdire.

l'utilisation de listes EasyPrivacysur un bloqueur de publicité.

Le module umatrix encore lui:

Activation de;

«Mettre à jour les fichiers hosts automatiquement»

«Modifier l'Identification du navigateur toutes les... minutes en choisissant au hasard une des chaînes de caractères suivantes :»

Blocage/déblocage de tous les sripts; mais là il faut avoir du doigté, donc réservé aux experts.

Pour finir, bonne nouvelle pour les fidèles de Firefox, c'est tout chaud!

Citation :
Firefox 58 ne permettra pas le pistage des internautes grâce à l'élément HTML Canvas

Le navigateur demandera d'abord la permission de l'utilisateur — https://www.developpez.com/actu/169700 ... mission-de-l-utilisateur/[/url]

Pour approfondir les connaissances,

Canvas fingerprinting : le successeur du cookie — https://www.1and1.fr/digitalguide/web- ... age-internet-sans-cookie/

Le canvas fingerprinting est plus invasif que les cookies. Mais faut-il s'en inquiéter? — http://www.slate.fr/story/90339/canvas-fingerprinting

Pour tester le blocage/déblocage du canvas; https://browserleaks.com/canvas