La vie privée sur internet

DJ Namurlug 2017

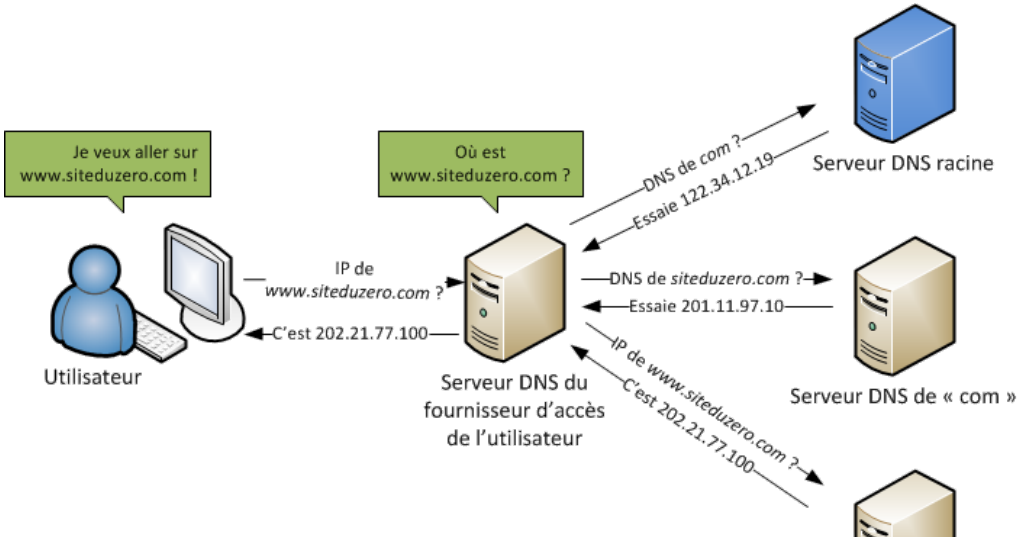
Avant propos

- Le plus possible, le pseudonymat tu utiliseras
- De nombreuses adresse émails, tu disposeras
- Des mots de passe fort, tu retiendras

Les bases de l'internet

DNS (Domain Name System)

Il s'agit de la solution permetant de transformer une IP en une adresse humainement mémorisable



Risques

Par défaut les ordinateurs sont configurés pour se connecter au DNS de leur Box. Donc le DNS de leur fournisseur d'accès.

1. Le serveur DNS sait par principe que l'adresse IP 172.16.0.0 a demandé l'adresse IP de fr.wikipedia.org
2. Le serveur peut mentir =
    - pour des raisons légales

Risques

Par défaut les ordinateurs sont configurés pour se connecter au DNS de leur Box. Donc le DNS de leur fournisseur d'accès.

1. Le serveur DNS sait par principe que l'adresse IP 172.16.0.0 a demandé l'adresse IP de fr.wikipedia.org
2. Le serveur peut mentir =
    - pour des raisons légales
    - pour des raisons financières

Risques

Par défaut les ordinateurs sont configurés pour se connecter au DNS de leur Box. Donc le DNS de leur fournisseur d'accès.

1. Le serveur DNS sait par principe que l'adresse IP 172.16.0.0 a demandé l'adresse IP de fr.wikipedia.org
2. Le serveur peut mentir =
    - pour des raisons légales
    - pour des raisons financières
    - pour faire "plaisir" aux surfeur : ex :Free avec son adgate (j'en parle plus loin)

Solutions

Niveau 1: Utiliser un serveur DNS alternatif

- DNS de Google : 8.8.8.8 

- DNS de FDN
- La liste de wikileaks

Niveau 2 :Installer son propre serveur DNS

Par exemple Unbound

- La doc d'ubuntu-fr
- Du hollandais volant
- homeserver.diy
- sebsauvage

De plus avec son propre DNS on peut bloquer les résolutions DNS vers certains type de site (régies pubs)

explication chez tuxicoman ou chez Antoine Magnier

HTTPS

Schéma de chez l'EFF

TOR

Idem schéma

Tor est un réseau en oignon. Bob demande A qui demande a B, B demande a C, C qui demande au site web.

B ne connait que A et C, aucune autre personne avant ou après

Les requêtes externes et les cookies

Un site sur fr.wikipedia.org ne fait des requetes que chez wikipedia.org. Mais c'est plus une exception qu'autre chose.

Les requêtes externes et les cookies

Un site sur fr.wikipedia.org ne fait des requetes que chez wikipedia.org. Mais c'est plus une exception qu'autre chose.

