À tous les niveaux, la sécurité

Christophe Villeneuve
@hellosct1

Passage en Seine Juillet 2016

PSES HSF 2016

Qui ???

AUSY

mozilla reps

Christophe Villeneuve

afup

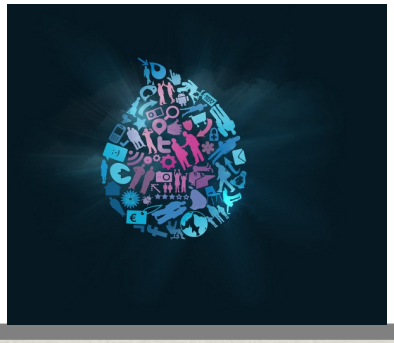
MySQL User Group

[libre@toi[

MariaDB

Agora CMS

PHPTOUR2016 Clermont-Ferrand



FORUMPHP PARIS2016

On aurait pu parler de…

~~Serveur~~

~~Langage~~

~~Base de données~~

~~CMS~~

Aujourd'hui →

Le programme...

Utilisateurs

Navigateurs

Site internet

On aurait pu parler de...

~~Serveur~~

~~Langage~~

~~Base de données~~

~~CMS~~

Aujourd'hui →

PSES HSF 2016

Utilisateurs



Humour : La sécurité...

Ça ne sert rien.

C'est de la vente forcée.

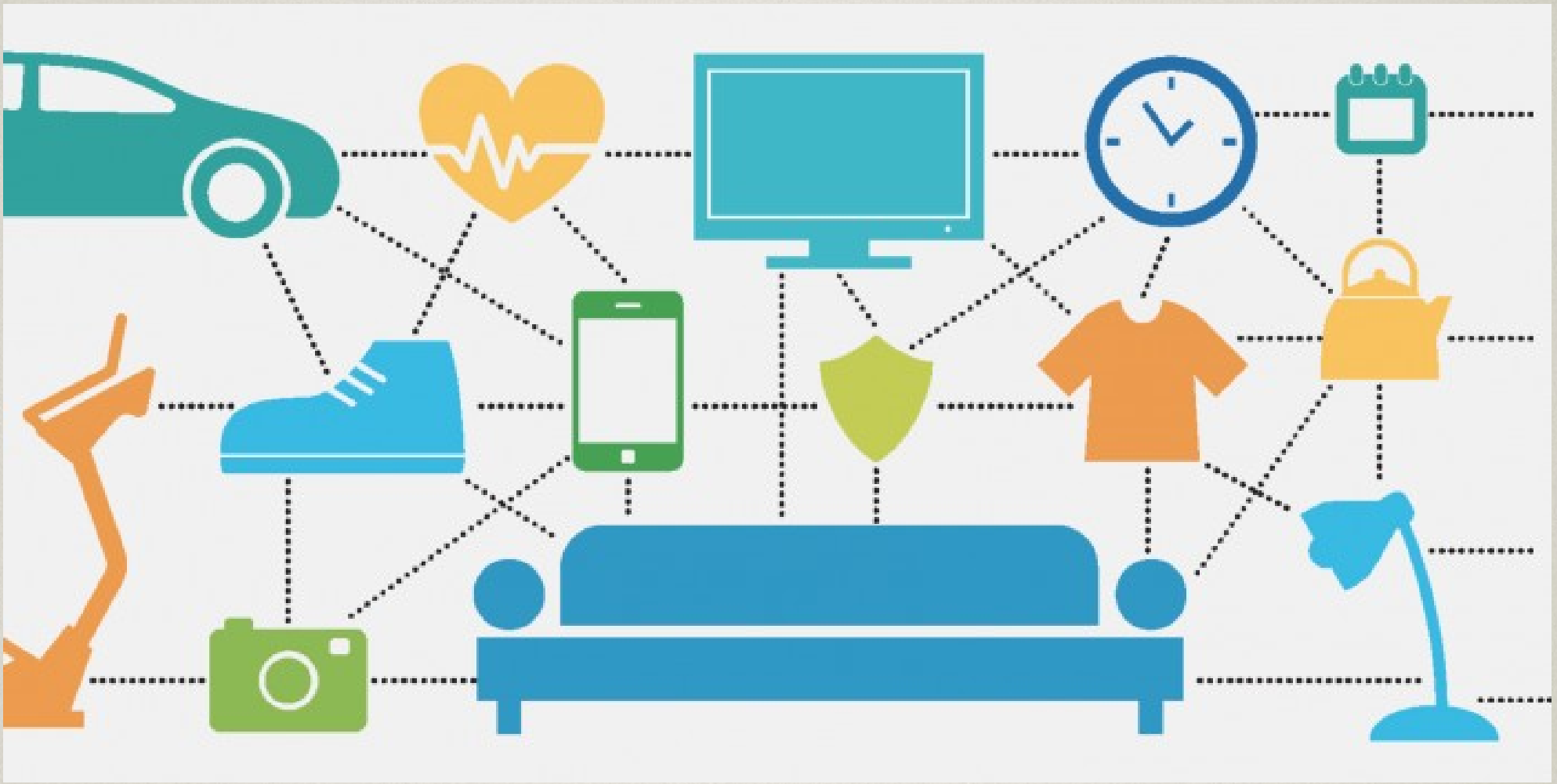
Ce n'est pas pour moi.

Le numérique

BotNet

- Programmes connectés à Internet
- Communiquent avec d'autres programmes identiques
- Exécution de certaines tâches
  - Machines zombies
  - Spam / Virus
  - DDoS

Internet des objets / *Internet of Things* / IoT



Cloud

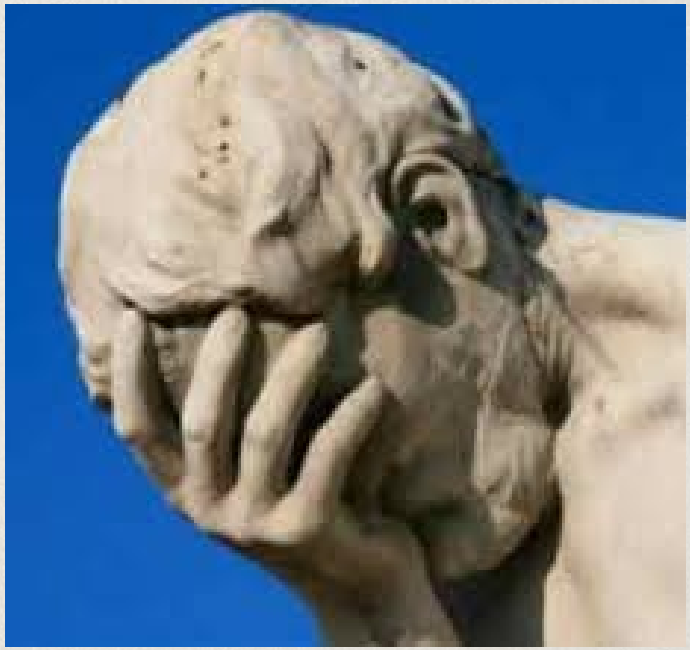
- Grand nombre de fonctions de sécurité disponibles
- Emplacement
- Définir les limites
- Attaques
  - Applications
  - Activités suspectes

Le pistage

- Méthodes utilisées : À partir de la publicité
  - Adware, hijacking
  - Envoi de fichiers par le téléchargement
- Certains services
- Réseaux sociaux
- Incrustations de *tracking* dans les pages
  - Image invisible (1 px)
  - Tags (Js, flash, ActiveX, Java…)
  - Les cookies
- Provoquer la cassure des flux par les Add-ons *On en reparle*

À retenir

- L'utilisateur n'est pas le seul fautif.
- C'est nous



Site Internet

Un site Internet…. Les actions

- Pistage… pas possible
- Anonymat
- Limiter le pistage
- Non observabilité
- L'IP
- Le navigateur
- Protection des données, de votre vie
- Pas de confidentialité

