

# Le réseau Tor

Genma

SCE2015 - 13 juin 2015



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.



# A propos de moi

## Où me trouver sur Internet ?

- Le Blog de Genma
- Twitter : @genma

## Mes projets - contributions

Plein de choses dont :

- Promotion de Tor, traduction...
- A.I.<sup>2</sup> Apprenons l'Informatique, Apprenons Internet

**Le Blog de Genma**

**Rencontre avec Genma IRL.**

publié le 2 août 2013 par **Genma**

Si tu es un lecteur régulier de ce blog, que tu souhaites me voir autour d'un verre, pour manger dans un resto où/ou tout simplement discuter, contacte moi que l'on se fixe un rendez-vous. En effet, je serai disponible du dimanche 11 août au mardi 20 août, en fin de journée ou le soir. À l'endroit que tu souhaites, sur Paris, France. Si tu es partant, fais signe... À la suite de cette rencontre, je pourrais faire (ou non), si tu es d'accord, un petit compte-rendu sur mon blog, ainsi que quelques (...)

**POUR LIRE LA SUITE...**

**Lifehacking - L'importance du matériel**

publié le 2 août 2013 par **Genma**

Un bon artisan doit avoir de bons outils pour faire du bon travail. Le meilleur ouvrier ne sera pas avec lui si son instrument de musique n'est pas de qualité. Il en est de même pour l'informatique. Ce n'est pas la taille qui compte.

En fait... Pendant deux ans, sur ma machine précédente, j'avais pour travailler du bricolage, un écran 15" et un clavier 15" (celui du portable). Ton ordinateur de l'autre. Avec ma nouvelle machine, je suis passé sur un unique écran de 17", avec un PC plus fort (je (...))

**POUR LIRE LA SUITE... TAGS : Lifehacking**

# Introduction



# Présentation du réseau TOR

Tor est l'acronyme de The Onion Router, littéralement « le routeur oignon », en référence au *routage en oignon*.

- Le réseau Tor est composé de routeurs organisés en couches, appelés nœuds de l'oignon, qui transmettent de manière anonyme des flux TCP.
- Tor est un logiciel libre (logiciel client et serveur) soutenu par l'organisation The Tor Project.

# A quoi sert TOR?



# A quoi sert TOR ?

Concrètement, utiliser Tor peut permettre :

- d'échapper au fichage publicitaire,
- de publier des informations sous un pseudonyme,
- d'accéder à des informations en laissant moins de traces,
- de déjouer des dispositifs de filtrage (sur le réseau de son entreprise, de sa Université, en Chine ou en France...),
- de communiquer en déjouant des dispositifs de surveillances,
- de tester son pare-feu,
- ... et sûrement encore d'autres choses.

⇒ Tor dispose également d'un système de « services cachés » qui permet de fournir un service en cachant l'emplacement du serveur.

# Qu'est-ce que TOR ?

Tor peut donc être vu comme un proxy socks5 un peu particulier, par lequel on peut faire passer tout type de connexion (dès lors qu'elle est *de type TCP*).

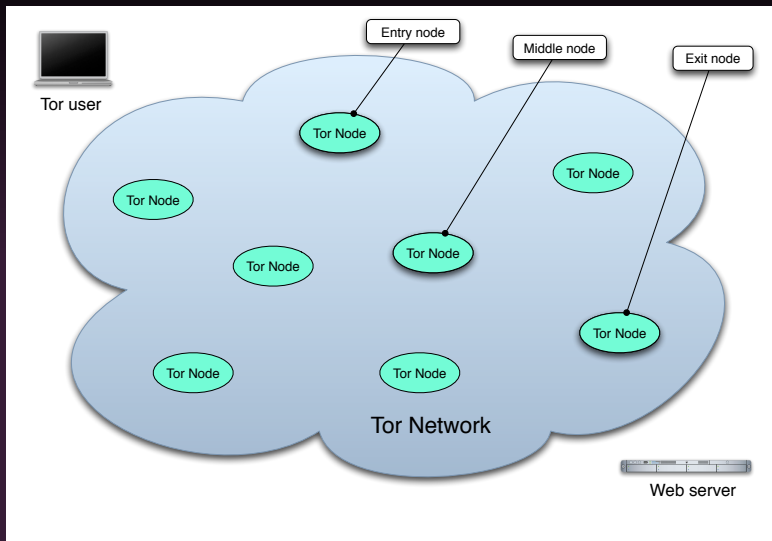
Rq : comme il s'agit d'un proxy, on peut lui associer un autre logiciel qu'un navigateur dès lors que ce dernier accepte de se connecter via un proxy (client de messagerie par exemple).

