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

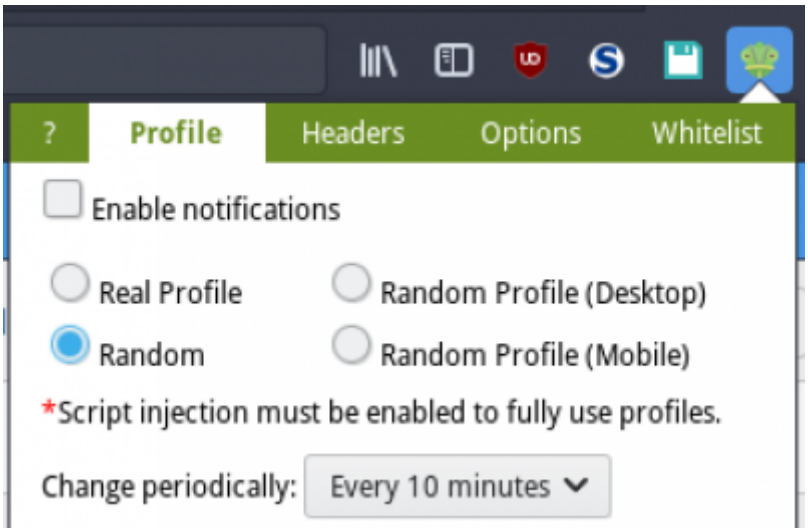
Etape 2: installer quelques extensions (libres !)

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

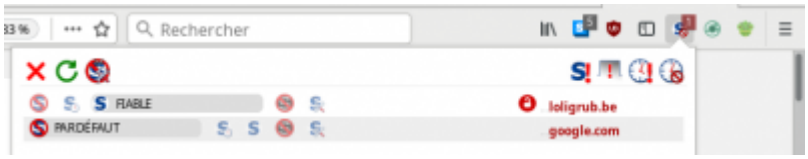
Etape 3: configurer ces extensions

- **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



Etape 3: configurer ces extensions

- **NoScript**: fonctionne par domaine à activer au coup par coup



Etape bonus: les profils de Firefox

Les profils Firefox permettent l'utilisation de Firefox pour des usages précis comme le shopping, le web banking, ...

Pour utiliser les profils:

- Arrêter Firefox
- Démarrer Firefox avec l'option -P

Précautions supplémentaires

Rien qu'avec ça on rend quasi-impossible tout pistage.

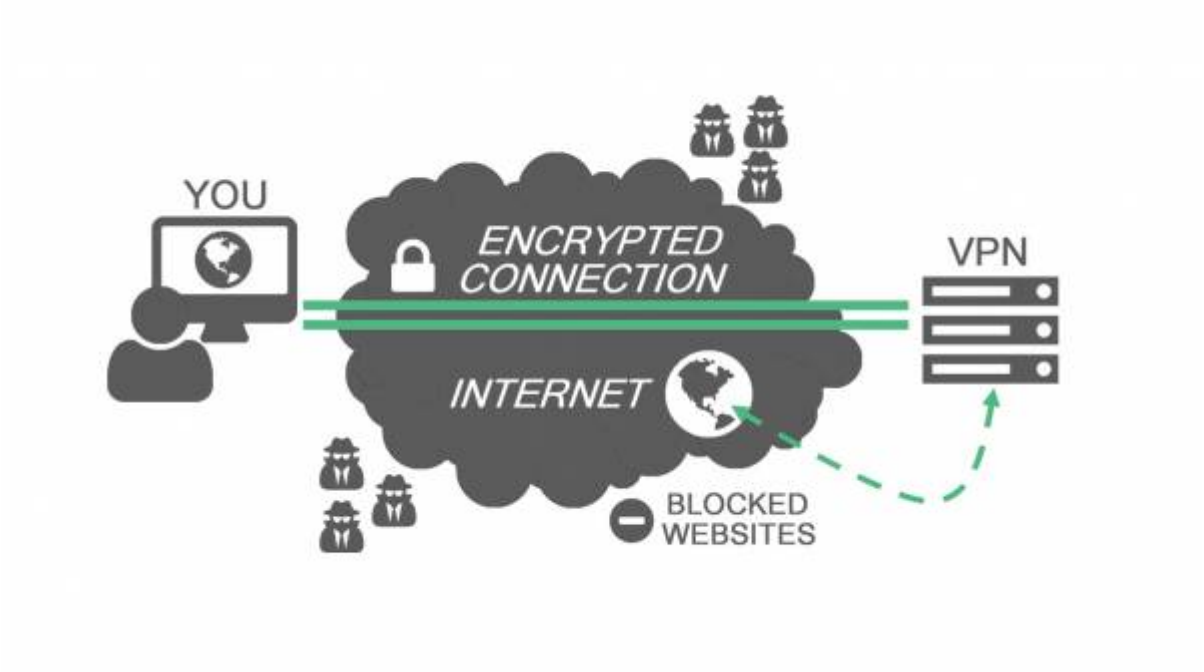
Mais il reste encore un élément exposé aux yeux de tous: l'adresse IP.

