L’anonymat en ligne avec Tor, c’est Nos oignons !

Comme beaucoup d’internautes, vous êtes ces dernières années de plus en plus préoccupé par la confidentialité de vos données et de vos communications.

Vous avez renforcé et renouvelé vos mots de passe, installé des extensions qui filtrent ou bloquent les contenus indésirables, vous luttez contre le pistage des GAFAM au cours de votre navigation, vous êtes en voie de dégooglisation, mais vous n’avez peut-être pas osé aborder une étape plus délicate et technique comme celle qui consiste à chiffrer vos échanges et vos disques durs, pas osé non plus utiliser le réseau Tor. C’est bien compréhensible, vous reculez un peu devant ce qui vous semble plus complexe et vous ne savez pas exactement de quoi il retourne… On entend dire des choses tellement inquiétantes aussi !

Tout le monde peut trouver des

avantages à utiliser
Tor

Eh bien nous vous proposons aujourd'hui d'apprendre un peu mieux ce qu'est réellement ce réseau Tor, pour démystifier ce qui peut s'avérer d'un usage quotidien pour beaucoup d'entre nous.

Vous en doutez ? Pourtant emprunter les trajectoires zigzagantes de Tor est non seulement parfaitement légal mais aussi tout à fait utile et à la portée d'un vaste public.

Mais pour commencer, qu'est-ce que c'est au juste que Tor ? Comment ça marche, est-ce que c'est dangereux ? Comment peut-on l'essayer sans trop de difficultés ?

Pour répondre à ces questions, autant s'adresser directement à ceux sont sur le terrain et connaissent la question. Nous avons la chance d'avoir Nos oignons une jeune association francophone qui s'active pour multiplier les nœuds de sortie dont… STOOOOP ! Écoutons-les plutôt.

Merci à **ned, syl, Chre, Cor, gagz, nicoo, Lunar, aeris** *et à tous ceux de l'association qui ont collectivement et gentiment répondu aux questions un peu… comment dire – enfin des questions de Goofy, quoi.*

Tor c'est pour aller sur le *Darknet*, là où se trouvent les trafiquants de drogue et les terroristes, pourquoi vous voudriez que les internautes ordinaires y accèdent aussi ?

Utiliser Tor permet de retrouver un peu d'intimité quand on utilise Internet. Tout comme mettre une lettre dans une enveloppe, des rideaux à nos fenêtres ou son téléphone sur liste rouge, cela permet de retrouver le pouvoir de décider avec qui partager notre quotidien.
Des personnes qui veulent se livrer à des activités illégales vont bien entendu chercher à se cacher. Mais cela ne peut pas justifier d'espionner tout le monde. Tor est là pour nous

