وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي

LETTRE D'INFORMATION : BON A SAVOIR (N°18)

Qui a peur du grand méchant «darknet»?

Il est, régulièrement, le terrain virtuel de reportages propres à effrayer la fameuse «ménagère de moins de 50 ans».

Bienvenue dans «le darknet», présenté comme un Internet «bis» sans foi ni loi... Mais qu'y a-t-il, au juste, derrière le fantasme?

Sur la page web consacrée au reportage «Darknet: la face cachée du Net» diffusé vendredi 14 novembre sur France 2 dans l'émission Envoyé spécial, le «pitch» donne le ton : *«On y trouve de tout: drogues, armes, numéros de cartes de crédit. En toute liberté et dans l'anonymat total.»*

Avant d'ajouter, histoire de rétablir un peu la balance: *«Mais c'est de là aussi que peuvent agir les cybermilitants traqués par les dictatures.»*

Si l'Internet est aujourd'hui, pour le député PS Malek Boutih, *«une sorte de Far West»* où s'exprimeraient *«les pires pulsions»* – comme il était hier pour l'UMP Frédéric Lefebvre un repaire pour *«les psychopathes, les violeurs, les racistes et les voleurs»*, ou pour Jacques Séguéla *«la pire saloperie qu'aient jamais inventée les hommes»* –, alors «le darknet» en constituerait les bas-fonds, une *terra incognita* quadrillée de ruelles obscures, plus coupe-gorge que coin tranquille. Du pain béni pour les reportages en mode gonzo et les récits sensationnalistes façon *«j'ai rencontré un trafiquant d'armes»*.

«Quelle part de réalité, quelle part de boursouflure journalistique?», interrogeait récemment Daniel Schneidermann sur @rrêt sur images, pronostiquant au sujet *«un bel avenir de mythologie terrifiante»*. Comme souvent sur le réseau, pour déconstruire un fantasme – qui contient par définition sa part de vérité –, il faut commencer par les tuyaux et les machines. Et se poser les questions dans l'ordre.

«Le darknet» existe-t-il?

Techniquement, non: il n'y a pas *un* darknet mais des darknets, autrement dit des réseaux privés anonymes construits entre pairs de confiance, «d'ami à ami» (friend to friend). Ce type de réseau peut être mis en place par un tout petit nombre d'utilisateurs, ou par une communauté plus large, par exemple à l'aide de logiciels comme Freenet, Retroshare ou GNUnet, et sert le plus souvent au partage de fichiers et à la communication.

Parler «du darknet» comme d'une entité cohérente – et, le plus souvent, menaçante – relève d'un glissement sémantique, entretenu par la polysémie du qualificatif – *dark* pouvant faire écho aussi bien à l'opacité de l'anonymat qu'au «côté obscur». Son usage actuel renvoie moins aux darknets qu'à un Internet «caché», c'est-à-dire à des serveurs non accessibles par les protocoles et les logiciels usuels. C'est le cas, par exemple, des services cachés (hidden services) du réseau Tor, uniquement accessibles via celui-ci.

Internet «caché», et non pas «profond»: là encore, la confusion est fréquente avec ce qu'on nomme le *deep web*, par opposition au web «surfacique». Le deep web, c'est celui qui n'est pas indexé par les moteurs de recherche. Non parce qu'il n'est pas accessible, mais parce que les algorithmes ne permettent pas son indexation, ou parce qu'il est protégé (au sens strict, un

document partagé sur Google Drive pourrait être classé dans le *deep web*). En 2001, sa taille était estimée à plus de 400 fois celle du web de surface. Avec le développement du *cloud*, c'est certainement beaucoup plus aujourd'hui.

À quoi sert le réseau Tor?

Qu'est-ce donc que Tor, ce réseau régulièrement présenté comme «la porte d'entrée du darknet»? Comme l'indique (presque) l'acronyme, The Onion Router, Tor est un réseau d'anonymisation. Il fait transiter le trafic par plusieurs «n*œ*uds», comme à travers les couches d'un oignon, de telle façon qu'on ne puisse plus, à la sortie, en déterminer l'origine.

Originellement construit sous l'égide de la Navy américaine, Tor est aujourd'hui développé par une organisation indépendante, le Tor Project. Pour l'année fiscale 2011, 60% de son financement provenait du gouvernement américain, et 18% de fondations et de subventions, comme l'indique son dernier rapport. Éternel paradoxe: la protection offerte par le réseau est à la fois utilisée par les militaires américains, à des fins de renseignement notamment, et combattue par la NSA et le GCHQ, son équivalent britannique.

L'accès aux services cachés – déployés depuis 2004 – n'est qu'un des usages possibles de Tor. On peut tout aussi bien consulter son courrier, faire de la messagerie instantanée ou se connecter au web «visible» via le réseau. Les «nœuds» (en relais ou en sortie), les «ponts» (relais non publics) et les «points de rendez-vous» (permettant l'accès aux *hidden services*) étant décentralisés, il est par définition impossible de savoir quelle proportion des connexions va vers les services cachés, sauf à surveiller l'ensemble du trafic.Comme nous l'indique avec un brin d'humour noir Andrew Lewman, le directeur exécutif du Tor Project: *«En théorie, la NSA et le GCHQ pourraient répondre à cette question.»*

Qui trouve-t-on sur l'Internet caché?