# Comment fonctionne Tor ?





# Comment fonctionne Tor ?



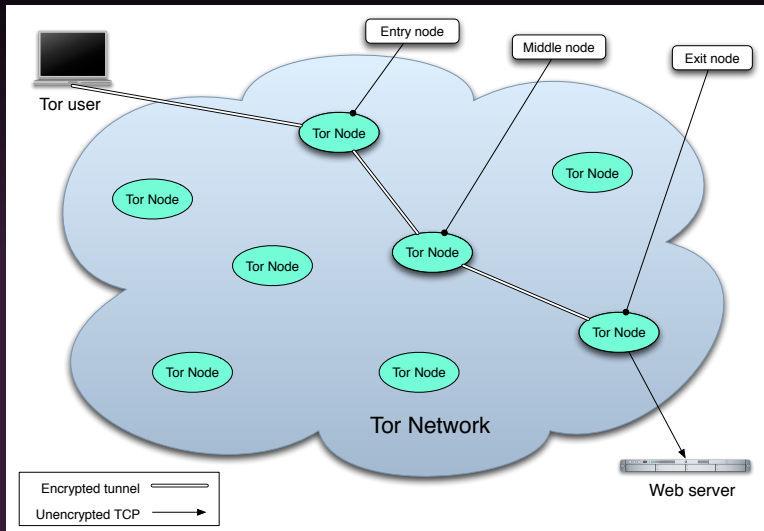
# Comment fonctionne Tor ?

- Tor fait un routage en oignon avec des couches de chiffrement empilées.
- Le client sélectionne trois noeuds (à minima) parmi les différents "relais" Tor disponibles.
- Il sélectionne un noeud d'entrée, un noeud de sortie et un ou plusieurs noeuds intermédiaires (selon sa configuration).

⇒ Attention : Tor ne chiffre pas après le noeud de sortie.

⇒ Il faut utiliser une connexion httpS (les clés étant négociées entre le client et le serveur web final).

# Comment fonctionne Tor ?



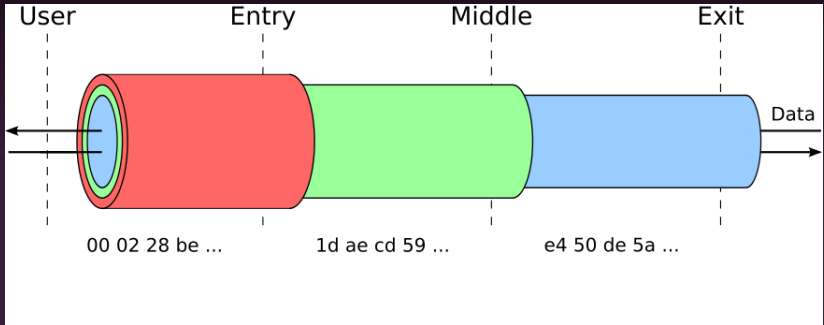
# Comment fonctionne Tor ?

Rq : cette partie est peu documenté et assez complexe.

Après sélection des différents "noeuds-relais" dans le réseau, le client effectue un échange de clefs de sessions (Diffie-Hellman). Il y a une première clé de chiffrement pour le noeud d'entrée, une seconde clé pour le noeud du milieu et une dernière pour le noeud de sortie.

- Chaque noeud envoie donc une clé de session.
- Le premier noeud envoie sa clé au client.
- Le deuxième noeud envoie sa clé au 1er noeud qui la chiffre avec la clé négociée avec le client et l'envoie au client.
- Idem pour le troisième noeud (qui envoie de sa clé au 2nd noeud...)

