

Le réseau Tor

Genma

Ubuntu Party - 30-31 mai 2015





A propos de moi

Où me trouver sur Internet ?

- Le Blog de Genma :
<http://genma.free.fr>
- Twitter :
<http://twitter.com/genma>

Mes projets-contributions

Plein de choses dont :

- Promotion de Tor
- A.I.² Apprenons l'Informatique, Apprenons Internet

Le Blog de Genma

Rencontre avec Genma IRL
publié le 9 août 2013 par Genma

Si tu es un lecteur régulier de ce blog, que tu es habitué de me voir autour d'un verre, pour manger dans un resto d'être tout simplement d'habitude, attends moi sur l'un ou l'autre de nos rendez-vous. En effet, je serai disponible du dimanche 11 août au mardi 13 août, en fin de journée ou le soir. L'endroit sera tu es habitué, sur Paris, France. Si tu ne parles, français... A la suite de cette rencontre, je pourrais faire (ou non), et tu es d'accord, un post-mortem rendu sur mon blog, ainsi que suivantes (...)

POUR LIRE LA SUITE...
f t 6

Lifelacking - 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 moulin ne sera pas aussi bon si son mécanisme de moulin n'est pas de qualité. Il en est de même pour l'informatique. Et n'est pas le fait sur simple.

En fait, pendant deux ans, sur ma mission précédente, j'avais pour travailler du matériel. Un écran 22" et un écran 15" (celui du portable). Un ordinateur de l'autre. Avec ma nouvelle mission, je suis passé sur un unique écran de 17", avec un PC plus lent (je (...))

POUR LIRE LA SUITE... TAGS : Lifelacking
f t 6

Syndication
chabot

Date de mise à jour :
Le 9 août 2013

rechercher

Catégorie :
Actualités GEEK de la semaine
Blog - tout et rien

Remerciements

Je remercie l'association NosOignons.net, qui propose des nœuds de sortie Tor financés par la communauté. <https://nos-oignons.net>



Introduction



Présentation du réseau TOR

Tor est un logiciel libre,

- grâce auquel existe le réseau d'anonymisation Tor
- soutenu par l'organisation The Tor Project.

⇒ Techniquement, Tor nous permet de se connecter à des machines sur Internet via des relais.

⇒ Et cela de façon à ce qu'elles ne puissent pas identifier notre connexion (et donc de nous localiser).

A quoi sert TOR?



A quoi sert TOR ?

Concrètement, ça sert pour :

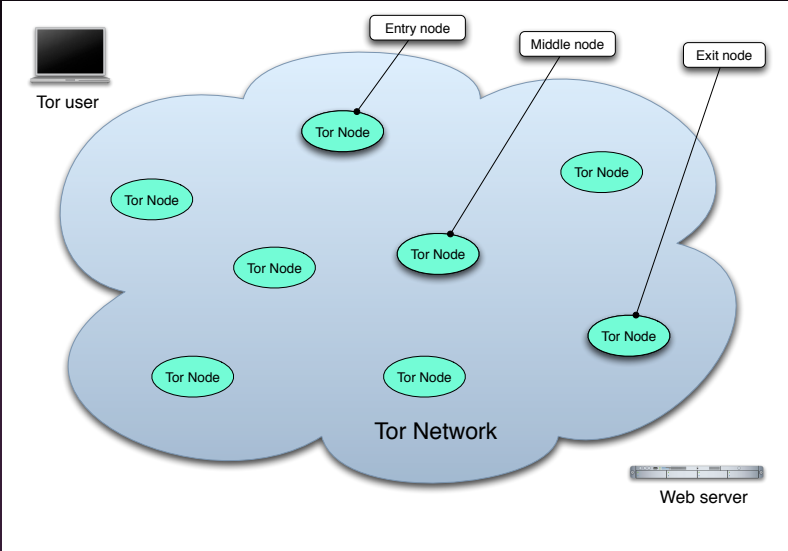
- échapper au fichage publicitaire,
- publier des informations sous un pseudonyme,
- accéder à des informations en laissant moins de traces,
- déjouer des dispositifs de filtrage (dans sa fac, en Chine ou en Iran...),
- communiquer en déjouant des dispositifs de surveillances,
- tester son pare-feu,
- ... 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.