Par définition, des personnes qui ne souhaitent pas être surveillées, mais aussi des personnes en butte à la censure de l'Internet dans leur pays. Ainsi, pour les trois derniers mois, en consultant les statistiques de Tor, on trouve une moyenne de 2.000 utilisateurs quotidiens au Bahreïn, entre 15.000 et 20.000 en Iran, ou encore 6.000 en Syrie – pour ne prendre que quelques exemples des «pays ennemis d'Internet» identifiés par Reporters sans frontières. En Russie, pays *«sous surveillance»*, ils sont 120.000 chaque jour.

Le nombre total d'utilisateurs quotidiens – faussé depuis la fin août par un afflux attribué à un réseau de bots informatiques – est évalué à un million environ par les membres du Tor Project. L'humanité étant diverse, on trouvera parmi eux des militants, des lanceurs d'alerte, des journalistes, des blogueurs, mais aussi des militaires et des policiers, voire des citoyens «lambda» plus soucieux de vie privée que la moyenne. Et, en effet, des criminels. Mais là encore, impossible, sauf à monitorer l'ensemble du trafic, de faire la part statistique des usages socialement utiles et des activités socialement néfastes.

Il n'existe pas de répertoire exhaustif des services cachés mais uniquement un portail, *The Hidden Wiki*. Lequel, sans hiérarchie, liste aussi bien un site-miroir de WikiLeaks et des forums hacktivistes qu'un site de vente de faux passeports britanniques, un *black hat* qui loue ses services (moyennant 50 euros et beaucoup de fautes d'orthographe) ou encore un «Assassination Market» dont le fondateur a été récemment interviewé par le journaliste américain Andy Greenberg. Sans oublier The Silk Road, «l'eBay de la drogue», remis en orbite un mois après l'arrestation de son fondateur présumé, Ross Ulbricht.

Faut-il alors donner raison aux reportages à sensation? C'est évidemment plus compliqué. À moins de tester toutes les offres, difficile de faire la part des «plaisantins» pratiquant l'escroquerie pure et simple, et de ceux qui ne le sont pas. Plus fondamentalement: cette réalité-là existe, et la glisser sous le tapis n'aurait pas de sens; mais l'effet de loupe peut être trompeur. À titre d'exemple, d'après l'acte d'accusation de Ross Ulbricht, il se serait échangé sur Silk Road, entre février 2011 et juillet 2013, l'équivalent de 1,2 milliard de dollars, entre 3.800 vendeurs et 147.000 acheteurs. À mettre en regard avec les 320 milliards annuels

auxquels les Nations unies estiment le marché mondial du trafic de stupéfiants, dont la vente en ligne n'est qu'une des modalités, encore minoritaire.

Bitcoin, la «monnaie du crime»?

Une partie de la «mythologie du darknet» repose sur la monnaie utilisée pour les échanges: Bitcoin, une devise numérique décentralisée, dont l'émission, dégressive, est régie par des algorithmes (avec un plafond de 21 millions d'unités fixé pour 2030), et le cours, par la loi de l'offre et de la demande. Lancé en 2009 par un mystérieux Satoshi Nakamoto, Bitcoin est conçu comme une tentative d'échapper à l'autorité des banques centrales. Mais pas, loin s'en faut, aux mouvements spéculatifs, comme le prouvent ses flambées récentes.

À quoi servent les bitcoins ? D'après une étude publiée l'an dernier par deux universitaires israéliens – dont Adi Shamir, coinventeur de l'un des plus fameux algorithmes cryptographiques –, la majorité d'entre eux (55% selon l'hypothèse la plus basse) passeraient, en réalité, leur temps... à dormir sur les comptes de leurs propriétaires.

Quant aux devises qui circulent, on ne peut pas, techniquement, différencier les usages légaux de ceux qui ne le sont pas. Toutes les transactions laissent une trace, mais l'identité des utilisateurs, elle, est cachée – comme avec l'argent liquide. En tout état de cause, la réputation sulfureuse du Bitcoin pourrait s'évaporer peu à peu, de nouveaux usages ne cessant d'apparaître – de l'achat de matériel électronique à la commande de pizzas, des frais universitaires à Chypre aux voyages dans l'espace organisés par Richard Branson.

Il n'est pas anodin que le Sénat américain se soit penché sur le «cas Bitcoin», ni que le président sortant de la Banque centrale US lui ait reconnu *«du potentiel»*. Si elle n'est régulée par aucune autorité, sa reconnaissance progressive – comme cet été par l'Allemagne – la soumet aux taxations et aux déclarations, y compris auprès du fisc français.

Au-delà de la nature des transactions, Bitcoin pose de nombreuses questions, à commencer par la sécurité des dépôts. Quant à savoir l'effet que pourraient avoir, à terme, les devises virtuelles, par définition imperméables aux politiques monétaires, difficile aujourd'hui de le dire. C'est bien sur cet aspect que portent nombre de critiques, qui pointent le risque d'une spirale déflationniste – ce qui nous emmène, pour le coup, assez loin du «darknet».