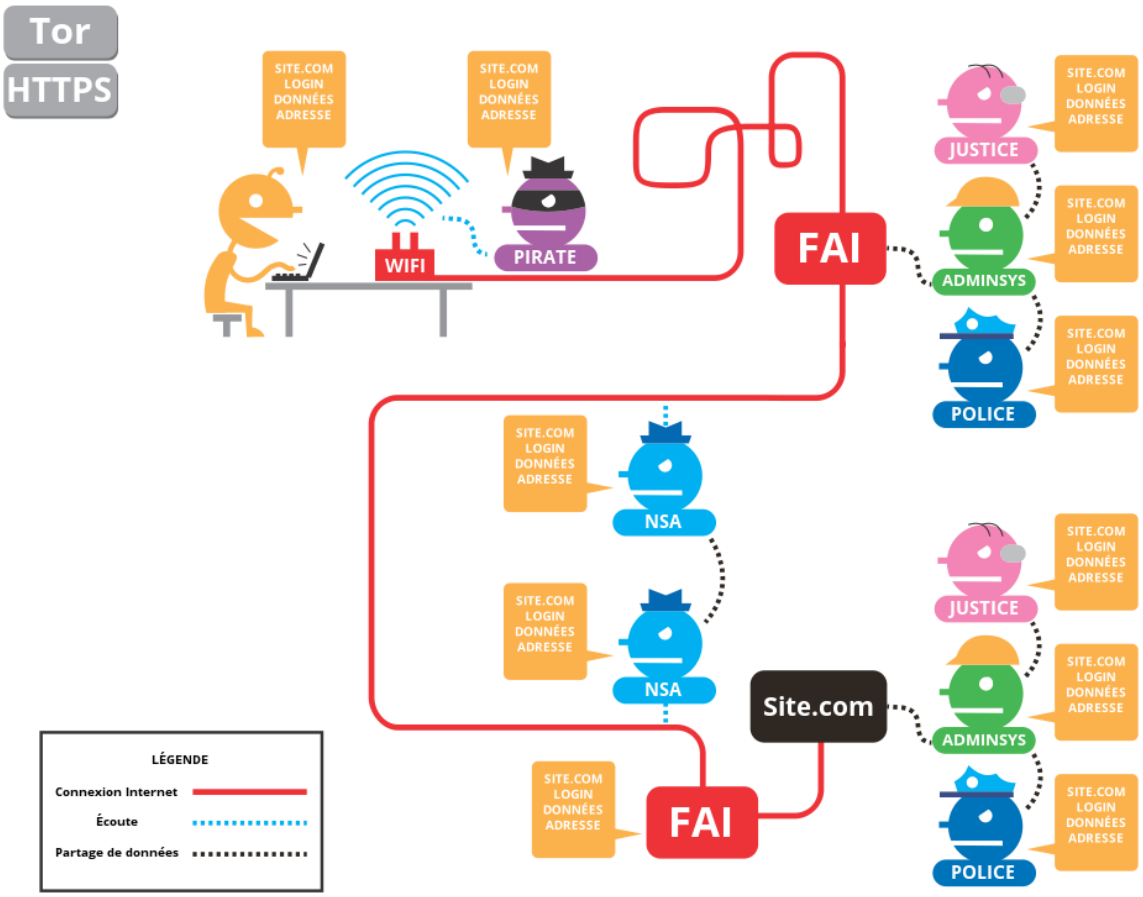
aider à disposer de nos droits fondamentaux : libertés d'opinion, d'expression, d'association, de communication. Ces droits humains s'appliquent à tou·te·s, sans discrimination.

Ce qu'il faut comprendre, c'est que même si Tor était interdit, des activités illégales continueraient d'exister sur Internet sous d'autres formes et en utilisant d'autres outils. Il y a déjà sur Internet des activités illégales n'utilisant pas Tor.