Intérêt de pister à travers un site Internet

- Pour une société
  - Le moyen de vous vendre des produits supplémentaires
  - Savoir d'où vous venez
  - Ce qui est bon pour l'utilisateur est bon pour les affaires
- Pour un espion / services secrets...
  - Vos centres d'intérêts
  - Vos ami(e)s
  - Vos proches

Résultat


mozilla
Reported Attack Page!
This web page at nsa.gov has been reported as an attack page and has been blocked based on your security preferences.
Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.
Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.
Get me out of here!
Why was this page blocked?
Ignore this warning

Eviter les menaces

Pour un site Internet

OWASP

- OWASP : Open Web Application Security Project
- Communauté pour la sécurité des applications Webs
- Publications :

  TOP 10 / Cheat sheets / Owasp : secure Contrat
- Outils :

  Owasp Zed attack Proxy / ESAPI : API for / AppSensor :: a IDS / IPS
- Jeux :

  Owasp cornicoppia / Owasp Snake

ZAP (1/2)

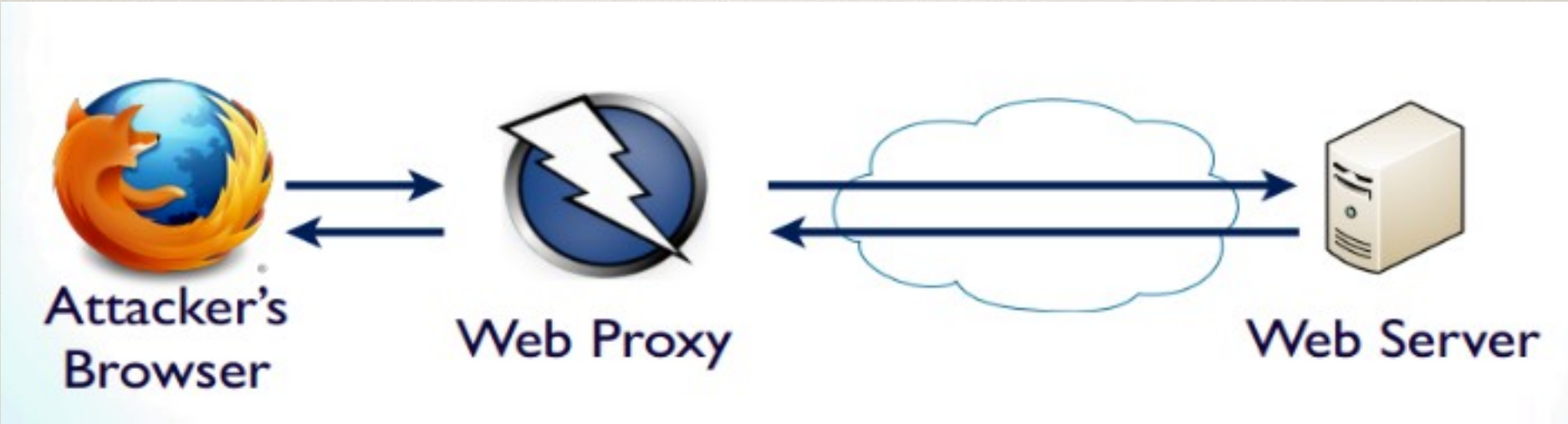
- A destination des développeurs
- OWASP Zed Attack Proxy (ZAP)
- Open Source
- Tests de sécurité

code pénal
R323-1 et R323-5

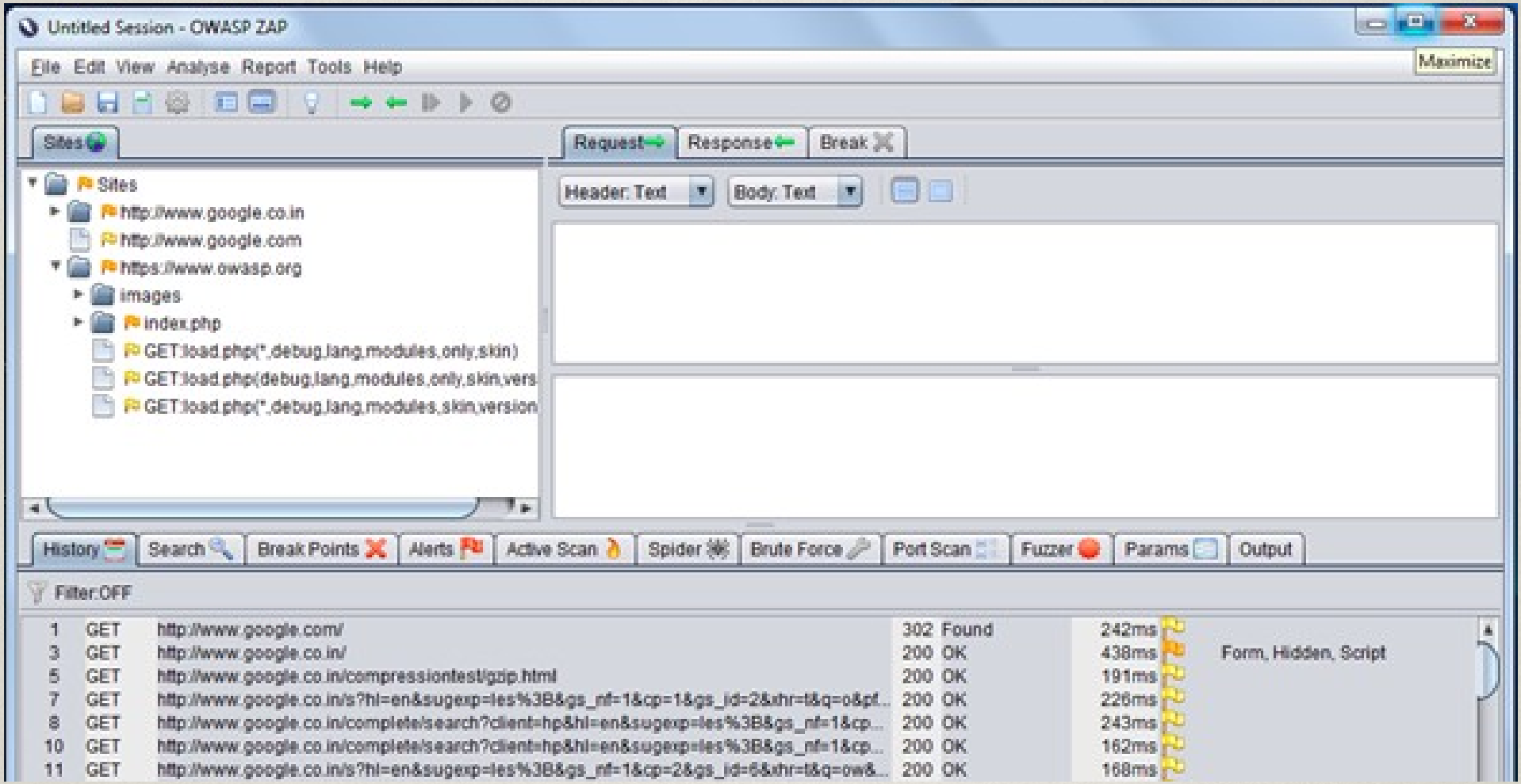
ZAP (2/2)

- But :
  - Aider les utilisateurs à développer et appliquer des compétences de sécurité des applications
  - Construire une solution open source, et orientée vers la communauté plate-forme compétitive,
  - Fournir une plate-forme extensible pour les tests
  - Conçu pour être facile à utiliser
  - Élever la barre pour d'autres outils de sécurité

Zap : Utilisation (1/2)



Zap : Utilisation (2/2)



OWASP TOP 10

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

Quelques conseils

Professionnels (1/2)

- Sécurisez votre application
  - Librairies / plugins / mise à jour du code...
- Créer des politiques de gestion d'accès
  - Roles / Profil utilisateurs / ...
- Adopter une approche de gestion de correctifs
  - Infrastructure / patches / Standardisations...

