

Le réseau Tor - Annexes

Genma

SCE2015 - 13 juin 2015



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

Annexes

Annexes

- Polémiques
- Quelques chiffres
- Installer des extensions dans le navigateur Tor
- Les types de noeuds
- Vérification des signatures
- La commande Torify
- Torbirdy
- Les bridges et l'obfuscation
- Précisions sur le DNS
- Les échanges de clefs
- Le financement
- TorFlow
- DHT des Hidden Service Directories
- Série de liens

Les polémiques

Utilisation pour des actes malveillants - Le "Darknet"

Les sites Web des services cachés ne représentent que 2% du trafic total d'Internet, d'après Roger Dingledine.

<http://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites>

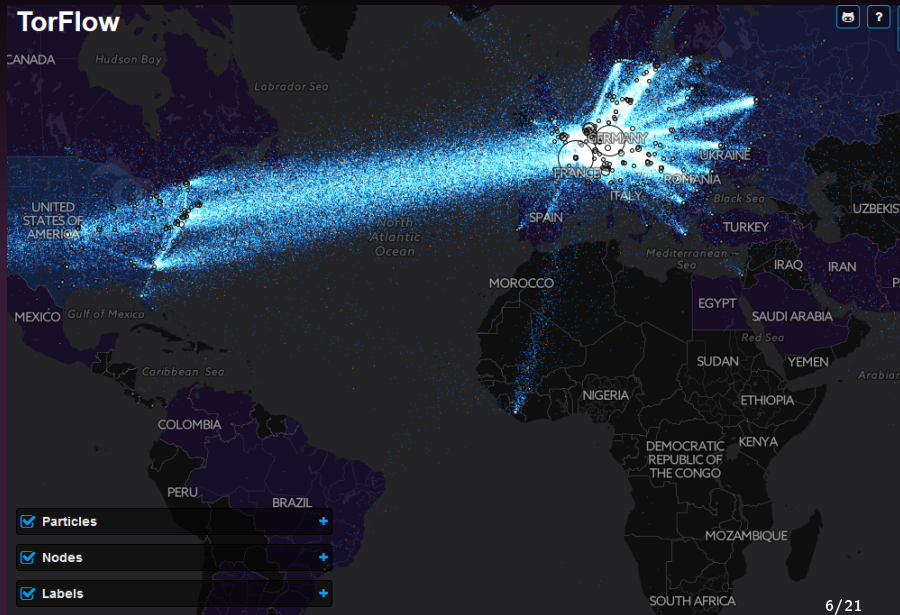
Who use Tor? Tor user

<https://www.torproject.org/about/torusers.html.en>

Quelques chiffres datant de nov 2013

- 4.600 relais présents dans le réseau ;
- 900 noeuds de sortie ;
- 40 Gb/s de bande passante ;
- 25 Gb/s utilisés ;
- 500k utilisateurs (6% de français).

TorFlow <https://torflow.uncharted.software/>



Installer des extensions dans le navigateur Tor?

L'installation des add-ons dans le navigateur Tor peut ajouter des failles de sécurité potentielles :

- Certaines extensions pourraient ne pas prendre en compte la configuration (tout faire passer par Tor) et laisser fuiter des informations privées.
- Certaines extensions pourraient révéler des informations sur vos habitudes de navigation, l'historique de navigation, ou des informations du système, que ce soit à dessein ou par erreur.
- Les extensions peuvent avoir des bogues et des failles de sécurité qui peuvent être exploitées à distance par un attaquant.
- Les extensions peuvent avoir des bogues casser la sécurité offerte par d'autres add-ons, par exemple Torbutton, et de casser votre anonymat.
- Elles changent votre navigateur en le démarquant, rendant unique.

Sauf preuve du contraire, aucun add-on, en dehors de ceux déjà inclus dans le TorBrowser (qui ont été sérieusement vérifiés et peuvent être considérées comme sûr) ne sont à ajouter.

Les types de noeuds

- Guards : noeuds d'entrée publics ;
- Bridges : noeuds d'entrée publics ;
- Midlle : noeuds intermédiaires ;
- Exit : noeuds de sortie ;
- Obfsproxy : noeuds d'obfuscation.

