Darknet

Description

Réseau informatique permettant de communiquer de manière anonyme. Des réseaux assurant la sécurité des communications existaient déjà dans les années 1970, à l'époque de l'Arpanet, ancêtre de l'internet. L'usage du terme *darknet* s'est répandu à la suite de la publication en 2002 d'un article intitulé « *The Darknet and the Futur of Content Distribution* », qui démontrait que les *darknets* empêchaient l'application des mesures de protection des droits des œuvres numériques (DRM, *Digital Rights Management*). Comme l'internet est un réseau de réseaux, il n'existe pas un *darknet* unique, mais des *darknets* qui constituent des outils de communication en ligne, alternatifs à ceux de l'internet grand public. Baptisés F2F, pour *friend-to-friend*, les *darknets* sont des réseaux privés virtuels (VPN ou *Virtual Private Network*) permettant à un nombre limité d'utilisateurs de confiance de communiquer, sans laisser de traces, grâce à l'anonymisation des adresses IP et, souvent, le chiffrement des informations transmises. Parmi les *darknets* les plus connus, Freenet, GNUnet, RetroShare ou I2P sont utilisés afin de partager des fichiers pair-à-pair (P2P ou *peer-to-peer*) et dialoguer en toute confidentialité par courrier électronique ou par messagerie instantanée.

S'appuyant sur une architecture décentralisée (l'ordinateur de chaque utilisateur fait office de relais), un protocole de transmission spécifique et des logiciels *open source*, les *darknets* se distinguent du web visible – cette infime partie d'internet balayée par les moteurs de recherche, en opposition au web invisible – ainsi que des services internet grand public tels que la messagerie électronique, dont le fonctionnement est centralisé, les logiciels propriétaires et le stockage des données en clair par défaut.

Conduite par le FBI et Europol en novembre 2014, l'opération Onymous a permis de mettre fin aux activités d'un site dénommé Silk Road 2 (le n°1 ayant été fermé par le FBI en octobre 2013), spécialisé notamment dans la vente de drogues et de faux documents d'identité, payables en *bitcoins*, la devise numérique échappant à toute autorité monétaire. Cette saisie record de serveurs situés aux Etats-Unis, en France, aux Pays-Bas, en Allemagne et en Bulgarie a relancé la polémique sur l'existence « d'un *darknet* », synonyme de plaque tournante d'activités illégales en tout genre. Silk Road, ainsi que des dizaines de sites de vente de drogue en ligne pris dans les filets du FBI et d'Europol (l'office européen de la police) étaient accessibles sur le réseau TOR (*The Onion Router*). Sur le marché des stupéfiants, estimé par l'ONU à plus de 300 milliards de dollars par an, seulement plus de 1 milliard aurait transité par le site Silk Road entre février 2011 et juillet 2013.

Conçu par l'US Navy pour ses propres activités, TOR est désormais le plus utilisé des P2P anonymes. Il rend les connexions anonymes en organisant un routage aléatoire avec chiffrement des données à chaque nœud relais. Mais c'est aussi parce qu'il permet de cacher les adresses IP de sites internet en .onion, que le réseau TOR est devenu l'emblème d'un internet sombre, un *darknet*, composé de sites cachés (*hidden services*), aux activités criminelles. Après le scandale des écoutes généralisées révélé par Edward Snowden (utilisateur de TOR), l'organisation indépendante qui développe le TOR Project a des raisons de s'inquiéter

: quels moyens ont été utilisés par les agents fédéraux pour passer outre le système d'anonymisation ? Ils sont en effet bien plus nombreux que les délinquants et les criminels, ceux dont l'activité légitime nécessite de passer par des voies détournées pour collecter ou échanger des informations librement, en toute confidentialité, à l'instar des chercheurs, des journalistes et des lanceurs d'alerte protégeant leurs sources, des reporters sur des zones de conflits, des ONG, des dissidents politiques contournant la censure, des activistes, des blogueurs, des militants et plus généralement des citoyens désireux d'échapper au siphonnage de leurs données personnelles dû à la traçabilité généralisée sur le web. Le projet TOR comptait environ un million d'utilisateurs quotidiens fin 2013.

La réussite de l'opération Onymous a entamé la crédibilité du projet TOR, au moment même où la fondation Mozilla annonce sa volonté de s'en rapprocher. Lancé en 2004 par Mozilla, le logiciel libre Firefox comprend quelques outils permettant aux internautes de mieux protéger leur vie privée en surfant sur l'internet (comme le moteur de recherche DuckDuckGo qui n'enregistre pas les données de navigation ou encore un assistant de vie privée). En novembre 2014, pour les dix ans de Firefox, la fondation Mozilla s'associe au projet TOR et au Center for Democracy et Technology (organisme à but non lucratif) pour lancer Polaris, une initiative invitant les acteurs du web soucieux des questions de vie privée à travailler ensemble. Ainsi, dans le cadre de Polaris, les développeurs de TOR et de ceux de Mozilla vont partager leur savoir-faire, afin, d'un côté, d'ajouter de nouvelles fonctionnalités de sécurité et de protection de la vie privée dans Firefox et, de l'autre, d'intégrer TOR dans Firefox. En outre, des serveurs de la fondation Mozilla deviendront des nœuds relais TOR afin d'accroître les capacités du réseau, encore beaucoup trop lent.