Une visite sur lemonde.fr donne

lemde.fr	138
cedexis.com	23
outbrain.com	21
googlesyndication.com	20
adsafeprotected.com	16
adnxs.com	13
adhese.com	12
doubleclick.net	9
atemda.com	7
kameleoon.com	6
nuggad.net	6
stickyadstv.com	6
cxense.com	5
cedexis-test.com	4
po.st	4
theadex.com	4
weborama.fr	4
audiencesquare.com	3
chartbeat.net	3
google-analytics.com	3
msedge.net	3
pulpix.co	3
pebblemedia.be	2
predicubemedia.com	2
scorecardresearch.com	2

112038398dc590fd910f04439eba2dc2.ovh	1
ajax.googleapis.com	1
barnebys.com	1
cedexis-radar.net	1
chartbeat.com	1
facebook.com	1
facebook.net	1
googletagmanager.com	1
googletagservices.com	1
ligatus.com	1
netmng.com	1
nuggad.net	1
null	1
pulpix.com	1
visualrevenue.com	1
xiti.com	1
youtube.com	1
ytimg.com	1

Exemples communs

Les boutons "like" de facebook :

- Interdiction dans un land allemand
- Condamnation en belgique

Exemples communs

Les boutons "like" de facebook :

- Interdiction dans un land allemand
- Condamnation en belgique
- Puis victoire en appel

Google analytics

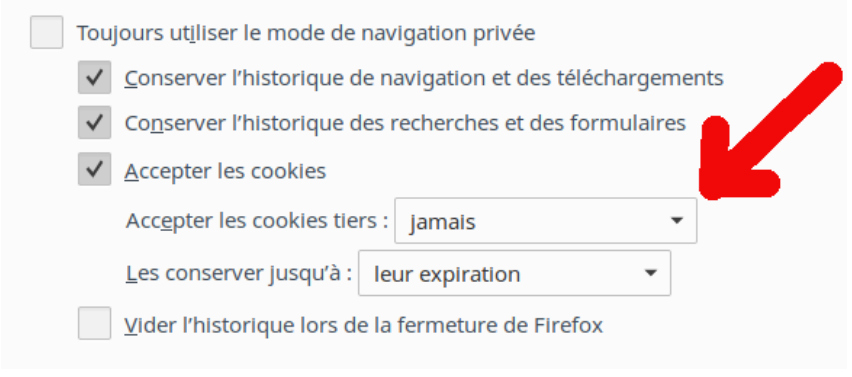
Google fournit une solution gratuite pour suivre ses visiteurs, données qui sont stockés chez eux. **Exemple fictif** Une personne qui cherche sur google après "namurlug" de là va sur site de UNamur et puis sur la liste des chercheurs, le site web du chercheur, et de là va sur le site web personnel du chercheur, puis sa page wikipédia

Le namurlug ne verrait que l'entrée via google, la sortie vers le site de l'unif. L'unif ne verrait que l'entrée via le namurlug, et la sortie vers le site du chercheur. Google lui verrait absolument toute la navigation de la personne -> super profil d'utilisateur

solutions :

Solution simple pour les cookies,dans firefox -> Préférence -> Vie privé -> Historique

Mettre les "Règles de conservation" à "utiliser des paramètres personnalisés" et pour les cookies tiers indiquer "jamais"



ou utiliser l'extension cookies manager

un article de la CNIL

On peut aussi activer le "do no track" un peu plus haut

Extrème : Utiliser noscript, qui bloque par défaut tout le javascript d'une page. Mais ça demande une configuration

Ainsi que l'extension Request Policy,mais qui est remplacé par Request Policy Continued car le mec n'as plus le temps

En plus simple uBlock Origin, où (du meme auteur uMatrix)

~~Ghostery~~ il demande si on veut bien etre traqué pour lui rapporter de l'argent

Les extensions javascript

La très grande majorité des sites web utilisent du javascript.

Le problème est que ça augmente le poids de la page, de plus certaines librairies sont utilisé sur énormément de site (jquery par exemple)

Si chaque visiteur doit télécharger a chaque fois la bibliothèque jquery lors de chaque visite sur un site web ça commence a faire bcq

Les sites web ont donc pris l'habitude d'utiliser des CDN pour stocker les bibliothèques javascript à l'extérieur. Comme ça le navigateur ne charge qu'une seule fois le fichier et le garde en cache

Solutions

Decentraleyes

L'extension télécharge et remplace les appels vers les bibliothèques chez les CDN vers une copie locale

Article de Korben

Et un de debian-fr, avec une explication utile en bas

et un article d'assiste.com

Les CDN : Content Delivery Network

En plus de stocker des librairies, les CDN sont utilisés pour absorber les pics de trafics, limiter les attaques, augmenter la vitesse et d'autres trucs (genre modifier le contenu a la volée).

