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

LETTRE D'INFORMATION : BON A SAVOIR (N°23)

TOR, le réseau Internet parallèle infiltré par le crime

30 % des contenus relèvent d'activités illicites et criminelles, financées essentiellement à l'aide du bitcoin.

Un Web de l'ombre parallèle, décentralisé, sans règles ni modérateurs et garantissant un grand anonymat à l'aide d'un navigateur Web approprié. Créé par et pour les activistes politiques, il a été dès son origine infesté et infiltré par les activités criminelles, notamment pédophiles. 30 % des contenus relèvent en effet d'activités illicites, confirment des chercheurs.

Sur 5.205 sites analysés entre janvier et mars 2015, 1.547, soit 30 %, proposaient des produits et services illégaux, avec une large palette. En tête figurent les sites de ventes en ligne de drogues, 423 recensés, et qui représentent plus du quart des sites illégaux sur TOR. Ils sont suivis par la finance (21 % des sites illégaux) - blanchiment, cartes de crédit volées, faux billets...- la contrebande-contrefaçon de documents officiels (12

%), les sites extrémistes et violents (9 %) et la pornographie infantile (8 %). Une vingtaine de sites proposaient les services de tueurs à gage, une quarantaine vendait des armes et une centaine mettait en relation avec des pirates informatiques... *« Le bitcoin est la devise la plus couramment utilisée dans ces activités illégales ",* estiment les chercheurs, souvent avec l'aide de services (CleanCoin, Bitcoin Fog...) qui se sont créés et qui ont pour but de brouiller encore davantage les pistes et rendre les transactions 100 % anonymes : en clair rendre le bitcoin « plus blanc que blanc ".

Devise de transaction historique

Le bitcoin est la devise de transaction historique des supermarchés en ligne des drogues, qui ont émergé et qui l'ont adopté dans le sillage de Silk Road, le site précurseur, ainsi que pour toutes les activités financières illégales.

L'année dernière, la police allemande a fermé 5 marchés noirs du Web. Cette semaine, ce sont les autorités suédoises qui ont arrêté un vendeur de drogues opérant sur plusieurs plates-formes. Car la demande est soutenue. La proportion d'individus qui ont acheté des drogues sur Internet a été multipliée par 5 depuis 2009 à 25 %. 6,4 % des personnes sont passées par le Web de l'ombre pour acheter ces produits, et dont 4,5 % durant les douze derniers mois. C'est en Suède où cette proportion est la plus élevée (25 %), elle est de 15 % au Royaume-Uni, 12 % aux Etats-Unis et 7 % en France, un pays dans la moyenne mondiale.

Les drogues les plus couramment achetées sur le Web de l'ombre sont la MDMA, une amphétamine connue sous le nom d'ecstasy, puis le LSD, un hallucinogène, le cannabis et la cocaïne. « Il y a peu de sites extrémistes islamiques sur TOR. Ce dernier est moins adapté à leurs opérations de propagande qui nécessitent pour être efficaces d'avoir accès à une large audience. En outre, les terroristes préfèrent communiquer entre eux sur d'autres plates-formes et avec d'autres moyens », estiment les auteurs de l'étude.

Lien : http://www.lesechos.fr/02/08/2016/LesEchos/22246-100-ECH_tor--le-reseau-internet-parallele-infiltre-par-le-crime.htm

Les botnets :
Acteurs majeurs de l'ombre

L'écosystème d'Internet est d'une complexité insoupçonnée, et en particulier sa part obscure. Au cœur de cet écosystème, les botnets tiennent une place de choix, et sont à l'origine d'un très grand nombre de menaces qui occupent à plein temps les différents acteurs de la sécurité informatique.

Mais tout d'abord, qu'est-ce qu'un botnet ?

Littéralement, un botnet est la contraction de deux termes: "robot" et "network". Il s'agit donc d'un réseau de robots – robot désignant un agent ou un programme informatique – dont la finalité est malveillante.

Les exemples d'activité malveillante sont nombreux, et l'envoi de spam et de virus par email sont des exemples-types de l'activité des botnets.

