# Surfer sans être pisté

Philippe Wambeke - LoliGrUB (19 janvier 2019)

# Le pistage

Avec tout ce qu'on "sème" derrière nous lors des séances de surf, il est très facile de nous pister. Quelques exemples:

- Notre adresse IP
- Notre "User Agent" (version du navigateur)
- Des caractéristiques du système:
  - 1. résolution
  - 2. mémoire
  - 3. CPU

# **Comment est-ce possible?**

#### L'adresse IP

- Elle vous est propre et est unique au monde.
- Nécessaire à la connexion à tout site web.
- Elle permet de vous géolocaliser.
- Impossible à cacher, complexe à falsifier

#### Le "User Agent"

- Information renvoyée automatiquement par le navigateur.
- Il s'agit d'une sorte de "signature" de votre navigateur.
- Elle permet de connaître le type et la version du navigateur.
- Impossible à cacher, simple à falsifier

#### Le javascript

- Code exécuté sur le navigateur pour rendre les sites "dynamiques"
- Voie royale pour faire à peu près tout et n'importe quoi, comme connaître la résolution, la mémoire, le cpu, ...
- simple à désactiver, mais peut rendre le site non-fonctionel

### Au final

Tous ces éléments combinés (adresse IP, user agent, ...) forment une espèce d'identifiant unique permettant de nous suivre.

#### Et c'est tout?

Non, il existe d'autres menaces pour notre vie privée:

- Les cookies tiers presque toujours associés à des publicités
- Les CDN (Content Delivery Network), typiquement des polices de caractères ou des programmes javascript communs

# Un dernier pour la route

- Failles de sécurité du navigateur
- Failles de sécurité générales (Spectre, Meltdown)

Ces failles permettent à un attaquant (site web ou autre) d'accéder à des parties de l'ordinateur en principe inacessibles. Cela peut aller de la perméabilité des onglets à l'accès \*total\* de la mémoire de l'ordinateur.

# Que peut-on y faire?

La navigation privée va nous sauver! Et bien non.

La navigation privée ne sert pas à ça: elle sert à ne garder aucun historique sur l'ordinateur.

Mais avec une bonne "hygiène" informatique et quelques techniques simples, il est possible de se rendre presque "invisible".

#### Etape 0: utiliser un navigateur libre

- Firefox (que tout le monde connaît)
- Chromium (la version open-source de Chrome)

#### Etape 1: cocher les bonnes options dans le navigateur

Dans Firefox: Préférences → Vie privée et sécurité → contenus à bloquer:

Traqueurs: toujours

· Cookies tiers: Tous les cookies tiers

• Ne pas me pister: toujours

#### **Etape 2: installer quelques extensions (libres!)**

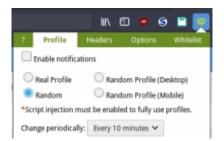
Dans Firefox: Modules complémentaires → Extensions

- un bloqueur de pub: \*μBlock Origin\* (oubliez AdBlock et ses dérivés) GPL
- un générateur de User-Agent aléatoire: \*chameleon\* GPL
- se passer des CDN sans perdre en confort: \*decentraleyes\* MPL
- un tueur de javascript: \*NoScript\* GPL

https://loligrub.be/wiki/ Printed on 2025/12/13 07:16

#### **Etape 3: configurer ces extensions**

- μBlock Origin: facile, rien à faire
  decentraleyes: facile, rien à faire
- **chameleon**: cliquer sur l'icône → profil et choisir "Random Profile (Desktop)" toutes les 10 minutes



From:

https://loligrub.be/wiki/ - LoLiGrUB

Permanent link:

https://loligrub.be/wiki/atelier20190119-safe-browsing-run?rev=1548249704

Last update: **2019/01/23 13:21** 