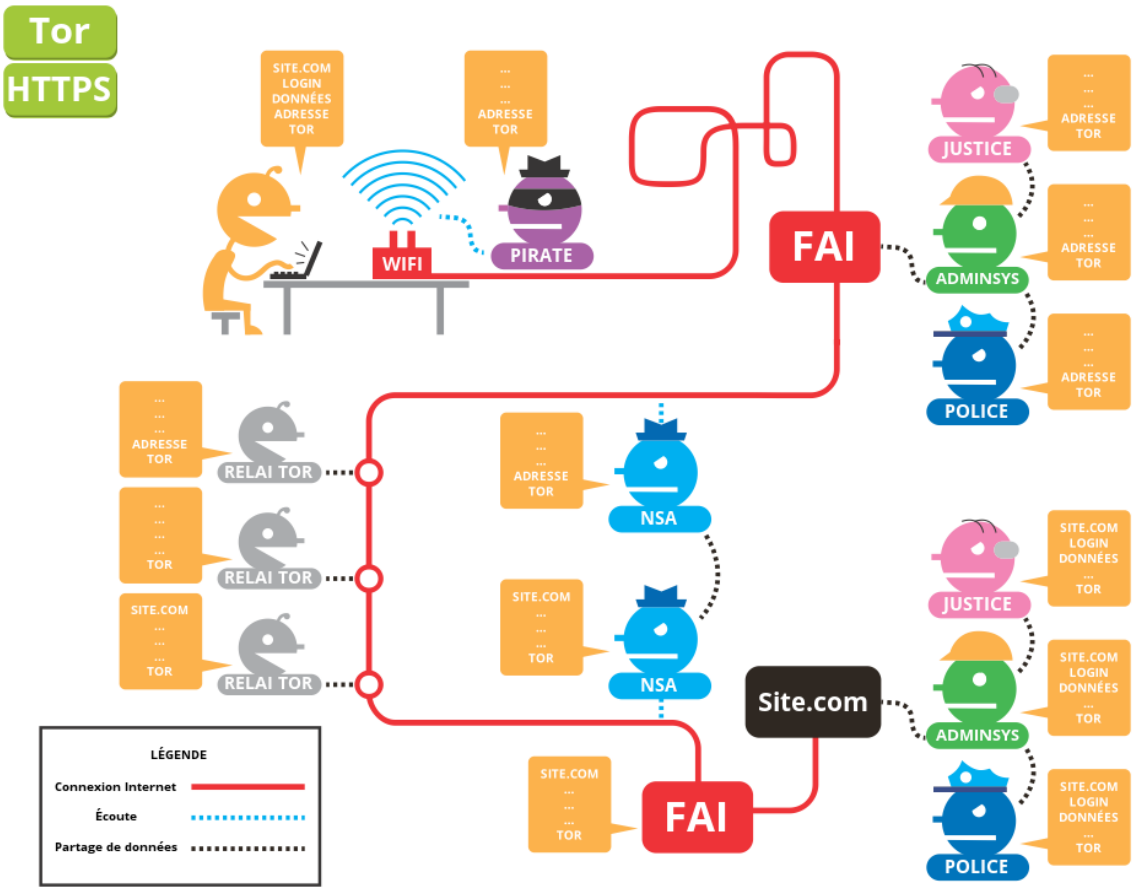
Moi je veux bien essayer Tor, mais je ne veux pas d'ennuis avec la police, hein. Qu'est-ce que vous faites quand les services de police vous demandent de fournir des renseignements sur des utilisateurs considérés comme suspects ?
On leur dit la simple vérité : nous n'avons pas ces renseignements, d'une part parce que nous ne gardons pas trace de ce que les usagers font avec Tor, d'autre part parce que le réseau est conçu pour qu'il nous soit impossible de remonter à la source des communications.

C'est le moment de schématiser le fonctionnement de Tor.

Regardez d'abord comme la transmission des informations numériques est perméable à toutes sortes de gens ou institutions lorsqu'on n'utilise ni Tor ni https (le protocole sécurisé) :



Maintenant, avec ces deux outils mis en place, observez que les diverses oreilles indiscrètes n’ont plus d’accès aux données que vous transmettez. Les trois relais Tor qui assurent ainsi votre anonymat sont d’ailleurs eux-mêmes « aveugles » à vos données. Chacun d’eux ne reçoit et transmet que des données chiffrées dont il ignore l’émetteur d’origine.



Il paraît que la NSA a glissé ses propres nœuds Tor dans le réseau, alors il est compromis ou bien je peux avoir confiance ?

Même si c'est toujours intéressant intellectuellement d'y réfléchir, on a rarement affaire à une organisation aussi puissante que la NSA. La plupart du temps, on cherche à se protéger de publicitaires qui veulent nous bourrer le crâne, de patrons qui veulent nous empêcher de bosser tranquilles, de conjoints inquisiteurs, d'un filtre trop agressif dans une gare… Moins souvent, on veut protéger des communications confidentielles avec des médecins, des avocat·e·s, des journalistes… On est donc rarement une cible directe de la NSA. Et c'est tant mieux parce que si elle se débrouille pour pirater notre ordinateur, il sera facile de nous espionner, que nous utilisions Tor ou non.

