

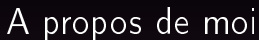
Ubuntu Party

Le réseau Tor

Genma - Café vie privée

5 mai 2015





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

Plein de choses dont :

- Organiser des Cafés vie privée



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.

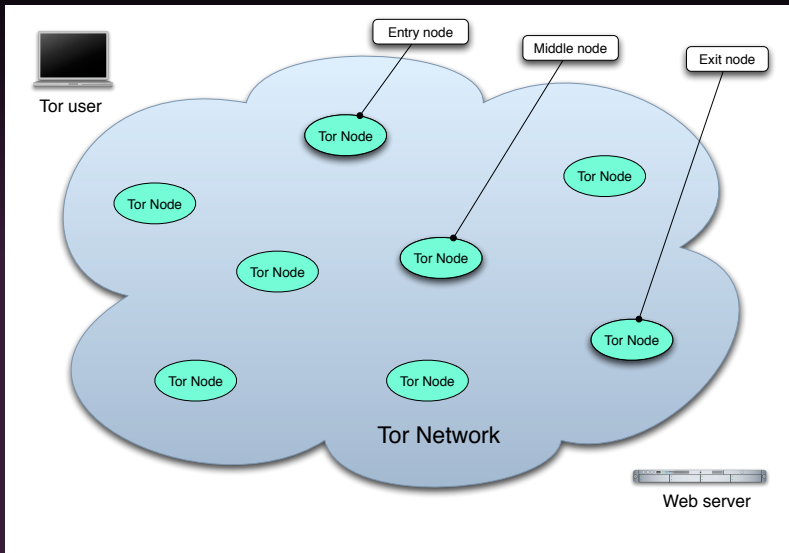
A quoi sert TOR ?

Tor est un réseau d'anonymisation, donc par définition, c'est difficile de faire un compte précis. Tor ne fait rien pour cacher que nous utilisons Tor. Donc quand en utilisant Tor, nous nous mettons au milieu de la foule des gens qui utilisent Tor. Plus cette foule est grande, meilleur est l'anonymat.

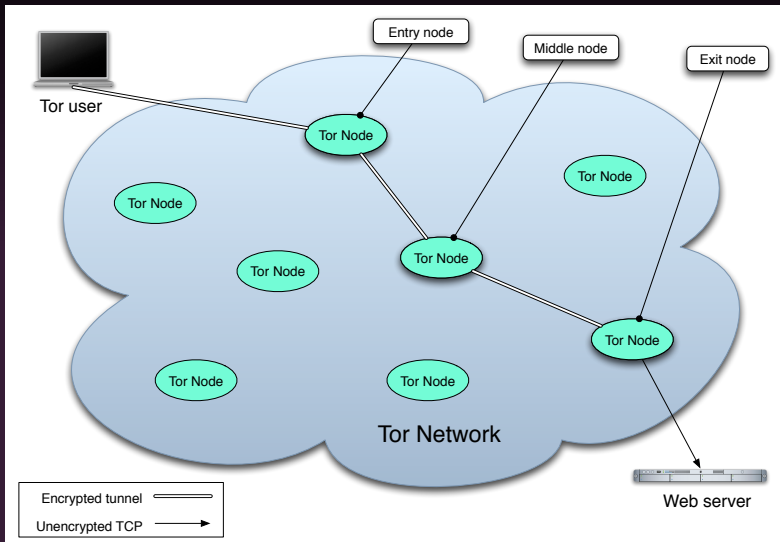
Comment fonctionne Tor ?



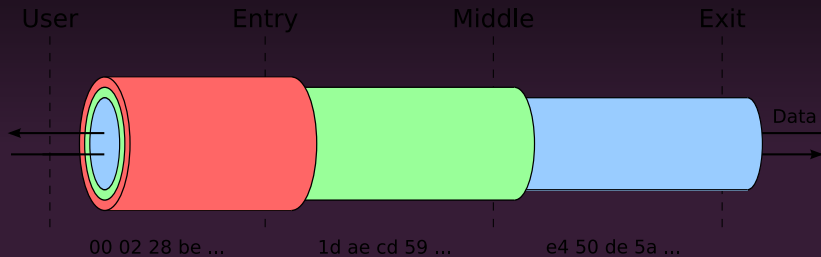
Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?

Ce tunnels se fait « en oignon » avec des couches de chiffrement empilées. Il y a une première clé de chiffrement vers le nœud d'entrée, une second clé vers le nœud du milieu et une dernière pour le nœud de sortie.