Vérification des signatures

Via la commande

```
gpg --verify torbrowser-install-4.5.1exe.asc  
torbrowser-install-4.5.1exe
```

Cf. [https:](https://www.torproject.org/docs/verifying-signatures.html.en)

[//www.torproject.org/docs/verifying-signatures.html.en](https://www.torproject.org/docs/verifying-signatures.html.en)

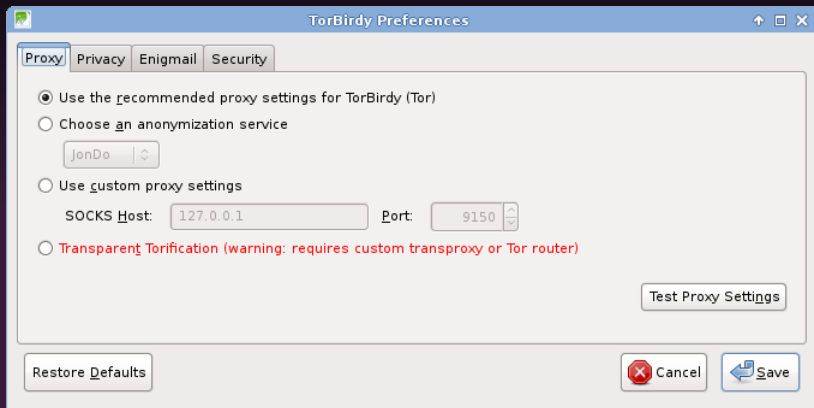
La commande Torify

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).

TorBirdy



The image shows a 'TorBirdy Preferences' window with a blue title bar and standard window controls. It features four tabs: 'Proxy' (selected), 'Privacy', 'Enigmail', and 'Security'. The 'Proxy' tab contains three radio button options. The first option, 'Use the recommended proxy settings for TorBirdy (Tor)', is selected. The second option, 'Choose an anonymization service', is followed by a dropdown menu showing 'JonDo'. The third option, 'Use custom proxy settings', is followed by 'SOCKS Host' (127.0.0.1) and 'Port' (9150) fields. A fourth option, 'Transparent Torification', is shown in red text with a warning. A 'Test Proxy Settings' button is at the bottom right of the main area. At the bottom of the window are 'Restore Defaults', 'Cancel', and 'Save' buttons.

TorBirdy Preferences

Proxy Privacy Enigmail Security

☒ Use the recommended proxy settings for TorBirdy (Tor)

☐ Choose an anonymization service

JonDo

☐ Use custom proxy settings

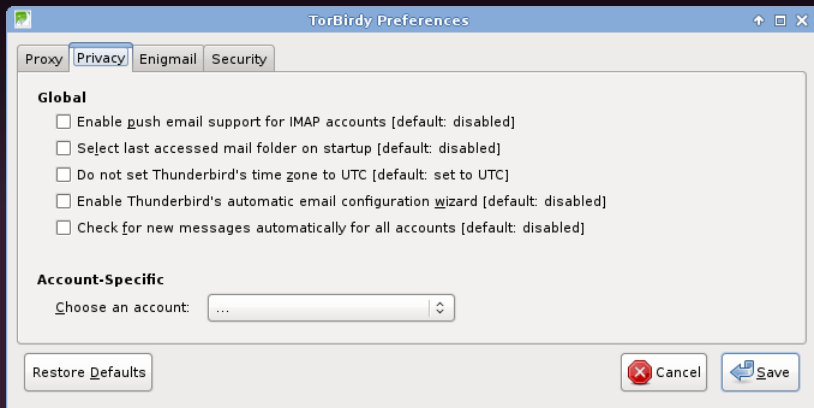
SOCKS Host: 127.0.0.1 Port: 9150

☐ Transparent Torification (warning: requires custom transproxy or Tor router)