# Comment fonctionne Tor ?



# Comment fonctionne Tor ?

Une fois les clés de sessions échangées,

- Le client chiffre le paquet avec les 3 clés de session, l'envoie au 1er noeud qui pèle la première couche,
- qui l'envoie au deuxième noeud qui pèle la deuxième couche de chiffrement,
- et ainsi de suite jusqu'au noeud de sortie.

# Comment fonctionne Tor ?

Une fois le paquet arrivé au noeud de sortie

- La requête est envoyé au serveur web par le noeud de sortie (qui expose donc son adresse IP).
- Le noeud de sortie reçoit la réponse.

# Comment fonctionne Tor ?

Une fois la réponse reçue, les différents noeuds savent quel paquet doit suivre quel circuit car ils enregistrent la correspondance IP/Port source (*une sorte de NAT*).

- Pour le chemin inverse, le dernier noeud chiffre avec sa clé de session ;
- le passe au noeud d'avant qui chiffre aussi avec sa clé de session
- jusqu'à remonter au client qui déchiffre les couches avec les clés qu'il a reçu lors de la construction du circuit.

Ainsi au niveau des échanges client noeud d'entrée, le paquet est chiffré par  $n$  fois ( $n$  étant le nombre de noeud).



# Tor hidden service

## les services cachés de TOR



# Tor hidden service - les services cachés de TOR 1/3

Tor permet aux clients et aux relais d'offrir des services cachés. Il est possible de proposer l'accès à un serveur web, un serveur SSH, etc, sans révéler son adresse IP aux utilisateurs.

- Tous ces sites ne sont accessibles que via le réseau Tor.
- Ils portent une adresse qui se termine par .onion.
- Des wikis et moteurs de recherches référencient ces services.

# Tor hidden service - les services cachés de TOR 2/3

## Exemple de sites existants ayant une adresse .onion

- Duckduckgo `http://3g2upl4pq6kufc4m.onion`
- Facebook : `https://facebookcorewwi.onion`
- Le blog de Stéphane Borztemeyer  
`http://7j3ncmar4jm2r3e7.onion`
- Techn0polis d'Amaelle Guiton  
`http://ozawuyxtechnopol.onion`

⇒ Il existe des annuaires /wiki listant les sites en .onion

# Tor hidden service - les services cachés de TOR 3/3

## Tutoriaux pour mettre en place un .onion

- Configuring Hidden Services for Tor  
<https://www.torproject.org/docs/tor-hidden-service.html.en>
- Tor, les .onion, le "darknet" à votre portée par Benjamin Sonntag  
<https://benjamin.sonntag.fr/Tor-les-onion-le-darknet-a->
- Mon blog dans les oignons par Stéphane Bortzmeyer  
<http://www.bortzmeyer.org/blog-tor-onion.html>

Comment utiliser Tor ?



# Utiliser Tor - Le Tor Browser

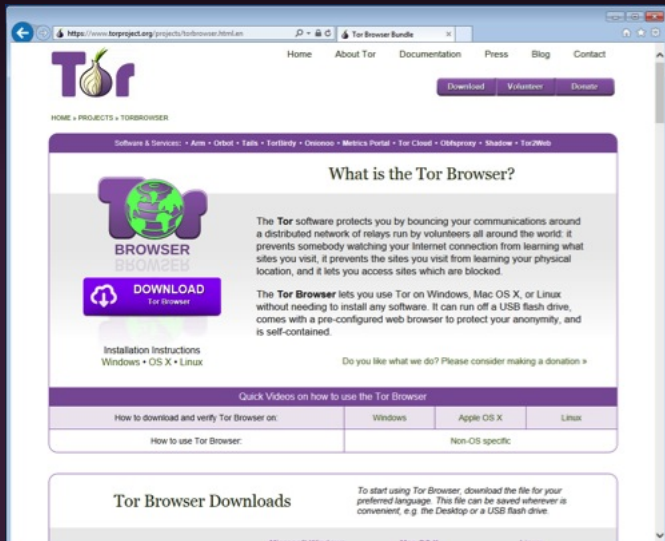
Le Tor Browser est basé sur la version Extended Support de Firefox, auxquelles sont ajoutée les extensions préconfigurées permettant qu'au lancement du navigateur, celui-ci se connecte à Tor.