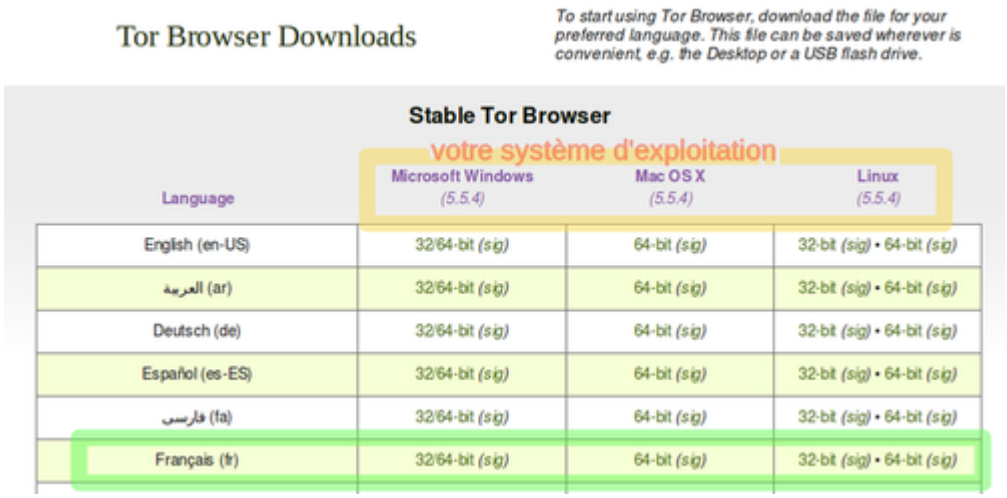
Néanmoins, si la NSA faisait tourner des nœuds, ce ne serait pas nécessairement un problème. Le réseau Tor est conçu pour résister à la présence de nœuds sous surveillance tant qu'ils

ne sont pas nombreux ou qu'ils sont surveillés par des adversaires différents. Des bénévoles font activement la chasse pour trouver des nœuds qui interfèrent avec les données échangées, ou des nœuds trop semblables qui apparaissent.

Il faut savoir qu'un adversaire comme la NSA, qui dispose de la capacité de surveiller directement les réseaux de communication, n'a nul besoin de faire tourner des relais Tor pour tenter de *désanonymiser* ses utilisateur·ice·s. En effet, plutôt que de s'embêter à faire tourner des relais, il suffit d'observer d'où vient et où va le trafic qui transite par les relais.
Tout serait donc perdu ? De ce qu'on en sait, bien au contraire : les documents internes que nous a transmis Edward Snowden nous ont permis de mieux comprendre l'étendue des possibilités de la NSA. La présentation interne intitulée « *Tor Stinks* » (Tor, ça pue), datée de 2012, explique qu'il est possible de retrouver le chemin d'une fraction des connexions traversant Tor, mais il est impossible de « désanonymiser » toutes les connexions tout le temps et il est très difficile de le faire avec une cible précise en tête.

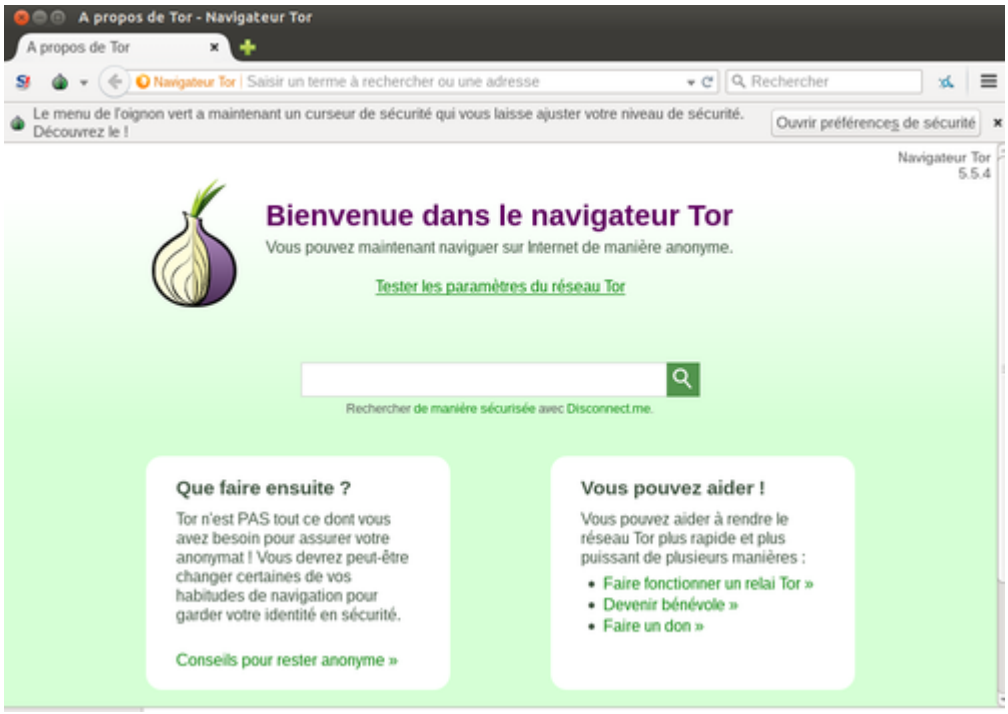
À notre connaissance, Tor reste efficace contre la surveillance de masse, et rend bien plus compliquées les attaques ciblées.