Conclusion: faut-il avoir peur du «darknet»?

Que faut-il retenir de tout ça? Que les réseaux d'anonymisation, la cryptographie, les monnaies virtuelles sont autant de technologies dont les usages, plus ou moins légitimes, ne sont pas inscrits dans le code. L'Internet – visible et caché – est un espace social, qui rassemble aujourd'hui plus des trois quarts de la population des pays occidentaux et 40% de celle de la planète.

L'accent mis sur «le darknet» n'est pas seulement anxiogène, il est aussi superficiel, en ce qu'il ne replace aucune des questions soulevées en perspective. Le trafic d'armes ou de stupéfiants, le blanchiment, la pédophilie ne sont pas des problèmes «du darknet», mais des problèmes sociaux.

On ne trouve, sur l'Internet caché, que ce qu'on est venu chercher. Le coffre-fort numérique du New Yorker, destiné aux sources sensibles, est un *hidden service* accessible via Tor, comme le «UK Guns & Ammo Store». Le meilleur et le pire coexistent dans le même réseau – comme ailleurs. Bien sûr, plus les technologies protégeant la vie privée sont robustes, plus les mésusages qui en sont faits seront difficiles à détecter et à combattre. La police n'est pas pour autant démunie, comme l'ont montré la fermeture, cet été, de l'hébergeur Freedom Hosting par le FBI, ou l'arrestation début octobre de Ross Ulbricht.

C'est là une donnée fondamentale à l'ère de la surveillance numérique généralisée: la course-poursuite entre surveillants et surveillés, la dialectique entre centres et périphéries, le rapport de forces entre utopies techno-libertariennes et pouvoirs institutionnels.

Bien malin qui pourrait deviner où et quand s'établira le point d'équilibre. Une chose est sûre: «le darknet», sa mythologie et sa réalité, ressemblent plus au doigt qu'à la lune. Avant d'affoler le chaland, il faudrait peut-être commencer par regarder au bon endroit.
http://www.slate.fr/monde/80471/qui-peur-du-grand-mechant-darknet

«Le Darknet est devenu la poubelle du web»

Le premier rapport sur la cybercriminalité développé par le Centre européen de lutte contre la cybercriminalité (EC3) a été présenté à Bruxelles, lundi 10 février, dans le but d'élaborer des techniques pour faire face à ce nouveau danger. Aujourd'hui, bon nombre des crimes commis sur la toile sont effectués sur le « Darknet », un ensemble de réseaux garantissant l'anonymat aux utilisateurs. Comment accède-t-on à cette partie du web? Qui sont les internautes qui y s'aventurent ? Éléments de réponse avec Jean Harivel, Chargé d'enseignement au sein du master Droit numérique à l'Université Panthéon-Sorbonne (Paris-I).

JOL Press : Comment définiriez-vous le "strong>Darknet ? A quoi sert-il ?

Jean Harivel : A l' origine, le Darknet regroupait les réseaux isolés d'ARPANET, l'ancêtre de l'internet. Le Darknet est un ensemble de réseaux permettant un échange de fichiers de particulier à particulier de confiance, un réseau peer to peer.

Comme il n'y existe aucun contrôle, il peut s'y échanger tout type d'information. Pour y pénétrer, il faut une certaine initiation car aucun des moteurs de recherche fonctionnant sur le net (Google, Bing ou autres) ne référence les adresses du Darknet. Bien entendu, il faut aussi utiliser un programme d'accès spécifique puisque les explorateurs du marché (Internet Explorer, Chrome, Firfox, Opera, etc.) ne peuvent accéder au darknet.

JOL Press : Comment pénètre-t-on dans cet "internet parallèle" ?

Jean Harivel : Pour entrer dans le Darknet, il faut d'abord un logiciel d'accès, mais également être informé et initié. En prenant l'exemple de TOR (The Onion Router) qui est l'un de ses logiciels d'accès, il ne suffit pas de l'installer sur un PC pour accéder au Darknet. Tor ne donne pas accès à des sites "oignon" dès son utilisation, il fournit seulement une manière cryptée, chiffrée et surtout masquée pour accéder au Web normal. L'accès aux services cachés – déployés depuis 2004 – n'est qu'un des usages possibles de Tor. Il est tout aussi bien possible de consulter son courrier, faire de la messagerie instantanée ou se connecter au web "visible" via le réseau.

Pour accéder aux sites "oignon", il faut être conscient qu'ils existent et connaître leurs adresses dans le réseau Tor. L'installation de Tor n'est pas suffisante pour accéder au Darknet associé, le réseau Tor, il faut utiliser un navigateur spécifique à Tor (installé avec le package Tor, *Tor Browser Bundle*) et connaître les adresses des sites à visiter, toutes se terminant par "*.onion*".

JOL Press : Qui sont ceux qui se retrouvent dans cet espace et quelles sont les raisons qui les poussent à y entrer ?

Jean Harivel : Au départ, le Darknet a été conçu comme un espace de liberté, la discrétion y est de mise et tout y est fait pour protéger l'anonymat des intervenants.

Cet anonymat est une des raisons qui ont poussé certaines pratiques à se développer sur le Darknet : pédophilie, vente de matières prohibées et illicites comme les drogues et les armes.

