Sécurité informatique

Navigation web sécuritaire avec TOR

Tor est un service maintenu par des volontaires qui fournit à la fois une intimité et un anonymat en ligne en masquant qui vous êtes et d'où vous vous connectez. Ce service vous protège également du réseau Tor lui-même.[1)]

Pour les personnes ayant besoin d'un anonymat et d'une intimité occasionnels lorsqu'elles accèdent à des sites Web, le Navigateur Tor met à leurs disposition une manière rapide et facile d'utiliser le réseau Tor.

> **Le navigateur Tor est basé sur Firefox ESR et inclût les extensions Torbutton, TorLauncher, NoScript, and HTTPS-Everywhere.**

La manière la plus facile d'utiliser le réseau Tor est d'utiliser le Tor Browser Bundle, qui allie un navigateur Web et le logiciel Tor à d'autres logiciels utiles qui vous permettront de disposer d'un accès plus sécurisé au Web.

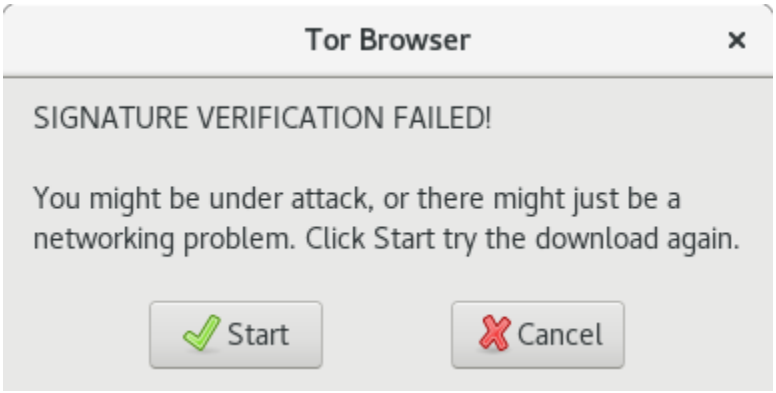
Le Navigateur Tor fonctionne de la même manière que les autres navigateurs Web, excepté le fait qu'il achemine vos communications à travers le réseau Tor, rendant ainsi plus difficile, pour les personnes qui vous surveillent, de savoir exactement ce que vous faîtes en ligne, et rendant encore plus difficile, pour les personnes surveillant les sites que vous utilisez, de savoir depuis quel endroit vous vous connectez. *Gardez à l'esprit que seules les activités que vous réalisez via le Navigateur Tor lui-même seront anonymes.* **Le fait d'installer le Navigateur Tor sur votre ordinateur n'anonymise pas les autres tâches que vous réalisez sur le même ordinateur en utilisant un autre logiciel (comme votre navigateur Web habituel)**.

Installer TOR

GNU/Linux (Debian et Ubuntu)

- Installez le paquet `torbrowser-launcher`
- À partir des menus ou de la ligne de commande, lancez `torbrowser-launcher`

Après le téléchargement il est possible de voir ce message:



Vous devrez rafraîchir les clés de chiffrement permettant la vérification du téléchargement (vor le rapport de faille sur GitHub pour plus de détails):

```
$ gpg --homedir "$HOME/.local/share/torbrowser/gnupg_homedir/" --refresh-keys
--keyserver pgp.mit.edu
gpg: refreshing 2 keys from hkp://pgp.mit.edu
gpg: requesting key 63FEE659 from hkp server pgp.mit.edu
gpg: requesting key 93298290 from hkp server pgp.mit.edu
gpgkeys: key 8738A680B84B3031A630F2DB416F061063FEE659 can't be retrieved
gpg: key 93298290: "Tor Browser Developers (signing key)
<torbrowser@torproject.org>" 93 new signatures
gpg: key 93298290: "Tor Browser Developers (signing key)
<torbrowser@torproject.org>" 1 new subkey
gpg: Total number processed: 1
gpg:            new subkeys: 1
gpg:         new signatures: 93
gpg: no ultimately trusted keys found
```

Windows et Mac OS

Pour Windows et Mac OS, téléchargez le Tor Browser Bundle et installez-le comme à l'habitude pour d'autres applications.