Professionnels (2/2)

- Vérification régulière
  - Logs / Monitoring...
- Construire une boite à outils de sécurité
  - Antivirus / Détection malwares / Anomalies...
- Restez informés des dernières vulnérabilités
- Comprendre les services de sécurité

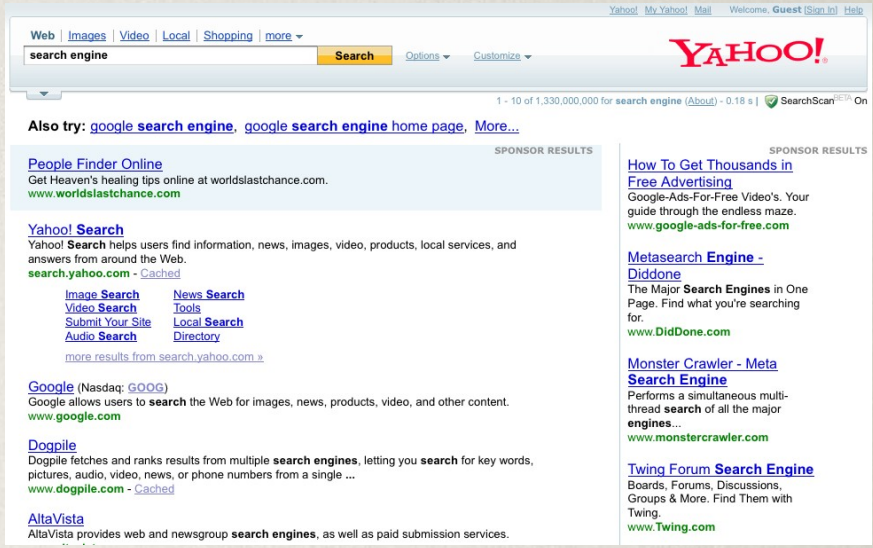
Les solutions : Navigateurs

Navigateur Firefox

- Navigateur moderne
- Outil libre et gratuit
- Protège votre sécurité et votre vie privée
- Développé par la fondation Mozilla
- Forte communauté d'utilisateurs et de développeurs
- Existe pour tous les OS
- Populaire
- Respectueux des standards W3C
- Des milliers d'extensions

Moteur de recherche (1/2)

- Différents selon le pays / le continent
  - Yahoo : États-Unis
  - Yandex : Russie
  - Baidu : Chine
  - Google : France… /!\

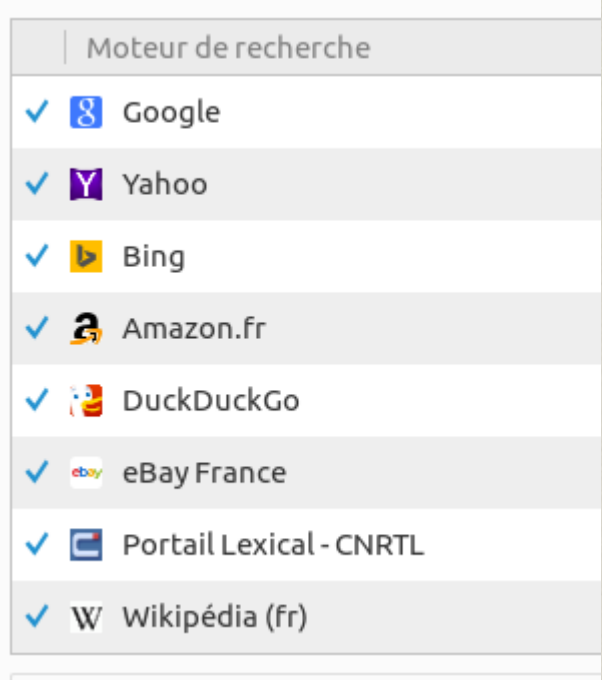


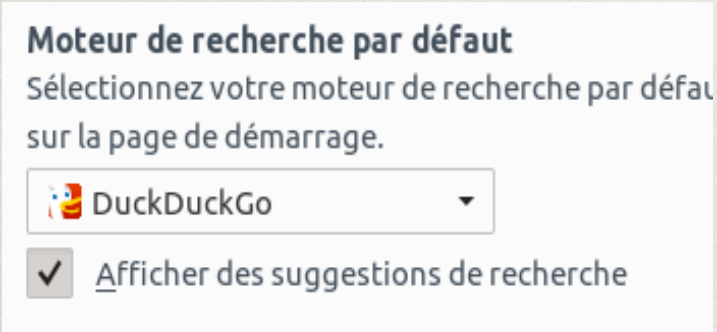
- Choix des distribution Linux
  - Duck Duck Go

Moteur de recherche (2/2)

- Choix des utilisateurs
  - Configuration :

    Préférences → recherche





Moteur de recherche : QWANT

- Moteur français
- Neutre dans l'affichage des résultats

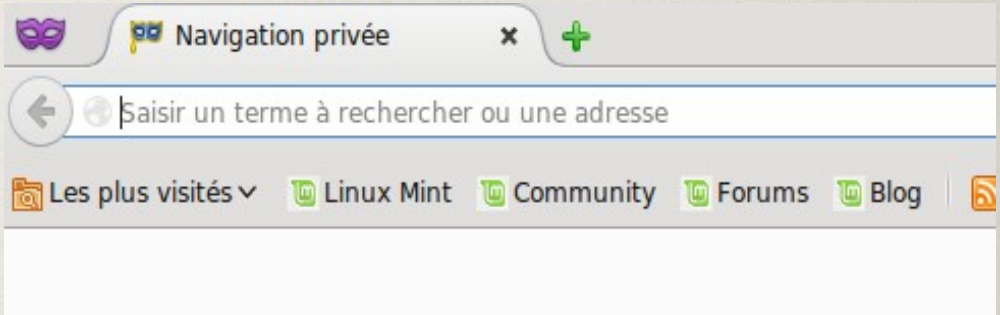
Do Not Track = DNT

- Disponible depuis 2011 - Amélioration en 2013
- Est une entête HTTP
- Indique aux sites que l'on ne souhaite pas être pisté

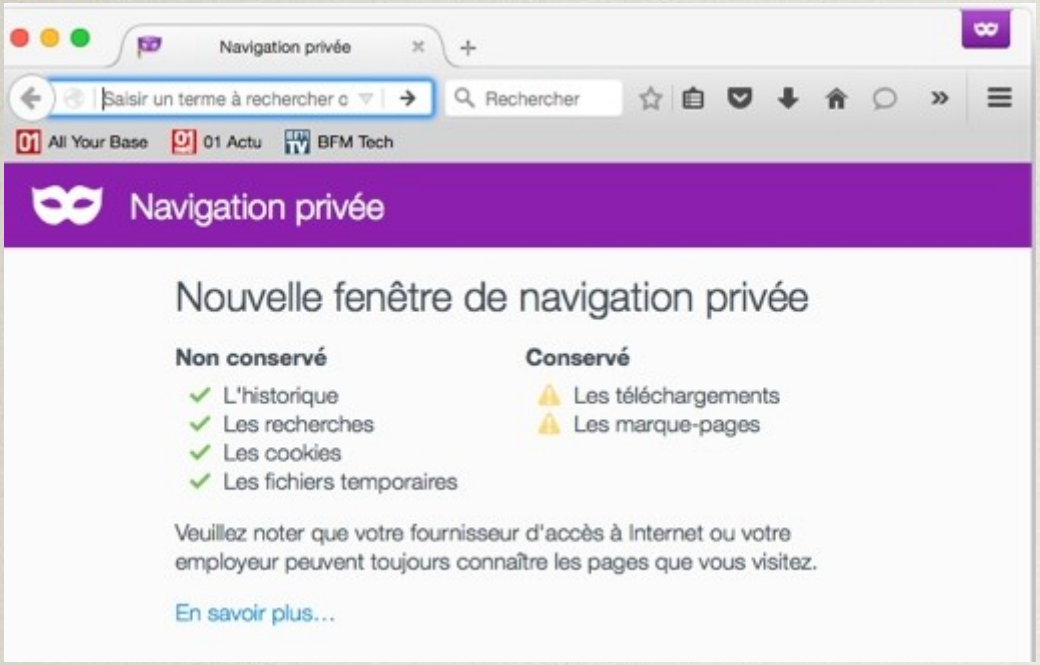
- Configuration
  - Préférence → Vie privée