JOL Press : Comment les échanges sont-ils rémunérés ?

Jean Harivel : Grâce aux bitcoins, une monnaie virtuelle qui y a un cours d'échange non légal et non garanti, mais qui permet aussi un blanchiment d'argent discret et sans trace.

JOL Press : Quels sont les principaux crimes commis dans cet espace ?

Jean Harivel : Le Darknet est devenu la "poubelle du web" puisque il y est possible, par exemple, d'engager un tueur à gage, d'acheter de la drogue ou des armes, d'acheter une

fausse carte d'identité et consulter des sites pédophiles… Bref tout ce que l'humanité a inventé de pire est présent sur le Darknet.
Il ne faut pas oublier le blanchiment d'argent via la manipulation des bitcoins. Les euros ou les dollars s'échangent contre des bitcoins auprès de changeurs officieux et non régulés. Fondé sur la cryptographie, un porte-monnaie bitcoin, souscrit en ligne, possède deux clés. La première clé est publique - c'est en quelque sorte l'équivalent d'un RIB, - destinée à recevoir de l'argent. La seconde est privée, c'est elle qui permet de régler les achats de manière totalement anonyme. Pour les gouvernements, le bitcoin devient le nouveau véhicule du blanchiment d'argent.

JOL Press : Comment opère le crime organisé dans le Darknet ?

Jean Harivel : Darknet est un outil garantissant l'anonymat dons l'impunité presque totale. Cet anonymat total sur le web a donné bien des idées à certains groupes, les premiers ont été les Farc (Force armées révolutionnaires de Colombie) qui ont vu dans le Darknet la possibilité de pouvoir communiquer entre eux, mais surtout un moyen de communiquer plus facilement, de vendre de la drogue et donc de créer un site e-commerce de vente de produit stupéfiant sans aucune contrainte sur le web.

JOL Press : Le Darknet peut-il être comparé à Silkroad ou XStore ? Est-il exact de dire qu'il n'existe pas un seul mais plusieurs "darknets" ?

Jean Harivel : Silkroad ou la Route de la Soie utilise ou plutôt utilisait le Darknet pour y écouler de la drogue.
Début octobre 2013, le site Silk Road créé en février 2011 est placé sous le feu des projecteurs. Silk Road - "la route de la soie" - en français - , présenté comme "l'eBay de la drogue", est fermé par le FBI et son fondateur supposé, Ross William Ulbricht, 29 ans, arrêté. Il est accusé d'un "massif blanchiment d'argent", de complot, de violations des lois sur les stupéfiants et de piratage informatique. En deux ans et demi, ce site du Darknet aurait généré des ventes de 1,2 milliard de dollars (l'équivalent de 880 millions d'euros) en monnaie virtuelle bitcoin, pour un montant total de 80 millions de dollars (soit 60 millions d'euros) de commissions.
Pour accéder au Darknet, il faut posséder une clé, en fait le logiciel d'accès à un espace. Il y a donc autant de Darknet que de clés. C'est pourquoi, il faudrait plutôt parler de Darknets. L'un de ces programmes est TOR (The Onion Router), il permet d'accéder à des sites dont l'adresse se termine par *.onion*.

JOL Press: Quelle est la différence entre "Darknet" et le "Deep Web" ?

Jean Harivel : Le Deep Web ne doit pas être confondu avec le Darknet. Le Deep Web est la dénomination de l'ensemble des pages non référencées dans les moteurs de recherche. Elles restent accessibles via les explorateurs classiques et possèdent une adresse licite.

JOL Press : L'utilisation du Darknet est-elle uniquement criminelle ? Après le scandale de la NSA, révélé par Edward Snowden, son usage révèle-t-il une volonté d'échapper à toute traçabilité ?

Jean Harivel : Darknet a été créé à l'origine pour aider les dissidents chinois à communiquer entre eux sans pouvoir être identifiés. La création du Darknet a donc permis aux dissidents d'exister, de pouvoir communiquer entre eux et le reste du monde, et donc de faire suivre l'information à travers le web sans aucun risque pour leur sécurité.
Les défenseurs de la vie privée considèrent le Darknet comme un bon outil pour les internautes désireux de se protéger. Des journalistes l'utilisent également pour ne pas être repérés dans des régimes répressifs ou échanger avec des sources sensibles sans risquer de les compromettre. "*C'est un besoin légitime pour certains acteurs d'avoir des plateformes sécurisées, anonymisées. Quand je bosse avec Wikileaks, je bosse sur le Darknet*", explique à l'AFP Jean-Marc Manach, journaliste spécialiste des questions de surveillance et de vie privée.