Il faut noter que Tor ne s'occupe pas de chiffrer après le nœud de sortie. Comme n'importe qui peut mettre en place un nœud de sortie, c'est une bonne idée de chiffrer sa communication en plus (par exemple en se connectant aux sites web que l'on visite en HTTPS). Après, se déroule tout un processus pour établir un tunnel chiffré jusqu'au nœud de sortie.

Tor hidden service

les services cachés de TOR



Tor hidden service - les services cachés de TOR

Tor permet aux clients et aux relais d'offrir des services cachés. Il est possible d'offrir 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.
- Facebook, Wikipeida, des blogs...

Comment utiliser Tor ?



Utiliser Tor - Le Tor Browser

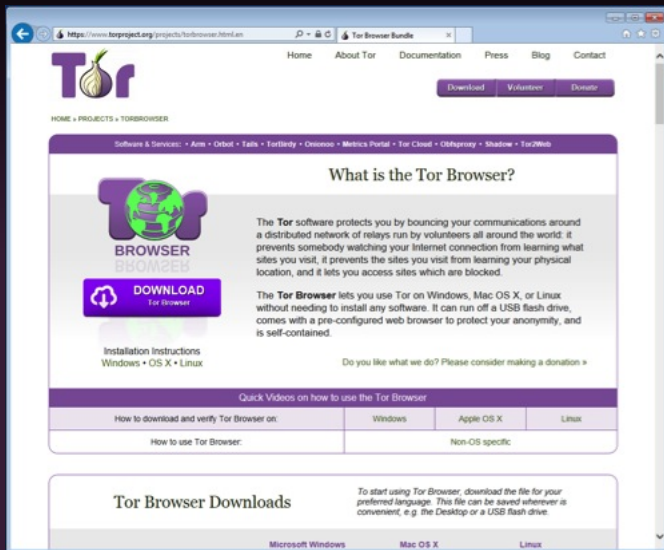
Le Tor Browser est une version Extended Support de Firefox, auxquelles sont ajoutée les extensions préconfigurées permettant qu'au lancement du navigateur, celui-ci se connecte à Tor.

⇒ 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: Home, About Tor, Documentation, Press, Blog, and Contact. There are buttons for Download, Volunteer, and Donate. The main heading is "What is the Tor Browser?". Below this, there is a section with the Tor Browser logo and a large "DOWNLOAD Tor Browser" button. To the right of the button, there is text explaining what the Tor Browser is and how it works. Below the button, there are links for "Installation Instructions" for Windows, OS X, and Linux. At the bottom, there is a section titled "Tor Browser Downloads" with links for Microsoft Windows, Mac OS X, and Linux.

HOME • PROJECTS • TORBROWSER

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

What is the Tor Browser?

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>



HomeAbout TorDocumentationPressBlogContact

DownloadVolunteerDonate

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 [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://gpg4win.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).

Pour Ubuntu, GNU/Linux c'est un programme autonome/portable.

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 !

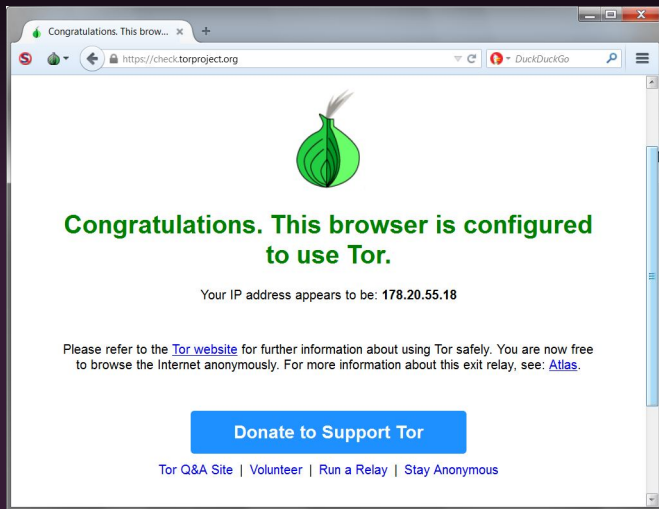
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

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

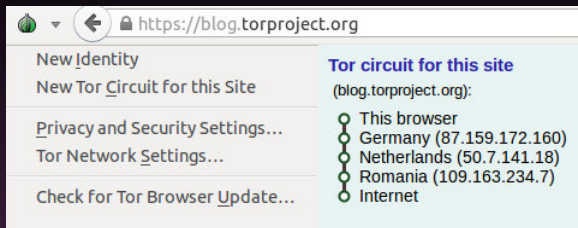
Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor »](#)