Un botnet est contrôlé par une personne physique : il s'agit du *botmaster (Il peut évidemment y avoir plusieurs botmasters pour un même botnet.)*

Nous allons présenter plus en détail les botnets, en nous intéressant au cycle de vie de ces derniers : ce choix de perspective permettra d'appréhender toute la problématique relative aux botnets, autant d'un point de vue technique que d'un point de vue économique et juridique.

Naissance d'un botnet

Le support physique d'un agent malveillant – ou *malware* – est une *machine zombie* : il s'agit en général d'un ordinateur contrôlé par le botnet, à l'insu de son utilisateur légitime.

Un exemple typique de machine zombie est un ordinateur familial placé derrière une connexion ADSL, dont des éléments essentiels à la sécurité ne sont pas à jour (système d'exploitation, navigateur internet, anti-virus…) et qui a été compromis soit par l'exécution d'une pièce jointe contenant un virus, soit par la visite d'un site web infecté.

S'appuyer sur une telle infrastructure a des avantages indéniables d'un point de vue économique : les coûts, que ce soit le hardware, la bande passante ou l'électricité sont intégralement à la charge de son utilisateur légitime.

Donner naissance à un botnet revient à constituer un réseau de machines zombies, par l'intermédiaire d'une phase d'infection virale de grande ampleur. Cette phase d'infection se déroule en plusieurs étapes :

Le développement d'un malware qui permettra à la machine zombie de communiquer avec le botnet, et d'effectuer les activités malveillantes. Ce développement nécessitera en outre l'exploitation d'une faille de sécurité, qui peut être innovante, ou bien déjà connue, pour installer le malware à l'insu de l'utilisateur légitime.

A noter que certaines failles de sécurité innovantes – et pouvant potentiellement affecter des systèmes d'exploitation ou des logiciels récents – peuvent être achetées ou vendues sur le marché noir.

La constitution d'un carnet d'adresses, qui est la liste des utilisateurs cibles de la phase d'infection virale. Ces listes peuvent être constituées par des robots qui collectent des adresses emails trouvées sur Internet (En parcourant des forums de discussion par exemple.) ou bien être achetées directement sur le marché noir.

L'envoi d'une campagne d'emails qui, soit contient le malware sous forme de pièce attachée, soit fait référence à ce malware par l'intermédiaire d'un lien vers un site web infecté. L'envoi de cette campagne peut d'ailleurs être sous-traité en sollicitant les services d'un autre botnet.

La réception d'un email contenant le malware sous une des formes précisées précédemment et l'installation de ce dernier par certains utilisateurs cibles de la phase d'infection virale.

Le taux d'infection est très variable et dépend d'une part du niveau de protection de chaque utilisateur, et d'autre part de la qualité de la faille de sécurité exploitée.

Suite à cette phase d'infection initiale qui permet au botnet de prendre vie, d'autres phases d'infection peuvent avoir lieu pour agrandir le botnet (De la même manière, des phases d'infection peuvent avoir lieu pour reconstituer un botnet qui a été partiellement démantelé.).
Un botnet peut atteindre une taille considérable : on estime par exemple que le botnet Bredolab était constitué à son paroxysme de près de 30.000.000 de machines zombies.