"*L'anonymat fait partie de la liberté d'expression. Sans anonymat, les journalistes n'auraient pas de source*", ajoute Jérémie Zimmermann, cofondateur de la Quadrature du Net, organisation de défense des droits des internautes.
Tor fait partie des outils recommandés par Reporters sans frontières (RSF) qui forme des journalistes dans les pays particulièrement surveillés. "*On a fait une formation au Tadjikistan, où beaucoup de sites internet sont bloqués. Tor peut être extrêmement utile dans ce cas, ça permet de s'affranchir du réseau national*", déclare Grégoire Pouget, de RSF.
Il est important de rappeler que l'anonymat n'est pas garanti à 100% sur Darknet. Lola City, un site pédophile, a été la cible du collectif Anonymous, qui a identifié 1589 pédophiles qui se connectaient sur ce site.
JOL Press : Quelles sont les mesures européennes mises en place pour lutter contre la cybercriminalité ?
Jean Harivel : Des cellules spéciales existent au niveau de l'OTAN et des polices des différents pays. Il faudrait une lutte globale, mais aujourd'hui les actions sont faites pays par pays. La coopération entre pays reste donc à réaliser.
http://www.jolpress.com/darknet-crimes-drogues-armes-internet-illegal-pedophilie-cle-usb-article-824421.html

La fraude et le darknet

Début novembre, un homme a été arrêté, suspecté d'avoir acheté de la fausse monnaie via le darknet, 40 faux-billets de 50€, achetés pour 20% de leur valeur. Cet événement illustre l'évolution de la fraude à l'ère du numérique.
En effet, la fraude à la loi évolue avec le développement des nouvelles technologies de l'information et la communication, un phénomène face auquel les autorités peinent à lutter.
Une nouvelle forme de fraude via TOR
Cette fraude passe désormais par TOR, The Onion Router, un des navigateurs permettant l'accès au darknet, un internet « masqué » sur lequel il est possible de naviguer anonymement, à condition de prendre certaines précautions (ne pas donner sa véritable identité, ne pas utiliser une adresse mail déjà utilisée sans TOR,…). Cette navigation anonyme s'exerce à la fois sur les sites classiques auxquels on pourrait avoir accès depuis n'importe quel navigateur, mais aussi aux sites du darknet, aussi appelé deepweb, dont l'extension est en « *.onion* » et qui ne sont accessibles que via TOR et sur lesquels sont exercées les activités illégales.
En se connectant via TOR, la requête (envoyée au serveur pour, en échange, récupérer, sur son écran, le site demandé), transite par plusieurs routeurs choisis de façon aléatoire. Quand l'information sera transmis au serveur, il ne verra donc que le routeur TOR duquel émanera la requête, et ne pourra voir l'adresse IP de l'individu[3] (qui peut être rattachée à son identité par le Fournisseur d'Accès à Internet sur simple ordonnance du juge des requêtes d'un Tribunal de Grande Instance ou d'un Tribunal de Commerce[4]).
La création de ce réseau anonyme s'est faite dans le but de pouvoir garantir la liberté d'expression à ses utilisateurs, par exemple, dans des pays où est exercée une censure ou une répression en cas d'opinion dissidente, TOR permet aux résidents ainsi qu'aux journalistes étrangers, de s'exprimer sans que l'Etat ne puisse remonter jusqu'à eux, et permet de contourner le blocage de certains sites. Il a cependant été rapidement détourné de son objectif premier et est devenu le support de nombreuses activités répréhensibles. Utiliser TOR est bien sûr légal, ce qui peut être illégal, c'est uniquement ce que l'on y fait[5], comme pour les logiciels de partage en peer to peer.
Parmi ces activités se situe en premier lieu la pédopornographie qui y a pris une place très importante, mais aussi le trafic de drogue, d'armes ou de contrefaçons via des sites de marché

noir tel que *the Silkroad*. Si ce site est loin d'être le seul à vendre des produits illicites, il montre bien les problèmes qu'ont les autorités à lutter contre ces marchés noirs en ligne. En effet, fermé en 2013 par le FBI, le site ouvre à nouveau seulement quatre semaines après et recouvre très rapidement toute sa clientèle. Il aura fallu une deuxième tentative du FBI, aidé par Europol et Eurojust pour finalement mettre fin à *The Silkroad*, en procédant à l'arrestation de son créateur. Cependant il subsiste encore beaucoup d'autres sites qui ont alors récupéré cette clientèle.

Se faire livrer de la drogue et des armes, est-ce risqué ? Malheureusement non. La réception du produit se fait par relais colis, un colis, qui d'après l'étiquette contiendra tout autre chose, puis dans le cas de la drogue, le dealer livre désormais ses clients par simple courrier postal[6]. Si la marchandise venait à être saisie par les douanes, l'expéditeur est alors impossible à identifier, et le destinataire, quant à lui, n'est pas responsable du contenu de l'envoi, un contenu qu'il aurait, bien sûr, immédiatement signalé à la police à la réception du courrier… Ce risque est d'autant plus faible que la douane ne contrôle qu'environ 2% du courrier qui transite par la Poste. La drogue passe donc sous le nez des douaniers…comme une lettre à la poste !

L'anonymat s'intensifie d'autant plus avec l'utilisation des bitcoins[7] qui permet de réaliser l'intégralité d'une opération sous couvert d'anonymat, un paiement par carte bancaire pourrait par exemple être retracé, via PayPal également, pas en utilisant des bitcoins. Ceux-ci permettent également de réaliser des fraudes financières, en masquant des transactions ou en cachant de l'argent, à la Direction Générale Des Finances Publiques, pour qui il sera difficile de retrouver ces sommes et les associer à une identité, comme pour un compte dans un Etat ou Territoire Non-Coopératif[8] (couramment appelé « paradis fiscal »). Rappelons toutefois, qu'en théorie, les bitcoins sont imposables[9].