⇒ Ainsi, toute la navigation qui se fait via ce navigateur est faite au travers du réseau Tor.

# Télécharger le Tor Browser

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet :

<https://www.torproject.org/>



The screenshot shows the Tor Project website's page for downloading the Tor Browser. The browser's address bar displays the URL <https://www.torproject.org/projects/torbrowser.html.en>. The page features the Tor logo (a purple onion) and a navigation menu with links: Home, About Tor, Documentation, Press, Blog, and Contact. Below the navigation menu are buttons for Download, Volunteer, and Donate. The main content area is titled "What is the Tor Browser?" and includes a sub-header "Software & Services: • Arm • Orbot • Tails • Tortillero • Onionoo • Metrics Portal • Tor Cloud • Obfsproxy • Shadow • Tor2Web". The central graphic shows the Tor Browser logo with a globe and a "DOWNLOAD Tor Browser" button. To the right of the graphic, text explains that the Tor software protects users by bouncing communications around a distributed network of relays, preventing surveillance and access to blocked sites. It also states that the Tor Browser allows using Tor on Windows, Mac OS X, or Linux without installing additional software. Below this, there is a link to "Installation Instructions" for Windows, OS X, and Linux, and a link to "Do you like what we do? Please consider making a donation". A section titled "Quick Videos on how to use the Tor Browser" contains a table with links to videos for downloading and using the browser on different operating systems.

| Quick Videos on how to use the Tor Browser |                 |            |       |
|--|-----------------|------------|-------|
| How to download and verify Tor Browser on: | Windows         | Apple OS X | Linux |
| How to use Tor Browser:                    | Non-OS specific |            |       |


**Tor Browser Downloads**

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

# Vérifier le Tor Browser téléchargé

Via les clefs GPG, cf. le tuto sur le site de Tor.

<https://www.torproject.org/docs/verifying-signatures.html>



HomeAbout TorDocumentationPressBlogContact

DownloadVolumeerDonate

HOME » VERIFYING SIGNATURES

Documentation Overview

▼ Installation Guides

Installing on Windows

Installing on Linux/BSD/Unix

Installing Tor on Debian/Ubuntu

Installing Tor on Fedora/CentOS

Installing Tor on Mac OS X

Installing Tor on Android

Installing Tor on Maemo/N900

Verify our GPG signatures

► Manuals

Tor Wiki

General FAQ

Abuse FAQ

Trademark FAQ

Tor Legal FAQ

Tor DMCA Response

## How to verify signatures for packages

### What is a signature and why should I check it?

How do you know that the Tor program you have is really the one we made? Many Tor users have very real adversaries who might try to give them a fake version of Tor — and it doesn't matter how secure and anonymous Tor is if you're not running the real Tor.

An attacker could try a variety of attacks to get you to download a fake Tor. For example, he could trick you into thinking some other website is a great place to download Tor. That's why you should always download Tor from <https://www.torproject.org/>. The https part means there's encryption and authentication between your browser and the website, making it much harder for the attacker to modify your download. But it's not perfect. Some places in the world block the Tor website, making users try [something else](#). Large companies sometimes force employees to use a modified browser, so the company can listen in on all their browsing. We've even [seen](#) attackers who have the ability to trick your browser into thinking you're talking to the Tor website with https when you're not.

Some software sites list [SHA1 hashes](#) alongside the software on their website, so users can verify that they downloaded the file without any errors. These "checksums" help you answer the question "Did I download this file correctly from whoever sent it to me?" They do a good job at making sure you didn't have any random errors in your download, but they don't help you figure out whether you were downloading it from the attacker. The better question to answer is: "Is this file that I just downloaded the file that Tor intended me to get?"

