

NOUVEL HAY MAGAZINE

SANS FRONTIÈRES

T'as pas Tor ?

Internet est né dans les laboratoires de l'armée américaine (de l'IPTO, le bureau des techniques de traitement de l'information de la DARPA, l'organisme de recherche et développement militaire), & la technique du routage en oignon (*onion routing*) est un produit de la marine américaine.

Avec un principe élaboré par trois chercheurs du US Naval Research Lab, David Goldschlag, Mike Reed, and Paul Syverson: pour conserver la nature privée des échanges, on transite par plusieurs nœuds de communications (qui changent à chaque nouveau message) avec un chiffrement à chaque étape. D'où le nom d'oignon, passant par plusieurs couches avant d'accéder au message.

Le but était de brouiller les pistes, de ne pas



if
r
e
c
i
r
c
u
l
e
r

des messages en clair dans un tuyau identique.
C'est TOR (The Onion Routing).

Utilisé par les technophiles protégeant leur anonymat et les activistes susceptibles d'être

pistés par le gouvernement ou une entité privée, le Projet [Tor](#) se développe à partir de 2005. Il regroupe les initiatives de bénévoles favorables au projet pour un réseau fiable ainsi que des outils simples d'usage, à commencer par un navigateur. Cette entreprise se justifie durant les évènements du printemps arabe en 2011.

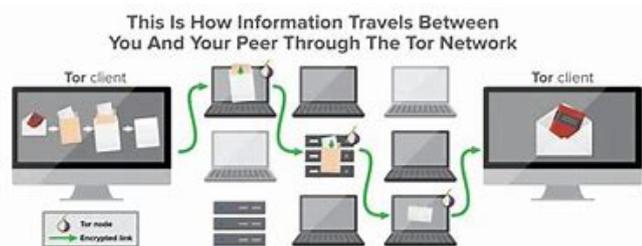
Depuis 2015, l'ICANN (l'agence répertoriant et attribuant les noms de domaine sur Internet) a réservé le Onion Routing pour les serveurs liés à cette technologie, lui offrant une reconnaissance de premier ordre.

Le Projet Tor est soutenu par l'Electronic Frontier Foundation (organisation non gouvernementale basée à San Francisco et prônant la liberté des communications électroniques): le manque de confiance dans les acteurs étatiques des télécommunications.

Un rapport administré-administration corroboré par le Patriot Act (ensemble de lois restreignant les libertés individuelles et publiques suite aux attentats du 11 septembre 2001) puis par l'affaire Edward Snowden, (contractuel œuvrant pour la NSA ayant exfiltré plusieurs documents confidentiels sur la surveillance généralisée de la population américaine).

Ces deux évènements suscitent des initiatives comportementales et technologiques en vue de se soustraire à la vue des yeux d'un État jugé indiscret et débordant du cadre de la nécessaire sécurité intérieure. Cette défiance s'observe vis-à-vis des sociétés privées désireuses de faire du business avec des données recueillies, avec des méthodes limites à la loi et à l'éthique, lorsque celles-ci ne sont pas franchies par «pure inadvertance».

Mais «si l'on n'a rien à cacher, pourquoi



la
?
»
P
a
r

ce que la liberté c'est pouvoir garder pour soi même ce qui est insignifiant et inutile. Bien sûr il y a un devoir d'assistance à la justice et à la police dans des enquêtes diligentées au nom de l'ordre public, mais il n'y a pas de devoir de transparence.

La directrice générale du Tor Project, précise : «La police et les autres forces de l'ordre utilisent aussi Tor pour leur travail. Nous pouvons en citer des exemples non seulement aux États-Unis, mais également dans d'autres pays d'Europe et du monde. Nous ne compliquons le travail de personne, la police est en mesure de mener ses enquêtes indépendamment de

l'existence de nos outils.

Autrement, n'importe qui pourrait prétendre que tout ce qui a déjà servi à se cacher ou à dissimuler ses crimes, comme des banques offshore, des paradis fiscaux ou une voiture utilisée pour fuir, est une invention qui complique le travail de la police.»

Tor Project puise son intérêt dans l'approche vis-à-vis d'Internet : un mode actif et un mode passif. Le mode passif consiste à exploiter Internet sans être visible et laisser de traces. Le mode actif contourne une censure du réseau Internet opérée dans un pays.

TorBrowser

Si TorBrowser s'est déployé au sein des systèmes d'exploitation Linux et Windows, le domaine des communications mobiles est plus difficile à régler.