Une identification possible de l'utilisateur ?

Trouver l'identité de la personne est-il totalement impossible ? L'anonymat est-il sans faille sur le Darknet ? La réponse est négative. Comme les informaticiens le disent, 90% des problèmes se situent entre la chaise et l'écran. La faille humaine est souvent la plus importante. Par exemple, dans les cas de diffamation, d'injure,… sur internet (qui sont très nombreux et qui représentent une grande partie du travail des avocats spécialisés), l'individu enverra un message depuis une adresse électronique en passant par TOR, une adresse qu'il aura, souvent, créée ou utilisée au moins une fois via un navigateur classique, ce qui permettra son identification.

Même sans cette erreur, TOR n'est pas techniquement infaillible, mais suppose d'utiliser un procédé nouveau, assez lourd. Il s'agit de la cyberperquisition, instaurée par la loi LOPPSI II[10], qui permet aux enquêteurs, en matière pénale, et avec l'autorisation du juge judiciaire, de capter les données à distance en introduisant un malware (ou cheval de Troie), qui permettra à l'enquêteur de « *voir et enregistrer en temps réel, à distance, les données informatiques telles qu'elles s'affichent sur un ordinateur, même lorsque les données ne sont pas stockées sur le disque dur* », c'est à dire voir tout ce qui s'affiche sur l'écran (mais aussi enregistrer la frappe clavier). Dès lors utiliser TOR ne permet plus de masquer ses activités si l'enquêteur peut voir l'individu utiliser ce navigateur et donc y faire des activités potentiellement répréhensibles.

Ce procédé, très attentatoire au droit à la protection de la vie privée, n'est toutefois utilisé que pour des infractions graves en pratique, et est très encadré, le Code de Procédure Pénale prévoyant l'intervention de deux magistrats pour l'autoriser[11].

En attendant que ce nouvel outil d'investigation ne soit généralisé à d'autres infractions (et il le sera certainement au vue de sa nécessité, les preuves étant désormais toutes dématérialisées), TOR est un nouveau moyen de fraude qui met en échec la police judiciaire ainsi que les douanes, les pouvoirs publics devront donc lutter contre les applications de cet outil, notamment en raison des activités de pédopornographie présentes, contre lesquelles, les

Anonymous sont, pour le moment, les plus efficaces[12]. Or, leurs activités ne sont pas plus légales…
http://www.lepetitjuriste.fr/droit-des-ntic/la-fraude-et-le-darknet/

Raid contre les "marchés noirs" sur le Darknet aux USA et en Europe

Les polices des Etats-Unis et de 16 pays européens ont fermé des centaines de sites internet transformés en marché noir de la drogue et des armes, cachés derrière le paravent du réseau Tor.
Dix-sept personnes ont été arrêtées lors de cette large opération internationale lancée jeudi par les polices américaine et de 16 pays européens, a précisé vendredi l'office européen de police Europol.
Un total de 414 sites ont été fermés, assure l'organisation, qui a refusé d'indiquer comment les policiers avaient réussi à identifier les vendeurs et administrateurs des sites.
"Il faut bien se rendre à l'évidence que les délinquants utilisent des technologies de pointe pour commettre leurs méfaits et dissimuler les preuves et ils se cachent derrière les frontières internationales pour échapper aux forces de police", a affirmé la procureure adjointe du ministre de la Justice américaine, Leslie Caldwell.
Cette vaste opération commune visait ces marchés noirs "fonctionnant comme des services cachés sur le réseau Tor", a expliqué Europol. Tor, logiciel libre et gratuit, est une plateforme qui garantit l'anonymat sur internet. "The Onion Router", son nom originel d'où est tiré l'acronyme Tor, permet de superposer des couches de protection afin de ne pas être découvert.
Il procède à l'encodage d'activités en ligne, comme des visites de sites internet ou des envois de messages, et expédie ces données à travers un réseau mondial de relais qui les épluche au fur et à mesure pour n'en garder que les couches infimes indispensables pour faire passer l'information au sein de ce qui est connu comme le "Darknet", la face cachée de l'internet.

"Ni invisibles, ni intouchables"

L'opération, menée notamment par les polices française, allemande, et britannique, "avait pour but d'arrêter la vente, la distribution et la promotion d'objets illégaux et dangereux, dont des armes et des drogues, qui étaient vendus sur des marchés noirs en ligne", a expliqué Europol.
De la monnaie virtuelle Bitcoin, utilisée dans les transactions, a également été saisie pour une valeur d'un million de dollars (800.000 euros) ainsi que 180.000 euros en cash et de la drogue.
"Nous ne faisons pas que +juste+ retirer ces services de l'internet public", a assuré Troels Oerting, chef de l'unité de crimes sur internet d'Europol.
"Cette fois, nous avons également touché des services sur le Darknet qui utilisaient Tor où, pendant longtemps, les criminels se sont considérés comme intouchables", a-t-il dit, ajoutant: "nous pouvons désormais prouver qu'ils ne sont ni invisibles ni intouchables".