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

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



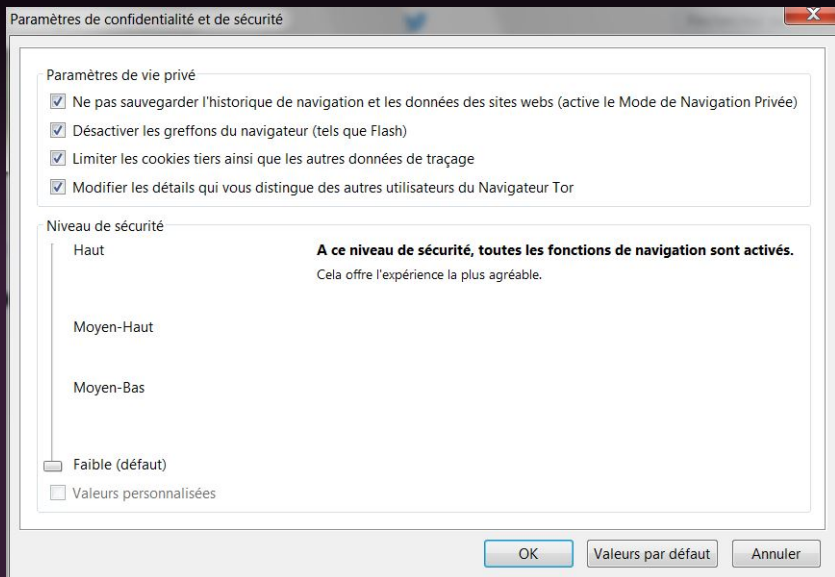
Les nouveautés de la version 4.5 1/2



Pour la vie privée

- Visualisation et 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

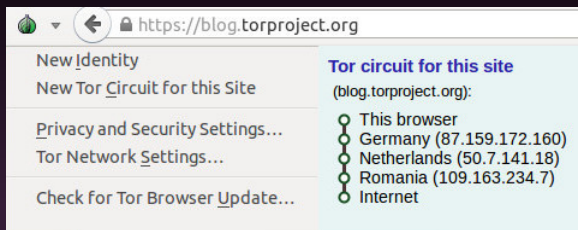
- Haut - JavaScript est désactivé sur tous les sites par défaut, certains types d'images sont désactivées.
- Moyen-Haut - Tous les optimisations de performances JavaScript sont désactivés, certains police fonctionnalités de rendu sont désactivées, JavaScript est désactivé sur tous les non-sites HTTPS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

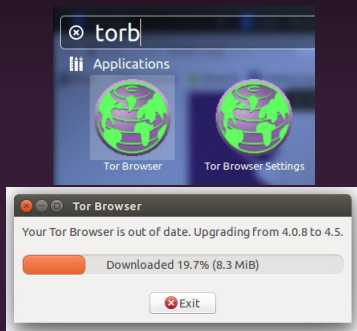
- Cliquer sur "Vérifier les mises à jour"

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 :

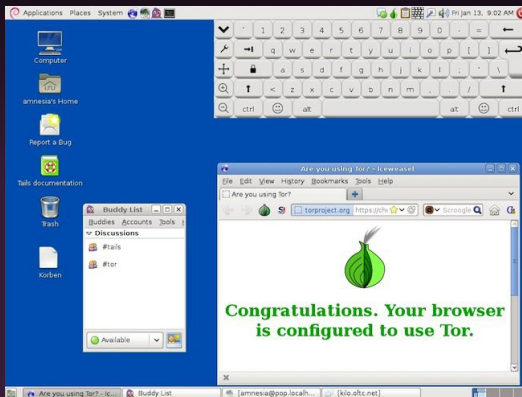
- le téléchargement de la version la plus récente de TBB, dans votre langue et pour votre architecture
- la mise à jour automatique (tout en conservant vos signets et préférences) manuel
- la vérification de la signature GnuPG du TBB (pour être sûr de l'intégrité des fichiers)
- ajoute un lanceur d'application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



<https://tails.boom.org>

Utiliser Tor - Tails

Tails 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 plugins 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

Soutenir le projet Tor



Soutenir le projet Tor

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
- Devenir membre de la communauté
- Faire des tutoriaux, de la traduction, contibuez au code...

Les cafés vie privée



Café *vie privée*

<https://café-vie-privée.fr/>

@chiffrofete #cafevieprivée

Questions et discussion