Pour la cacher, deux choix possibles:

- Utiliser un VPN
- Utiliser Tor

Le VPN

VPN: Virtual Private Network: c'est un ordinateur distant qui agit comme un relai entre vous et le reste d'Internet.



Les avantages

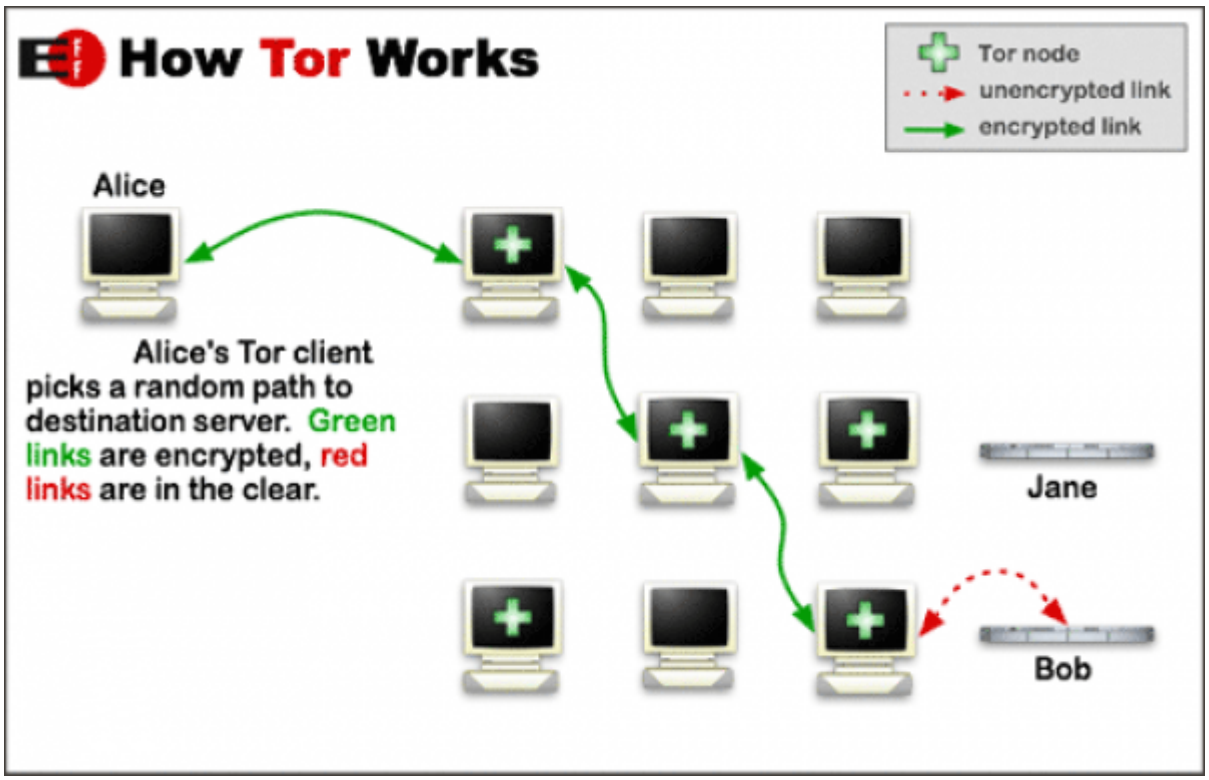
- Votre IP est inconnue de tous, sauf du VPN
- Trafic entièrement chiffré entre vous et le VPN
- Supporte tous les protocoles (pas seulement le web)

Les inconvénients

- Parfois compliqué à mettre en place
- Les prix et la qualité du service peut varier d'un fourisseur à un autre

Tor: The Onion Router

Il s'agit d'un protocole permettant de surfer de manière anonyme grâce au réseau Tor.



Les avantages

- Votre IP est inconnue de tous
- Personne ne connaît les sites que vous consultez
- Simple à utiliser et gratuit

Les inconvénients

- Ne fonctionne que pour le web
- Navigation un peu plus lente
- Mauvaise “presse” ?

Un peu de vocabulaire

Deep Web

Il s'agit simplement de contenu web qui n'est pas indexé par les moteurs de recherche, que ce soit voulu ou non.

Dark Net

Il s'agit d'un réseau de machines utilsant des protocoles spécifiques permettant des échanges complètement anonymes. Comme tous les échanges sont anonymes, il peut servir à des activités malveillantes, mais il est surtout utilisé par les lanceurs d'alerte ou les dissidents.

Reporters Sans Frontières propose un “kit de survie numérique” et y fait la promotion du Darknet.

Merci

Questions ?

From:
https://www.loligrub.be/wiki/ - **LoLiGrUB**

Permanent link:
https://www.loligrub.be/wiki/atelier20190119-safe-browsing-run?rev=1548250025

Last update: **2019/01/23 13:27**