Le chiffrement, maintenant (4)

Aujourd'hui, un rapide coup d'œil sur le projet Tor, un réseau décentralisé de routeurs qui permet de faire « rebondir » vos communications sur Internet parmi plusieurs trajectoires dont chaque étape fait appel au chiffrement. Ainsi l'adresse de votre ordinateur d'origine devient-elle très difficile à retrouver.

Ne dissimulons pas toutefois que la mise en œuvre de Tor n'est pas triviale et que le réseau est probablement déjà soumis à des tentatives d'attaques, en raison de l'anonymat qu'il vise à y garantir…

Anonymisez votre localisation avec Tor

Tor est un service logiciel qui vous permet d'utiliser Internet en dissimulant votre adresse IP, qui constitue, en général, une représentation assez précise de votre localisation. Le réseau Tor est composé de 3600 serveurs, maintenus par des bénévoles, appelés nœuds. Quand quelqu'un utilise le réseau Tor pour visiter un site, sa connexion est relayée à travers trois de ces nœuds (appelé circuit) avant de finalement accéder à l'Internet normal. Quiconque interceptera le trafic pensera que votre emplacement est le nœud final duquel sort votre trafic.
Il est important toutefois de se souvenir que le fait d'anonymiser votre connexion à Internet ne la rend pas magiquement sécurisée. EFF a créé un schéma interactif montrant comment Tor et le HTTPS peuvent travailler ensemble pour protéger votre vie privée.

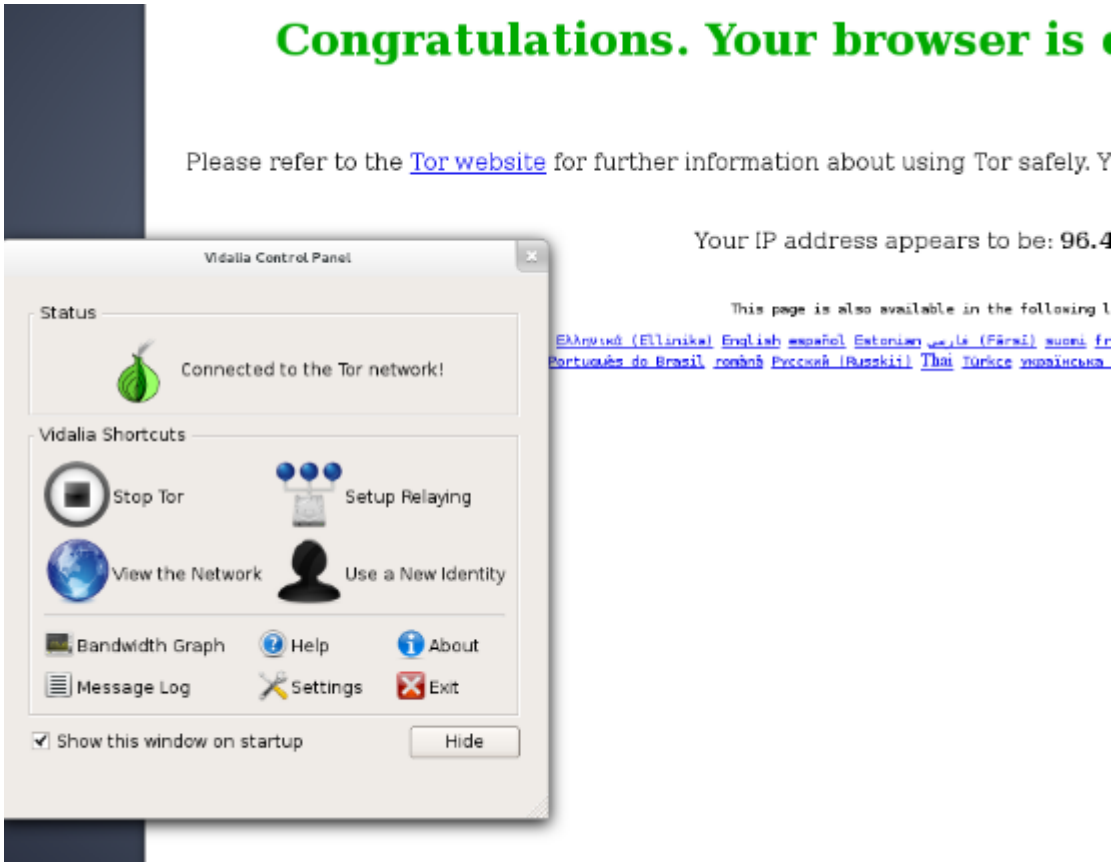
Comme tout bon logiciel de cryptographie, Tor est un logiciel libre, avec un logiciel de suivi de bogues ouvert, des listes de diffusion et un code source disponible.
La documentation de Tails, la distribution live GNU/Linux qui force tout le trafic du réseau de l'utilisateur à passer par le réseau Tor, dit ceci à propos des adversaires globaux :

> *Un adversaire passif serait une personne ou une entité capable de surveiller le trafic entre tous les ordinateurs d'un même réseau simultanément. En étudiant, par exemple, la synchronisation et le volume de données des différentes communications sur le réseau, il pourrait être possible d'identifier les circuits Tor et ainsi identifier les utilisateurs de Tor et les serveurs de destination.*

On peut considérer que la NSA et la GHCQ comptent parmi les adversaires globaux, car nous savons qu'ils surveillent une large portion d'Internet. On ne peut savoir de manière sûre à quelle fréquence ces agences de renseignement peuvent mettre en échec l'anonymat du réseau Tor. Récemment, le réseau Tor a fait l'objet d'une attaque par Botnet. Il est probable que la guerre contre le chiffrement a déjà commencé.

Même si cela leur est possible, utiliser Tor nous procure toujours plusieurs avantages. Cela rend leur travail plus difficile, et nous laissons moins de données nous identifiant sur les serveurs par lesquels nous nous connectons au réseau Tor. Cela rend une attaque MITM plus difficile dans notre réseau local ou au niveau de notre fournisseur d'accès à internet (FAI). Et même si certains circuits Tor peuvent être infiltrés par un adversaire global, si suffisamment de personnes font transiter leur trafic par le même nœud Tor au même moment, il sera difficile pour l'adversaire de dire quel trafic correspond à quel circuit.

Le moyen le plus simple pour utiliser Tor est de télécharger et d'installer le Tor Browser Bundle.



Des informations détaillées sur l'installation et la configuration de Tor selon votre système d'exploitation figurent sur le site du projet Tor. Elles sont malheureusement en anglais. Vous trouverez une documentation en français pour Ubuntu sur cette page.

Lorsque Snowden a répondu aux questions sur le site du Guardian depuis une « connexion sécurisée à Internet », il routait probablement son trafic par le réseau Tor. Il peut avoir également eu recours à un « pont » pour se connecter au réseau Tor afin de rendre le fait qu'il utilise Tor à partir de son adresse IP moins évident pour les oreilles indiscrètes.

(à suivre…)