Vie d'un botnet

Suite à l'installation du malware sur la machine cible, ce dernier va contacter un des nombreux serveurs de contrôle et de commande du botnet (Les serveurs de contrôle et de commande sont généralement installés chez des hébergeurs, car ils doivent avoir une capacité – en terme de bande passante, de stockage et de traitement – importante. Le pilotage et la supervision de millions de machines zombies nécessite des ressources importantes et un niveau de compétence technique élevé). Ces serveurs servent à piloter (La communication entre les machines zombies et les serveurs de contrôle et de commande est effectuée selon un protocole propre au botnet, qui peut être éventuellement crypté.) les activités des machines zombies, à collecter des informations, et également à mettre à jour le malware : ils constituent la clé de voûte de l'infrastructure de communication du botnet.
Le malware va espionner la machine cible, et remonter toute information utile : numéro de cartes bancaires, mots de passe, données personnelles (nom, prénom, numéro de sécurité sociale… utilisés à des fins d'usurpation d'identité), carnet d'adresses….
Ces données seront ensuite agrégées, et utilisées directement ou bien revendues sur le marché noir par le botmaster. A noter que les adresses email collectées sont d'une grande importance pour le botnet, car elles permettent d'effectuer de nouvelles phases d'infection virale permettant d'agrandir ce dernier.
En outre, le malware va effectuer les différentes tâches qui lui seront affectées, parmi lesquelles :
L'envoi d'une campagne de spam ou de virus, en utilisant un modèle d'email et une liste de destinataires : à ce modèle seront ajoutés des éléments variables et aléatoires, de manière à échapper aux systèmes de filtrage par signature.
Effectuer une attaque par déni de service distribué (Une attaque par déni de service consiste à rendre indisponible un service internet en le saturant de demandes de connexion. On parle d'une attaque par déni de service distribué si un grand nombre de machines participe à cette opération, ce qui est toujours le cas pour un botnet. On pourra citer par exemple l'attaque menée en décembre 2010 par le groupe Anonymous contre les sites de Paypal, Visa et Mastercard, lors de l'affaire Wikileaks, et qui a été largement médiatisée)
Effectuer de la fraude au clic (Le fraude au clic consiste à effectuer de manière automatisée des clics sur des liens publicitaires, ce qui remet en cause le modèle économique des liens sponsorisés, qui est très populaire sur Internet. On estime que plus de 20% des clics sur les liens publicitaires sont d'origine frauduleuse) pour générer des revenus publicitaires frauduleux.
Effectuer du calcul intensif, en particulier pour casser certaines clés de cryptage.
Ces activités peuvent être exercées pour le compte du botmaster, mais dans la plupart des cas elles sont vendues comme une prestation à d'autres acteurs : industriels de la contrefaçon (La contrefaçon concerne principalement les montres de prestige, les produits de luxe, les médicaments – dont le fameux Viagra – et l'édition logicielle), organisations criminelles…

Prenons l'exemple classique du spam :

Une organisation souhaite proposer à la vente des contrefaçons (montres de prestige, produits de luxe…).
Elle contacte le botmaster, et lui demande d'envoyer une campagne publicitaire à grande échelle. Le botmaster joue donc le rôle de prestataire de service pour le routage des emails : il fournit - contre rémunération (Les prix sont variables, et dépendent surtout

de la qualité du carnet d'adresses. On estime que l'envoi d'un million de spams coûte en moyenne moins de 100$ pour le client) – les moyens techniques d'envoi ainsi que les carnets d'adresses des destinataires.
La campagne de spam est envoyée, avec une volumétrie souvent considérable (On a estimé par exemple la capacité d'envoi quotidienne du botnet Rustock à environ 30.000.000.000 d'emails. C'est un volume considérable, et cela donne la mesure de la dangerosité des botnets).
Du fait des moyens techniques mis en œuvre pour limiter le spam, un pourcentage assez faible atteindra le destinataire final, et le taux de transformation sur le site de contrefaçon sera d'autant réduit.
Toutefois, la volumétrie considérable en amont – souvent plusieurs millions voire milliards d'emails – lié au coût quasi-nul en terme d'infrastructure – le coût financier étant à la charge des propriétaires des machines zombies – font que ce modèle reste très rentable.
L'organisation qui vend les contrefaçons reçoit par la suite un grand nombre de commandes, qu'elle pourra choisir d'honorer ou pas : si elle honore la commande, elle enverra donc la contrefaçon au client et crée ainsi une relation commerciale classique ; si elle ne l'honore pas, elle utilise les données bancaires capturées pour un autre usage.
L'argent gagné par l'organisation vendant des contrefaçons restant dans un cadre illégal, elle devra le blanchir.
A ce titre, elle pourra encore une fois utiliser les services proposés par le botmaster en envoyant une campagne d'emails pour recruter des money mules (A noter que le terme de mule désigne dans le langage courant une personne transportant de la drogue d'un pays à l'autre, et parfois à son insu.*)*.
Une money mule est une personne physique acceptant – contre forte rémunération – d'effectuer des opérations bancaires pour le compte d'une entreprise : ces opérations bancaires permettent à l'entreprise de blanchir des sommes d'argent, et la money mule prend à son insu toutes les responsabilités légales relatives à cette opération.