Navigation privée (1/2)

- Permet de naviguer sur Internet sans enregistrer aucune information
- Ne stocke pas :
  - Les informations dans l'historique
  - Les pages et sites visités
  - Les mots de passes
  - La liste de vos téléchargements
  - Cookies
- Pas de hors-ligne
- Utilisation → Menu : Fenêtre privée
- Configuration → Préférence → Vie privée



Navigation privée (2/2)



Firefox 42 renforce :

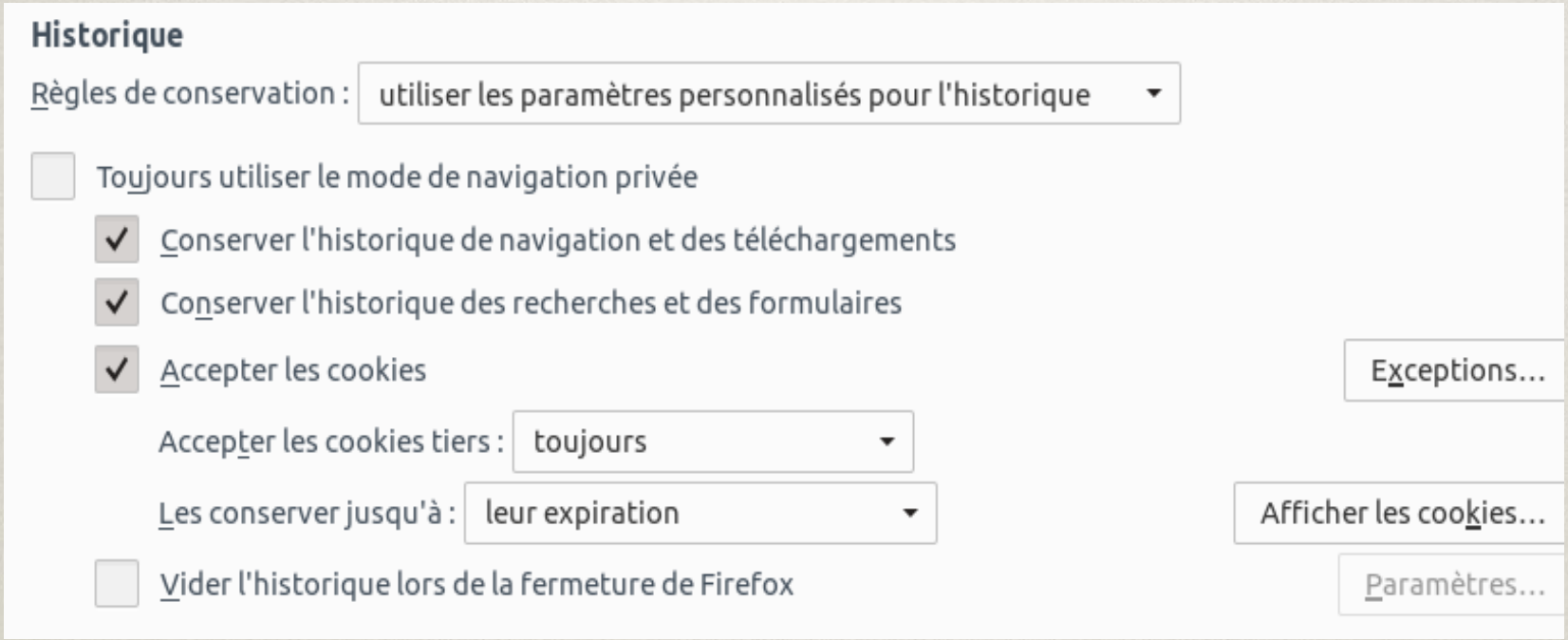
- Les sessions
- Le pistage
- Réglages
- Contre outils analytiques, boutons des réseaux sociaux ou pub

Nettoyage (1/2)

- Quand on quitte le navigateur
  - Réglages de l'historique
- Configuration
  - Préférence → Vie privée

Nettoyage (2/2)

- Quand on quitte le navigateur
  - Réglages sur les cookies
- Configuration
  - Préférence → Vie privée



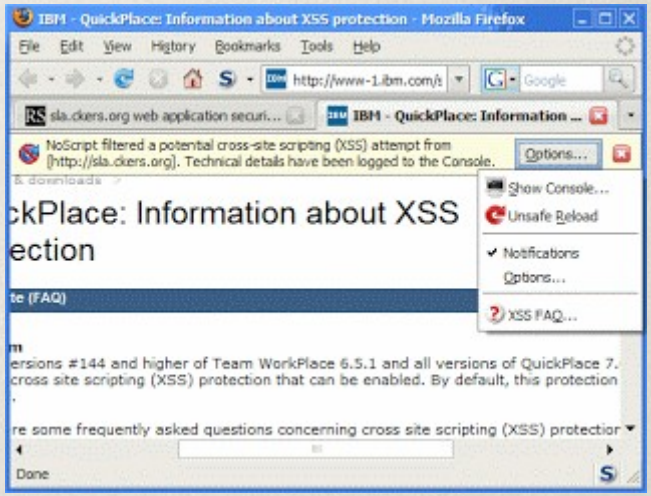
Les extensions

Extensions ?

- Modules = add-ons
- Modules complémentaires
- Améliore le navigateur (thème, collections, fonctionnalités…)
- Milliers d'extensions

No Script

- Module : No Script
- Exécute les scripts Javascript que sur les sites de confiances (ex : banque)
- Blocage en préventif
- Bloque les failles de sécurité sans perte de fonctionnalités



https://addons.mozilla.org/fr/firefox/addon/noscript/

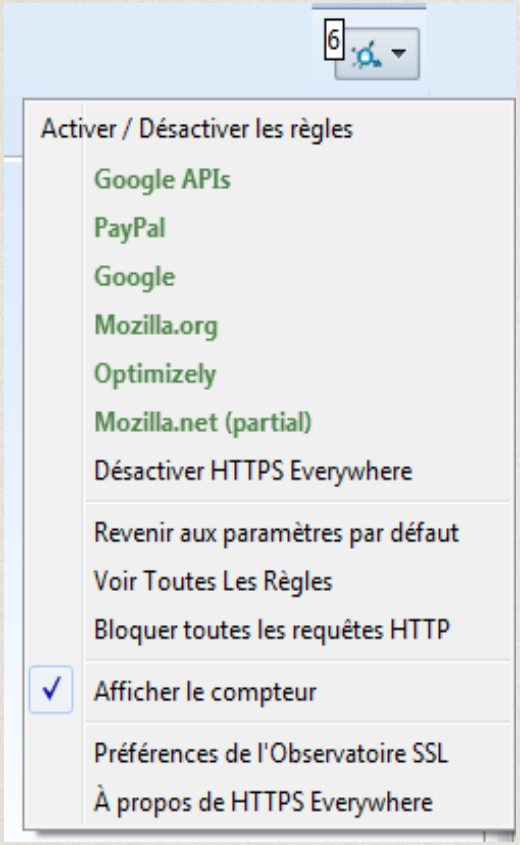
HTTPS Everywhere

- Crypte vos communications avec internet
- Rend illisibles les informations envoyés et reçus
- Différence avec HTTP et HTTPS
- Collaboration entre

  TOR Project et Electronic Frontier Foundation

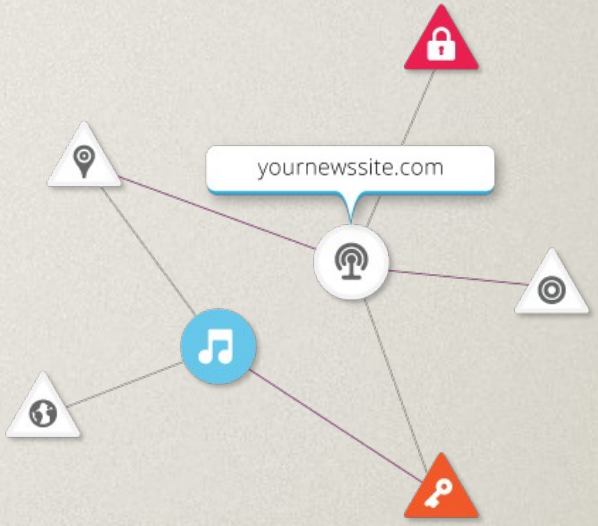
https://addons.mozilla.org/fr/firefox/addon/https-everywhere