Certains sites utilisent des CDN (Content Devilery Network)

Ses services s'insèrent juste avant le site web qu'on veut visiter, ils voient donc passer **tout** le contenu : mot de passe, données etc

Exemples de CDN : cloudfare, akamai, maxcdn, cachefly, ...

Il a justement eu la semaine dernière un problème avec Cloudfare article de nextinpact, Une fuite de mémoire toutes les 3 300 000 requêtes

Solution : ???

On peut regarder si un site utilise cloudfare graçe à Does It Use Cloudflare

Flash

Depuis la dernière présentation sur la vie privée, Flash est en train de pousser son dernier souffle. C'est une bonne chose pour la sécurité

-> Dans firefox il n'y a plus de lancement automatique de flash, mais une demande à chaque fois

Exemple de site web utilisant encore ici

Donc les cookies flash et l'extension BetterPrivacy est devenue moins utile.

La page de macromedia pour voir les cookies flash sur le pc

Les referer

Certains sites pour suivre les liens par lesquels les gens sortent de leur site utilisent ce genre de solution

```
http://somesite.com/?to=www.example.com ➜ http://www.example.com/
```

Les referer

Certains sites pour suivre les liens par lesquels les gens sortent de leur site utilisent ce genre de solution

```
http://somesite.com/?to=www.example.com ➜ http://www.example.com/
```

exemple concret

https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi9_ujpuLDSAhUrDMA
les-publicites-et-traqueurs-au-niveau-du-dns-avec-unbound.html&usg=AFQjCNHVT-10cWY17QXKP7gvRuki2KKWJQ

Solution

L'extension Clean links

l'empreinte digitale d'un navigateur

Quand on visite un site web, le navigateur transmet des informations comme le nom du navigateur, la plateforme (ubuntu, mint, windows 7/8/10), la résolution de l'écran, les polices d'écritures installées, les plugin etc.

C'est utile pour afficher un site web adapté en fonction du support. Mais vu le nombre de paramètre, celà peut conduire à disposer d'une "empreinte" unique pour le navigateur

Demo chez sur cette page de l'EFF (Electronic Frontiere Fondation)

Il y a moyen de changer quelques paramètres via l'extension Random agent spoofer

Tor Browser conseille de ne pas mettre son navigateur en plein écran.

Et récemment des chercheurs ont réussis a creer une empreinte quasi uniquement mais pas que pour le navigateur, mais pour le pc completarticle chez nextinpact. L'empreinte serait donc la même quand on ouvre un autre profil ou un autre navigateur.

L'autocompletion des formulaires

Pierre nous a montré un problème qu'on peut rencontrer avec l'autocomplétion des formulaires.

Si on a déjà remplis beaucoup de donnée dans un formulaire (nom, prénom, adresse (mail + postale), numéro de gsm, numéro national)

Un autre site web qui demanderait juste le nom et l'adresse mail, on clique sur la case du formulaire pour qu'il remplisse tout.

Mais en fait, le site web peut masquer des champs plus important (demande de numéro de gsm) qui seront aussi remplis automatiquement

Explication

Demo

un des rare article en français

Solution génériques

Mode "vie privé"

ça peut être une bonne solution, même s'il y a moyen de détecter une personne qui surfe en navigation privée (ici sur gist.github)[https://gist.github.com/cou929/7973956]

Et donc certains sites refusent l'accès (des journaux qui permettent de lire X articles gratuits : La Croix d'après cet article de nextinpact)

Profils multiples

Utiliser plusieurs profils firefox en même temps

Ligne de commande :

```
firefox -p
```

ou directement

```
firefox -p lenomduprofil
```

ça fonctionne aussi avec des icones : un tuto sur ubuntu-fr

Ou alors on peut utiliser l'extension priv8. Firefox est en train de tester une solution équivalente (un seul profil mais des contextes) un article sur Mozfr