Silk Road 2.0

Selon Lodewijk van Zwieten, expert en cybercrimes au parquet néerlandais, cette opération ne marque pas "la fin". "Derrière ces marchés noirs se cachent des personnes qui gagnent des millions d'euros. Cela sera bientôt leur tour", a-t-il ajouté dans un communiqué publié sur le site du parquet néerlandais.
Cette intervention survient quelques jours après l'arrestation à San Francisco de l'administrateur présumé d'une seconde version du site internet Silk Road, surnommé "l'eBay de la drogue".
Blake Benthall, 26 ans, a été interpellé mercredi par le FBI. Accusé d'associations de malfaiteurs dans le but de commettre un trafic de drogues, de piratage internet, de faux en documents et de blanchiment d'argent, il encourt une peine de prison à vie.

Selon les procureurs des Etats-Unis, Silk Road 2.0 a permis à plus de 100.000 personnes d'acheter ou de vendre des drogues illégales et d'autres objets de contrebande après la fermeture de la première version du site en 2013. Silk Road 2.0 avait annoncé un mois plus tard "renaître de ses cendres".
Le cerveau présumé de Silk Road, Ross William Ulbricht, attend l'ouverture de son procès à New-York après avoir plaidé "non coupable" en février d'accusations de blanchiment d'argent et de trafic de drogue.
Silk Road 2.0 est identique à son prédécesseur, uniquement accessible via le réseau Tor, et est décrit par l'accusation comme le marché criminel en ligne le plus exhaustif, le plus sophistiqué et le plus populaire.
http://www.huffpostmaghreb.com/2014/11/08/silk-road-tor-darknet_n_6125218.html

BlackMarket : données bancaires piratées

Des informations privées piratées volées à un ancien conseiller de la Reine ainsi qu'à des avocats, des banquiers, des médecins et d'autres sujets britanniques vendus dans le blackmarket
Je vous le montre souvent, dans le blackmarket, il est possible de trouver de tout.
Le black market, ce n'est pas que des sites cachés dans le dark net, le deep web. C'est aussi des sites Internet référencés par Google. Dernier exemple en date : Bestvalid.cc. Un site Russe faisant parti d'une constellation de portails web accessibles en deux clics de souris.
Le cas de Best Valid remue les méninges des autorités britanniques. Ce dernier propose une base de données bancaires de 100 000 comptes de britanniques. Via ce site, des pirates vendent des cartes de crédit et de débit. Jusqu'ici, rien de bien nouveau. 100 000 étant même un chiffre assez banal. Ce qui est moins banal, les propriétaires des cartes bancaires : un ancien conseiller de la Reine ainsi que des avocats, des banquiers, des médecins et d'autres sujets de sa gracieuse majesté. Les autorités britanniques tentent de faire fermer ce site en passant par la NCA (National Crime Agency), mais sans résultat pour le moment.
Une boutique étonnante donc, qui permet, via quelques bitcoins, d'acquérir des données bancaires volées. Un journaliste du Times a acheté quelques informations sur BestValid, avec la permission de la victime [Comment pouvait-il connaître la victime avant d'avoir les informations bancaires en main ? NDR]. Les données « acquises » comportaient le numéro de la carte bancaire, son code de sécurité, la date d'expiration, le numéro de téléphone portable et l'adresse postale. Des données qui semblent provenir de piratages de sites Internet tels que Talk Talk.
Lien : http://www.zataz.com/blackmarket-donnees-bancaires-piratees-pour-des-conseillers-de-la-reine-dangleterre/#axzz4Ihhqf5mv

Un député français se procure du cannabis sur le darknet

Pour illustrer les dangers des réseaux souterrains, le député Les Républicains de Paris Bernard Debré s'est procuré du cannabis sur un site étranger.
En compagnie d'un journaliste de l'hebdomadaire Valeurs actuelles et le président de l'association Parents contre la drogue Serge Lebigot, M.Debré a payé sa commande avec la carte bleue avant de recevoir, par la Poste, deux enveloppes en plastique "pour éviter les odeurs et les chiens renifleurs" couvertes de papier kraft. Par la suite, l'élu a acheminé les

stupéfiants achetés avec ses deux complices jusqu'à l'Assemblée nationale, en vue de prouver qu'il était possible d'acheter des drogues "aussi facilement que l'on commande une paire de chaussures". Selon M.Debré, le darknet, réseau souterrain où s'opère la majorité des transactions illégales telles que le trafic d'armes, d'hommes ou d'organes, constitue "le plus grand supermarché de l'horreur du monde". "Je demande que soit mis en place un véritable programme de lutte contre le trafic au sein de l'Union européenne", a-t-il déclaré devant les députés. Il a également appelé le premier ministre Manuel Valls à interdire les bitcoins, une monnaie virtuelle qui, selon lui, profite aux trafics et au blanchiment d'argent. 29.06.2016

Liens : https://fr.sputniknews.com/france/201606291026258739-france-depute-cannabis/

BlackMarket : 2 hommes arrêtés pour vente de drogue

Deux dealers passant par le blackmarket arrêtés à New York. Ils commercialisaient de la drogue via une importante boutique du dark web.