HTTPS Everywhere : exemple

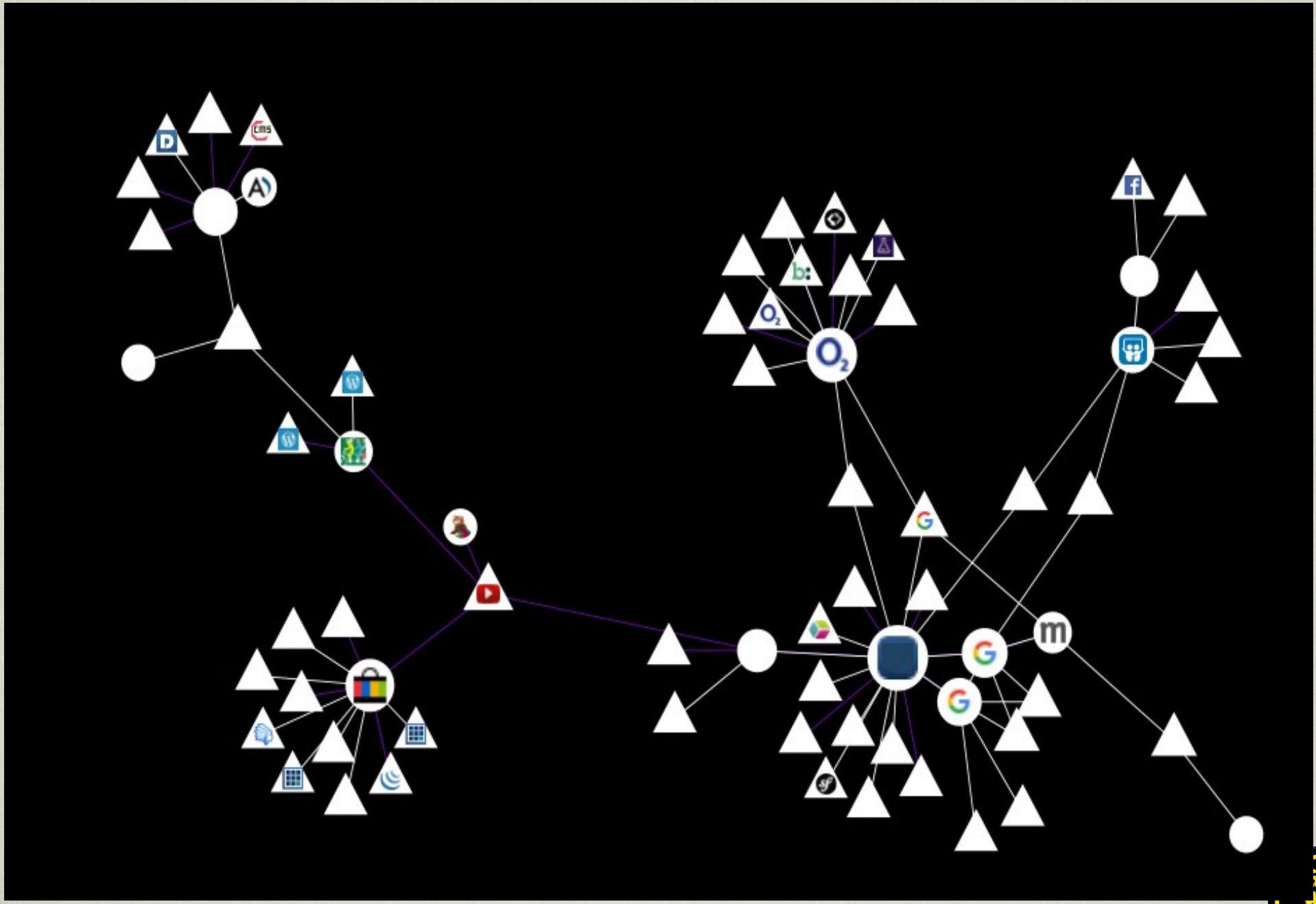


Light beam

- Visualisation interactive
  - Les requêtes vers les sites tiers
  - Les cookies déposés
- Analyse et montre les fuites d'informations
- Enregistre et schématise votre historique de navigation
- Permet de pister les pisteurs
- https://www.mozilla.org/fr/lightbeam/

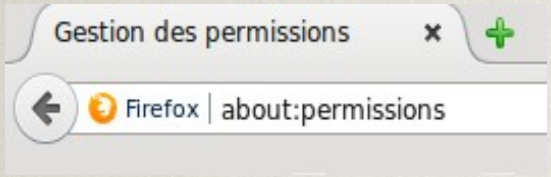


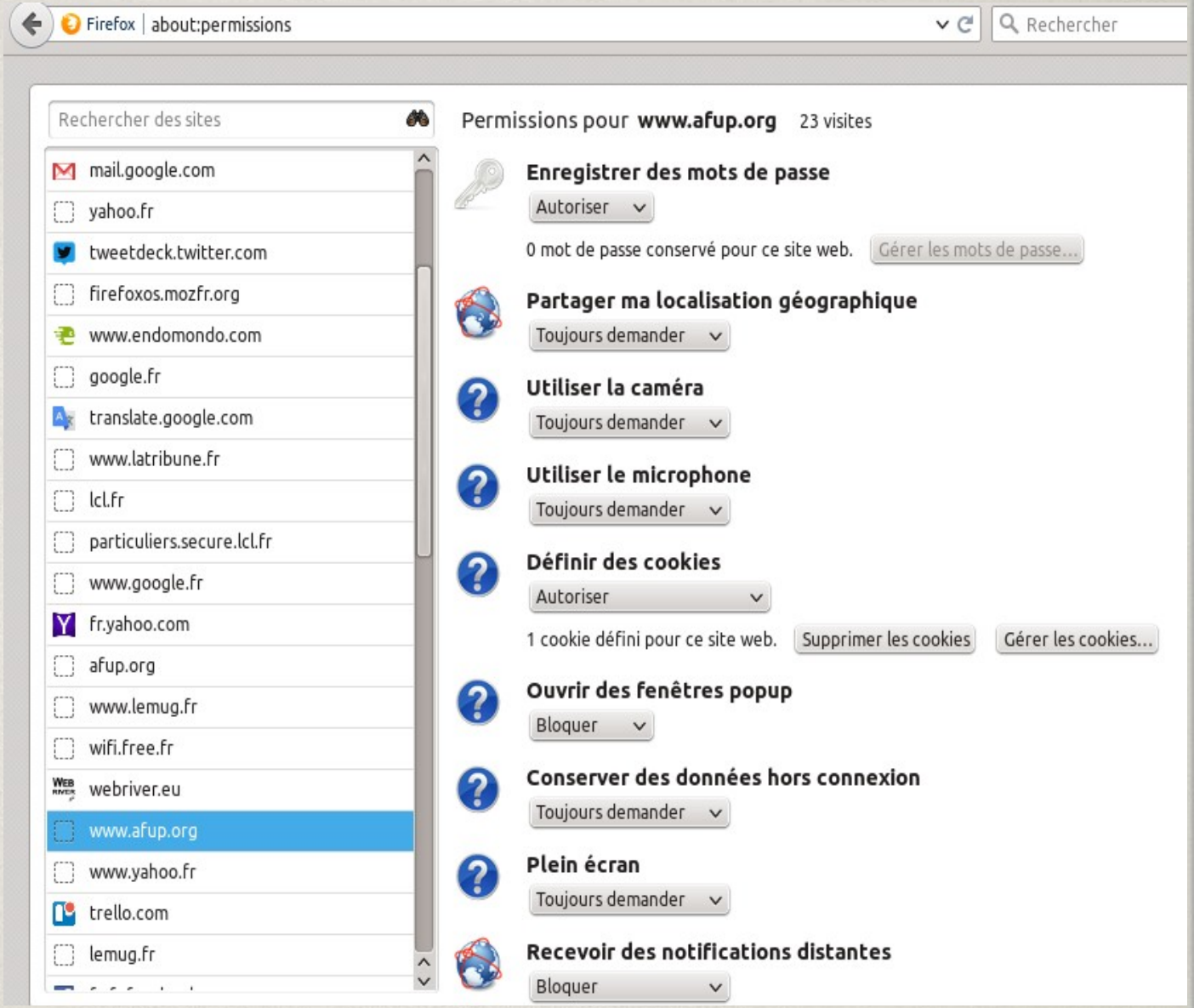
Light beam : exemples (2/2)