### Where do I get the signatures and the keys that made them?

Each file on [our download page](#) is accompanied by a file with the same name as the package and the extension ".asc". These ".asc" files are GPG signatures. They allow you to verify the file you've downloaded is exactly the one that we intended you to get. For example, `torbrowser-install-4.5_en-US.exe` is accompanied by `torbrowser-install-4.5_en-US.exe.asc`. For a list of which developer signs which package, see our [signing keys](#) page.

### Windows

You need to have GnuPG installed before you can verify signatures. Download it from <http://gnupg4win.org/download.html>.

Once it's installed, use GnuPG to import the key that signed your package. Since GnuPG for Windows is a command-line tool, you will need to use `cmd.exe`. Unless you edit your `PATH` environment variable, you will need to tell Windows the full path to the GnuPG program. If you installed GnuPG with the default values, the path should be something like this: `C:\Program Files\GnuPG\gpg.exe`.



# Installer le Tor Browser

Le Tor Browser s'installe comme n'importe quel logiciel Windows, OS X. (voir les tutoriaux si besoin).

Rq : le Tor Browser déclenche une alerte avec la suite Symantec (faux positif).

Pour Ubuntu, GNU/Linux c'est un programme autonome/portable. On peut aussi l'installer en compilant les sources.

# Lancer le Tor Browser

A propos de Tor - Navigateur Tor

A propos de Tor

Saisir un terme à rechercher ou une adresse

Google

Le menu de l'oignon vert a maintenant un curseur de sécurité qui vous laisse ajuster votre niveau de sécurité. Découvrez le !

Ouvrir préférences de sécurité

Navigateur Tor 4.5



## Félicitations !

Ce navigateur est configuré pour utiliser Tor.

Vous pouvez maintenant naviguer sur Internet de manière anonyme.

[Tester les paramètres du réseau Tor](#)



### Que faire ensuite ?

Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.

[Conseils pour rester anonyme »](#)

### Vous pouvez aider !

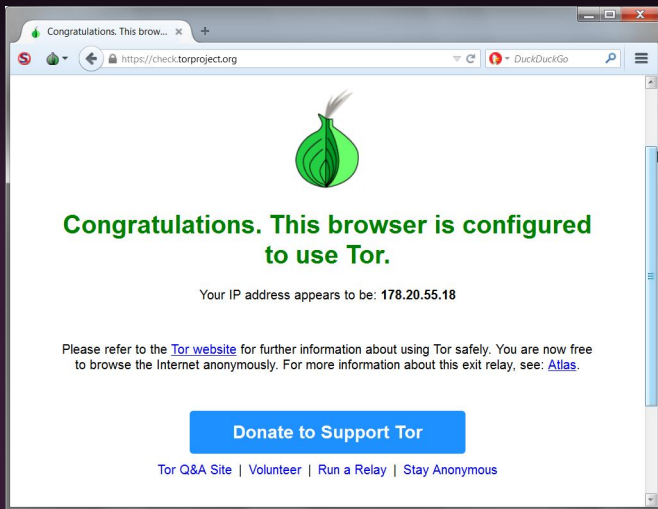
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relais Tor »](#)
- [Devenir bénévole »](#)
- [Faire un don »](#)

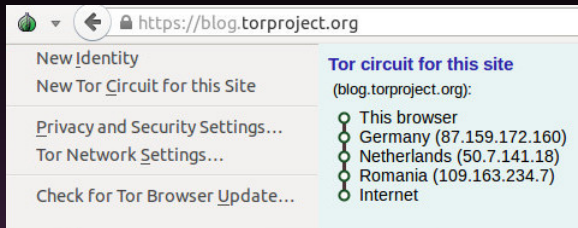
Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor »](#)