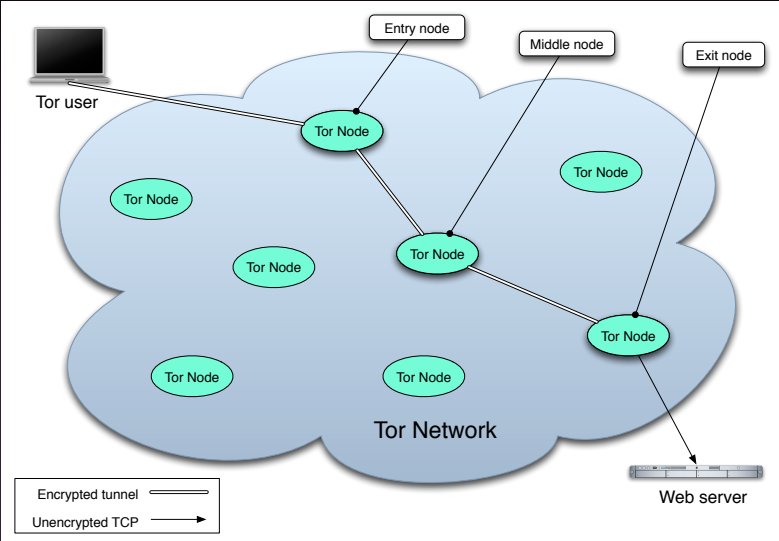
Comment fonctionne Tor ?



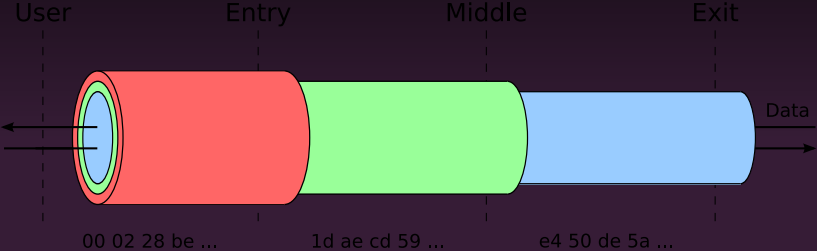
Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?

- Tor fait un routage en oignon avec des couches de chiffrement empilées.
- Il y a une première clé de chiffrement pour le nœud d'entrée, une seconde clé pour le nœud du milieu et une dernière pour le nœud de sortie.
- La résolution DNS est faite par le nœud de sortie.

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

⇒ Il faut utiliser une connexion `https`.

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>

Analogie pour bien comprendre



Cas 1 - Http

Imaginer une zone pavillonnaire avec différentes maisons dont celle de votre ami.

- Toutes les maisons ont des murs transparents.
- On vous voit aller chez lui, on peut entendre ce que vous dites et voir ce que vous faites.

Il s'agit là d'une connexion http à un site web.

Cas 2 - Hhttps

Les maisons ont des murs pleins.

- On vous voit aller chez lui, mais on peut plus entendre ce que vous dites et voir ce que vous faites (on met de côté l'aspect micro/caméra).
- Mais on sait à quelle heure vous êtes venu le voir et quand vous repartez.

Il s'agit là d'une connexion https à un site web.

Cas 3 - Connexion via TOR

Dans la zone pavillonnaire, il y a des maisons 'Tor' qui sont un peu particulières. À savoir : elles ont forcément des murs pleins et 'Tor' écrit dessus.

- vous entrez dans une première maison Tor, et en ressortez avec un déguisement,
- puis vous entrez dans une seconde maison au hasard et en ressortez avec un autre déguisement
- et entrez enfin dans une troisième maison au hasard et en ressortez avec un autre déguisement.

Et quand on sort déguisé de la dernière maison 'Tor', on va chez l'ami qui peut avoir des murs pleins ou des murs transparents mais ce n'est pas une maison 'Tor'.

Cas 4 - les Hidden Services

- Vous entrez dans différentes maisons TOR, en ressortez déguisé.
- Sauf qu'à la dernière maison, vous y entrez par la porte située à l'arrière de la maison, côté jardin.