Vérification

- Info sur le site

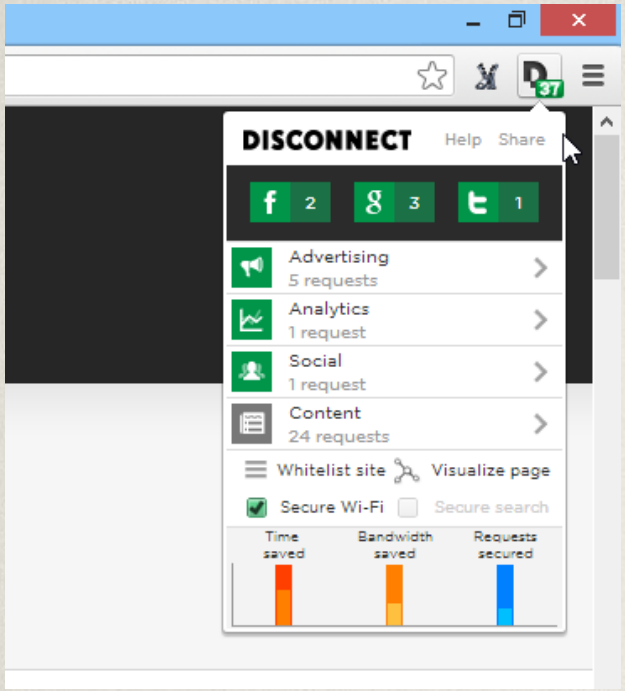


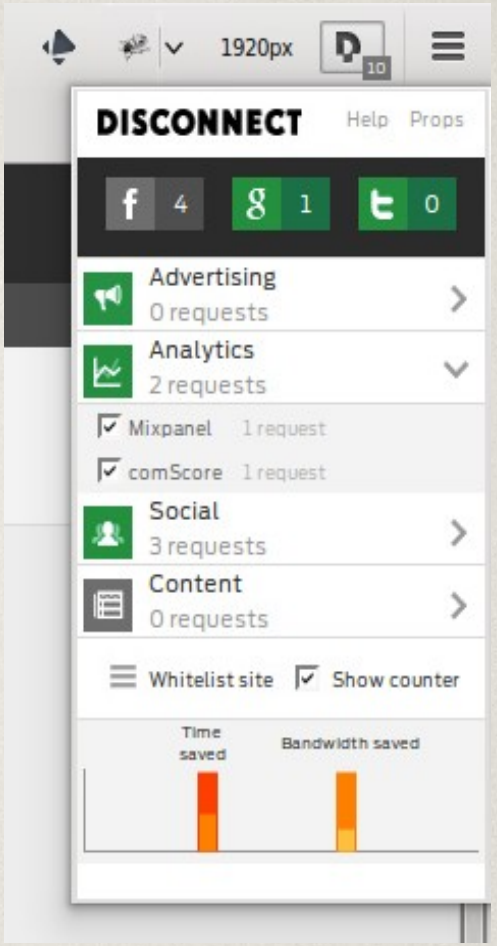


Disconnect

- Accélère le navigateur
- Améliore la vie privée
- Plus sécurisé
- https://addons.mozilla.org/fr/firefox/addon/disconnect/

Disconnect : exemple



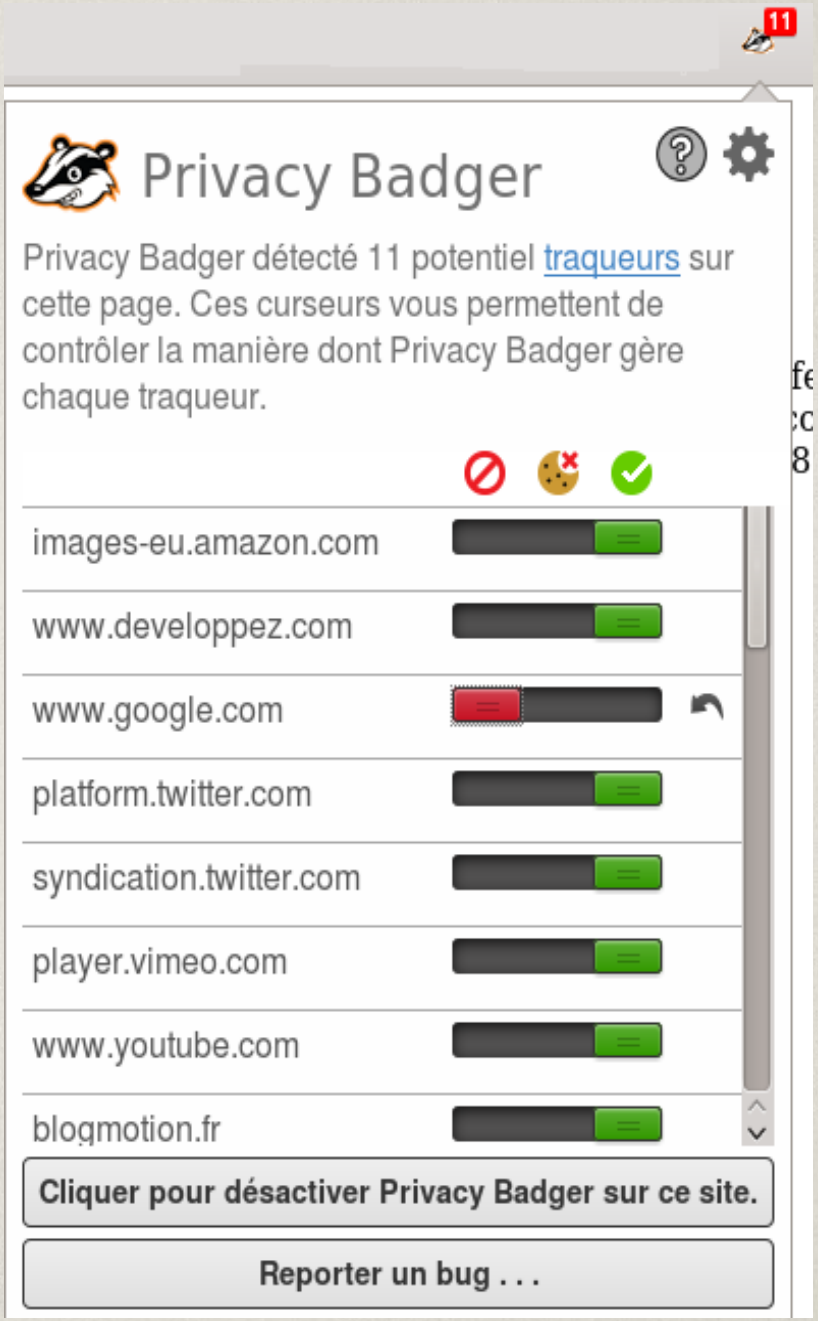


Privacy Badger

- Protège votre vie privée
- Bloque les pisteurs invisibles
- Bloque les espions
- Représenter par :

https://addons.mozilla.org/fr/firefox/addon/privacy-badger-firefox/

Privacy Badger : exemple

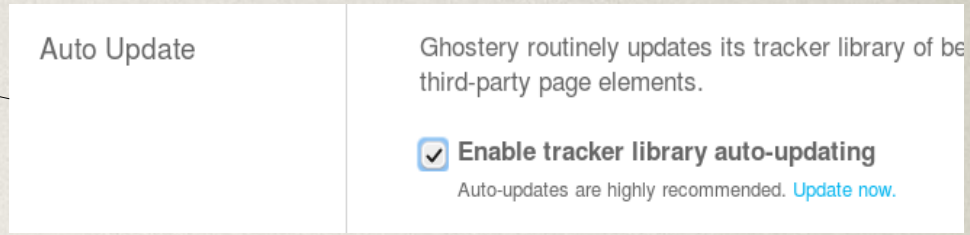


Ghostery

- Protège votre vie privée
- Voit ce qui ne se voit pas sur le Web.
- Surveille votre navigation
- Il détecte
  - les mouchards,
  - les bogues Web,
  - les pixels
  - les balises placés sur les pages Web par Facebook,
- Module à éviter (voir slide précédent)