Mort d'un botnet

Étant donné le rôle essentiel donné aux serveurs de contrôle et de commande, le démantèlement d'un botnet passe par la mise hors service de ces derniers, et cette opération nécessite une intervention des autorités auprès des sociétés hébergeant les serveurs de contrôle et de commande.
On pourra ainsi citer le cas du botnet Bredolab, qui le 25 octobre 2010, a été fortement affaibli suite à la saisie par les autorités hollandaises de 143 serveurs auprès de l'hébergeur hollandais LeaseWeb.
Autre exemple: le botnet Grum, qui a été complètement démantelé en juillet 2012, avec des opérations menées conjointement par les autorités en Hollande, au Panama et en Ukraine.
La capacité à mettre hors service un botnet est par conséquent principalement conditionnée par la bonne volonté des autorités des pays où sont hébergés les serveurs de contrôle et de commande : la problématique n'est plus d'ordre technique, mais d'ordre juridique et politique.
Lien : http://www.sih-solutions.fr/les-botnets-acteurs-majeurs-de-lombre/

SILK ROAD et commerce en ligne de la drogue

La réouverture du site illégal SILK ROAD, preuve de l'impuissance des Autorités face au commerce en ligne de la drogue
Le 6 novembre 2013, le site de vente de produits illégaux Silk Road (« route de la soie ») est à nouveau en ligne, un mois seulement après sa fermeture par le FBI le 2 octobre 2013.

Ce site, ouvert en 2011, est connu pour être « l'Amazon.com de la drogue » ou encore «l'eBay de la drogue », car, outre les faux papiers et les contrefaçons d'objets de marque proposés à la vente, on y trouve surtout à la vente différentes drogues. Il s'agit en effet d'un site internet destiné à mettre en contact des vendeurs et des acheteurs dans le but d'opérer des transactions de produits illégaux, « entre adultes consentants », à la seule condition que la marchandise en question ne soit pas destinée à « blesser ou escroquer » autrui (selon les conditions d'utilisation du site). C'est pourquoi ces conditions générales interdisent par exemple la vente de données personnelles bancaires, ou encore « les services de tueurs à gage et contenus pédopornographiques ».

Pourtant, le site offre la possibilité aux utilisateurs d'avoir à leur disposition des notices explicatives sur les moyens de pirater un distributeur automatique, ou encore des logiciels permettant de déverrouiller des ordinateurs ou récupérer des mots de passe. On voit mal comment ce genre de pratiques peut ne pas nuire à autrui. De même, le contrôle sur la vente des armes est assez faible, puisqu'il est possible d'en trouver sur le site bien que les conditions d'utilisation le proscrive également. Ces dernières sont donc plutôt indicatives et ne semblent servir qu'à prouver une prétendue bonne foi de la part des gérants du site litigieux.

Une double sécurité mise en œuvre pour protéger le site et ses utilisateurs

Silk Road, appartenant au «marché noir» d'Internet, appelé le « web profond » (« deep web » ou encore « dark net » en anglais) bénéficie d'une sécurité technique du fait qu'il est impossible de le trouver via les moteurs de recherche classiques. En effet, seuls les internautes appartenant au réseau anonyme TOR (« The Onion Router ») peuvent trouver le site, en passant par des bases de données spécifiques capables de trouver son chemin d'accès. Ce réseau TOR brouille en fait les connexions et seul un navigateur configuré pourra avoir accès à ces bases de données. Le principe est qu'au lieu d'utiliser un seul serveur pour accéder au site en question, l'ordinateur va être programmé pour se déplacer de serveur en serveur avant d'atteindre le site illicite, rendant quasiment intraçable l'adresse de l'internaute. Enfin, une fois qu'on a réussi, par des manipulations informatiques, à entrer sur le réseau TOR, l'adresse du site n'est elle-même pas évidente à trouver car il s'agit de < ianxz6zefk72ulzz.onion >. Ainsi, connaître le nom du site par la rumeur ne suffit pas à pouvoir y accéder et il est donc pratiquement impossible de trouver ce site internet sans y avoir été invité par quelqu'un qui aura précisément expliqué comment y accéder.

La deuxième protection utilisée par le site Silk Road est l'utilisation d'une monnaie virtuelle appelée Bitcoin, créée en 2009 par des passionnés d'informatique. Le Bitcoin a la particularité de permettre des échanges anonymes entre les internautes. C'est pourquoi le secteur des transactions illégales et du blanchiment d'argent s'est intéressé à cette monnaie qui garde cryptée l'identité des acteurs.