On ne voit même pas que vous êtes entré et resté dans cette dernière maison...

Comment utiliser Tor ?



Utiliser Tor - Le Tor Browser

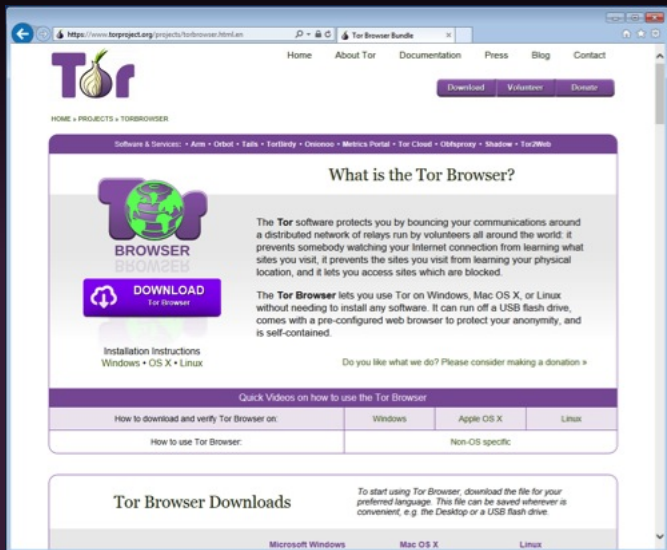
Le Tor Browser est une version Extended Support de Firefox, auxquelles sont ajoutée les extensions préconfigurées permettant qu'au lancement du navigateur, celui-ci se connecte à Tor.

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

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

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

Télécharger le Tor Browser



The screenshot shows the Tor Project website's page for downloading the Tor Browser. The browser's address bar shows the URL <https://www.torproject.org/projects/torbrowser.html.en>. The page features the Tor logo (a purple onion) and navigation links for Home, About Tor, Documentation, Press, Blog, and Contact. A purple navigation bar contains buttons for Download, Volunteer, and Donate. Below this, a breadcrumb trail reads HOME > PROJECTS > TORBROWSER. A secondary navigation bar lists various software and services: Arm, Orbot, Tails, TorBirdy, Onionoo, Metrics Portal, Tor Cloud, Obfsproxy, Shadow, and Tor2Web. The main content area is titled "What is the Tor Browser?" and includes a graphic of the Tor logo with a globe. The text explains that the Tor software protects users by bouncing communications around a distributed network of relays. A prominent purple "DOWNLOAD" button with a download icon is visible. Below the button are links for "Installation Instructions" and "Windows • OS X • Linux". A section titled "Quick Videos on how to use the Tor Browser" contains a table with links for downloading and using the browser on different operating systems. At the bottom, there is a "Tor Browser Downloads" section with instructions to download the file for the user's preferred language and save it to a convenient location like the Desktop or a USB flash drive. The footer lists the supported operating systems: Microsoft Windows, Mac OS X, and Linux.


Home About Tor Documentation Press Blog Contact

Download Volunteer Donate

HOME > PROJECTS > TORBROWSER

Software & Services: • Arm • Orbot • Tails • TorBirdy • Onionoo • Metrics Portal • Tor Cloud • Obfsproxy • Shadow • Tor2Web

What is the Tor Browser?



BROWSER
BROWSER

DOWNLOAD
Tor Browser

Installation Instructions
Windows • OS X • Linux

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world. It prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Do you like what we do? Please consider making a donation »

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

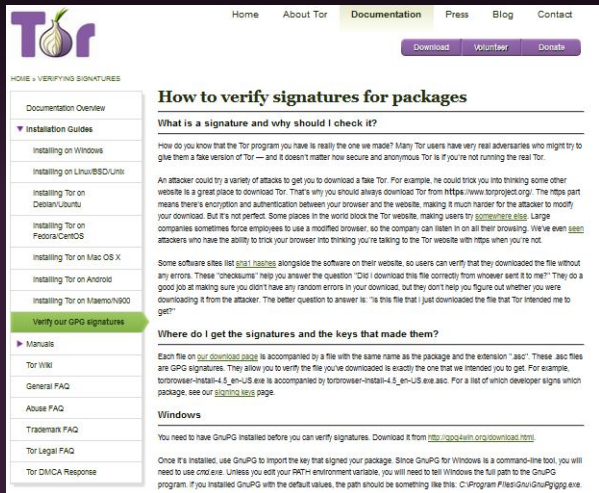
To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Microsoft Windows Mac OS X Linux