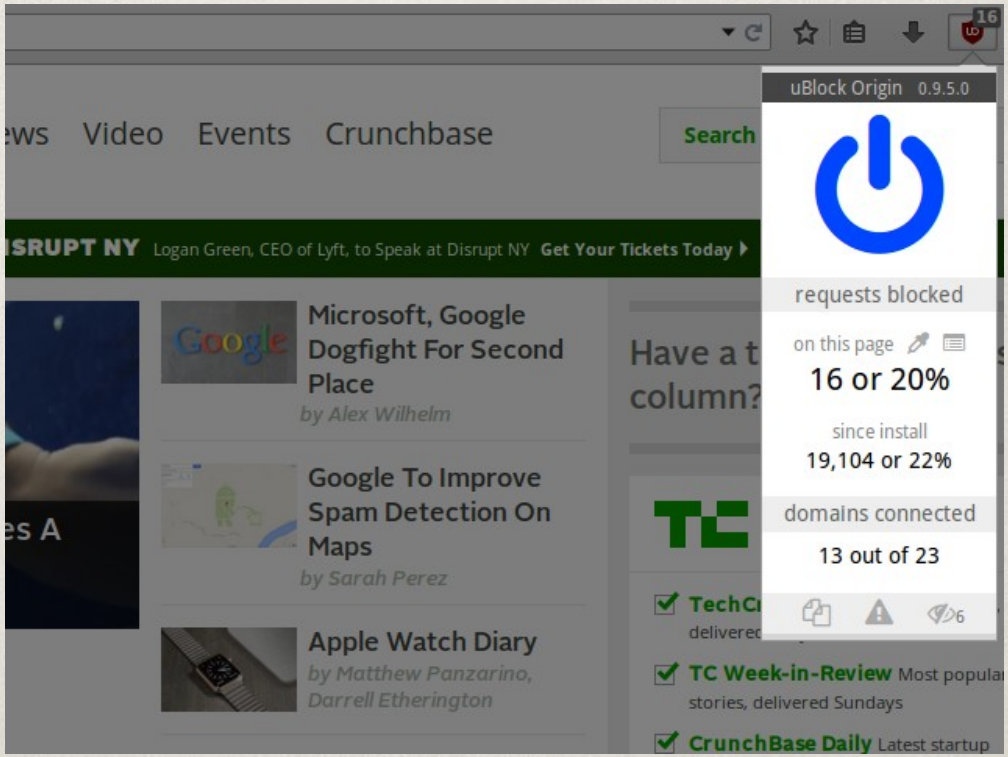
https://addons.mozilla.org/fr/firefox/addon/ghostery/

Ghostery : exemple



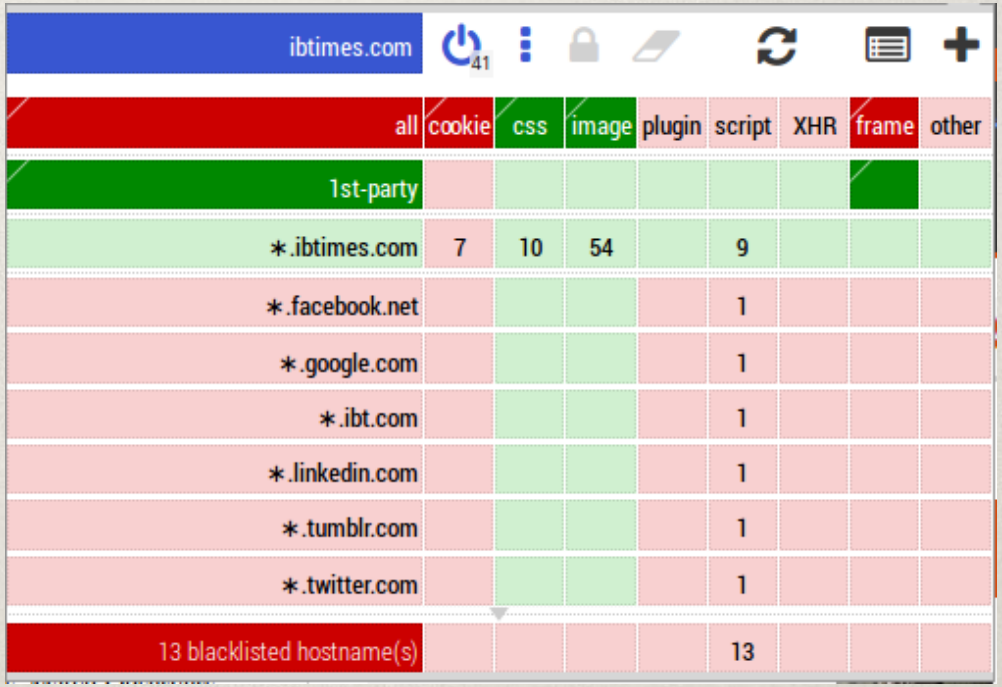
Ublock Origin

- Original : Adblock Plus
- Bloqueur les publicités et les pisteurs
- Traiter des milliers de filtres



uMatrix

- Equivalent à RPC
- Parefeu matriciel
- Configurable à la volée
- Pleins les pouvoirs
- Bloque cookies

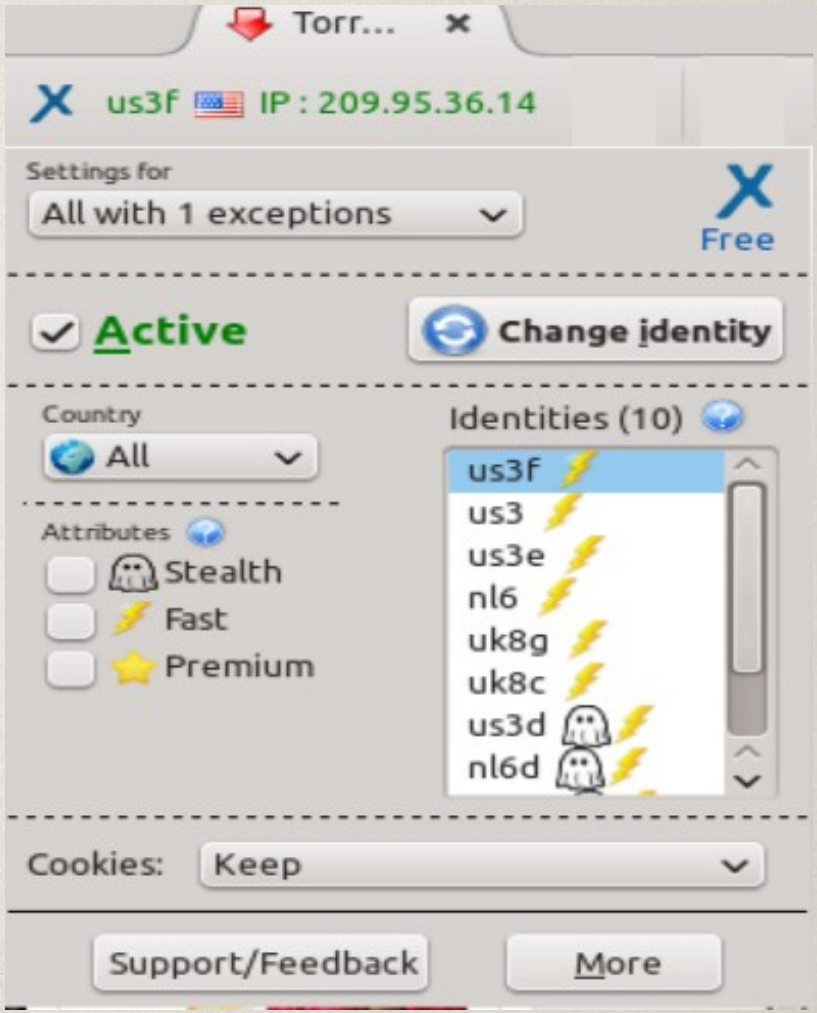


Messagerie

- Addon dans Firefox : Gmail S/Mime
- Va sécuriser
- Va chiffrer vos emails directement sur votre webmail
- Message Gmail