Car le système d'exploitation des terminaux mobiles évolue rapidement, et son architecture diffère de ses homologues sur poste fixe. Or les possesseurs de mobiles sont, selon les derniers chiffres de , évalués à 5,11 milliards (sur une population de 7,69 milliards), dont 4 milliards sont actifs.

«Les fonctionnalités de base que nous proposons sur toutes les plates-formes sont les mêmes: tant sur les moyens de défense contre le suivi des utilisateurs, ainsi que les fuites d'adresses IP, que sur les moyens de contourner une éventuelle censure. Sur Android, nous n'avons pas encore mis en œuvre toutes les améliorations en termes de convivialité, que nous avons apportées au fil des années, comme l'affichage du trajet ou la possibilité d'atteindre rapidement un état correct, mais celles-ci figurent sur notre feuille de route» .



«Il existe d'importantes différences entre la conception de Tor Browser pour Android et son développement. La raison en est que la plate-forme est très

différente de celle des ordinateurs de bureau, tels que Windows, MacOS et Linux. Donc, ce n'est pas simplement une autre plate-forme que nous supportons, même si nous avons pu réutiliser une partie du code que nous avons déjà écrit pour Tor Browser sur desktop.»

Si TorBrowser est parvenu à une version stable sur Android, le développement devrait bénéficier du retour des utilisateurs ainsi que des tests effectués par la communauté soudée autour de cette initiative":

«Nous espérons pouvoir encore ajouter [sur les versions Android, nldr] certaines fonctionnalités qui n'ont pas été intégrées à Tor Browser 8.5, comme une meilleure intégration F-Droid ou un affichage de trajet Tor sur mobile.»

Le navigateur Tor devra conquérir les terminaux mobiles iOS, et gagner le gestionnaire d'applications App Store, contrôlé de très près par la firme à la pomme.

Le projet Tor perfectionne son navigateur sur poste fixe : «Nous sommes en train de migrer Tor Browser vers une nouvelle version majeure de Firefox (68 ESR) ...».

«Nous pensons que tous les navigateurs devraient offrir le même niveau de protection que le navigateur Tor. Si vous examinez les recherches récentes publiées par DuckDuckGo, vous verrez que les utilisateurs s'attendent à ce que les "onglets privés" ou le "mode de navigation privée" fassent ce que Tor Browser effectue déjà, mais ce n'est pas le cas.

Les constructeurs de navigateurs devraient en tenir compte, car de plus en plus de personnes exigent une protection accrue de la vie privée en raison de la série de scandales et d'informations sur la manière dont les entreprises (et parfois les gouvernements) explorent également leurs données personnelles.»

sources : directrice du Projet Tor, WeAreSocial

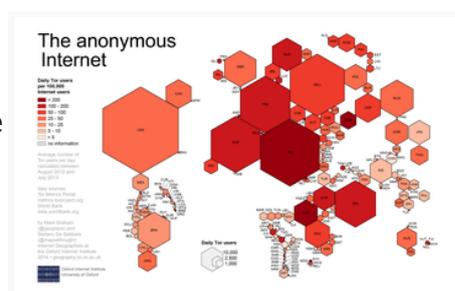
or est utilisé pour se protéger contre une certaine forme de surveillance sur Internet, connue sous le nom d'*analyse de trafic*. Cette analyse est utilisée pour déterminer qui communique avec qui sur un réseau public. Connaître la source et la destination de votre trafic peut permettre à des personnes de traquer votre comportement et vos intérêts.

Tor est aussi un outil de contournement de la censure sur Internet. Il permet aux personnes l'utilisant d'accéder à des sites, contenus ou services bloqués dans certaines zones du monde. [Facebook](#)¹¹ ainsi que le site internet de [The New York Times](#)¹² proposent ainsi une version de leur site utilisant le système de service caché du réseau.

Tor fait circuler le trafic des personnes utilisatrices via une série de relais. Ce procédé permet de ne pas être suivi par les sites web consultés, d'accéder à des services, contenus ou sites bloqués par un [FAI](#). Il est aussi possible pour chaque personne utilisatrice de publier des contenus via les services « onion » de Tor, sans révéler la position de ces services.

Ces avantages peuvent être utiles pour chaque personne utilisatrice qui souhaite maîtriser ses traces laissées en ligne. Ils sont notamment mis en œuvre dans les échanges entre personnes lanceuses d'alerte, journalistes, avocats, dissidents politiques, représentants d'organisations non gouvernementales, ou pour échanger en maîtrisant la sécurité de leurs données, de leur connexion, de leurs destinataires et de leur position. Il peut aussi servir à des personnes ou organisations malveillantes en permettant un certain anonymat .

source : wikipedia



Cartogramme de l'usage de Tor à l'international.



