La face cachée du Web caché, le « dark Web »

	La face cachée du Web caché, le « dark Web »

Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaire.

«Sur Internet, on peut acheter une kalachnikov en deux clics.» Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge.

Depuis les attentats de janvier notamment, Internet (1) est au cœur des préoccupations. «Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles?», interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web… Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un navigateur personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une adresse IP, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

«Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre, explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet.»

Une fois sur TOR, pas de moteur de recherche. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches… C'est l'Internet «surfacique», une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur… C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden Wiki (le «wiki» caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 € ou un pistolet SIG Sauer de calibre 9 mm pour 790 €.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas… Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en bitcoins, une monnaie virtuelle et chiffrée, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire «confiance» à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un «facilitateur de la performance criminelle», selon Solange Ghernaouti: «Internet reflète notre réalité sociale, économique, politique et criminelle, poursuit-elle. Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation – on agit caché derrière un écran – à distance.»

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les «internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques», poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins.

———

LES MOTS POUR COMPRENDRE

Internet représente un réseau de télécommunication international reliant des ordinateurs à l'aide du protocole TCP/IP. Il sert de support à la transmission de données: pages Web, courriels, fichiers informatiques.

Une adresse IP (Internet Protocol) est un numéro d'identification attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Une adresse IP est un numéro unique permettant à un ordinateur de communiquer dans un réseau.

Un moteur de recherche est un site Internet régi par une application sur lequel, en entrant des mots-clés, on obtient une liste de sites correspondant à la demande. Exemple: Google.

Un réseau virtuel privé est un passage ou un lien qui permet d'ouvrir un réseau local vers l'extérieur et de le connecter à un autre réseau local, grâce à une connexion Internet et avec une sécurité optimisée.

Le wiki est une application Web participative dont les internautes peuvent modifier les contenus.

Le terme bitcoin (de l'anglais « bit », unité d'information binaire, et « coin », pièce de monnaie) désigne à la fois un système de paiement virtuel et l'unité de compte utilisée par ce système.

Le chiffrement est une technique d'écriture en langage crypté ou codé. C'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant de clés.

Réagissez à cet article

Source : http://www.la-croix.com/Ethique/Sciences-Ethique/Sciences/La-face-cachee-du-dark-Web-2015-12-08-1390141