Je me rends compte que tester Tor est à ma portée ! Un navigateur est disponible pour cela, c'est Torbrowser. Il me suffit d'aller sur le site https://www.torproject.org/projects/torbrowser.html.en et de choisir la bonne version :



une fois qu'elle est téléchargée et installée, je choisis mon type d'usage :

et me voilà prêt à naviguer en circulant de façon anonyme sur le Web.



Bon, Tor c'est bien, mais quelles précautions faut-il que je prenne en plus selon vous, car Tor n'est pas une garantie contre tous les risques, hein ?
En effet ! Tor permet vraiment deux choses : empêcher le fournisseur d'accès Internet de surveiller les sites qu'on visite ; et empêcher que les sites apprennent où l'on se trouve malgré nous. Tor Browser contient des myriades de petites fonctionnalités pour empêcher que deux sites différents puissent apprendre qu'une même personne les visite tous les deux. Mais utiliser Tor Browser ne protégera pas forcément la connexion jusqu'au site visité, pour cela il faut veiller à ce que la connexion se fasse en HTTPS.

Tor n'est pas une poudre magique à « sécuriser » : la plupart des logiciels ont des défauts, Tor Browser est par exemple mis à jour toutes les six semaines afin de pouvoir colmater des brèches de sécurité le plus vite possible. Les connexions entre le réseau Tor et le site Internet auquel on accède peuvent être surveillées. Tor ou pas Tor, l'heure d'une connexion peut parfois permettre d'identifier une personne lorsqu'il y a peu de suspects.
Pour établir une analogie un peu bancale : mettre sa ceinture en voiture n'empêche pas les accidents, mais est-ce une bonne

raison pour ne pas la mettre ?

Utiliser Tor ne protégera pas les échanges à partir d'un site : ça ne change rien à la sécurité des messages échangés via Twitter ou un webmail. Se « garantir contre tous les risques », c'est forcément un processus, pas un produit. Par exemple, des images contenant le numéro de série de l'appareil qui a servi à prendre les photos dans les métadonnées peuvent permettre d'identifier la source d'une journaliste, que les images aient été transférées en utilisant Tor ou pas.

Ah ben je découvre qu'il existe une liste impressionnante de projets connexes à Tor ? Pourquoi a-t-on besoin de tout cet écosystème ? Quels sont les principaux types de projets associés et quels sont ceux auxquels vous (Nos oignons) participez ?
Il y a effectivement plein de projets liés à Tor, en plus de Tor (le logiciel qui sert à faire tourner le réseau) : le navigateur Tor, HTTPS Everywhere, les logiciels de messagerie instantanée Tor Messenger et Ricochet, Pond (une alternative aux *emails*)…
C'est principalement pour pouvoir mieux protéger les usagers de Tor : par exemple, Tor Browser est une version de Mozilla Firefox équipée de contre-mesures pour éviter qu'on puisse vous pister de connexion en connexion. Pond est un logiciel expérimental qui vise à fournir un service similaire aux *emails,* mais qui masque l'existence même d'une communication entre deux usagers donnés…
Il existe également Tails qui est un système d'exploitation *live* (i.e. qui peut fonctionner sur une clé USB sans installation sur un ordinateur) dont tous les logiciels intégrés passent par Tor. Utiliser un système spécialement conçu pour limiter les traces et les fuites comme *Tails* constitue une aide précieuse pour s'épargner des erreurs.
Notre équipe d'administration système contribue aussi à l'amélioration du projet Debian (la distribution GNU/Linux que nous utilisons principalement), entre autres sur la sécurité

des services que nous utilisons, et une importante quantité de documentation, accessible à tou·te·s, couvre la configuration de nos services, leur sécurisation et les procédures que nous employons. Des membres de Nos oignons ont également créé graphnion pour afficher des graphes de relais.