Mobile et tablettes Android

Pour les téléphones et tablettes Android, l'installation des applications nécessaires se fait par ces étapes:

- Installer F-Droid
- Ajouter les dépôts de Guardian Project
- Installez les applications `OrWeb` et `OrFox`

Les bonnes pratiques pour bien utiliser TOR

- **Ne téléchargez pas de torrent sur le réseau Tor**[2)]

On a observé que les applications de partage de fichiers Torrent ignorent les paramètres proxy et établissent des connexions directes même lorsqu'on leur demande d'utiliser Tor. **Même si votre application torrent se connecte uniquement via Tor, vous enverrez souvent votre véritable adresse IP dans la requête GET tracker**, car c'est comme ça que les torrents fonctionnent. Non seulement vous désanonymisez votre trafic torrent et votre autre trafic Web Tor simultané de cette façon, vous ralentissez aussi le réseau Tor entier pour tout le monde.

- **N'activez pas et n'installez pas d'extensions de navigateur**

Tor Browser bloque les plugins du navigateur tels que Flash, RealPlayer, Quicktime et autres: **ils peuvent être manipulés pour révéler votre adresse IP**. De même, nous ne recommandons pas l'installation d'addons supplémentaires ou de plugins dans Tor Browser, car ceux-ci peuvent contourner Tor ou nuire à votre anonymat et votre vie privée.

- **Utilisez les versions HTTPS des sites Web**

Tor va chiffrer votre trafic vers et à l'intérieur du réseau Tor, mais le chiffrement de votre trafic vers le site de destination final dépend de ce site Web. Pour assurer le cryptage privé des sites Web, Tor Browser inclût HTTPS Everywhere pour forcer l'utilisation du cryptage HTTPS avec les principaux sites Web qui le supportent. Toutefois, vous devez toujours surveiller la barre d'URL du navigateur pour vous assurer que les sites Web fournissent des informations sensibles pour afficher un bouton de barre d'URL bleu ou vert, incluez https: dans l'URL et affichez le nom attendu approprié pour le site Web. Voir aussi la page interactive de l'EFF expliquant comment se rapportent Tor et HTTPS.

- **N'ouvrez pas les documents téléchargés via Tor en ligne**

Tor Browser vous avertira avant d'ouvrir automatiquement les documents traités par des applications externes. NE PAS IGNORER CET AVERTISSEMENT. Vous devez être très prudent lors du téléchargement de documents via Tor (en particulier les fichiers DOC et PDF, à moins que vous n'utilisiez le visualiseur PDF intégré à Tor Browser) car **ces documents peuvent contenir des ressources Internet qui seront téléchargées en dehors de Tor par l'application qui les ouvre. Cela révélera votre adresse IP non-Tor.** Si vous devez travailler avec des fichiers DOC et / ou PDF, nous vous recommandons fortement d'utiliser un ordinateur déconnecté, de télécharger le logiciel libre VirtualBox et de l'utiliser avec une image de machine virtuelle avec mise en réseau désactivée ou utilisant Tails. En aucun cas, il est sûr d'utiliser BitTorrent et Tor ensemble, cependant.

- **Utiliser des ponts et / ou trouver de la compagnie**

Tor essaie d'empêcher les attaquants d'apprendre à quels sites de destination vous vous connectez. Cependant, par défaut, cela n'empêche pas quelqu'un qui regarde votre trafic Internet d'apprendre que vous utilisez Tor. Si cela vous importe, vous pouvez réduire ce risque en configurant Tor pour utiliser un relais de pont Tor plutôt que de vous connecter directement au réseau Tor public. En fin de compte, la meilleure protection est une approche sociale: plus les utilisateurs Tor sont près de vous et plus leurs intérêts sont divers, moins il sera dangereux que vous soyez l'un d'entre eux. Convainquez les autres à

utiliser Tor, aussi!

Liens utiles

- https://ssd.eff.org/fr/module/guide-dutilisation-de-tor-pour-windows
- https://ssd.eff.org/fr/module/guide-dutilisation-de-tor-pour-mac-os-x

1)

https://ssd.eff.org/fr/module/guide-dutilisation-de-tor-pour-windows

2)

https://www.torproject.org/download/download-easy.html.en#warning