# Comment être sûr qu'on est bien connecté à Tor ?

`https://check.torproject.org/`



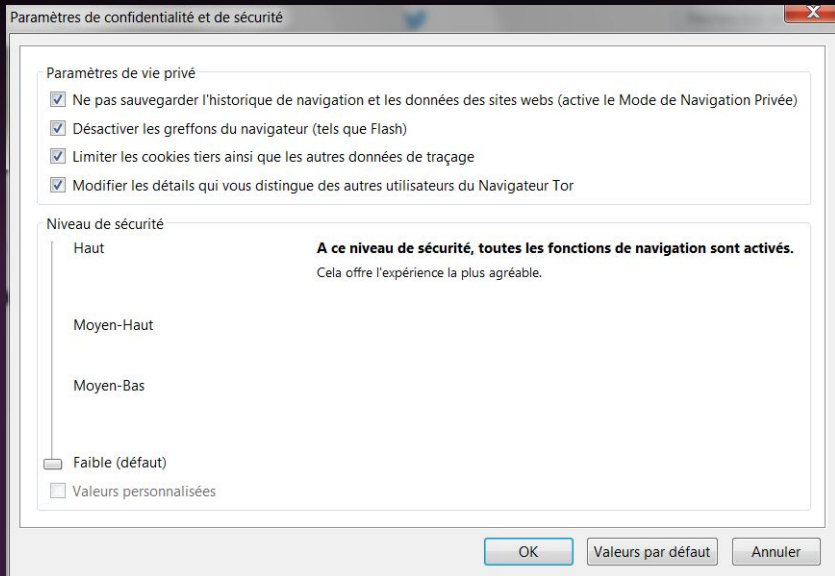
# Les nouveautés de la version 4.5 1/2



## Pour la vie privée

- Visualisation du circuit emprunté (désactivable) ;
- Changement de circuit par onglets ;
- Cloisonnement des applications tierces à l'onglet ;
- Moteur de recherche par défaut : Disconnect (qui fournit des résultats de recherche Google).

# Les nouveautés de la version 4.5 2/2



# Les nouveautés de la version 4.5 2/2

## Le curseur de sécurité

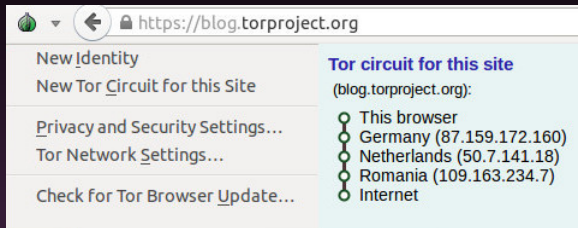
- Haut - JavaScript est désactivé sur tous les sites par défaut, certains types d'images sont désactivées.
- Moyen-Haut - Tous les optimisations de performances JavaScript sont désactivés, certains police fonctionnalités de rendu sont désactivées, JavaScript est désactivé sur tous les non-sites HTTPS par défaut.
- Moyen-Bas - HTML5 audio et vidéo sont en mode click-to-play, quelques optimisations de performances JavaScript sont désactivés, les fichiers JAR à distance sont bloqués et quelques méthodes pour afficher des équations mathématiques sont désactivées.
- Faible (par défaut) - Toutes les fonctions du navigateur sont activés.

La compatibilité diminue et la sécurité augmente avec chaque niveau de sécurité.

# Maintenir le Tor Browser à jour ?



# Vérifier et installer les mises à jour



## Depuis un TorBrowser

- Cliquer sur "Vérifier les mises à jour"

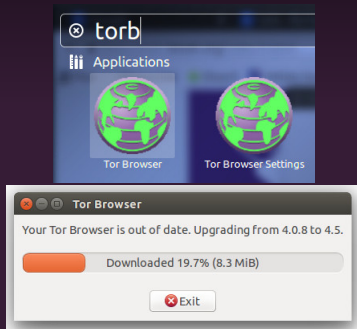
La mise à jour se fait via Tor.



# Tor Browser Launcher

Pour avoir un Tor Browser toujours à jour, on peut installer le Tor Browser Launcher.