Cette monnaie virtuelle a d'autres avantages que l'anonymat dont elle fait profiter ses utilisateurs. En effet, elle permet également des virements entre portefeuilles numériques à un taux extrêmement faible (0,99%) par rapport à celui que proposent les banques (entre 1,5% et 7% en fonction des Etats), et les opérations de virement en Bitcoin sont bien plus rapides que celles des banques. En effet, une transaction de Bitcoin entre deux portefeuilles numériques se fait de façon immédiate alors qu'il faut entre deux et cinq jours pour une opération de virement bancaire. En outre, l'argent est immédiatement récupérable en échangeant des Bitcoins contre une devise bancaire. Cette monnaie qui n'appartient à aucune catégorie juridique pour le moment échappe donc aux règles classiques du marché bancaire et n'est contrôlée par aucune banque centrale.

Il semblerait par ailleurs que les utilisateurs dans certains pays aient plus confiance en cette monnaie qu'en leur propres banques dont ils se méfient depuis la crise des subprimes. Ainsi, dès qu'un petit doute sur le système bancaire s'installe, les gens ont tendance à acheter des

Bitcoins qui sont plus «rassurants», faisant de cette monnaie une devise extrêmement volatile. C'est notamment ce qui s'est passé à Chypre au cœur de la crise, lorsqu'une limitation de sortie des capitaux avait été mise en place. Les Chypriotes avaient alors utilisé le Bitcoin pour contourner cette limitation.

Si certains économistes pensent qu'une telle monnaie est vouée à s'autodétruire, d'autres misent de grands espoirs en elle, et notamment les fondateurs d'Ebay ou de Google qui commencent à l'intégrer dans leurs services. Le Bitcoin est d'ailleurs entrain de se normaliser dans de plus en plus de pays. L'Allemagne l'a par exemple reconnu en août 2013 comme une « monnaie privée ».

Le Bitcoin fonctionne de façon complexe et est créé par des algorithmes générés par les ordinateurs des utilisateurs de la monnaie. C'est donc une monnaie « mathématique et totalement décentralisée ». Il existe deux façons de se procurer des Bitcoins: soit sur des plateformes en ligne qui permettent d'acheter des Bitcoins avant de les stocker sur un portefeuille numérique, soit lors de ventes publiques organisées dans les grandes villes (par exemple à New-York dans le quartier d'Union Square). Des distributeurs automatiques de Bitcoins commencent également à être installés par des grandes entreprises spécialisées dans le monde entier, distributeurs qui permettront de stocker des Bitcoins sur un smartphone ou sur une carte prépayée.

Un contournement de la loi permis par l'informatique

Le site Silk Road, accessible depuis le monde entier, est contraire à la loi de la plupart des pays qui prohibent le commerce de la drogue, et souvent la vente d'armes également. En France par exemple, « l'usage, le trafic, la production, des stupéfiants, dont le cannabis) sont réprimés par la loi N° 70-1320 du 31 décembre 1970, plusieurs fois modifiée », la dernière modification datant de l'entrée en vigueur du nouveau code pénal de 1994.

Pourtant on constate que, grâce à des génies de l'informatique, les ventes de ces produits illicites sont possibles et de façon très simplifiée pour les acheteurs. Le problème de la transaction dans la rue ne se pose plus, et de surcroît, un système de forums et d'avis sur les vendeurs permet également d'éviter le risque que la marchandise ne soit pas de bonne qualité. Les acheteurs choisissent tranquillement leurs produits sur un site communautaire convivial, et payent en toute sécurité avant de recevoir de la drogue ou des armes simplement par voie postale.

Les autorités se voient démunies devant cette pratique car, bien qu'elles aient réussi à arrêter le créateur du site, Ross William Ulricht, ce dernier avait remis les codes sources de Silk Road à un autre informaticien qui a repris le flambeau seulement un mois après, avec une sécurité renforcée. Il semblerait donc que le site soit encore moins facilement accessible aujourd'hui qu'il ne l'était initialement.