Mais… c'est quoi les « services cachés » de Tor, encore un truc de fraudeurs pour échapper à la TVA sur les services ?
Pas vraiment… on parle de plus en plus de services « .onion » ces temps-ci car de plus en plus de services sont accessibles publiquement ainsi.
Le fonctionnement habituel de Tor, c'est de permettre de se connecter à des sites Internet existants. Quand on utilise les services .onion, la connexion se fait vers un serveur qui utilise lui aussi Tor. Par exemple, cela permet pour une personne qui tient un blog politique d'être plus difficile à identifier par celles et ceux qui voudraient lui chercher des noises. Un autre intérêt est de s'assurer que les usagers du service « onion » n'y accèdent pas accidentellement sans Tor ; c'est en particulier utilisé par les systèmes de prise de contact avec les journalistes (comme « SecureDrop »), pour s'assurer que les sources ne s'exposent pas accidentellement. Depuis peu, on voit aussi de plus en plus de sites proposer un accès en .onion en plus de leur accès Internet habituel. Le plus utilisé est probablement Facebook. L'usage du .onion permet de garantir que la connexion se fait au bon serveur, et de bénéficier de la totalité de la bande passante du réseau Tor, sans être contraint par le nombre limité de nœuds de sortie.

Votre association gère aussi des « signalements d'abus ». De quoi s'agit-il ?
Parfois, des gens nous contactent pour nous informer d'un problème en provenance de nos serveurs : une tentative d'utiliser « toto123 » comme mot de passe sur un service Web, l'envoi de spam, ou encore des services qui trouvent que recevoir autant de connexions en provenance d'une même adresse

Internet partagée par plusieurs personnes, c'est suspect. On leur explique alors que nous gérons des relais Tor et que nous ne sommes donc pas la source du problème. Cela dit, notre expérience est que seule une petite quantité de personnes utilisent Tor pour être pénibles : le nombre de signalements que nous recevons est bien faible en comparaison de la quantité de données que les relais de Nos oignons font transiter chaque mois.

En lisant votre documentation, on voit que vous cherchez à avoir davantage de « relais » ou des « nœuds de sortie », c'est la même chose ou non ?
Pas tout à fait : les relais (ou nœuds) sont les ordinateurs faisant partie du réseau Tor ; les nœuds de sortie sont ceux qui permettent de joindre des sites Internet existants. Pour ces sites, il est facile de penser que le nœud de sortie est à l'origine de la connexion. En cas d'usage malintentionné de Tor, c'est donc souvent l'opérateur du nœud de sortie qui est consulté. Ça représente plus de travail que de faire tourner un relais « simple ».

Est-ce que tous les opérateurs acceptent qu'on mette son ordinateur au service du réseau Tor ?
Pour les nœuds de sortie, beaucoup d'opérateurs ou d'hébergeurs ont des clauses qui leur permettent de couper l'accès sans préavis, à cause des plaintes qui pourraient leur arriver. Cela n'empêche pas d'utiliser Tor ou de faire tourner des points d'entrée prévus qui permettent de contourner les dispositifs de censure (appelés « *bridges* »).
D'autre part, faire tourner un nœud de sortie chez soi n'est pas très utile, à cause de la bande passante limitée et de la gestion des risques liés aux abus. Il est plus utile d'aider Nos oignons à financer de nouveaux nœuds de sortie.

Le projet Tor se bat contre tous ceux qui voudraient faire disparaître l'anonymat, partout dans le monde. Mais en France, quelle est la situation, avec les lois sécuritaires qui s'empilent ? Tor est-il menacé ? Faut-il dès maintenant

envisager un repli vers autre chose ?

L'anonymat est essentiel pour l'exercice des libertés fondamentales, particulièrement la liberté d'opinion. Tor n'est pour l'instant pas directement menacé en France. On sait toutefois que certains policiers souhaiteraient empêcher son usage, et que plus généralement, l'élite politique comprend mal les enjeux autour du chiffrement, comme on peut le voir autour de l'affaire FBI contre Apple couverte par les médias aux mois de mars-avril 2016.