<https://github.com/micahflee/torbrowser-launcher>



# Tor Browser Launcher

Il gère :

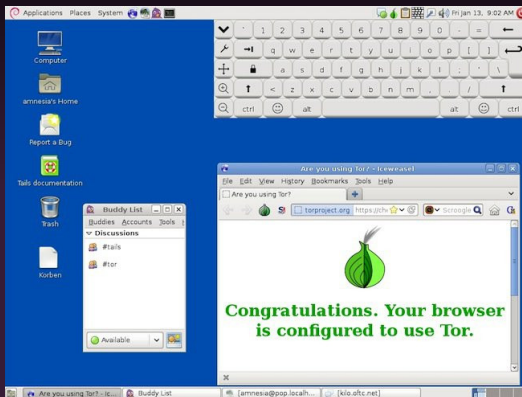
- le téléchargement de la version la plus récente de TBB, dans votre langue et pour votre architecture ;
- la mise à jour automatique (tout en conservant vos signets et préférences) manuel ;
- la vérification de la signature GnuPG du TBB (pour être sûr de l'intégrité des fichiers) ;
- ajoute un lanceur d'application "Tor Browser" dans le menu de votre environnement de bureau.



<https://tails.boom.org>

# Utiliser Tor - Tails

Tails (The Amnesic Incognito Live System) est un système d'exploitation complet basé sur Linux et Debian, en live.



<https://tails.boom.org>

Vous voulez que Tor  
marche vraiment ?



# Vous voulez que Tor marche vraiment ?

Vous devrez changer quelques-unes de vos habitudes, et certaines choses ne marcheront pas exactement comme vous le voudrez.

- Ne faites pas de Torrent via Tor.
- N'activez pas et n'installez pas de plugins dans le navigateur.
- Utiliser la version HTTPS des sites webs.
- Comme avec un navigateur "normal", ne consultez pas/n'ouvrez pas de documents téléchargé pendant que vous êtes connecté si ceux-ci présentent "un risque".
- Un noeud de sortie malveillant peut corrompre un binaire...

# Limites à l'usage de Tor



# Limites à l'usage de Tor

## Utiliser Tor amène certaines contraintes pour l'utilisateur

- Il n'y a pas de plugin flash (mais les vidéos HTML5 passent).
- Il faut régulièrement activer le javascript (avec parcimonie).
- Beaucoup de noeuds de sorties sont bloqués (Cloudflare) etc.
- Il y a nécessité de saisir des captchas pour ne pas être assimilé à un bot (et d'activer le javascript).
- On ne peut pas créer de compte (Gmail, Twitter...)
- On sait qu'on utilise TOR (sauf si on utilise l'obfuscation).



# Soutenir le projet Tor

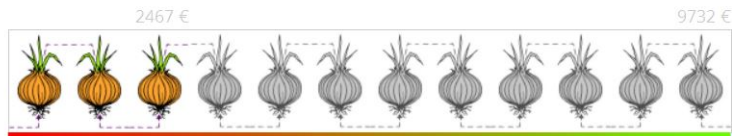


# Soutenir le projet Tor 1/3

## NosOignons

L'association NosOignons.net propose des nœuds de sortie Tor financés par la communauté. <https://nos-oignons.net>

### État de la trésorerie



Un oignon correspond à 1 mois de fonctionnement.

Au delà de 6 mois, nous essayons de mettre en place un nouveau relai. En dessous de 3 mois, nous serons amenés à fermer un relai existant.

# Soutenir le projet Tor 2/3

## Tor Project

- Devenir membre de la communauté Tor, Tails
- Contribuez au code...
- Faire des tutoriaux, de la traduction...

⇒ <https://www.torproject.org/>

# Soutenir le projet Tor 3/3

## Enlever les noeuds de sortie Tor des listes noires

Si vous utilisez Cloudflare pour protéger votre site, un script ajoute les relais/noeud de sortie sur une white-liste :

<https://github.com/DonnchaC/cloudflare-tor-whitelister>

⇒ Cela permet aux utilisateur de Tor ne pas avoir à saisir de *captcha*.

# Questions et discussion

# Annexes

# La commande Torify

Torify est une commande qui, placée devant le nom d'une commande/d'un programme qui utilise le réseau, permet que ce dernier/cette dernière fasse passer son trafic par TOR. Ainsi, n'importe quelle application pourra passer par TOR au lieu de se connecter directement à Internet, et ce, à la demande de l'utilisateur.

# TorBirdy

TorBirdy est une extension pour le courriel Thunderbird qui permet de faire la réception et l'envoi de mail en passant par Tor (on n'expose alors pas sa propre IP aux serveurs IMAP/SMTP).