Ulricht a été accusé par le parquet de New York non seulement de massif blanchiment d'argent, de trafic de drogue et de piratage informatique, mais également de tentative de meurtre. En effet, grâce à un informateur du FBI, il a été découvert que le propriétaire du site clandestin avait donné l'ordre en 2012 d'assassiner un utilisateur de Silk Road qui avait menacé de dévoiler les identités d'Ulricht lui-même et d'autres utilisateurs. Un an plus tard, en mars 2013, Ulricht aurait commandité un autre meurtre, s'agissant cette fois-ci d'un utilisateur qui avait menacé de divulguer l'identité d'un internaute et le chemin d'accès au site par le réseau TOR au grand public. Selon Ulricht, « des besoins comme ça, ça arrive de temps en temps pour une personne avec des responsabilités comme moi ». Ici encore, on peut se demander si le site est toujours aussi innocent que ses conditions générales d'utilisation veulent bien nous le faire croire…

La rapide remise en ligne du site internet litigieux montre la difficulté de l'application du droit sur les nouveaux supports. En effet, face à une technologie de plus en plus performante et à des personnes qui savent développer des systèmes de protection de plus en plus inviolables,

les autorités se voient dans l'impossibilité d'opérer leur rôle de contrôle sur ce domaine et se retrouvent impuissantes face à ces trafics. Ainsi, le Comité sénatorial permanent pour la sécurité nationale a annoncé lui-même que « la nature en perpétuelle évolution de la technologie [rend] inutile un jeu de chat et de la souris dans lequel les autorités [risquent] d'avoir toujours un train de retard ».

Une sécurité finalement relative pour les internautes

Cependant, un espoir est donné aux autorités quant à la sécurité elle-même de ce genre de site, qui n'est finalement pas si inviolable qu'elle n'y paraît.

Si le passage par le réseau TOR et l'utilisation du Bitcoin rassurent les utilisateurs de ces sites illégaux, l'anonymat n'y est pourtant pas infaillible selon les experts. En effet, selon Jon Matonis, chercheur sur la monnaie électronique, le Bitcoin n'est pas totalement anonyme et il faut un certain paramétrage de la part de l'utilisateur pour réussir à protéger son identité.

De plus, le réseau TOR serait lui aussi peu protecteur car relativement facile à cracker par des professionnels selon Richard Stiennon, auteur du livre « Survivre à la cyberguerre ». C'est d'ailleurs pour cela que les services de police voient se multiplier parmi leurs membres des informaticiens professionnels capables de plus en plus aisément d'infiltrer ce genre de réseau, ce qui permet un nombre croissant d'arrestations dans le monde de la cybercriminalité. Notamment, ces agents sont capables d'intégrer la communauté même des utilisateurs des sites illégaux, et ce fut le cas pour Silk Road qui a vu près de cent agents sous couverture infiltrer sa communauté et effectuer des transactions afin d'arrêter les vendeurs de produits illicites.

Ces infiltrations par des agents ont également eu pour but de tester dans des laboratoires la qualité de la marchandise échangée sur le site, qui s'est révélée par ailleurs plutôt bonne.

La remise en question de la monnaie Bitcoin

D'après les rapports du FBI et suite aux enquêtes menées depuis l'ouverture initiale du site, et donc en seulement deux ans de temps, près de 1,2 milliard de dollars aurait été généré pour plus de 1,2 million de transactions sur le site. Cela représente environ 9,5 millions de Bitcoins, dont le cours s'élève à peu près à 300 dollars. Sur chacune de ces transactions, le site Silk Road ponctionnait une commission d'environ 8 à 15% qui lui a permis sur la même période de récupérer pas moins de 80 millions de dollars (soit 600 000 Bitcoins).

Le Bitcoin, utilisé également par des entreprises légales, et notamment des start-up, voit sa réputation ternie par son utilisation massive sur ce site internet, et sur d'autres sites illicites du même acabit. En effet, Silk Road représente près de la moitié de l'activité de cette monnaie virtuelle, et la fermeture du site avait provoqué une forte chute du cours (près de 20% de baisse) du Bitcoin suite à la saisie par le FBI de 26 000 Bitcoins stockés sur le site. Le site bitcoin.fr se réjouissait donc le 2 octobre de la fermeture par le FBI de Silk Road, considérant cela comme une «excellente nouvelle pour tous ceux qui militent en faveur d'un usage responsable de Bitcoin ».