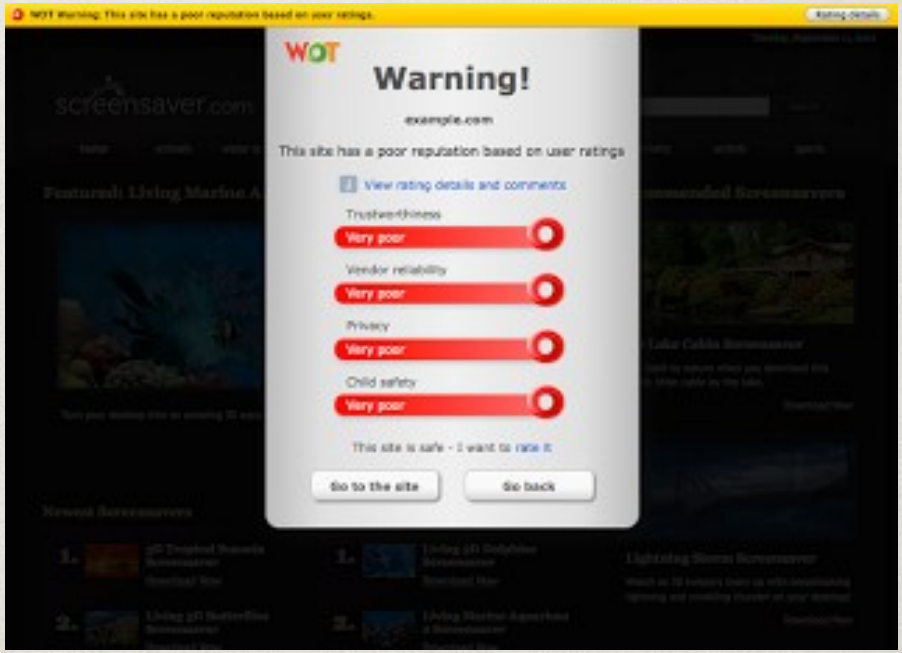
Proxy : Anonymox

- Facilite la navigation anonyme sur Internet.
- Changez l'IP et le pays
- Bloque les sites Web
- Supprimer les cookies
- IP Cachée



Anti Phishing

- Déf : Hameçonnage (obtenir des renseignements personnels)
- Vous renseigne si le site est fiable
- S'appuie sur un partage des utilisateurs à travers le monde



https://addons.mozilla.org/fr/firefox/addon/wot-safe-browsing-tool/

Spam

- Module TrashMail.net
- Obtenir des adresses emails jetables
- Evite les spams

- *A utiliser temporairement*

https://addons.mozilla.org/fr/firefox/addon/trashmailnet/

Mot de passe

- Module Keefox
- Permet de gérer et sécuriser vos mots de passe
- S'intègre à Keepass

https://addons.mozilla.org/fr/firefox/addon/keefox/

Génération de mots de passe

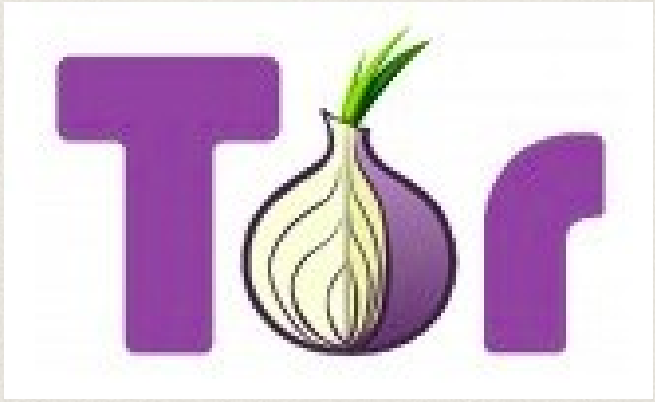
- Module : safe password
- Générateur de mots de passe sécurisé
- Évite de chercher un mot de passe

https://addons.mozilla.org/fr/firefox/addon/safe-password/

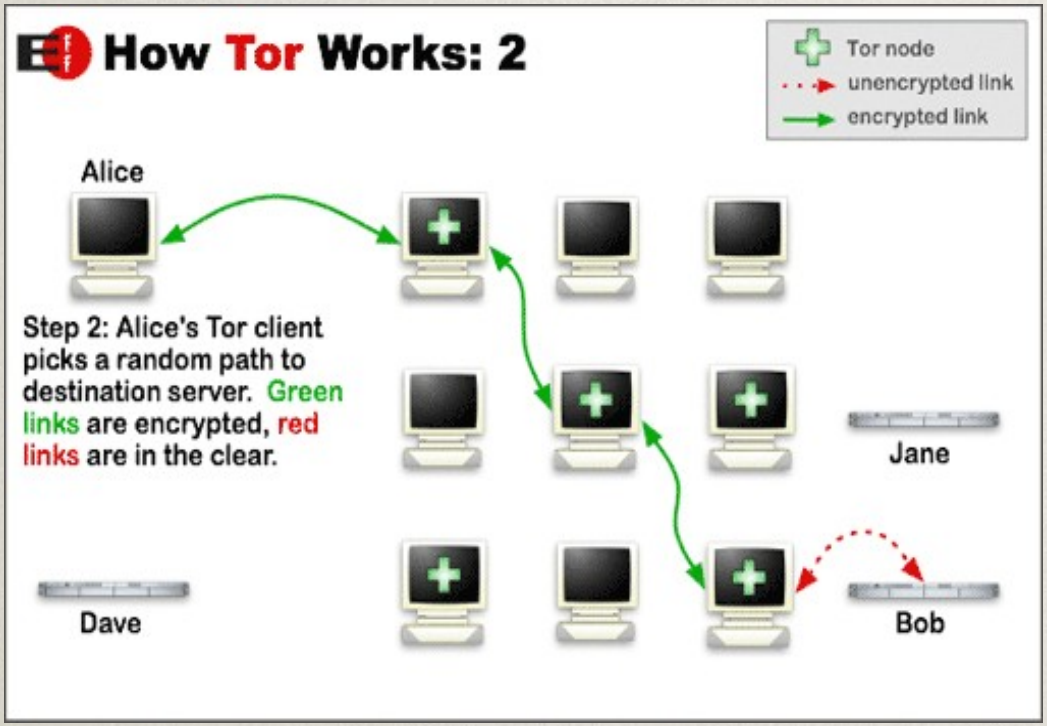

Tor
TorProject.org

Navigation

- Projet TorButton
- Permet de surfer anonymement avec Firefox
- Dispo : https://www.torproject.org/torbutton/



- Tor Browser
- Change automatiquement l'IP
- Blocage de nœuds, publicités...



ANSSI

- = Agence nationale de la sécurité des systèmes d'information
- Source
  - http://www.ssi.gouv.fr/particulier/

- https://www.mozilla.org/en-US/security/
- https://addons.mozilla.org/fr/firefox/extensions/privacy-security/
-

Mozilla Security

Merci

Questions

Christophe Villeneuve
@hellosct1