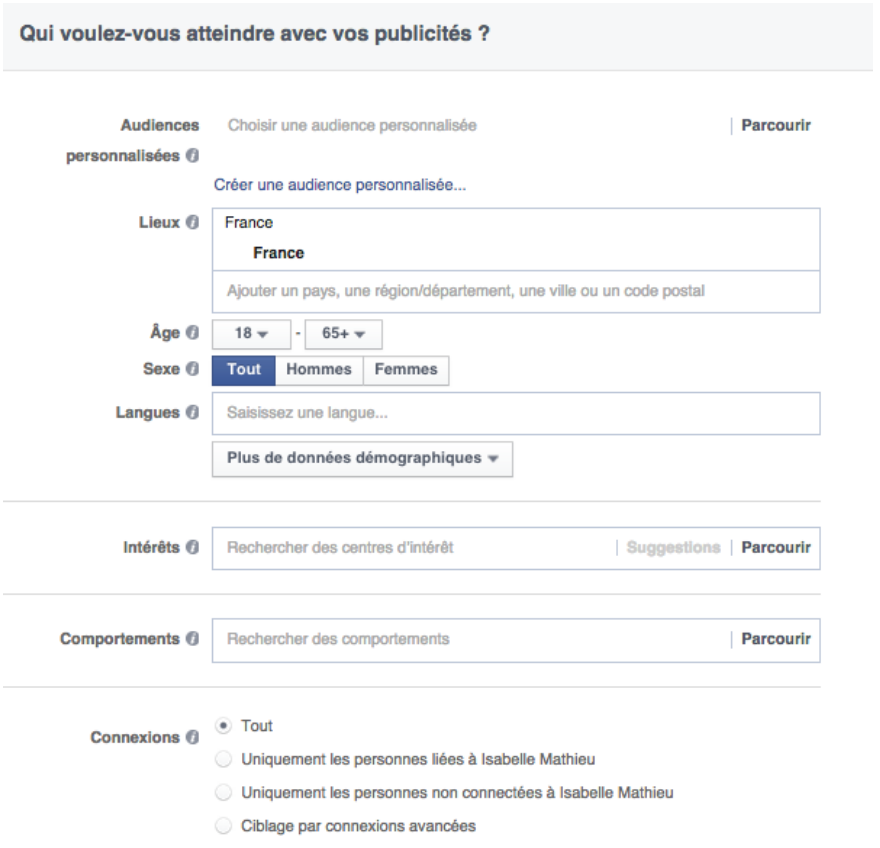
Divers

Ne pas utiliser Chrome

Utiliser le moins possible de réseaux sociaux.

En plus de leurs manipulations des émotions, leurs capacités de tracking sont énorme (un petit exemple avec cet article qui explique que facebook analyse les formes sur les images pour mieux profiler)

Une personne qui poste souvent des photos de soirée -> on lui proposerait bien de l'alcool ou des crèmes anti cernes


Qui voulez-vous atteindre avec vos publicités ?
Audiences personnalisées
Choisir une audience personnalisée
Parcourir
Créer une audience personnalisée...
Lieux
France
France
Ajouter un pays, une région/département, une ville ou un code postal
Âge
18
65+
Sexe
Tout
Hommes
Femmes
Langues
Saisissez une langue...
Plus de données démographiques
Intérêts
Rechercher des centres d'intérêt
Suggestions
Parcourir
Comportements
Rechercher des comportements
Parcourir
Connexions
Tout
Uniquement les personnes liées à Isabelle Mathieu
Uniquement les personnes non connectées à Isabelle Mathieu
Ciblage par connexions avancées

Hors internet, ne pas donner des données sans raison.

- Mediamarkt demande ta carte d'identitée pour le ticket de caisse -> non, ils ont ton adresse en plus
- Un numéro de GSM sur une carte de fidélité idem

Liens

Cnil.fr : Maitriser mes données

Un jeu pour parler des données personnelles

Guide d'autodéfence numérique

youronlinechoices une ASBL qui installe (s'ils n'y sont pas) les cookies de 121 sociétés de tracking comportemental. Mais où via cette page on peut demander aux sociétés de ne plus nous suivre. (Je suis très dubitatif sur l'idée)

http://www.revoltenumerique.herbesfolles.org/

https://donottrack-doc.com/fr/episode/1

http://assiste.com/Principe_d_encerclement.html

(https://news.ycombinator.com/item?id=11009794)

http://tousfiches.blogspot.be/2013/08/ip-tracking-cookie-publicite-ciblee-et.html

la page de google pour sa pub

un article sur les nouveautés de html5 qui permettaient de nouvelle formes de tracking

http://valerieaurora.org/hash.html