Interrogé dans l'émission *Place de la Toile* diffusée le 30 novembre 2013 sur France Culture, Jérémie Zimmermann, porte-parole et cofondateur de La Quadrature du Net, s'insurgeait contre la gigantesque campagne de diabolisation de l'internet orchestrée, selon lui, par les géants du Net comme Google et Facebook « *marchant main dans la main avec la NSA* », visant à faire croire en l'existence d'une zone numérique de non-droit baptisée « le *darknet* », et qui n'existe pas. Cela dans le seul but de justifier une surveillance de masse des internautes, en empêchant la circulation anonyme des informations sur internet. Communiquer grâce à un protocole autre que celui du web ne donne pas naissance à « un internet sombre », à moins que celui-ci ne désigne pas autre chose qu'un internet anonyme, entendu comme l'intégralité de l'internet à l'exception du web grand public, soit l'immense majorité des informations qui transitent par le réseau des réseaux, auxquelles les moteurs de recherche n'ont pas accès : à commencer par les intranets et extranets d'entreprises, d'associations, de syndicats, de chercheurs, sans oublier tous les contenus hébergés dans le *cloud*. Selon Jérémie Zimmermann, l'anonymat est inhérent à la liberté d'expression et il est une composante de la protection de la vie privée : « *La solution, l'anti-NSA, l'anti-société de surveillance, ce serait ce que l'on appelle aujourd'hui le darknet. Et voyez le paradoxe, d'un côté, il y a Google qui est blanc, le blanc de la pureté, et de l'autre côté, il y a ce qui est dark, ce qui est sombre, mais en réalité la liberté se trouve du côté sombre et non pas du côté clair.* »

Relayé par de nombreux médias pour démontrer l'existence d'une face vile et obscure du web (encore confondu avec l'internet), l'usage du mot « *darknet* » devrait raisonnablement se limiter à désigner des sites internet illégaux, et non les programmes d'anonymisation des communications en ligne comme TOR. Cet amalgame sémantique ne doit pas pour autant faire oublier que

l'anonymat absolu est une illusion sur l'internet. Le projet TOR est aujourd'hui encore principalement financé par le ministère de la défense américain. Ayant reçu le prix du logiciel libre 2010 dans la catégorie « *Projet d'intérêt social* », TOR est aussi un instrument au service des forces armées et de la police pour lutter contre la vente d'armes ou la pédophilie, fléaux qui n'ont rien de virtuel. Selon Mediapart, une étude menée par des chercheurs de l'université du Luxembourg en 2013 montre que sur près de 40 000 *hidden services* recensés, on compte autant de services illégaux que de sites consacrés à la politique ou à l'anonymat, tandis que les plus visités servent à contrôler des réseaux de robots informatiques (*botnets*) pour mener des attaques informatiques. Si les outils d'anonymisation sont efficaces pour lutter contre le ciblage comportemental ou pour télécharger illégalement des films, les experts sont d'accord pour souligner l'inefficacité de ces programmes à garantir un anonymat total sur l'internet face à la détermination des agences de renseignement.

Comme l'indique *Le Monde* (25-26 janvier 2015), la liste est longue des programmes de surveillance utilisés par la NSA et par le GCHQ, service électronique britannique de renseignements : Muscular pour espionner les grands services internet privés à leur insu (et non avec leur accord comme le programme Prism) ; Tempora du GCHQ pour intercepter le trafic internet directement sur les câbles transatlantiques; Bullrun pour affaiblir des systèmes de chiffrement utilisés dans le monde entier ; Quantumhand pour espionner grâce à un serveur clandestin les utilisateurs de Facebook ; Dishfire pour collecter et analyser les SMS ; Wellspring pour stocker des photos de visage circulant sur le réseau, etc.

Sources :

- Darknet, http://fr.wikipedia.org
- « Après l'affaire Snowden, l'anonymat sur internet en question », Jérôme Hourdeaux, Mediapart.fr, 9 septembre 2013.
- « Darknet : immersion en réseaux troubles », Olivier Tesquet, *Télérama*, n°3322, 14 septembre 2013.
- « Qui a peur du grand méchant « darknet« », Amaelle Guiton, Slate.fr, 27 novembre 2013.
- Mythologies du Darknet, émission Place de la Toile, Franceculture.fr, 30 novembre 2013.
- « Mozilla s'associe au projet Tor et va promouvoir la navigation anonyme dans Firefox », Eric LB, 01net.com, 10 novembre 2014.
- « Darknet : le mystère autour des méthodes de la police inquiète le projet Tor », Pierre Fontaine, 01net.com, 12 novembre 2014.
- « Nouvelles révélations sur les pratiques de la NSA », Yves Eudes et Christian Grothoff, avec Monika Ermert, Laura Poitras, Matthias Wachs et Jacob Appelbaum, *Le Monde*, 25-26 janvier 2015.

Categorie

1. A retenir

date créée
21 avril 2015
Auteur
francoise