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>



The screenshot shows the Tor Project website's documentation page titled "How to verify signatures for packages". The page has a navigation bar with links for Home, About Tor, Documentation (highlighted), Press, Blog, and Contact. Below the navigation bar are buttons for Download, Volunteer, and Donate. The main content area is on the right, and a sidebar with a table of contents is on the left.

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**
- Manuels
- 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 [somewhere 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\Gnu\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 devez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.

[Conseils pour rester anonyme »](#)

Vous pouvez aider !

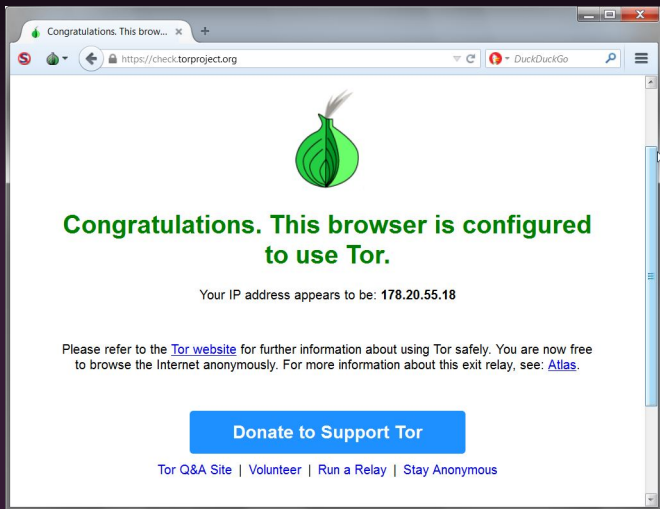
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relai 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/`



Congratulations. This browser is configured to use Tor.

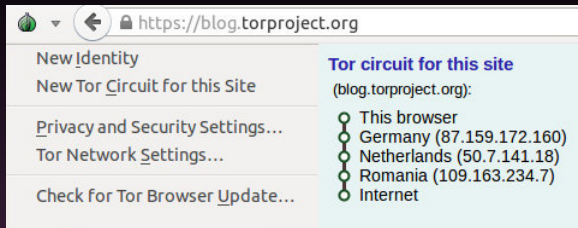
Your IP address appears to be: 178.20.55.18

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Atlas](#).

[Donate to Support Tor](#)

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

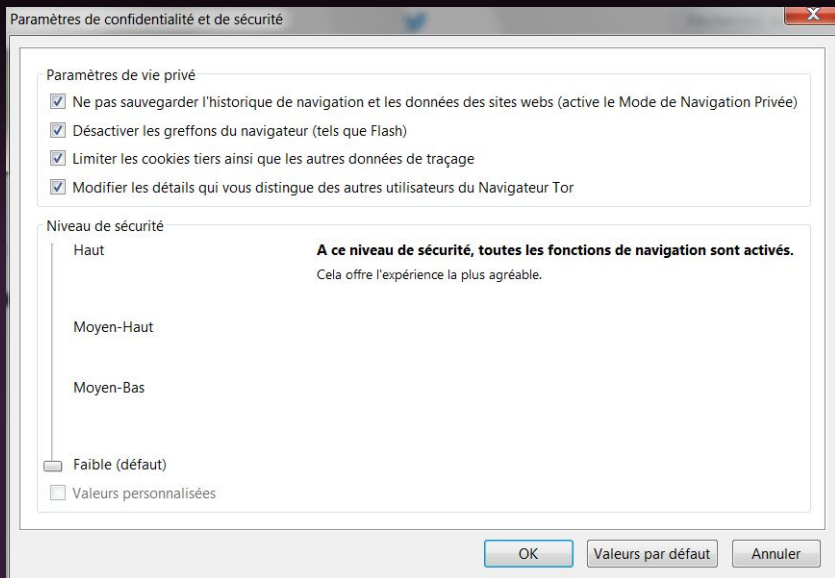
Les nouveautés de la version 4.5 1/2



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 (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