Quoi qu'il en soit, Tor est conçu pour être un outil de contournement de la censure. Tor fonctionne même dans des pays particulièrement répressifs comme la Chine ou l'Iran qui disposent pourtant d'une capacité de filtrage et d'une politique répressive bien supérieures à ce qui existe en France actuellement. Réprimer l'utilisation de Tor risque d'être aussi efficace que de réprimer le partage d'œuvres en pair-à-pair : c'est un logiciel libre, facile à installer et à diffuser. En revanche il est clair que contribuer au projet, sous forme de code ou de relais pourrait être rendu plus difficile ou dangereux.

Il est donc important que les dizaines d'organisations et la

centaine de particuliers qui font tourner des relais en France s'allient aux millions de personnes (dont une centaine de milliers en France !) qui utilisent régulièrement Tor. Restons vigilant·e·s et défendons nos libertés.

Tor a été conçu en partant du principe qu'il existera toujours des endroits où il sera possible de faire tourner des relais, où il sera possible de travailler à améliorer les logiciels et en faire la promotion.

Plusieurs projets envisagent un modèle beaucoup plus distribué et encore plus difficile à arrêter, mais c'est tout de suite plus compliqué comme problème à résoudre : ça pose la question de la compatibilité avec l'existant, et pour l'instant, rien n'est prêt pour le grand public. Il aura fallu dix ans à Tor pour être accessible à tout le monde. C'est important de soutenir ces projets le temps qu'ils mûrissent. Si Tor est remplacé un jour par un système plus fiable, ce sera tant mieux !

Je vois que vous utilisez une ribambelle de logiciels libres (Debian, Postfix, Mailman, Schleuder, SpamAssassin, BIND, Apache, Ikiwiki, Git, Keyringer, et encore de nombreux autres…) : le projet Tor serait-il possible sans des logiciels libres ?
Au-delà du fait qu'on ne peut pas faire confiance à un logiciel dont il est impossible de vérifier le fonctionnement, Tor doit rester accessible à toutes et tous. Personne de devrait avoir à payer pour pouvoir échapper au sentiment d'être surveillé·e. Mais partant de là, les ressources du projet sont plutôt limités. L'intérêt des logiciels libres est aussi de permettre de construire des solutions sur-mesure en assemblant plusieurs logiciels qui existent déjà. Ou alors de pouvoir demander de l'aide à d'autres personnes qui partagent les objectifs du projet Tor tout en travaillant sur d'autres projets. C'est important de pouvoir faire confiance à une communauté. Le projet Tails, par exemple, explique bien cette question de la chaîne de confiance en œuvre dans le logiciel

libre.

De quoi avez-vous le plus besoin ? De compétences techniques, d'argent, de matériel, d'hébergement… ?

Le saviez-vous ? TOR est l'acronyme de The Onion Router, le routeur oignon. Sur le logo de l'association on voit en pointillés le trajet des données, chaque oignon-relais assure l'anonymat.

Nos oignons a bien sûr besoin d'argent pour payer l'hébergement de ses relais actuels et en ouvrir de nouveaux. Les dons réguliers sont précieux car ils nous permettent de mieux voir venir. Pour ce qui est des activités bénévoles, il y a beaucoup plus à faire côté communication et administratif que technique. On essaye d'accueillir toutes les bonnes volontés au mieux !

Actuellement, nous sommes particulièrement à la recherche de nouveaux hébergeurs, prêts à accepter un nœud de sortie Tor avec une bande passante conséquente. C'est nécessaire pour contribuer à la diversité du réseau : répartir les relais Tor chez le plus possible d'hébergeurs participe à la sécurité du réseau.

Message reçu ! Que nos lecteurs les plus aguerris rejoignent Nos oignons !

Quelques liens pour aller plus loin :

- L'article Tor de Wikipédia

- Un bon article sur Tor
- Une longue interview de Lunar aux RMLL
- Plusieurs façons de participer à Nos oignons
- Déployer un nœud Tor
- Pour répondre à pas mal d’autres questions