Par ailleurs, même les utilisateurs du site clandestin ont moins confiance à ce jour dans le Bitcoin et dans la nouvelle version de Silk Road. En effet, d'après le site américain All Things Vice, les consommateurs craignent que cette réouverture ne soit un piège de la part du FBI pour arrêter de nouvelles personnes en flagrant délit de trafic de drogue, de contrefaçon ou autres activités illicites. De plus, d'autres sites internet illégaux ont profité de l'absence de Silk Road pour proposer les mêmes services, or ils ont rapidement fermé, emportant avec eux des Bitcoins stockés dans leurs portefeuilles numériques par des utilisateurs imprudents. Ainsi, les internautes ont une perte de confiance à la fois dans le site et dans ce système de paiement virtuel qui n'a pas de statut juridique et sur lequel ils n'ont finalement pas le contrôle du stockage.

Vers une légalisation des drogues?

Ainsi, deux courants se dégagent de cette affaire. Certains pensent que ce genre de site clandestin va se multiplier de plus en plus et être de plus en plus performant au niveau de la sécurité qu'ils proposeront aux internautes. De l'autre côté, certains pensent que les autorités, bien qu'elles soient pour le moment prises de court, vont réussir à rattraper au niveau technologique les informaticiens au service de ces sites. Les autorités vont effectivement développer des techniques informatiques pour lutter contre ce marché noir en ligne. Le cas de Silk Road fait en tout cas parler de lui car révèle au grand public l'existence de tels sites et pose la question de la légalisation de ces produits.

En effet, aux États-Unis, on constate que la DEA (Drug Enforcement Administration), organisation de lutte contre la consommation et le trafic de drogues aux États-Unis depuis quarante ans, ne réussit aujourd'hui qu'à saisir 1% de la drogue qui est échangée sur le territoire américain. De plus, le fait même de prohiber les drogues semble avoir des effets pervers, à savoir la création d'un marché noir et une gestion de la qualité des stupéfiants remise aux mains des trafiquants. On constate également que le prix des drogues chute vertigineusement depuis quelques années (les prix de l'héroïne, de la cocaïne et du cannabis ont chuté de près de 80% entre 1990 et 2007), preuve qu'il y en a de plus en plus sur le marché (ces produits répondent comme toutes les marchandises à la loi de l'offre et de la demande, donc plus il est facile d'en trouver, et plus le prix est faible). Enfin, les épidémiologistes déclarent que le lien entre la répression et la consommation est malheureusement inverse: les pays qui ont les politiques les plus sévères face aux drogues sont en réalité ceux où la consommation est la plus élevée.

C'est pourquoi de plus en plus de personnes, constatant que la guerre contre les drogues ne fonctionne pas, souhaiteraient qu'elles soient légalisées afin d'être mieux contrôlées. Aux États-Unis par exemple, le juge Gray, qui fait partie d'un groupe international rassemblant les membres de la police et de la justice qui souhaiteraient une « refonte des lois contre la drogue », pense que « la marijuana devrait être taxée et vendue aux adultes par des marchands autorisés, comme les cigarettes et l'alcool ». Certains États des États-Unis ont d'ailleurs déjà passé le cap en légalisant la marijuana pour une consommation « thérapeutique ou récréative ». Les partisans de la légalisation des drogues pensent en effet que cela éviterait l'existence de ce marché noir, très lucratif, qui attire les criminels. Enfin, légaliser les drogues permettrait à l'État américain d'économiser les 51 milliards annuels dépensés uniquement dans la guerre contre la drogue.

Ce courant de pensée est international, d'autant que les sites internet qui proposent ces produits illicites, et notamment Silk Road, mettent en relation des acheteurs et vendeurs de toutes nationalités, même si la majorité d'entre eux sont américains. Ainsi, les analyses des drogues échangées sur le site ont prouvé qu'étaient en jeu au moins une dizaine de pays européens dont les Pays-Bas, le Royaume-Uni, la France et l'Espagne. La question de la légalisation des drogues est donc également posée à ces pays là, dont la plupart sont encore réticents.