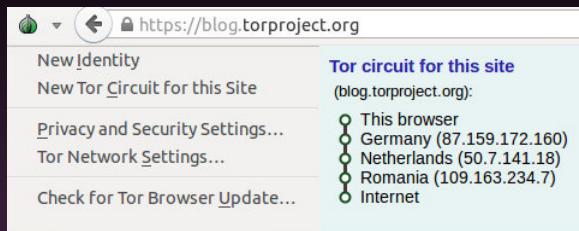
- Haut - JavaScript est désactivé sur tous les sites par défaut, certains types d'images sont désactivées.
- Moyen-Haut - Tous les optimisations de performances JavaScript sont désactivés, certains police fonctionnalités de rendu sont désactivées, JavaScript est désactivé sur tous les non-sites HTTPS 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

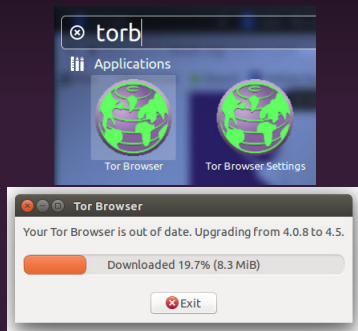
- Cliquer sur "Vérifier les mises à jour"

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 :

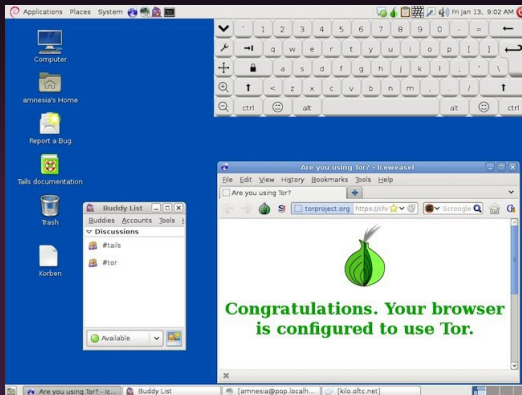
- le téléchargement de la version la plus récente de TBB, dans votre langue et pour votre architecture ;
- la mise à jour automatique (tout en conservant vos signets et préférences) manuel ;
- la vérification de la signature GnuPG du TBB (pour être sûr de l'intégrité des fichiers) ;
- ajoute un lanceur 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 faîte pas de Torrent via Tor.
- N'activez pas et n'installez pas de plug-ins dans le navigateur.
- Utiliser la version HTTPS des sites webs.
- Ne consultez pas/n'ouvrez pas de documents téléchargé pendant que vous êtes connecté via Tor.

Limites à l'usage de Tor



Limites à l'usage de Tor

- Pas de flash. Mais les vidéos HTML5 passe.
- Il faut activer le javascript (avec parcimonie).
- Beaucoup de noeuds de sorties sont bloqués (Cloudflare) etc.
- 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 (ou pas, obfuscation).

Soutenir le projet Tor



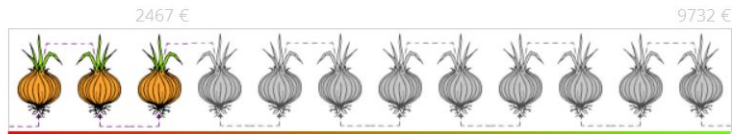
Soutenir le projet Tor 1/4

NosOignons

Il existe l'association NosOignons.net, qui propose des nœuds de sortie Tor financés par la communauté. <https://nos-oignons.net>

- En parler
- Faire un don à NosOignons

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 2/4

Tor Project

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

Soutenir le projet Tor 3/4



Soutenir le projet Tor 4/4

Si vous utilisez Cloudflare pour protéger votre site, un script permet aux utilisateurs de Tor d'y accéder

<https://github.com/DonnchaC/cloudflare-tor-whitelister>
en ajoutant les relais/noeud de sortie sur une white-liste, permettant aux utilisateur de Tor ne pas avoir à saisir de Captcha.

Questions et discussion