Selon un rapport de la justice américaine, les deux hommes, Abudullah Almashwali (Area51 – 31 ans – ressortissant yéménite) et Chaudhry Ahmad Farooq (DarkApollo – 24 ans – ressortissant Pakistanais), vendaient de l'héroïne et de la cocaïne via une importante boutique du blackmarket. 139,000 dollars ont pu être gagnés via leur business Internet en vendant pour environ 1.5kg d'héroïne et 72 grammes de cocaïne. Ils se faisaient payer en monnaie Bitcoin (btc, ndr). Ils acheminaient leurs drogues … via les bureaux de poste de New York. Pour connaitre la ville et ses habitudes, les chiens et les « renifleurs » électroniques de drogue sont légions dans les locaux de l'administration de la Grosse Pomme et les services « secrets » d'enquêtes de la poste US sont loin d'être manchots. Les deux hommes ont été tracés après l'achat de drogue par les policiers. Les colis ont pu être tracés. Les deux dealers risquent 20 ans de prison et 1 million de dollars d'amende en cas de reconnaissance de leur culpabilité. Alpha Bay est l'une de ces nombreuses boutiques du blackmarket qui permettent d'acheter et vendre drogue, arme, données piratées…

Pendant ce temps dans le blackmarket …

… en Allemagne, la police fédérale a mis la main sur quatre dealers locaux qui commercialisaient cannabis, amphétamines, héroïne, cocaïne et ecstasy dans le black market. L'un des individus arrêtés possédaient un porte feuilles bitcoin d'une valeur de 340 000 euros, preuve que son business semblait bien fonctionner. Si une fois de plus les autorités mettent en avant le moyen de paiement Bitcoin, il est évident que le Btc n'est qu'une monnaie parmi d'autres utilisées par les criminels. 11 kg d'amphétamines et 250 grammes d'héroïne ont été saisis, ainsi que 1.425 pilules d'ecstasy et 150 grammes de cocaïne, des cartouches de cigarettes, sans parler d'importantes liquidités en Euros.

La fête aux Bitcoins

L'été 2016 aura été particulièrement communicant sur le sujet du bitcoin. Plusieurs affaires ont mis en avant l'utilisation de cette monnaie dématérialisée et électronique dans des affaires criminelles. L'Australie, l'Allemagne, les USA. Dans ce dernier cas, George Cottrell, a été arrêté par le FBI sur des accusations de blanchiment d'argent de la drogue via des paiement en bitcoins. Les autorités parlent de 62.000 livres. Cottrell n'est pas n'importe qui. Il était en charge de la communication de Nigel Farage, politicien britannique membre du Parlement européen et ancien chef de l'Independence Party (UKIP). George Cottrell agissait dans le dark web sous le pseudonyme de Bill ! Posted On 29 Août 2016.

Lien : http://www.zataz.com/black-market-2-hommes-arretes-vente-de-drogue/#axzz4Ihhqf5mv

Business du Darknet : vendeurs de drogue et d'armes arrêtés

Business du Darknet – Un homme de 31 ans, qui passait par une boutique vedette du blackmarket pour vendre de la drogue, vient d'être arrêté à Vienne par la Bundeskriminalamt. Même chanson, en Allemagne pour un vendeur d'armes à feu.

Le blackmarket, des boutiques ou il est possible de croiser des vendeurs/acheteurs d'armes à feu, de contrefaçons de papier, de places de cinéma pour quelques euros… mais aussi de drogue. Un homme de 31 ans originaire de Vienne avait été arrêté par les « *amis du petit déjeuner* » de la Bundeskriminalamt, la police Autrichienne, en octobre 2015. Connu sous le pseudonyme du vendeur ShanSa, son arrestation vient tout juste d'être révélée (Très certainement en raison d'une infiltration locale par les autorités, NDR). On vient d'apprendre que lors de son arrestation, 2,8 kg d'amphétamine et un kilogramme d'ecstasy avaient été saisis. Lors de l'enquête, il a été découvert que 182 ventes de drogue, sur cinq mois, avaient été orchestrées en Europe, aux États-Unis, en Australie, en Inde et en Autriche. 15.000 euros de chiffre d'affaires, en Bitcoins.

Business du Darknet

… en Allemagne, j'apprends que le procureur général de Francfort vient d'accueillir dans son bureau un ressortissant germano-russe de 26 ans. L'homme, originaire d'Hanovre, est soupçonné d'avoir organisé un trafic d'arme sur Internet. Il est accusé d'avoir vendu et acheté pistolets, fusils, silencieux et munitions via le darknet. Un adepte du blackmarket, des cartes bancaires contrefaites ont été retrouvées à son domicile. L'enquête est toujours en cours.

Comme je vous le révélais ces derniers jours, le business du Darknet n'a jamais été aussi prolifique avec des ventes et des achats d'armes hétéroclites, comme ces tasers cachés dans des téléphones, clés de voiture, de ce pistolet à ultra son, de drogues venues des 4 coins du globe, de faux papiers, mais aussi de bases de données piratées. Les arrestations, elles aussi, se multiplient partout dans le monde, comme à Rouen, en décembre 2015

Lien : http://www.zataz.com/business-du-darknet/#axzz4Ihhqf5mv