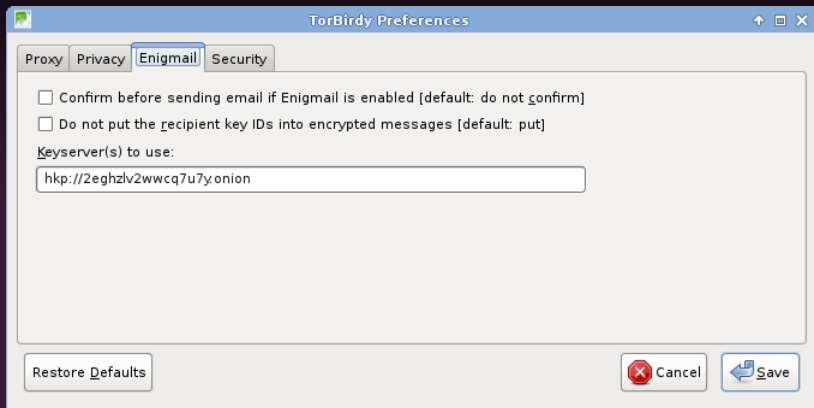
Test Proxy Settings

Restore Defaults Cancel Save

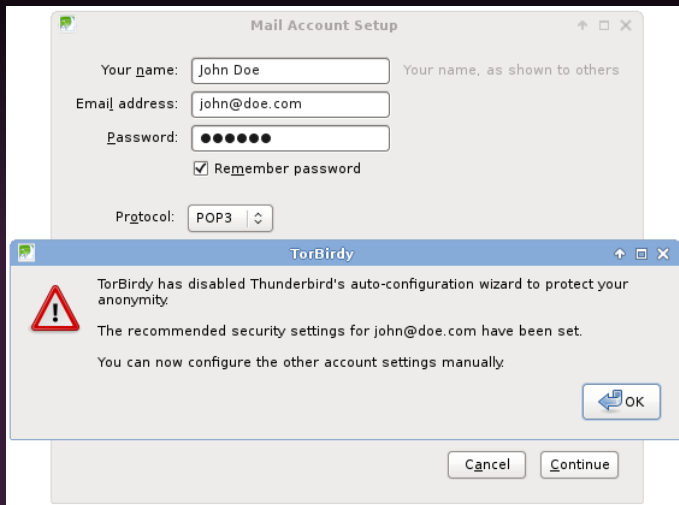
TorBirdy



TorBirdy



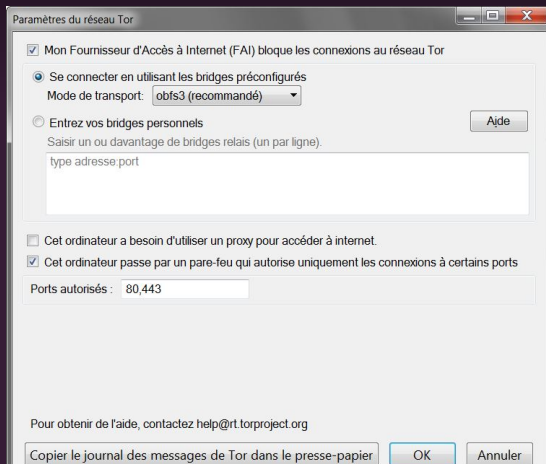
TorBirdy



Les bridges et l'obfuscation

Les Bridges sont des relais Tor qui ne sont pas listés dans l'annuaire principal de Tor.

Un bridge obfsproxy permet d'obfusquer le trafic Tor, c'est à dire cacher les connexions au réseaux Tor (encapsulation dans du trafic neutre).



Précisions sur le DNS

Tor ne peut assurer la protection de paquets UDP, et n'en soutient donc pas les utilisations, notamment les requêtes aux serveurs DNS.

Cependant Tor offre la possibilité d'acheminer les requêtes DNS à travers son réseau, notamment à l'aide de la commande *torsocks*.

Les échanges de clefs

Les paquets à acheminer sont associés à une identification du propriétaire du circuit (la personne qui l'a construit). Mais cette identification est un code arbitraire qui a été choisi au moment de la construction du circuit. L'identification réelle du propriétaire est inaccessible.

Cette construction fait appel au concept de cryptographie hybride. Chaque nœud d'oignon possède une clef publique, mais la cryptographie à clef secrète (clef symétrique) est bien plus rapide que celle à clef publique. L'idée est donc de distribuer à chaque nœud du circuit une clef secrète chiffrée avec leur clef publique.

Après la phase de construction, chaque nœud du circuit dispose d'une clef secrète qui lui est propre et ne connaît que son prédécesseur et son successeur au sein du circuit.

Source [https://fr.wikipedia.org/wiki/Tor_\(réseau\)](https://fr.wikipedia.org/wiki/Tor_(réseau))

Le financement

Le projet coûte 2 M\$ annuellement pour son développement et pour payer les nombreux serveurs. En 2012 :

- 60% proviennent du gouvernement américain (soutien à la liberté d'expression et à la recherche scientifique) ;
- 18% proviennent de fondations et autres donateurs (John S. and James L. Knight Foundation (en), SRI International, Google, Swedish International Development Cooperation Agency;
- 18% proviennent de la valorisation des contributions des bénévoles.

Source [https://fr.wikipedia.org/wiki/Tor_\(réseau\)](https://fr.wikipedia.org/wiki/Tor_(réseau))

Ce que financent plusieurs branches différentes du gouvernement des USA est le développement des logiciels à travers l'organisation The Tor Project. Le réseau Tor est quant à lui mis en place par des bénévoles et des organisations comme Nos oignons.

Nom de domain .onion

Les nom de domain .onion sont-ils publiés quelque part ?

Réponse d'Aeris : "les DHT des Hidden Service Directories de Tor. Mais comme c'est une *Distributed*HT, personne n'a la liste complète. En tout cas pas facilement et pas sans risquer de se faire blacklister violamment par le @torproject en tant que BadNode"

S'informer - Série de liens

- <https://www.torproject.org>
- <https://blog.torproject.org>
- <https://tails.boum.org/>