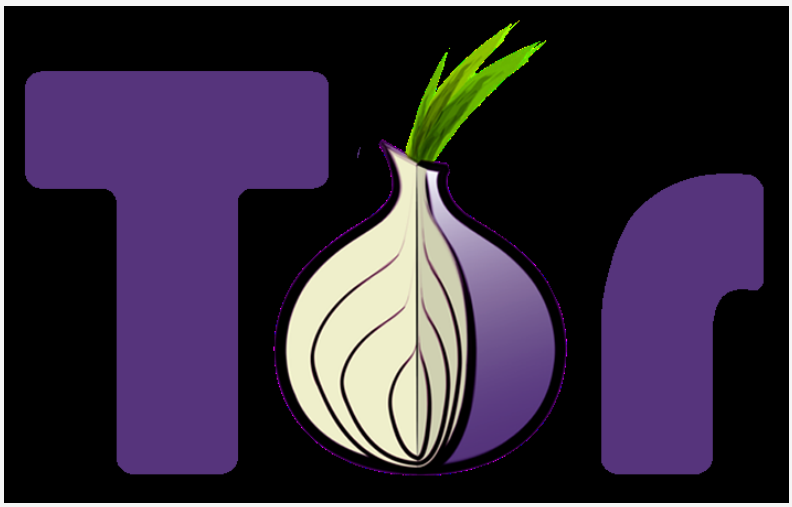
Toutelaculture.com

URL : http://www.Toutelaculture.com/
PAYS : France
TYPE : Web Grand Public

► **11 août 2015 - 16:55**

Cliquez ici pour accéder à la version en ligne

Tor, un réseau fiable ?



Depuis sa création en 2001, le réseau Tor, qui permet de naviguer sans dévoiler ses informations personnelles, fait de plus en plus d'adeptes. Mais cet outil de cybercensure est aussi parfois accusé de cybercriminalité. Alors, Tor est-il vraiment un réseau fiable ? Le point avec Toute La Culture.

Tor (The Oignon Router) est un réseau informatique parallèle au Web classique entièrement décentralisé. Il est composé de noeuds aussi appelés routeurs qui transmettent de manière anonyme des flux TCP. Autrement dit, ce qui circule dans ces flux reste anonyme grâce à une cryptologie hybride. Depuis 2001, date de sa création, Tor est utilisé chaque jour par 2,5 millions d'internautes selon Karen Reilly, directrice du développement du réseau. Preuve de son utilité.

En effet, contrairement au Web sur lequel nous sommes en permanence en train de partager des données personnelles (photos, vidéos, date de naissance, localisation etc), Tor permet de naviguer anonymement et permet de se rendre sur des sites cachés dont l'adresse se termine par « .onion ». De plus, selon ses utilisateurs, Tor est un bon moyen d'échapper aux publicités intempestives ainsi qu'aux vols de données personnelles par les hackers, l'Etat mais aussi les grosses entreprises qui utilisent des cookies. Largement utilisé par les journalistes, militants et dissident du monde entier, Tor permettrait notamment de contourner les systèmes de censure étatique pour communiquer. Enfin, le réseau permettrait aux « opposants ou dissidents à une régime autoritaire de déjouer les écoutes téléphoniques et la cybercensure », rapporte La Tribune. Des pays comme la Chine, la Russie, l'Iran ou encore les Etats-Unis tenteraient par exemple de bloquer le trafic sur Tor et espionnerait les utilisateurs du réseau afin de déceler toutes formes de terrorisme/cyberterrorisme/espionnage etc.

En 2011, le site RevolteNumérique révélait d'ailleurs que des chercheurs français avaient réussi à piraté Tor afin de montrer les limites du réseau. « La cryptographie implantée dans TOR est mauvaise… On a réduit considérablement le degré de deux des trois couches de chiffrement. [...] On ne peut pas imaginer que la fondation derrière TOR ne soit pas consciente de ses failles » confiait Eric Filiol, directeur du laboratoire de recherche en cryptologie et virologie de l'**ESIEA**. Failles qui au fils des années se feraient de plus en plus nombreuses. La première : la NSA aurait mis en place plusieurs noeuds Tor Browser afin de collecter des informations sur le réseau et deuxièmement le trafic de certains sites consultés par les activistes seraient également contrôlés par la NSA. Résultat : l'anonymat indiqué comme complet ne l'est plus totalement.

Tor, ou la cybercriminalité

En plus de ses failles en matière de chiffrement, Tor est accusé par beaucoup de cybercriminalité,

de piratage, d'atteinte à la vie, de vols de données ou encore de produire un commerce de produits illicites. En effet, si le réseau informatique a tant à cacher c'est qu'il aurait pour certains beaucoup à se reprocher. Toujours selon La Tribune, c'est pour cette raison qu'une opération de cyberpolice intitulée « Onymous » avait été lancée par Europol, mettant « à genoux le site délinquant Silk Road en 2013 . La pérennité de Tor elle-même avait alors été remise en question.

De son côté, Karen Reilly, assurait le mars dernier lors du Circumvention Tech Festival de Valence, qui réunit les hackers, experts informatiques, journalistes et partisans de l'Internet libre que tout ce qui circule sur Tor n'est pas forcément critiquable. « La très grande majorité de nos 2,5 millions d'utilisateurs ne sont pas des criminels ! » expliquait-elle.

David Kaye, chargé de la promotion et de la protection du droit à la liberté d'opinion et d'expression à l'ONU, considérerait même Tor comme essentiel pour les droits de l'homme à la vie privée et à la liberté d'expression.

Des options alternatives

Cependant, il faut rappeler que Tor reste un réseau informatique pour le moins compliqué à utiliser, nécessitant des connaissances pointues dans le domaine. Il est donc difficilement accessible à la grande majorité du public comme l'atteste les chiffres d'utilisation du logiciel. Des solutions complémentaires et/ou alternatives à la gestion des informations à caractère confidentiel existent, parfois très simple d'utilisation ou poussées.

Cela va de la simple gestion des paramètres de confidentialité à régler sur le navigateur web utilisé ou l'utilisation d'un moteur de recherche respectueux de votre vie privée (Yacy, DuckDuck Go, Ixquick, Startpage…) au recours à un proxy (pour l'anonymisation) en passant par l'anti-virus qui intègre quasi automatiquement de nos jours des fonctionnalités permettant une navigation sécurisée (virus et hacker) et une protection de la vie privée.

Visuel : Logo officiel Tor

LAISSEZ UN COMMENTAIRE VIA FACEBOOK: