الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ا م

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Les États-Unis décapitent un vaste réseau de blanchiment d'argent

L'émetteur de monnaie numérique Liberty Reserve et sept de ses responsables ont été inculpés pour avoir blanchi 6 milliards de dollars en sept ans.

Liberty Reserve ne peut plus servir ses clients. Preet Bharara, le procureur fédéral de Manhattan, a inculpé l'émetteur de monnaie numérique et sept de ses dirigeants mardi soir. Le système de transfert électronique international de fonds «était intentionnellement créé et structuré pour faciliter les activités criminelles… Si Al Capone était vivant, c'est ainsi qu'il cacherait son argent», affirme ce représentant du département de la Justice à New York.

Établi au Costa Rica depuis 2006, Liberty Reserve a transféré des milliards de dollars au service d'environ un million de clients. On lui reproche d'avoir permis le blanchiment d'au moins 6 milliards de dollars. Ce n'était pas une banque. En opérant en dehors des circuits traditionnels de la finance, la société fondée par Arthur Budovsky était devenue, selon les autorités américaines, la plate-forme de paiement sur Internet de toutes sortes de criminels, des voleurs de numéros de carte de crédit aux trafiquants en pornographie enfantine, en passant par des marchands de drogue. Qu'ils soient implantés au Vietnam, au Nigeria, à Hongkong, en Chine ou aux États-Unis, tous appréciaient l'anonymat avec lequel ils pouvaient faire virer des millions d'un point à l'autre du globe.

Premier réseau de monnaie numérique

Tout ce dont un client avait besoin pour travailler avec Liberty Reserve était une adresse de courrier électronique. Son réseau de monnaie numérique était un des plus développés du monde. Les huit New-Yorkais arrêtés début mai pour complicité de vol de 45 millions de dollars dans des distributeurs automatiques de billets répartis dans 27 pays avaient, par exemple, recours aux services de Liberty Reserve.

Arthur Budovsky, citoyen américain qui a renoncé à sa nationalité, a déjà été arrêté en Espagne vendredi. Il fait partie des sept individus inculpés de blanchiment d'argent et de conspiration pour opérer sans licence une entreprise de transfert de fonds. Au total, cinq des collaborateurs concernés ont été appréhendés, mais deux autres sont encore en liberté au Costa Rica.

On estime à 200.000 le nombre de clients de Liberty Reserve aux États-Unis. Les personnes et entreprises de bonne foi qui faisaient appel à ses services sont priées de contacter le bureau du procureur fédéral de Manhattan.

Liens : http://www.lefigaro.fr/conjoncture/2013/05/29/20002-20130529ARTFIG00277-les-etats-unis-decapitent-le-plus-grand-reseau-de-blanchiment-d-argent-du-monde.php

Etats-Unis :
Un pilier du bitcoin accusé de blanchiment d'argent

Dans le sillon de la fermeture de Silk Road (« l'Amazon de la drogue »), Charlie Shrem de la Bitcoin Foundation a été interpellé et accusé de blanchiment d'argent.

Les activités illégales associées à **Silk Road** et la « monnaie P2P » **bitcoin** reviennent à la une des médias aux Etats-Unis. Et ce, alors que la plateforme Internet, surnommée « l'Amazon de la drogue » en raison des trafic illicites qu'elle soutenait, avait été fermée par le FBI en octobre 2013.

Dimanche 26 janvier, le dossier a rebondi dimanche avec l'interpellation à New York de Charlie Shrem (24 ans), CEO de BitInstant (plateforme d'intermédiation autour du bitcoin, qui a fermé ses portes l'été dernier) et par ailleurs Vice-Président de la Bitcoin Foundation, et la mise en accusation de Robert Faiella (52 ans), qui gère un autre service clandestine exploitant la « monnaie P2P » (The Company). Charlie Shrem est également accusé de ne pas avoir alerté les autorités judiciaires de transactions financières suspectes associées au bitcoin.

Pour être succinct, Charlie Shrem et Robert Faiella sont accusés de blanchiment d'argent en ayant contribué à la vente de bitcoins d'un montant équivalent à un million de dollars à des utilisateurs de feu Silk Road par l'intermédiaire de The Company, selon les éléments divulgués par le bureau du procureur de New York.

Charlie Shrem a été libéré dans la journée de lundi (27 janvier) après avoir payé une caution d'un million de dollars. Quant à Robert Faiella, il restera en détention au moins jusqu'à mercredi.

Bitcoin : les frères Winklevoss indirectement impliqués

De manière inattendue, cette affaire « underground bitcoin » retombe sur…les frères jumeaux Tyler et Cameron Winklevoss. Connus pour avoir revendiqué la paternité de Facebook, ils avaient investi dans le service BitInstant de Charlie Shrem dans le courant de l'automne 2012.

« A l'époque, l'équipe dirigeante s'est engagée auprès de nous à respecter la loi — y compris celle sur le blanchiment d'argent– et nous n'attendons pas autre chose que cela », ont réagi les frères Winklevoss dans un communiqué, assurant être « profondément préoccupés » par cette arrestation. Bien que la société BitInstant ne soit pas directement mêlée dans cet écheveau judiciaire, ils se sont déclarés inquiets de l'arrestation de Charlie Shrem.

Il y a donc toujours un parfum de scandale autour du bitcoin. Pourtant, lors d'une récente audition devant une commission du Sénat français, Gonzague Grandval, CEO d'une des rares sociétés françaises cherchant à exploiter le potentiel de la monnaie P2P (Paymium), déclarait que les transactions en bitcoins sur le réseau Silk Road ne représentaient qu'1% du volume global des échanges. Il faut croire que c'est encore trop pour la justice américaine.

Liens : http://www.itespresso.fr/etats-unis-pilier-bitcoin-accuse-blanchiment-argent-72134.html

La fraude et le blanchiment d'argent aux Etats-Unis pèsent 300 milliards de dollars

La fraude et le blanchiment d'argent aux Etats-Unis représentent annuellement quelque 300 milliards de dollars, la moitié provenant d'escroqueries à l'assurance santé et aux impôts, selon un rapport du Trésor américain publié vendredi 12 juin.

Les fraudes contre le gouvernement fédéral, notamment les fausses déclarations d'impôts donnant lieu à des remboursements indus, ainsi que les fausses déclarations à l'assurance médicale pour les plus pauvres et les plus âgés *« sont au moins deux fois plus importantes »* que le profit réalisé par le marché de la drogue, souligne ce rapport. L'utilisation d'Internet pour le vol d'identité a augmenté l'ampleur et l'impact de ces escroqueries, assure le Trésor ? sans pouvoir chiffrer cette évolution.

64 milliards générés par le trafic de drogue

Le trafic de drogue à lui seul génère environ 64 milliards de dollars annuels en liquide, une grande partie de la drogue passant par le Mexique. *« Le cash, bien qu'il soit nécessaire et omniprésent, est un instrument monétaire interchangeable par définition qui ne laisse pas de trace quant à sa source, son propriétaire ou sa légitimité »*, déplore le rapport.

Un autre rapport publié vendredi et évaluant pour la première fois les risques de financement du terrorisme, estime que les Etats-Unis ont rendu considérablement plus difficile aux organisations terroristes d'utiliser le système financier américain pour collecter et transférer de l'argent.

Liens : http://www.lemonde.fr/ameriques/article/2015/06/12/la-fraude-et-le-blanchiment-d-argent-aux-etats-unis-pesent-300-milliards-de-dollars_4653344_3222.html

Le créateur du site Silk Road condamné à la prison à vie

Ross Ulbricht a été condamné vendredi à la prison à vie aux États-Unis pour avoir abrité sur son site Internet Silk Road un trafic de drogue de plus de 200 millions de dollars via la monnaie virtuelle Bitcoin.

Âgé de 31 ans, Ross Ulbricht a été jugé en février coupable de trafic de drogue sur Internet et association de malfaiteurs en vue de commettre du piratage informatique et du blanchiment d'argent.

« Ce que vous avez fait est sans précédent », a déclaré la juge Katherine Forrest. « Et étant le premier à vous avancer sur ce terrain, vous êtes ici présent en tant qu'accusé ayant à en payer les conséquences. »

Le site Silk Road a fonctionné au moins entre janvier 2011 et octobre 2013, date de l'arrestation de Ross Ulbricht à San Francisco. Relié au réseau Tor, qui permet de communiquer dans le plus parfait anonymat, il permettait à des internautes d'acheter de la drogue et d'autres produits illicites en utilisant la monnaie virtuelle Bitcoin.

Joshua Dratel, avocat de Ross Ulbricht, a annoncé son intention de faire appel en qualifiant le jugement d'« excessif, injuste et inique ».

Ross Ulbricht, qui a reconnu au cours du procès être le fondateur de Silk Road, mais a démenti toute malversation, est resté silencieux à l'énoncé de sa peine, qui comprend aussi une amende de 184 millions de dollars.

Auparavant, il avait assuré que contrairement aux affirmations de l'accusation, il n'avait pas créé son site Internet par désir d'enrichissement.
« Je voulais offrir aux gens la possibilité de faire des choix dans leurs vies et de le faire dans le respect de leur vie privée et de manière anonyme », a-t-il dit à la juge.
Le procureur Serrin Turner a en revanche ramené Ross Ulbricht au rang de banal trafiquant de drogue rêvant de faire fortune via ses activités criminelles, quitte à prendre des mesures extrêmes comme commanditer des meurtres. Aucune preuve n'a été apportée au cours du procès d'assassinats commis à la demande de Ross Ulbrich.
Liens : http://ici.radio-canada.ca/nouvelles/international/2015/05/30/001-createur-site-silk-road-condamne-prison-a-vie.shtml

Drogue.
Le site Silk Road a fait des émules

Le fondateur du plus grand marché de la drogue en ligne a été condamné à la perpétuité le 29 mai. Mais la fermeture du site Silk Road a simplement ouvert la voie à ses successeurs.
Ross Ulbricht, alias Dread Pirate Roberts, a beau avoir été condamné à la prison à vie le 29 mai pour son rôle à la tête de Silk Road, qui était jusqu'à sa fermeture en octobre 2013 le plus grand site de vente de drogue en ligne, *"le vent a tourné"*, comme le dit **The Guardian,** *"et les sites de vente en ligne de produits illicites ne sont pas près de disparaître"*.
Ce constat, fait par les clients aussi bien que par les vendeurs, est corroboré par un graphique publié par **The Economist** à partir de chiffres de Digital Citizens Alliance, une organisation américaine à but non lucratif centrée sur les questions de sécurité sur Internet.
Si Silk Road contrôlait à sa fermeture 70 % du marché de la vente de la drogue en ligne, il n'a pas fallu longtemps à d'autres acteurs pour émerger, rappelle l'hebdomadaire. Un nouveau site Silk Road 2.0 est d'abord apparu, fermé à son tour par les autorités. Puis deux sites plus petits, Evolution et Agora, ont repris le flambeau. Le premier a disparu en mars dernier : des administrateurs sont partis avec plus de 12 millions de dollars de Bitcoins.
Il n'a fallu alors qu'un mois à de nouveaux sites pour prendre sa place. Le nombre d'offres serait aujourd'hui plus de deux fois plus important qu'en octobre 2013.
Bien plus sûr
"Tant que nos clients comprendront qu'acheter de la drogue via un marché sur réseau virtuel anonyme *[dark net market]* est bien plus sûr que de le faire en personne, cela continuera", *explique un utilisateur au Guardian.* "Les gens n'ont pas peur d'être volés, de prendre des coups ou de se faire tuer comme quand ils vont voir leur dealer du coin."
Les technologies utilisées par Silk Road – notamment le réseau Tor, qui permet de rendre anonymes les échanges Internet et la monnaie virtuelle Bitcoin – ont des implications au-delà du trafic de drogue, en termes de vie privée et de surveillance.
Des questions explorées dans un documentaire titré *Deep Web* ("Web profond") qui doit être diffusé ce 31 mai sur le réseau américain de télévision câblée Epix, rapporte le site Mashable**.**
Liens : http://www.courrierinternational.com/article/drogue-le-site-silk-road-fait-des-emules

Silk Road 2.0, supermarché de drogues et d'armes sur le Web, fermé par le FBI

Le FBI a annoncé avoir arrêté l'administrateur présumé du site de vente de produits illégaux, Silk Road 2.0. Le site est désormais inaccessible.

Son pseudo: «Defcon». A 26 ans, Black Benthall vient d'être arrêté par le FBI à San Francisco. Suspecté d'être l'administrateur du site SilkRoad 2.0, il est accusé, entre autres, de trafic de drogues et de faux documents, de blanchiment d'argent et de piratage. Si tous les chefs d'accusation sont retenus lors de son futur procès, il risque la prison à vie.

Après la fermeture du premier Silk Road en octobre 2013 par le FBI, Silk Road 2.0 a pris la relève. Comme son prédécesseur, ce site était accessible uniquement par le réseau anonyme «TOR». Il permettait aux internautes de commander toutes sortes de marchandises illégales dans le monde entier: drogues, armes, faux papiers... Pour payer, il fallait régler en bitcoin, la principale monnaie virtuelle. D'après les autorités américaines, la deuxième version de Silk Road aurait dépassé les 100.000 clients depuis son lancement fin 2013. En septembre, les ventes réalisées sur le site auraient généré environ huit millions de dollars. Silk Road prenait une commission de 8 à 15% sur chacune d'elles.

Une opération internationale de grande envergure

Lors de l'opération «Onymous», qui a permis l'arrestation de Black Benthall, seize autres personnes qui seraient liées au e-commerce illégal ont été arrêtées. Au total, c'est 414 sites qui ont été fermés. Les autorités américaines ont collaboré avec seize pays européens pour cette opération, dont la France, l'Allemagne et la Grande-Bretagne.

Les sites vendant des produits interdits comme Silk Road 2.0 sont accessibles sur une partie cachée d'Internet, appelée le Dark Web. «Pendant longtemps les criminels [du Darkweb] se sont considérés comme intouchables», a déclaré le chef de l'unité de crimes sur Internet d'Europol Troels Oerting, ajoutant «nous pouvons désormais prouver qu'ils ne sont ni invisibles ni intouchables». Les personnes à l'origine de ces sites, que la plupart des gens ne connaissent pas, et les individus qui y vendaient leurs produits sont difficilement identifiables. Le réseau «TOR» dont ils se servent rend intraçable l'activité des internautes du Dark Web. Pour cela, ce sont des serveurs répartis partout dans le monde qui sont utilisés, chacun créant une couche de protection. Les produits commandés sont eux envoyés par la Poste dans une enveloppe ou un colis, normal en apparence. La monnaie utilisée joue aussi un rôle important: le bitcoin n'est ni nominatif, ni lié à quelconque banque.

Dans son communiqué, le FBI déclare avoir découvert l'identité de Black Benthall en infiltrant l'outil d'administration de Silk Road 2.0. Aucun autre détail n'est communiqué, mais les autorités pourraient avoir trouvé un moyen de contourner l'anonymat de «TOR». Une hypothèse qui expliquerait le nombre important de sites saisis lors de cette opération.

Reste maintenant à savoir quand une éventuelle version 3.0 sera mise sur pieds et débarquera sur le Dark Web. Lorsque le premier Silk Road a été fermé par le FBI, il n'a fallu que quelques jours pour que son successeur arrive

Liens : http://www.lefigaro.fr/secteur/high-tech/2014/11/07/32001-20141107ARTFIG00358-silk-road-20-supermarche-de-drogues-et-d-armes-sur-le-web-ferme-par-le-fbi.php

Commerce en ligne : drogues et armes sont proposées sur le darknet

Drogues, armes, numéros de cartes de crédit: on trouve tout cela dans le darknet, une sorte de réseau dans le réseau, également utilisé par les cybermilitants surveillés par des dictatures ou les hacktivistes, qui militent pour un internet totalement libre et anonyme.

Début octobre, un site internet de l'ombre créé en 2011 est placé sous le feu des projecteurs. Silk Road ("la route de la soie"), 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. Ulbricht, lui, nie être le "capitaine" de Silk Road.

En deux ans et demi, ce site du darknet aurait généré des ventes de 1,2 milliard de dollars (880 millions d'euros) en monnaie virtuelle bitcoin, pour empocher un montant total de 80 millions de dollars (60 millions d'euros) sous forme de commissions.

La nature ayant horreur du vide, d'autres sites marchands "clandestins", comme Black market reloaded (BMR), ont pris la place de Silk Road sur internet. Mais pas n'importe quel internet. Ici, les adresses sont une suite de chiffres et de lettres qui changent régulièrement et se terminent en .onion et non pas en .fr ou .com.

Pour accéder anonyment à Black market reloaded, il faut passer par le logiciel libre et gratuit Tor (acronyme de "The Onion Router"), qui permet de naviguer sur internet par l'intermédiaire d'autres ordinateurs du réseau Tor, basés aux quatre coins de la planète.

Ainsi, l'adresse IP de l'ordinateur utilisé, véritable plaque d'immatriculation, apparaîtra, aléatoirement, au Japon, aux Etats-Unis ou en Grande-Bretagne, rendant sa localisation impossible ou plus difficile par les services de police, notamment.

Une fois sur ce marché noir virtuel, après un long et fastidieux processus d'inscription, ecstasy, cannabis, faux-papiers et armes sont à la vente contre des bitcoins, dont la première borne physique d'échange a été mise en service mardi, à Vancouver (Canada).

Sur BMR, un kilo de hachich népalais est mis en vente contre 14,7 bitcoins (soit 2.183 euros au taux actuel) et expédié "partout dans le monde" depuis l'Inde dans un "emballage discret". Comme dans tout site marchand, les acheteurs éventuels se renseignent : "L'envoyez-vous en un seul paquet ou plusieurs ?" ou "Pensez-vous que le paquet arrive sans problème en France ?".

Réseaux dans le réseau

Mais en dehors de cette utilisation à des fins criminelles, les défenseurs de la vie privée considèrent aussi le système Tor comme un bon outil pour les internautes désireux de se protéger contre le commerce en ligne. 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. C'est pareil pour les entreprises qui sont sur un marché sensible", 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.
Outre Tor, d'autre réseaux comme I2P, pour Internet invisible project, ou Freenet, permettent à plusieurs ordinateurs de communiquer entre eux uniquement.
"Ce sont des réseaux dans le réseau, il faut imaginer des îles", décrypte Guilhem Fouetillou, cofondateur de Linkfluence, entreprise spécialisée dans l'analyse du web social, qui s'est fait connaître par la cartographie d'internet
Liens : http://www.ladepeche.fr/article/2013/10/31/1743356-commerce-ligne-drogues-armes-sont-proposees-darknet.html

Raid contre les "marchés noirs" sur le Darknet aux USA et en Europe : 414 sites fermés

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 la police 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.

Liens : http://www.huffpostmaghreb.com/2014/11/08/silk-road-tor-darknet_n_6125218.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

(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).
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, 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. 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 (couramment appelé « paradis fiscal »). Rappelons toutefois, qu'en théorie, les bitcoins sont imposables.

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, 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.
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. Or, leurs activités ne sont pas plus légales…
Liens : http://www.lepetitjuriste.fr/droit-des-ntic/la-fraude-et-le-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 s'y 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 "strongDarknet ? 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.
Liens : http://www.jolpress.com/darknet-crimes-drogues-armes-internet-illegal-pedophilie-cle-usb-article-824421.html

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, 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.

Liens : http://www.slate.fr/monde/80471/qui-peur-du-grand-mechant-darknet

Deep Web : 20'000 lieues sous Google

« Près de 90% du contenu du Web échappe aux moteurs de recherche. C'est le «Deep Web» ou la face immergée de l'iceberg numérique. Un territoire invisible et profond où cohabitent incognito «whistleblowers», blogueurs dissidents, dealers, pédophiles et tueurs à gages. Bienvenue dans les abysses de la matrice.

La presse anglo-saxonne le surnomme «le plus grand conseiller en pornographie infantile au monde». Arrêté début août par le FBI, Eric Eoin Marques de son vrai nom est accusé d'être le cerveau de Freedom Hosting, un service web accessible sur le réseau anonyme Tor qui héberge des milliers de forums pédophiles. Cet Irlandais de 28 ans aurait favorisé l'échange de milliers de fichiers de pornographie infantile et conseillé d'autres pédophiles sur la manière d'abuser sexuellement des enfants sans se faire arrêter.

En Australie, Paul Leslie Howard croupit dans une prison de Melbourne en attendant le verdict du tribunal. Le trafiquant de 32 ans encourt jusqu'à 5 ans d'emprisonnement pour la vente de cocaïne, amphétamines, LSD, MDMA et marijuana. Une large palette de substances illicites qu'il se procurait et fournissait à des prix défiant toute concurrence sur la Silk Road (la route de la soie), la plateforme commerciale uniquement accessible sur le réseau anonyme Tor. Paul Leslie Howard et Eric Eoin Marques, deux cybergangsters au sein d'une nébuleuse criminelle cachée active sur le «Deep Web».

Les milliards d'internautes lambda l'ignorent. Le Web tel que nous le connaissons n'offre que 10% seulement de son contenu. C'est la pointe visible de l'iceberg. Les 90% restants représentent la face cachée de la Toile, soit plus d'un trilliard de données accessibles en ligne, mais invisibles des moteurs de recherche classiques. On l'appelle le «Deep Web» (Web profond) ou Web invisible, un cyberespace insondable et abyssal dont l'entrée et le contenu ne s'offrent qu'à une poignée d'initiés.

Profondeurs obscures

Le Web est à l'image d'un océan. A sa surface, les moteurs de recherche classiques. Avec l'aide de leurs robots d'indexation, ils parcourent les pages web en naviguant de lien en lien. Les moteurs de recherche aspirent, archivent et indexent le contenu de chaque page visitée. Cette matière visible et accessible à tous est stockée dans les serveurs. Ainsi, Google dispose de plus de 1 million de serveurs dans le monde, tout comme Microsoft. Yahoo! en compte plus de 50 000 et Facebook 180 000. Ces serveurs connectés entre eux hébergent notamment les milliards de pages web aspirées sur lesquelles nous surfons.

Lorsque l'internaute s'immerge dans la matrice, il rencontre des pages web isolées, indépendantes, volumineuses, écrites dans des formats illisibles pour les robots d'indexation, donc des moteurs de recherche classiques. A partir d'une profondeur de 200 mètres, là où la lumière du jour ne filtre pas, on pénètre dans les abysses de la Toile, où le surf est anonyme. Les ressources du Web invisible sont de grande qualité, car générées par des experts – informaticiens, hackers et *hacktivistes*. Un territoire où se côtoient le meilleur, mais aussi le pire de la Toile (pédophilie, images morbides, réseaux de tueurs à gages, trafic de drogue…). Bienvenue dans les profondeurs obscures de la matrice.

Immenses ressources documentaires

L'universitaire *Michael K. Bergman* fait figure de pionnier dans l'exploration du «Deep Web». A la fin des années 1990, l'Américain effectue sa première plongée. Il remonte dans ses filets une pêche miraculeuse. Le Web profond regorge d'immenses ressources documentaires sous forme de bases de données en ligne. On y trouve notamment l'ensemble du contenu des bibliothèques numériques, celles du Congrès américain par exemple, de la BNF-Gallica ou de la National Library of Medicine pour ne citer qu'elles. «Une richesse à couper le souffle», s'exclamera Michael K. Bergman à sa remontée, tant «la valeur du Web profond est incommensurable».

Pourquoi les fichiers jouent-ils à cache-cache ? Les documents et bases de données présents dans le Web profond sont trop volumineux ou trop complexes pour que leurs contenus soient indexés, donc visibles. Parallèlement, plusieurs internautes (des as du code informatique) choisissent délibérément de ne pas renforcer leur site pour privatiser l'information et préserver l'anonymat. L'unique manière d'accéder au contenu de ces pages est de connaître leur URL, soit leur adresse internet. Le développeur du site choisit ainsi de la divulguer à quelques élus. On retrouve ainsi dans ce «club VIP» les membres de WikiLeaks, les groupuscules libertaires d'Anonymous ou les activistes du Printemps arabe, qui conversent à leur guise et échangent des centaines de milliers de documents dans le plus grand secret.

Prévenons celui qui voudrait faire ses premières brasses dans le «Deep Web». Dans les profondeurs, tout est question d'anonymat. On accède aux pages ultra-sécurisées, souvent cryptées, via des réseaux décentralisés de routeurs, c'est-à-dire les appareils par lesquels transite l'information entre les ordinateurs. Le plus connu est *le réseau Tor* (The Onion Router), constitué de multiples strates comme des pelures d'oignon. Une fois à l'intérieur, vous êtes anonyme puisque le réseau Tor modifie constamment votre adresse IP (le numéro d'identification de votre ordinateur, comme il existe des numéros de téléphone). Vous surfez dans votre salon genevois alors que le *NSA* vous localisera à Acapulco. En conclusion, la traçabilité de vos recherches en ligne devient quasi impossible.

Dernier rempart libertaire

L'exploration peut commencer. Faut-il encore connaître l'adresse précise du site recherché. Dans les bas-fonds du Web, un lien internet prend la forme d'une succession de lettres et de chiffres se terminant par un .onion et non .com : *http://dppm78fxaaccguzc.onion*. Le projet Tor est géré par des bénévoles qui assurent aux utilisateurs un anonymat complet en ligne. Le réseau est un outil essentiel à certaines luttes politiques, *au point que Reporters sans frontières le recommande dans son kit de survie numérique*. Qui s'y connecte? Des hackers, des cybercriminels, mais aussi des opposants politiques, des blogueurs dissidents et des journalistes.

Les sites, chats et forums qui peuplent ce réseau sont réunis dans un «*Hidden Wiki*», soit un Wikipédia caché. Cette encyclopédie obscure rassemble toutes les tendances. On y trouve aussi bien la liste des sites tenus par des opposants au président syrien Bachar el-Assad que celle des défenseurs d'une «Europe blanche». D'autres plateformes invitent à financer la lutte islamique. La pornographie y tient une place de choix, du X classique aux tendances les plus déviantes. Mais l'anonymat garanti par le réseau Tor attire aussi les pires criminels.

Tueurs à gages et blanchiment d'argent

Le «Deep Web» a son côté obscur : le «Dark Web», où les marchés clandestins sont légion. On y trouve des sites non commerciaux, comme Shroomtastic, un forum pour «apprendre à faire pousser des champignons hallucinogènes». Et des sites commerciaux. Le plus connu se nomme Silk Road (route de la soie). L'offre illégale y est pléthorique. Le site CoinFog permet de blanchir de l'argent, Killer for Hire fournit

les services de tueurs à gages pour 9200 francs. All Purpose Identities explique la fabrication de faux papiers d'identité. EuroArms vend des AK-47, des kalachnikovs russes pour 680 francs. Sans parler de la longue liste de drogues, des produits Apple de contrebande à petit prix et des poisons utiles à l'élaboration de cocktails mortels.
Sur ce marché clandestin, les transactions se font dans une monnaie virtuelle : le bitcoin. Cette dernière a été créée en 2009 par un certain Satoshi Nakamoto – son nom d'emprunt. Les bitcoins sont générés par des algorithmes. Ils sont échangeables via un logiciel de partage pair-à-pair à installer sur son ordinateur. L'utilisateur met à disposition une partie de la capacité de calcul de son ordinateur au réseau et peut ainsi échanger de la monnaie virtuelle. Sa particularité ? Elle est intraçable. Les 5 grammes de résine de cannabis s'échangent à 0,59 bitcoins, soit 63,33 francs au dernier cours de change.
Selon l'étude de Nicolas Christin, professeur français à l'Université de Carnegie Mellon, en Pennsylvanie, le volume total des ventes du site Silk Road représentait l'an passé 1,3 million de francs par mois, dont 100 000 reversés aux administrateurs. Le chercheur et enseignant en sécurité informatique à l'EPFL, Philippe Oechslin, fait preuve de prudence : «Les outils cryptographiques sont si performants qu'il est impossible de remonter un circuit criminel pour le quantifier», explique l'expert, également fondateur d'Objectif sécurité, la société spécialisée dans la sécurité des systèmes d'information.
Le seul moyen de débusquer un cybercriminel reste de le pousser à la faute. Car pour livrer de la drogue ou une kalachnikov achetés sur Silk Road, il faut une adresse physique de livraison. Mais là aussi, les criminels disposent de boîtes aux lettres anonymes. Les marchés clandestins ont donc de beaux jours devant eux. D'autres sites comme Atlantis et Black Market Reloaded voient le jour sur le même modèle que Silk Road. Si ces plateformes sont parfois victimes d'attaques informatiques qui les mettent hors service, elles échappent au contrôle de la police, impuissante devant cette pieuvre qui profite des limites de la coopération internationale en matière de lutte contre la criminalité.
La «magie» du réseau Tor est qu'il est utilisé tant par l'Etat américain et son agence de renseignement (NSA) que par ses opposants. Les pionniers du réseau l'ont pensé pour le bien de la communauté numérique. Ils revendiquent le secret et la sécurité au milieu de l'océan qu'est le Web. «Il en va de la protection de l'information et de la sécurité des whistleblowers comme Edward Snowden ou Julian Assange», ajoute Philippe Oechslin. A mesure que la sphère privée des internautes s'effrite et que les gouvernements outrepassent les lois pour surveiller les communications, le besoin de confidentialité en ligne grandit. Les révélations sur le programme d'espionnage Prism de la NSA n'ont rien arrangé.
Malgré son apparente anarchie, le Web visible devient de plus en plus contrôlé. Il est surtout l'objet d'intenses convoitises commerciales de la part des fournisseurs d'accès à Internet. Petit à petit, les moteurs de recherche classiques – Google en tête – se cherchent des chemins dans le Web profond. Mais l'exploration vers les grands fonds promet d'être longue et semée d'embûches ».
Liens : https://olivierdemeulenaere.wordpress.com/2013/08/25/deep-web-20000-lieues-sous-google/

Deep Web
Arrestation du fondateur de Sheep Marketplace lors de l'achat d'une villa

Thomas Jiřikovský, le propriétaire présumé de l'un des sites les plus populaires du Darknet, "Sheep Marketplace", a été arrêté après le blanchiment d'environ 40 millions de dollars, ce qui en fait une des plus grandes escroqueries dans l'histoire du Deep Web.

Après l'arrestation de propriétaire de Silk Road, Ross Ulbricht, en 2013, Sheep Marketplace est devenu la place de marché underground la plus célèbre sur le réseau anonyme Tor. Les clients du marché noir y affluait pour la vente de produits illicites, en particulier les médicaments.

Mais après quelques semaines seulement, Sheep Marketplace a soudainement disparu après avoir été déconnecté par son propriétaire, qui avait été soupçonné d'avoir volé massivement des Bitcoins, montant estimé à 40 millions de dollars au moment où la valeur de marché du Bitcoin atteint des sommets historiques. Peu de temps après cette escroquerie au Bitcoin, un habitué du Darknet, Gwern Branwen, publie un "dox" sur le propriétaire présumé qu'il a lui-même identifié : Thomas Jiřikovský.

Cela est du à une erreur de Jiřikovský qui a oublié de cacher son identité et adresse résidentielle sur Internet, qui a été exposée par sa page Facebook. Cependant, immédiatement après la fuite de son identité, Jiřikovský a nié en bloc son implication dans la place de marché illicite Sheep Marketplace.

Lors d'une enquête pour ce vol d'argent en ligne, la police tchèque a remarqué un jeune programmeur suspect qui a tenté d'acheter une maison de luxe d'une valeur de 8,7 millions de couronnes tchèques (soit $ 345 000 USD) en Lusace, une région en République tchèque, sous le nom de son grand-père. Le complément d'enquête a révélé qu'en janvier de l'année dernière, un compte bancaire au nom d'Eva Bartošová, 26-ans, a reçu un énorme virement de près de 900 000 couronnes, émis par une société étrangère de change de Bitcoins. Bien entendu, la jeune femme était incapable de justifier l'origine de l'argent…

Selon les médias tchèques, Eva Bartošová est la femme de Thomas Jiřikovský, qui l'aurait aidé à transférer l'argent volé sur son compte de banque fraîchement créé. La division économique de la police tchèque a enquêté sur l'argent des Jiřikovský et a constaté que la maison avait été entièrement achetée en utilisant les Bitcoins incriminés.

Rappelons aussi qu'un autre grand marché de la drogue du Deep Web « Evolution », a soudainement disparu il y a quelques jours à peine, et que les rumeurs qui circulent sur ses propriétaires indiquent qu'une gigantesque arnaque aurait touché les utilisateurs après le vol de plusieurs dizaines de millions de dollars en Bitcoin. Une chose est sûre, le Darknet et le Bitcoin se portent mal !

Liens : https://www.undernews.fr/hacking-hacktivisme/deep-web-arrestation-du-fondateur-de-sheep-marketplace-lors-de-lachat-dune-villa.html

Le deep web,
Le côté obscur de la toile

Dans les bas fonds du web, inaccessibles via Google, pirates, dealers et même tueurs à gages naviguent incognito.

À la base, le deep web c'est…

Une partie du web accessible en ligne, mais non référencée par les moteurs de recherche classiques (Google, Explorer, Bing, Yahoo, etc.). Ces derniers possèdent des programmes appelés « robots d'indexation » qui parcourent le web à la recherche de liens hypertexte pour découvrir de nouvelles pages. Mais certaines pages sont isolées, indépendantes ou parfois écrites dans des formats illisibles par ces robots. Ces données « invisibles » constituent le deep web. Seuls 3 à 10% des pages seraient en fait indexées sur le web, comme l'expliquent Chris Sherman et Gary Price dans leur livre *The Invisible Web*. Il existerait plus d'un trilliard de données « cachées » des moteurs de recherche généralistes*.

Pourquoi les fichiers jouent à cache-cache et comment les retrouver

Certains documents sont trop volumineux. Certaines bases de données sont trop complexes pour que leurs contenus soient indexés. Et certains individus (grosso merdo des nerds qui s'y connaissent en bidouille) choisissent délibérément de ne pas référencer leur site. Pour « privatiser » l'information. Une seule façon d'accéder à ces pages : connaître leur url. Le développeur du site va alors choisir de diffuser l'adresse à quelques personnes, qui peuvent ensuite la faire circuler grâce au bouche à oreille. Le *deep web* ou le club VIP des ingénieurs informaticiens..

Au fin fond de cette partie immergée du net, certains outils de reconnaissance, eux-mêmes indétectables par les moteurs de recherche classiques et capables de décrypter des pages invisibles pour ces derniers, ont vu le jour. Et se sont vite transformés en bottin 2.0 des criminels…

Le côté dark du deep

Synonyme d'anonymat, le *deep web* a rapidement hébergé tous types de marchés noirs : des drogues aux armes. Le *Hidden Wiki* (sorte de jumeau maléfique de Wikipédia) se charge de référencer ces portes d'entrées sur le « *dark web* ».

On y trouve des sites non commerciaux, comme *Shroomtastic*, un forum pour « apprendre à faire pousser des champignons hallucinogènes et s'amuser ». Et des sites commerciaux, comme *Silk Road*, le plus connu. Un marché clandestin sur lequel on peut acheter toute sorte de drogues, grâce à une monnaie anonyme, virtuelle et universelle qui se passe des banques : le bitcoin.*Silk Road*, le plus connu. Un marché clandestin sur lequel on peut acheter toute sorte de drogues, grâce à une monnaie anonyme, virtuelle et universelle qui se passe des banques : le bitcoin.

L'offre commerciale, illégale et considérable, ne s'arrête pas aux drogues : *CoinFog* permet de blanchir de l'argent ; *Killer For Hire* offre les services de tueurs à gage ; *All Purpose Identities* propose de fabriquer de fausses cartes d'identité et *EuroArms* vends des AK47, des Glock, etc. Sans parler de tous les sites porno déviants et pédophiles.

Surfer dans le *deep web*, c'est safe ?

Avant de s'orienter du côté obscur de la force, mieux vaut mesurer les risques. Personne ne vous poursuivra pour avoir flâné sur le deep web. En revanche, les sanctions pour des transactions illégales sont loin d'être virtuelles. En février 2013, Paul Leslie Howard, trafiquant lié à Silk Road, s'est fait attraper en Australie. Jugé

coupable par le tribunal de Melbourne pour vente de cocaïne, amphétamines, LSD et marijuana, il encourt de trois à cinq ans de prison.
Et pourtant les marchés clandestins sont légions. Car les acheteurs, eux, n'ont encore jamais été inquiétés. Le « dark web » assure à ses internautes une ultra-sécurisation de la navigation. Pour cause, l'accès à cette partie du net promet, pour les novices, d'être un vrai parcours du combattant. Accrochez-vous.
Envie de faire vos premiers pas dans le *deep web* ?
L'entrée dans le *dark web* et ses pages ultra-sécurisées, souvent cryptées, se fait via des réseaux décentralisés de routeurs comme Tor, le plus connu et « maintream », ou d'autres outils comme Freenet, I2P, etc. Des programmes qui garantissent, plus ou moins, l'anonymat de votre connexion, en modifiant par exemple constamment votre adresse IP, qui devient alors très compliquée à identifier. Disons… pour le FBI. Vos requêtes passent par une multitude de relais à travers le monde, appelés « nœuds ». Le traçage de la requête originale devient alors quasi impossible. (Ceci n'est pas tiré d'un épisode des Experts.), le plus connu et « maintream », ou d'autres outils comme Freenet, I2P, etc. Des programmes qui garantissent, plus ou moins, l'anonymat de votre connexion, en modifiant par exemple constamment votre adresse IP, qui devient alors très compliquée à identifier. Disons… pour le FBI. Vos requêtes passent par une multitude de relais à travers le monde, appelés « nœuds ». Le traçage de la requête originale devient alors quasi impossible. (Ceci n'est pas tiré d'un épisode des Experts.)
Avant de vous rendre sur Tor, prenez quand même quelques précautions supplémentaires. Commencez par vous armer d'un solide antivirus. Au risque de choper tout un tas de virus pas jolis, jolis. Équipez-vous ensuite d'un VPN (un réseau privé virtuel qui masque le réseau local depuis lequel vous surfez). Ce n'est pas obligatoire, ça fait ramer l'ordi – la navigation sur le *deep web* est déjà lente – mais ça renforce les barrières de sécurité. Une fois que vous aurez téléchargé Tor, faites gaffe d'ajuster chaque paramètre d'installation**. Certaines pages web, par défaut, récupèrent des informations sur votre connexion (notamment grâce aux cookies). Quelques réglages suffisent à garantir leur suppression. Et assurer votre invisibilité., faites gaffe d'ajuster chaque paramètre d'installation**. Certaines pages web, par défaut, récupèrent des informations sur votre connexion (notamment grâce aux cookies). Quelques réglages suffisent à garantir leur suppression. Et assurer votre invisibilité. Vous voilà au cœur de la matrice. Attention à ne pas vous y perdre…
Liens : http://www.neonmag.fr/le-deep-web-le-cote-obscur-de-la-toile-313974.html

Drogues, armes, malwares… à la découverte du Deep Web

Des chercheurs en sécurité ont développé un moteur de recherche qui analyse les activités cybercriminelles qui se trament à l'ombre de la Toile. Les résultats sont, parfois, choquants.
Pour éviter d'être découverts, les cybercriminels opèrent toujours de façon cachée. Leurs échanges sont discrets, ils se tiennent au plus profond du « Deep Web », cette partie de la Toile qui n'est pas indexée par les moteurs de recherche usuels. On y trouve bien sûr les places de marché du Dark Web, accessibles uniquement par des logiciels spéciaux comme Tor, I2P ou Freenet. Mais aussi des sites hébergés dans des domaines alternatifs non gérés par l'Icann et qui ne sont pas pris en charge par les résolveurs DNS classiques. C'est le cas par exemple du .BIT adossé au Namecoin, de

la Toile libertaire d'OpenNIC et Name.space ou de l'Internet parallèle de l' « église césidienne » (si, si ça existe).
A l'occasion de la conférence Black Hat Europe 2015, qui se tient à Amsterdam, les chercheurs en sécurité Marco Balduzzi et Vincenzo Ciancaglini ont présenté leur « Deep Web Analyzer » (DeWA), un moteur de recherches qui permet de faire remonter une partie de ce contenu caché. L'objectif étant de mettre en lumière les tendances et les usages du monde de la cybercriminalité.
Leur système aspire des URLs trouvés sur diverses sources - forums publics, listes dans le Dark Web, Twitter, Pastebin, Reddit, etc. - puis analyse les pages. Elles sont traduites par le service Google Traduction, puis stockées, indexées et synthétisées au travers d'un nuage de mots-clés.
En l'espace de deux ans, DeWA a mis la main sur 611 000 URLs de 20 500 domaines. Sans surprise, il apparaît que la langue du cybercrime est l'anglais, qui représente 75 % du contenu aspiré. Loin derrière arrive le russe et le français. Le protocole le plus utilisé est, de loin, HTTP. Mais les chercheurs ont également trouvé plus d'une centaine de domaines dédiés aux échanges par IRC.
Au final, il se dégage de cette analyse une grande variété d'activités illégales. Les chercheurs sont tombés sur des sites de ventes (drogues, armes, passeports, données bancaires…), des services de blanchiment d'argent, des sites de révélations d'informations personnelles (« doxing ») pour provoquer une vindicte populaire (vis-à-vis d'agents du FBI ou de célébrités par exemple), etc.
Parmi les choses les plus choquantes figurent les services de tueurs à gage avec tarifs à la clé. *« En tant que chercheurs, il nous est impossible de savoir si ces services sont vrais ou non. C'est aux forces de l'ordre de se pencher sur cette question. D'ailleurs, nous coopérons régulièrement avec elles »*, souligne Vincenzo Ciancaglini.
L'un des sites de cette catégorie macabre était particulièrement étonnant : un service de meurtre à la demande basé sur le financement participatif. Des personnes ajoutent un nom et mettent au pot. L'assassin récupère la somme après avoir rempli son contrat. Et le tout se fait de manière anonyme. *« Pour l'instant, seules quatre personnes figurent sur ce site et personne n'a mis de l'argent. Il s'agit probablement d'un hoax »*, estiment les chercheurs.
Enfin, le Deep Web sert également d'infrastructure technique pour piloter les réseaux de botnets et diffuser les malwares. Le malware Vawtrak, par exemple, utilise Tor pour diffuser auprès des machines zombies les adresses IP des serveurs de commande et contrôle. Pour rendre la détection encore plus compliquée, ces adresses sont codées par stéganographie dans des images d'icône.
Liens : http://www.01net.com/actualites/drogues-armes-malwares-tueurs-a-gages-a-la-decouverte-du-deep-web-929845.html

Plongée au cœur du "Deep Web" Comment fonctionne le Web clandestin ?

Le "Deep Web" est en quelques sortes la partie immergée de l'Internet que vous connaissez tous, invisible aux yeux des moteurs de recherche et inaccessible aux non initiés. En bref, c'est une zone de non droit où la cybercriminalité rejoint la criminalité. Explications.

Comment y accède-t-on ?

TOR (The Onion Router), IP2 Web ou encore Freenet. Ces moyens permettent non seulement de naviguer incognito mais aussi d'héberger des sites en leur sein. Ces

derniers ne sont accessible qu'en connaissant leur adresse exacte et de ce fait, ils ne sont pas indexés par les moteurs de recherche. Cela implique qu'il faut avoir des connaissances dans le milieu afin d'y accéder.

Que pouvons-nous y trouver ?

Des produits physiques et virtuels (dématérialisés) y sont présents. La liste est longue et on ne peut mentionner qu'une partie qui représente la majorité des ventes illégales actuelles :

- drogues diverses (cannabis, héroïne, cocaïne, opium, Barbituriques, Amphétamines, LSD, et des dizaines d'autres psychotropes
- armes en tout genre
- services de piratage professionnel
- faux papiers et fausse monnaie
- malwares (trojans/botnets, password stealers, keyloggers, crypters FUD, binders, ransomwares, etc)
- hébergement "bulletproof" & VPN sans logs
- informations bancaires volées (dumps de cartes de crédit et identifiants bancaires en ligne)
- matériel volé ou acquis illégalement via le carding (blanchiment d'argent)
- photos et vidéos illégales (torture, pédopornographie, etc)
- documents classés secret défense

Quels sont les moyens de paiement qui y sont utilisés ?

Les monnaies virtuelles sont à l'honneur dans ce monde underground, le but étant bien entendu que ce genre de monnaie ne laisse aucune trace des transaction et permet aux deux parties de rester dans l'anonymat. Ces monnaies sont nombreuses et l'on peut en citer quelques unes :

- Bitcoin (cryptomon0naie)
- PayPal (dans certains cas seulement, les transactions peuvent êtres tracées)
- Liberty Reserve (récemment fermé par le FBI)
- Webmoney
- PerfectMoney

Les cartes prépayées anonymisées sont aussi très prisées des criminels. Tous ces nouveaux moyens de paiement en vogue dans l'underground n'offrent aucun contrôle possible de la part des institutions financières mondiales ou des autorités.

Pourquoi ces réseaux clandestins sont intouchables ?

Comme souvent, les autorités se retrouvent démunies face aux technologies avancées des cybercriminels. Le chiffrement de bout en bout est omniprésent et le seul moyen semble d'attendre que la cible commette un faux pas et révèle ainsi son identité (ou du moins une adresse IP pouvant être tracée afin de remonter jusqu'à ce dernier).

Liens : https://www.undernews.fr/undernews/plongee-au-coeur-du-deep-web-comment-fonctionne-le-web-clandestin.html

Qu'est-ce qui se passe dans le Deep Web ?

Des spécialistes en sécurité web ont conçu un outil de recherche permettant d'analyser les activités cybercriminelles sur la toile.

Pour ne pas se faire repérer, les cybercriminels opèrent généralement dans l'ombre d'internet. Ils font des échanges discrets depuis Deep Web, une face cachée d'internet qui n'est pas indexée au sien des moteurs de recherche. On peut y trouver des pages

Dark Web qui ne sont accessibles qu'avec des outils spéciaux comme I2P, Tor ou Freenet. Il y a aussi les sites hébergés au sein de domaines alternatifs qui ne sont pas sous la gestion de l'Icann et qui ne sont pas compatibles avec les résolveurs DNS courants. C'est notamment le cas du '.BIT'.
Durant la conférence 'Black Hat Europe', des spécialistes en sécurité web ont proposé DeWA (Deep Web Analyzer). Il s'agit d'un moteur de recherche permettant de mettre à jour une partie des contenus masqués. Le but est d'identifier la pratique des cybercriminels. Leur système cherche les URL localisées sur plusieurs sources, dont les listes de Dark Web, et analyse chaque page. Celles-ci sont ensuite traduites via le service Google Traduction, puis sauvegardées, indexées et synthétisées depuis un nuage de mots-clés.
En seulement 2 ans, DeWA a pu amasser 611 000 URL sur 20 500 domaines. 75% du contenu est en anglais**.** Le protocole utilisé est souvent HTTP. Les spécialistes ont aussi pu découvrir plus de 100 domaines consacrés aux échanges par IRC. En tout, cette analyse permet de connaître diverses activités illégales : drogues, faux passeports, armes, informations bancaires, blanchiment d'argent…
Et ce qui choque le plus ce sont les offres de tueurs à gages. On y trouve un site de meurtre à la demande. Il se fonde sur un financement participatif. Plusieurs personnes indiquent un nom et placent un pot. L'assassin prend la somme quand son contrat est achevé. Toute cette démarche se fait de manière anonyme. Sur ce site, il n'y a que 4 personnes qui sont inscrites jusqu'à présent. Et aucune somme d'argent n'a été déposée.
Le Deep Web est aussi une structure permettant de gérer les réseaux de botnets et de propager des malwares. À titre d'exemple, c'est à travers le réseau Tor que le malware Vawtrak est diffusé. Pour ne pas se faire détecter, les adresses IP sont cryptées par stéganographie. 12/01/2016
Liens : http://webmag.fr/2016/01/deep-web/

Découvrez le « deep web », l'ensemble des données non indexées par les moteurs de recherche classiques

Dans les profondeurs du Web : Armes, drogues, êtres humains : les trafics se dématérialisent et investissent ce que l'on appelle le "deep web", la partie immergée d'Internet. Ce "web profond" est aujourd'hui le théâtre d'affrontements sans répit entre dealers et forces de police, entre terroristes et agences de renseignements. Mais c'est aussi la dernière zone dans laquelle notre vie privée numérique se trouve en sécurité. —Rolling Stone (extraits)
L e 15 juillet, à Pittsburgh, le procureur américain David Hickton, cheveux gris et costume sombre, annonçait la dernière victoire du FBI dans la lutte contre la cybercriminalité. "Nous avons démantelé un réseau de pirates criminels que beaucoup croyaient impénétrable", a-t-il déclaré sur fond de drapeau américain. Le lendemain matin, dans plusieurs pays, plus de 70 personnes étaient inculpées, interpellées ou voyaient leur domicile perquisitionné dans le cadre de "la plus grande opération policière internationale jamais menée contre un forum en ligne de cybercriminels". L'enquête de dix-huit mois conduite par le FBI visait les utilisateurs du site Darkode, aujourd'hui accusés d'escroquerie bancaire, de blanchiment d'argent et de conspiration en vue de commettre une fraude informatique. Leurs méfaits atteignaient des proportions inédites : l'un d'eux avait réussi à s'introduire dans les réseaux sécurisés d'entreprises comme Microsoft et Sony ; un autre avait récupéré des

informations privées sur plus de 20 millions de personnes. Deux semaines plus tard pourtant, le principal administrateur de Darkode répondait aux autorités depuis un nouveau site. “L’essentiel de notre équipe est à l’abri, ainsi que nos membres les plus importants, écrivait-il alors. Il semblerait que l’opération visait principalement les membres les plus récents ou des gens qui n’étaient plus actifs depuis des années. Le forum sera de retour.” Et il promettait que l’organisation allait se réorganiser à partir de l’une des régions les plus secrètes du web – le “Darknet” (ou “darkweb”) –, une partie du web impossible à faire disparaître puisque ce sont les autorités fédérales qui l’ont créée et qui en financent toujours le développement. Pour accéder au Darknet, où l’anonymat est pratiquement garanti pour tous, y compris les criminels, il faut utiliser le navigateur Tor, un logiciel gratuit qui masque à la fois votre localisation et votre activité sur le réseau. Conçu par un laboratoire de recherche de l’armée américaine, le Naval Research Lab (NRL), et financé à 60 % par le département d’Etat et le ministère de la Défense, Tor devait à l’origine servir de réseau de communication sécurisé pour les agences gouvernementales ainsi que pour les dissidents résidant dans des pays à régime autoritaire. Aujourd’hui, il sert aussi bien pour le meilleur que pour le pire. Côté pile, Tor a permis à des militants de communiquer pendant le “printemps arabe”, il a offert un refuge à des victimes
Le harcèlement en ligne et a permis à des citoyens ordinaires de surfer sur la Toile sans être traqués par les mouchards publicitaires. Côté face, c’est aussi un sanctuaire pour des criminels comme Ross Ulbricht, le fondateur – aujourd’hui emprisonné – du site Silk Road [sorte de supermarché de la drogue], les auteurs du récent piratage contre le site de rencontre Ashley Madison et les membres de forums comme Darkode. Utilisé à la fois par des militants et des criminels, Tor devient de plus en plus problé- matique pour les autorités : à peine supprimés, les sites illégaux repoussent comme du chiendent. De la bataille pour faire régner la loi sur cet espace de non-droit qu’est le Darknet dépend peut-être la protection de nos vies privées en ligne aux Etats-Unis et dans le reste du monde. Le Darknet, résume David Hickton, “c’est le Far West d’Internet”. I maginez le web comme un iceberg : la plupart des internautes ne voient que le web “de surface”, soit toutes les infos, les ragots et le porno qu’une simple recherche sur Google vous permet de trouver. Plongez sous la surface et vous découvrirez le “deep web”, le web profond, c’est-à-dire l’ensemble des données qui ne sont pas indexées par les moteurs de recherche classiques et qui sont incomparablement plus nombreuses que celles que l’on peut observer “en surface”. Cela inclut tout ce qui se trouve protégé en surface par un paywall (comme le site Netflix), un mot de passe (votre boîte électronique) ou le moteur de recherche interne d’une page donnée (lorsque vous recherchez dans des archives judiciaires, par exemple). Et, comme les sites qui se trouvent là ne peuvent pas non plus être trouvés en passant par des moteurs de recherche classiques, c’est dans le web profond que se cache le Darknet. La principale différence [entre les deux notions], c’est qu’il s’agit d’un choix délibéré de la part des utilisateurs et des sites du Darknet, qui tiennent à leur anonymat et veulent rester introuvables au commun des mortels, qui n’utilise pas le navigateur Tor.

Les autorités ont créé le darknet et le financent

Ce logiciel qui vous permet de surfer sur le web de surface – exactement comme Firefox ou Safari – est aussi la clé pour accéder aux coulisses d’Amazon ou à des sites comme Silk Road. La plupart des utilisateurs de Tor ont recours à ce navigateur pour des raisons parfaitement légales de protection de leur vie privée. En fait, d’après les estimations du Tor Project – l’organisation non marchande financée par le gouvernement américain et chargée de la maintenance du logiciel –, le Darknet ne

représente que 3 % du trafic réalisé avec Tor. (Et seule une infime partie de ce pourcentage concerne des activités criminelles.) Mais, en raison de sa nature opaque et mystérieuse, le Darknet évoque généralement un sinistre fourre-tout regroupant tout ce que l'on peut trouver de pire en ligne, des groupes terroristes aux réseaux pédophiles, en passant par le trafic de drogue et les hackers mercenaires. Certains des aspects les plus inquiétants du Darknet sont en effet remontés à la surface ces derniers mois. En mai, le fondateur de Silk Road – qui avait vendu pour près de 200 millions de dollars de drogue à des consommateurs du monde entier – a été condamné à la prison à perpétuité. En août, des pirates informatiques ont publié des informations personnelles sur 36 millions d'utilisateurs du site de rencontres extraconjugales Ashley Madison. Enfin, en mai, c'est vers le Darknet que se sont portés tous les regards après que l'organisation Etat islamique (EI) a revendiqué la fusillade perpétrée au Texas en marge d'un concours de caricatures du Prophète. En dépit des coups de filet spectaculaires contre des sites comme Darkode ou Silk Road, les activités du Darknet restent florissantes. D'après une étude publiée en août par des chercheurs de l'université Carnegie Mellon [à Pittsburgh], la vente de drogue et d'autres produits de contrebande rapporterait chaque année près de 100 millions de dollars sur ces sites invisibles où les transactions sont réalisées à l'aide de bitcoins, cette monnaie virtuelle qui ne nécessite ni carte de crédit ni établissement bancaire.

Les enquêteurs n'ont pas seulement affaire à des réseaux criminels capables de rester invisibles sur la Toile, ils sont également confrontés à un afflux massif d'utilisateurs ordinaires à la recherche de produits illicites. Car, contrairement à ce que beaucoup pensent, il n'est pas nécessaire d'être un petit génie de l'informatique pour accéder au Darknet. En fait, il est même étonnamment facile de vendre ou d'acheter des biens et services illégaux : lancez le logiciel Tor et vous vous retrouverez sur un navigateur semblable à tout autre, à l'exception de la vitesse de navigation, très ralentie à cause des sché- mas de routage complexes des données.

"Ici c'est Le far west d'internet"

Au lieu de finir en ".com" ou ".org", les adresses des sites du Darknet se terminent en ".onion" (d'où leur surnom de "sites oignons"). Google n'indexant pas ces "sites oignons", il vous faudra utiliser les moteurs de recherche rudimentaires du Darknet ou des répertoires comme Hidden Wiki ou Onion Link pour trouver votre destination. Les sites marchands du Darknet ressemblent à n'importe quelle autre plateforme commerciale, sauf qu'en lieu et place des ustensiles de cuisine ou décorations de jardin vous trouvez des benzodiazépines, des stupéfiants et des Kalachnikov d'occasion. P aul Syverson, membre du NRL, est le créateur du logiciel Tor. "Nous savions pertinemment que des gens malintentionnés pourraient s'en servir, explique ce mathématicien de 57 ans. Mais notre objectif, c'était de proposer un outil aux gens honnêtes qui ont besoin de protection." Réputé dans le monde entier depuis sa création, en 1923, le NRL est notamment l'inventeur du radar et du GPS. En 1995, Syverson et son équipe imaginent un moyen de sécuriser les communications en ligne. L'idée est de permettre à qui que ce soit de partager des informations sans révéler ni son identité ni sa localisation. Après avoir obtenu un financement du ministère de la Défense, Syverson recrute deux jeunes diplômés du Massachusetts Institute of Technology (MIT), Roger Dingledine et Nick Mathewson, pour mener à bien son projet. Imaginez un espion prenant le train entre Paris et Berlin. Il est facile de le suivre s'il prend une ligne directe entre les deux villes mais, s'il fait Paris-Amsterdam, AmsterdamMadrid, puis Madrid-Berlin, la tâche devient beaucoup plus ardue. C'est la logique qu'ont adoptée Syverson et son équipe. Au lieu de prendre un train direct pour Berlin, l'utilisateur de Tor passe par une série aléatoire

d’ordinateursrelais qui masquent son véritable point de départ. C’est ce qu’on appelle le routage “en oignon” [Tor est l’acronyme de The Onion Router], c’est-à-dire par couches successives. Si le logiciel Tor était réservé aux militaires, toutes ses activités seraient logiquement en lien avec le gouvernement. Mais, poursuit Syverson, “nous voulions créer un réseau capable d’accueillir toutes sortes d’utilisateurs, de manière que nul ne puisse savoir si vous êtes un malade du cancer qui recherche des informations ou bien un soldat de la marine”. Pour ce faire, Syverson et son équipe prennent alors une décision “fondamentale pour la sécurité du système” : ils choisissent de faire de Tor un logiciel libre et open source, c’est-à-dire que n’importe qui dans le monde peut l’utiliser et l’améliorer. Accessible au grand public depuis 2003, Tor circule rapidement dans les milieux universitaires et chez les défenseurs de la vie privée. Très vite, il devient le navigateur préféré – et le plus fiable – des internautes désireux de ne laisser aucune trace sur le web. Ses premiers utilisateurs ne sont pas des criminels, mais des dissidents. L’un d’entre eux, Nima Fatemi, est un Iranien de 27 ans, tout vêtu de noir. Devenu l’un des principaux propagateurs du logiciel, il apprend aux internautes du monde entier comment l’utiliser pour lutter contre les régimes dictatoriaux. “Nous avions besoin de quelque chose de différent pour nous connecter en toute sécurité, se souvient-il. J’ai trouvé Tor et je me suis dit : ‘C’est ça qu’il nous faut.’ Ça nous a permis d’avoir l’esprit tranquille.” Au cours de l’été 2009, Fatemi prend des photos de manifestations pro-démocratie à Téhéran et se retrouve pourchassé par les forces de police. Les photos qu’il publie sur Facebook et Twitter témoignent de la répression menée par le gouvernement iranien contre les dissidents. De plus en plus étroitement surveillé, il se tourne alors vers le logiciel Tor pour continuer à travailler dans le secret de l’anonymat et aider ses camarades militants à échapper à la police. Fatemi organise des ateliers privés pour apprendre à sa famille et à ses amis comment utiliser le réseau Tor, dont la sécurité croît avec le nombre d’utilisateurs : plus il y a d’ordinateurs connectés, plus il y a de “nœuds” pour brouiller les traces. “Nous avons diffusé ce logiciel partout”, assure-t-il. Dans les dix ans suivant sa sortie, le navigateur Tor se répand ainsi massivement dans les cercles militants, en partie grâce aux efforts de l’Electronic Frontier Foundation [EFF, une ONG qui défend la liberté d’expression sur Internet], qui a financé son développement et le présente encore aujourd’hui comme l’un des meilleurs outils de lutte pour la démocratie. Alors que le Tor Project bénéficie encore largement des financements du ministère de la Défense américain, Mathewson et Dingledine continuent à faire évoluer leur logiciel et la communauté qui l’entoure. Aujourd’hui, la popularité du navigateur dépasse toutes ses espérances, reconnaît Mathewson, grand amateur de science-fiction de 38 ans. “Je reçois des courriels de gens qui me disent : ‘Je suis à peu près sûr que votre logiciel m’a sauvé la vie.’ Ce à quoi je réponds que je suis bien content qu’ils soient en vie, mais je ne suis qu’un programmeur informatique. J’espère juste ne pas faire de boulette !” L e 27 janvier 2011, Ross Ulbricht annonce sous le pseudonyme Altoid le lancement imminent de Silk Road [littéralement, la “route de la soie”], le premier marché noir sur le Darknet. Gérant son site sous le nom de Dread Pirate Roberts, Ulbricht est le premier à exploiter pleinement le potentiel criminel de Tor. Il s’agit moins d’une prouesse technique que d’une idée nouvelle. N’importe qui peut déjà créer son site illégal dans les profondeurs du Darknet, où il est aussi difficile d’identifier les auteurs des contenus que ceux qui les consultent. Mais Ulbricht va encore plus loin en utilisant le bitcoin comme monnaie d’échange, ce qui lui permet de rendre les transactions tout aussi intraçables. A l’été 2011, le terme “Darknet” fait son apparition dans les médias et le discours des politiques.

“Votre Logiciel m’a sauvé la vie”

En novembre 2013, le magazine Time évoque en une “un repaire de criminels où cohabitent les drogues, le porno et les vidéos de meurtres”. Un mois plus tôt, on a appris grâce à un document publié par Edward Snowden que l’Agence nationale de sécurité américaine (NSA) considérait le logiciel Tor comme une menace potentielle. Lors d’une réunion ultraconfidentielle en 2012, l’agence notait : “Nous ne pourrons jamais entiè- rement lever l’anonymat des utilisateurs de Tor, mais nous pouvons en identifier un très petit nombre.” (Contactée par Rolling Stone, la NSA s’est refusée à tout commentaire.) Toujours d’après les révélations de Snowden, l’agence de renseignements britannique [le MI6] conteste le caractère pro-démocratie du navigateur Tor, jugeant les “utilisations pseudo-légitimes” mineures par rapport aux “mauvais usages” qui sont faits du Darknet. Les autorités commencent alors à chercher de nouvelles manières d’infiltrer le Darknet. En juillet 2015, Interpol organise sa première formation pour “identifier les méthodes et stratégies utilisées par les réseaux du crime organisé pour échapper à toute détection sur le Darknet”. Le même mois, le directeur du FBI, James Comey, explique devant la commission judiciaire du Sénat l’impuissance de ses agents face aux communications cryptées. “Les outils qu’on nous demande d’utiliser sont de moins en moins efficaces”, déclare-t-il. Des courriels récemment rendus publics montrent pourtant qu’au moins une société semblait détenir la solution. Installée à Milan, Hacking Team est une entreprise de sécurité informatique qui fournit aux gouvernements des outils pour lutter contre les criminels, les activistes et les agitateurs du Darknet. “Il est possible de neutraliser/décrypter le Darknet dans sa totalité. La technologie existe. Faites-nous confiance”, écrivait le directeur de cette société, David Vincenzetti, dans un courriel adressé au directeur du FBI. L e responsable de l’innovation à la Darpa, l’agence en charge des projets de recherche avancés pour le ministère de la Défense américain, est un homme jovial aux cheveux blancs, ancien concepteur de jeux vidéo. Dans une salle de conférences du quartier général de l’agence à Arlington, en Virginie, Dan Kaufman m’explique sur un écran haute définition comment la Darpa tente de remporter le jeu du gendarme et du voleur à l’ère numérique. A titre d’exemple, il me montre une annonce vantant les services d’une prostituée appelée Cherry, une jeune femme mince, asiatique, qui semble avoir 19 ans mais qui pourrait en avoir 30. Mesurant 1 m 62, les cheveux bruns aux épaules, l’annonce précise qu’elle n’a ni tatouage ni piercing. Cherry est l’une des victimes de la traite des femmes organisée au niveau international, qui, d’après les estimations du département d’Etat américain, frapperait entre 600 000 et 800 000 femmes chaque année. Avec près de 100 millions de dollars de profit annuel, c’est l’une des activités les plus florissantes du crime organisé dans le monde. Comme tous les autres trafics – d’armes ou de drogue –, cette activité s’est délocalisée, délaissant la rue pour les profondeurs du web : forums anonymes, messageries cryptées, services d’abonnement et autres sites invisibles pour les moteurs de recherche. C’est cette lacune qui a incité la Darpa à intervenir. “Nous sommes partis d’un constat simple : tout ça est terrible, nous ne pouvons pas rester les bras croisés.”

Memex, L’arme des enquêteurs pour sonder le web caché

La Darpa a donc créé Memex, un moteur de recherche capable de sonder le deep web et le Darknet. Memex peut effectuer des recherches sur le web profond, trouver des sites et stocker des données qui permettront de les purger, exactement comme Google sur le web de surface. Il s’agit de la dernière et principale arme des enquêteurs pour jeter de la lumière sur le web caché. Kaufman me fait une démonstration : avec la seule adresse électronique de Cherry, Memex fait apparaître en un clic toute une liste

d'informations, dont des numéros de téléphone, des adresses de salons de massage et des photos en lien avec les annonces. Le créateur du moteur de recherche Memex s'appelle Christopher White. Ancien responsable des programmes de la Darpa, cet homme de 33 ans a d'abord fait ses classes comme haut responsable de la Darpa en Afghanistan avant de s'intéresser, il y a quelques années, au Darknet. L'idée lui est venue après avoir visité plusieurs agences gouvernementales et constaté leur niveau d'impréparation dans la lutte contre la cybercriminalité. "Ils utilisaient Google et Bing pour leur travail, se souvient-il. Les informations qu'ils recherchent ne leur sont pas accessibles par ces moyens, elles se trouvent dans les méandres du Darknet." Les agences gouvernementales et les forces de police coopèrent désormais étroitement avec la Darpa afin de calibrer Memex au plus près de leurs besoins. Il s'agit également d'explorer les possibilités offertes par ce moteur de recherche pour démasquer les recruteurs de l'organisation Etat islamique qui se cachent sur le réseau. Cette technologie est le produit d'une industrie en plein essor consacrée à la "domestication" du Darknet. Moyennant des sommes pouvant aller jusqu'à 500 000 dollars, des entreprises d'évaluation des "menaces liées au renseignement" promettent à leurs clients de passer le Darknet au peigne fin à la recherche d'éventuels pirates. D'après le cabinet de recherche technologique Gartner, ce marché pourrait représenter 1 milliard de dollars d'ici à 2017. Ce passage à la lumière du Darknet ne risque-t-il toutefois pas de faire disparaître le dernier espace de vie privée sur Internet ? Les défenseurs des libertés espèrent que l'arrivée du moteur de recherche Memex ne mettra pas en péril les internautes du Darknet qui respectent les lois. "Memex est un outil incroyable et fascinant, mais, comme n'importe quelle autre technologie, il peut servir à faire le bien autant que le mal", soulignait récemment un blogueur spécialiste de la sécurité en ligne. Pour l'heure, les policiers du Darknet ont toutefois de bonnes raisons de se réjouir. En dépit de leurs rodomontades, les anciens membres du forum Darkode n'ont pas encore redonné signe de vie (ce qui ne signifie pas qu'ils ne sont pas là) et les premières condamnations d'internautes devraient bientôt tomber. Mais, pendant que le FBI célèbre ses victoires, les gens dont la vie dépend de l'anonymat continuent à se battre. En août, la Cour suprême d'Arabie Saoudite a examiné le cas de Raif Badawi, un blogueur de 31 ans arrêté en juin 2012 et condamné à dix ans de prison et 1 000 coups de fouet, accusé d'avoir critiqué des religieux. Raif Badawi illustre bien l'importance de maintenir des zones d'anonymat et de liberté sur Internet, zones qui n'existent que grâce au logiciel Tor, sans lequel le Darknet n'existerait pas. Pour la représentante de la Californie au Congrès, Zoe Lofgren, les autorités ne devraient pas oublier pourquoi ce logiciel a été créé. "Tor a été développé avec le soutien du gouvernement américain pour défendre la liberté, at-elle déclaré. C'est pourquoi nous plaidons pour son maintien, c'est sa raison d'être." Alors que la bataille du Darknet fait rage, le navigateur connaît une popularité croissante. Facebook propose désormais une version ".onion" de son site pour ceux qui se sentent un peu trop épiés. Invité à un évé- nement organisé par l'organisation de défense de la vie privée et des libertés civiles Epic, le PDG d'Apple, Tim Cook, a ironisé sur les tentatives menées par le gouvernement pour pirater des appareils privés. "La suppression des dispositifs de cryptage de nos appareils – telle que la souhaitent certains à Washington – ne servirait qu'à nuire aux citoyens honnêtes qui nous confient leurs données", a-t-il argué. D'autres navigateurs, comme Firefox, devraient bientôt proposer des fonctionnalités Tor, prophétise Mathewson, qui espère que cette méthode sera "le mode de communication par défaut sur Internet" d'ici cinq ans. Mais la partie de cache-cache sur le Darknet est loin d'être terminée. Même si de nombreux

militants utilisent cet outil pour rendre le monde meilleur, il y aura toujours des criminels pour s'en servir. Et des policiers pour les traquer.
Liens : http://www.bsavenir.fr/2015/12/14/decouvrez-le-deep-web-lensemble-des-donnees-non-indexees-par-les-moteurs-de-recherche-classiques/

Italie : Arrestation d'un groupe de cybercriminels international (scam & blanchiment d'argent)

Nouveau coup de filet pour Europol qui s'est allié avec la Police financière italienne. 10 membres présumés d'un groupe de cybercriminels ont été arrêtés et inculpés pour arnaques en ligne, fraude bancaire et blanchiment d'argent.
La Police financière italienne (Guardia di Finanza) a arrêté plus de 10 personnes soupçonnées de faire partie d'une organisation criminelle internationale. Le groupe aurait blanchi de plus de 2,5 millions d'euros provenant d'escroqueries en ligne (scams) et fait face à des accusations de fraude et de blanchiment d'argent. L'opération a été menée en collaboration avec Euopol, qui vient de publier un communiqué.
L'opération a impliqué la coopération entre la police italienne, Europol et le Federal Bureau of Investigation (FBI). Des dizaines d'entreprises ont été touchées par ces cyberattaques sophistiquées visant à détourner les données des entreprises victimes et d'échanger ces informations contre des paiements par virement bancaire.
Beaucoup d'entreprises ont donc transféré d'importantes sommes d'argent aux cybercriminels. Des centaines de personnes ont également été affectées par des escroqueries en ligne où les fraudeurs ont créés de faux profils sur des sites de rencontres et ont convaincu des gens de leur envoyer de l'argent.
Selon les enquêteurs, le groupe a fondé un large réseau international dans le but de procéder à des retraits d'argent liquide dans le monde entier. 32 personnes sont encore activement recherchées dans le cadre de ce "*bank run*" d'envergure.
Liens : https://www.undernews.fr/hacking-hacktivisme/italie-arrestation-dun-groupe-de-cybercriminels-international-scam-blanchiment-dargent.html

Les nouvelles formes de scam : Les mules et le blanchiment

Méthode de nouveaux trafiquants: les scammeurs.
Les nouvelles victimes de scam ne sont plus des individus naïfs qui se font soustraire leur argent. Maintenant, ce sont des personnes crédules mêlées à des traffics d'argent.
Bientôt fini le temps du scams 419 où des correspondants soi-disant nigérians arnaquent des personnes naïves et leur soutirent jusqu'à plusieurs dizaines de milliers d'euros ? Il semble que la nouvelle forme de scam soit plus imaginative dans la mesure où le scammeur ne cherche plus à soutirer directement de l'argent à la victime. Il acquiert l'argent par d'autres moyens illégaux (vol de carte bleue, piratage de comptes bancaires ou de comptes paypal, etc…), mais se sert de la victime comme d'une mule.
En matière de trafic de drogue, une mule est une personne qui fait passer la drogue au travers des postes de contrôles. Le trafiquant a donc intérêt à choisir la mule qui

semble la plus innocente possible, de manière à ne pas alerter les contrôleurs. De même, il doit cloisonner totalement la mule, qui ne devra pas savoir qui est son commanditaire. En matière de fraudes sur l'Internet, le plus dur n'est pas la fraude elle-même, mais de pouvoir profiter des fruits de la fraude tout en restant intraçable. Or, pour recevoir l'argent ou les colis achetés grâce à une CB volée, il faut une identité et une adresse, tous les deux aisément traçables. C'est ici qu'interviennent les mules, que les scammeurs convainquent d'accepter de recevoir et garder un paquet ou une somme chez eux jusqu'à ce qu'on vienne les récupérer à une date future.
Le principe est le même que pour un scam traditionnel. Le scammeur entre en contact avec une mule potentielle. Il faut noter ici l'apport immense des réseaux sociaux du type Facebook ou Second Life, qui facilitent la tâche des scammeurs, puisque non seulement on peut y trouver les centres d'intérêts de la mule, mais on peut également la contacter plus facilement que par l'envoi d'un mail classique dont les gens se méfient de plus en plus. Imaginons un exemple typique : un scammeur va déterminer suivant le profil d'une personne qu'elle s'intéresse aux œuvres humanitaires destinées aux écoles du Tiers Monde. Il va alors imaginer un scam personnalisé en se faisant passer pour un directeur d'une école d'Afrique qui a besoin d'ordinateurs portables pour son école. Là où le scammeur classique va demander que la victime lui envoie de l'argent, le nouveau scammeur aura déjà obtenu l'argent autrement, et dira à sa victime que de généreux bienfaiteurs ont déjà acquis les matériels informatiques en question, mais que pour des problèmes d'acheminement (par ex, parce qu'un regroupement de marchandises dans un conteneur coûte moins cher), les matériels doivent être stockés temporairement en France. Malheureusement, le directeur d'école ne connaît personne en France et déposer le matériel dans un entrepôt spécialisé coûterait trop cher. Il cherche donc quelqu'un qui puisse les recevoir et les stocker le temps que toutes les marchandises soient prêtes à l'expédition, et à ce moment là un transitaire va les récupérer chez la victime. La victime a tout lieu de croire à la sincérité de son correspondant puisqu'en apparence, c'est celui-ci qui supporte les risques en entreposant du matériel coûteux chez un parfait inconnu, accepte que la marchandise soit envoyée à son nom à son domicile et consent à la garder jusqu'à ce qu'on vienne la récupérer. En réalité, il devient complice et receleur, et risque de sérieux ennuis judiciaires s'il ne parvient pas à faire la preuve du scam. Le scammeur, lui, récupère tranquillement les marchandises en se faisant passer pour un agent du transitaire, et disparaît avec dans la nature.
Parce que les mules ne se sentent pas escroquées (aucune tentative de soustraction d'argent, et il arrive même que les scammeurs leur versent de l'argent en compensation), et sont de plus sollicitées dans des domaines qui leur sont chers (grâce aux réseaux sociaux entre autres), cette forme de scam se répandra de plus en plus dans l'avenir, et permettra aux fraudeurs en tous genre sur l'Internet de blanchir l'argent ou les produits résultant de leurs sinistres actions.
Liens : http://www.altospam.com/actualite/2009/02/les-nouvelles-formes-de-scam-les-mules-et-le-blanchiment/

Arnaque de transfert d'argent

Arnaque de transfert d'argent est l'un des noms utilisés pour désigner les innombrables « Arnaques à l'africaine » sur l'Internet. Formellement : « Fraude 419 ».

Arnaque de transfert d'argent **»** est un synonyme de « Fraude 419 ». Le nom formel pour ces fraudes est « Fraude 419 » (419 étant la référence de la section du code pénal du gouvernement nigérian traitant de ce type d'arnaques**).**

Les « Arnaque de transfert d'argent » sont matérialisés par des « spams » ou des échanges sur les réseaux sociaux et les sites de rencontres, ou tout autre moyen d'entrer en contact avec une future victime (un pigeon, appelé « Mugu »). Tout cela relève de techniques de manipulations psychologiques mettant en œuvre de l'Ingénierie sociale (l'art du tirer les vers du nez afin de nuire, arnaquer, convaincre...).

Les « Arnaque de transfert d'argent » sont massivement utilisées par l'Afrique noire (Nigeria et autres pays, avec extension vers les « diasporas » dans le monde) visant à faire croire à une grosse part d'une énorme cagnotte, si vous aidez à transférer (à sortir de son pays d'origine) cette cagnotte (compte bancaire, argent liquide, coffre plein de lingots d'or ou de sacs de diamants, titres de sociétés, etc. ...).

Le point de départ de la cagnotte est toujours un pays connaissant des troubles, ce qui permet d'ajouter un aspect romanesque, et généralement tragique, à l'histoire qui va être racontée au pigeon (« Mugu ») pour l'appâter.

Ces « Arnaque de transfert d'argent » arrivent de partout :

1. Les pays d'origine sont tous les pays d'Afrique de l'Ouest (zone CEDEAO à savoir Bénin, Burkina Faso, Cape Vert, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée Bissau, Libéria, Mali, Niger, Nigeria, Sénégal, Sierra Leone et Togo) auxquels il faut ajouter Irak, Iran, Afrique du Sud, République Centrafricaine, Éthiopie, Congo, etc. ...).
2. D'autres pays, non africains, sont lourdement impliqués. Avec les « diasporas », ces arnaqueurs**,** criminels et cybercriminels, appelés « brouteurs », se retrouvent dans tous les pays du monde et c'est hors d'Afrique qu'ils sont les plus virulents.
3. L'Asie et les pays de l'Est, dans leurs populations non noires, sont également des pépinières d'arnaqueurs aux « Arnaque de transfert d'argent ».
4. Dans une faible proportion, des ressortissants occidentaux de pays démocratiques pratiquent également cette forme d'escroqueries.

Des statistiques, faites en 2006, sont formelles : les attaques de type « Fraude 419 » proviennent, géographiquement, et dans cet ordre décroissant, des pays suivants : États-Unis d'Amérique. Royaume Unis (Angleterre). Nigéria

D'autres pays sont des sources importantes de ces escroqueries de type «Fraude 419» : Côte-d'Ivoire (14 milliards de Francs CFA escroqués aux Européens - 27 janvier 2012), Togo, Afrique du Sud, Pays-Bas, Espagne

L'aide que croit apporter le pigeon (« Mugu ») au transfert de la cagnotte va bien engendrer quelques « menus frais à payer d'avance à l'escroc » (frais de dossier, frais de gestion, frais d'avocat, frais d'huissier, nécessité de corrompre un employé de banque, frais de déplacement, taxes, n'importe quoi d'autre qui peut sembler crédible, etc. ...), mais qu'est-ce que des frais qui vont finir par s'élever à 10.000 ou 20.000 € lorsque l'on rêve (mais ce n'est qu'un rêve) encaisser plusieurs millions d'€.

L'escroc va multiplier les preuves et mises en confiance avec des noms, adresses, titres, sociétés, banques, cabinets d'expertise, notaire, diplomates, numéros de téléphones, adresses e-Mail, etc. ... qui vont, si besoin est, vous confirmer que tout est exact et que tout n'attend que votre paiement des avances pour débloquer l'histoire.

Tous ces « contacts », à qui il faut avancer leurs frais, émoluments et honoraires, ne sont, évidemment, que le même et unique escroc.
Comme la victime compte sur une part d'un butin, cette fraude porte également le nom de « Fraude à la commission escomptée » (et le pigeon (« Mugu ») n'est pas une victime mais un complice).
Enfin, si l'on regarde la typologie des fraudes, selon l'étude du GIABA, ces fraudes, parmi d'autres, participent au « financement du terrorisme ». Le pigeon (« Mugu ») peut être considéré comme un « complice du financement du terrorisme » et nul ne peut se prévaloir d'imbécilité ou de naïveté pour échapper aux peines encourues. Le crétinisme n'est pas une circonstance atténuante. Respect, droiture et discipline doivent être les ressorts de la vie, pas la cupidité et la tentation de participer à une opération abracadabrantesque digne d'Indiana Jones si elle était vraie, ou de blanchiment frauduleux, pour finir par se faire estamper d'une part et poursuivre par la justice d'autre part
Liens : http://assiste.com/Arnaque_de_transfert_d_argent.html

Arnaque et recrutement de Mules

Depuis plusieurs années, il est devenu courant de recevoir dans sa boite mail des messages proposant un travail à temps partiel, depuis son domicile, qui consiste simplement à transférer des fonds pour le compte d'une société étrangère. Ces messages sont des spams classiques, c'est à dire qui proposent une escroquerie qui a de faibles chances de marcher, mais ils sont envoyés à un si grand nombre de cibles (pour un coût marginal) que plusieurs victimes finiront bien par se présenter. Dans le cas qui nous préoccupe les victimes ne vont pas acheter des fausses Rolex ou du Viagra, ni pianoter leur mot de passe bancaire, mais se présenter pour un « travail » d'appoint.
Ce travail d'intermédiaire est bien sûr une escroquerie et la personne ainsi recrutée est couramment appelé "une mule" (par analogie aux passeurs recrutés pour transporter – parfois à leur insu – de la drogue ou tout autre matériel illicite). Le travail qui est proposé à la mule consiste le plus souvent à :

- recevoir de l'argent sur un compte que son recruteur lui demande de créer (par exemple un compte PayPal),
- convertir cet argent en cash et transférer cet argent liquide vers l'étranger en utilisant des services de mandat international tel que Western Union,
- garder au passage, en rétribution du service rendu, un petit pourcentage du montant d'argent acheminé.

Ce phénomène de mule est connu depuis plusieurs années. Le CLUSIF lui consacrait par exemple en début 2007 un exposé détaillé à l'occasion de son Panorama 2006 sur la cybercriminalité (voir la rubrique "pour plus d'information"). A cette époque les emails proposant ce type d'arnaque étaient encore peu fréquents et rédigés très majoritairement en anglais.
Exemple d'e-mail
Depuis les choses ont bien évolué. Voici par exemple ci-dessous un e-mail que nous avons reçu à la mi octobre. Si l'on écarte l'objet de l'e-mail (qui est un peu maladroit), il est étonnant de voir le soin qui a été apporté à sa rédaction :

- il ressemble vraiment à une offre d'emploi,
- le français utilisé est tout à fait correct,
- les termes employés (CDD, CDI, etc..) sont crédibles.

Cet e-mail, comme tous les spams, a été envoyé en masse en utilisant des moteurs d'émission anonymes ou compromis, sans possibilité de remonter à la source. Le seul lien que l'on a avec l'émetteur est l'adresse d'un compte Gmail. Dans d'autres échantillons que nous avons examinés pour ce spam l'adresse de l'émetteur et l'adresse Gmail étaient différentes, mais le corps était lui inchangé.
Le seul élément suspect à la lecture est la mention "effectuer des versements par WU/ MG" qui fait en fait référence à "Western Union" et "MoneyGram" : deux services permettant d'envoyer de l'argent liquide à l'étranger …

Que se passe-t-il ensuite pour la mule ?

Une fois la mule recrutée, de nombreux scénarios sont possibles, en fonction du type d'escroquerie. Voici les plus classiques :

- Le blanchiment d'argent : La mule reçoit sur son compte de l'argent. Elle doit alors retirer cet argent en liquide et l'envoyer par mandat international vers son commanditaire.
- L'extraction d'argent volé dans une banque : Le commanditaire demande à la mule d'ouvrir un compte dans une banque précise. Ce compte est ensuite alimenté à partir d'autres comptes de cette même banque qui ont été piratés (les transferts entre comptes d'une même banque sont généralement moins surveillés). La mule est chargée alors de retirer l'argent et de le transférer par mandat international vers son commanditaire.
- Les fausse ventes sur Internet : Le commanditaire demande à la mule de créer un compte PayPal, puis vend un objet sur internet en indiquant à l'acheteur qu'il doit envoyer l'argent sur le compte PayPal de la mule. En fait l'acheteur ne recevra jamais l'objet qu'il a acheté et la mule aura déjà transféré l'argent au commanditaire lorsque la supercherie sera découverte.

D'après les témoignages, la mule n'est pas utilisée très longtemps : soit parce qu'elle va être repérée par la banque du fait des transferts et retraits qu'elle fait, soit parce que les victimes des escroqueries vont se plaindre et que la mule sera alors immédiatement repérée.
A titre d'anecdote, il a été identifié récemment que le malware URLZone (un cheval de Troie bancaire), lorsqu'il détecte qu'il est analysé, change de comportement et transfère l'argent qu'il détourne vers des victimes innocentes qui passent ainsi auprès des enquêteurs pour des mules…

La réaction des entreprises impliquées

Les sociétés impliquées par ces escroqueries (les banques, Western Union, les sites de ventes entre particuliers, etc…) sont bien conscientes de ce phénomène et prennent des mesures pour les contrer. Il s'agit en tout premier lieu de communications vers leurs clients pour les informer et les mettre en garde. Western Union a également annoncé en octobre 2008 la création d'une "Alliance" (avec Microsoft, Yahoo et African Development Bank) pour lutter contre les arnaques sur Internet. Il existe aussi sans doute des mesures techniques plus discrètes (non publiques). On peut par exemple imaginer qu'une banque puisse surveiller les opérations de ses clients et déclencher des alarmes lors d'événements jugés comme significatifs. Une banque avait indiqué lors de l'intervention du CLUSIF avoir identifié en 2006 12 mules parmi ses clients.

Conclusion

L'activité de mule est bien sûr illégale (la mule est considérée comme complice des escrocs qui l'embauchent), dangereuse (la première conséquence est en général l'exclusion immédiate de la mule par la banque) et de courte durée.

Il est par contre préoccupant de voir se multiplier ce type d'offre dans des emails de plus en plus crédibles. On le voit sur l'exemple que nous avons pris ici, il est tout à fait possible de se faire appâter par ce type d'e-mail.
Agir avec prudence et bon sens devrait permettre de se rendre compte qu'il s'agit d'une escroquerie, mais une fois appâté, on peut aussi être tenté de croire que l'on a déniché une bonne affaire…
Liens : http://www.cert-ist.com/public/fr/SO_detail?code=fraudes_mules

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 leurs 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.
Liens : http://junon.univ-cezanne.fr/u3iredic/?p=13074

Le carding

Une étude-reportage par Lycroft Eugenia. Comme vous le savez il existe un véritable business d'escroquerie et de fraudes sur le net. Voici un article complet pouvant être qualifié d'étude-reportage sur le carding.

Qu'est ce que le carding ?

Il s'agit des fraudes à la carte bancaire sur le net (achat, vols,blanchissement de fonds…). Nous nous intéresserons au carding général ainsi qu'à ses dérivés (trafic de faux-papiers, blackmarket, etc…).
Le *"deepweb"*, représentant 70% de l'internet n'est pas référencé par les moteurs de recherche tels que Google ou Yahoo!.
Véritable nid de tous les excès, il s'agit d'un endroit favorable et apprécié pour les groupuscules de carders.
Quelques recherches et de "bons contacts" suffisent pour vite trouver quelques adresses et aboutir à de telles annonces :
Et non, vous ne rêvez pas, les cartes bancaires sont tellement abondantes qu'elles ne coûtent que 10$ soit environ 8 euros pour des modèles européens !
Ce n'est pas tout, nous avions ici affaire à de petits vendeurs isolés, sachez que certains se réunissent et mettent en place un véritable système de vente sécurisé. Rappelez-vous les deux grandes places de marchés dédiées à la vente de CVV de part le monde qui ont été démantelées cette année…
Ici un groupe de carder distribue gratuitement un stock de numéros de cartes bancaires valides afin de se faire promouvoir :
Certains n'hésitent pas non plus à recruter publiquement :
Les comptes PayPals, Liberty Reserve et Moneybookers (la plupart étant volés via des malwares) se vendent dans chaque BlackMarket et certains sites en sont mêmes spécialisés :
Une question se pose alors :

Comment ces carders obtiennent-ils ces numéros de cartes bancaires et ces comptes ?

A cette question il y a plusieurs réponses.

Le phishing est responsable d'une partie non négligeable des données en circulation. Pour rappel, il s'agit de mails ou de faux sites se faisant passer pour votre banque (ou tout autre organisme officiel) voir même, plus récemment via des appels téléphoniques.
Ceux-ci vous demandent de saisir vos identifiants et/ou vos coordonnées bancaires et c'est alors qu'ils les obtiennent.
Ensuite arrive le piratage de sites Web. Si vous avez fait des achats en ligne, le site web conserve certaines de vos données bancaires en cas de litige pendant un temps défini. Dès l'instant ou le site web est piraté et que sa base de données à été corrompue et dérobée par un pirate informatique après une intrusion sur le serveur, les données personnelles et bancaires pourront alors être remises à des carders.
Exemple de "dump" :
Plus actifs et plus efficace encore, voici les malwares. Les botnets comme SpyEyes ou Zeus sont équipés pour dérober les comptes bancaires et les numéros de cartes de crédit. Ils embarquent des "grabbers" qui sont capables d'intercepter et d'enregistrer les données des formulaires par exemple.
D'autres virus sont spécialisés dans le vol d'identifiants, ils sont appelés Stealers ou Password Stealers. C'est le moyen le plus rapide de récupérer des données privées sur des ordinateurs. Certains sont relativement accessible du fait qu'ils se vendent à bas prix par rapport aux botnets.

Le shiping-droping

A titre d'explications sur le shipping-droping voici l'explication donner par notre « carderX » :
« Le drop-shipping (et là on parle bien de carding, le drop-shipping ayant de multiples définitions suivant comment il est utilisé et par qui il est proposé). Le drop-shipping donc est souvent proposé par de gros carders qui ont un stock de produits récupérés par le biais de cartes bancaires volées plutôt conséquent, on parle là de 50 iPads, 30 Macbooks, 80 iPhones par exemple.
Le drop-shipper (celui qui propose le produit) recherche donc des personnes pour vendre ses produits sur des sites de vente légaux (Ebay, Priceminister, le Bon Coin…)
Le revendeur (celui qui a accepté le contrat de revente) va donc mettre des annonces, sur son compte personnel pour vendre les objets du carder/drop-shipper, et une fois la vente finalisée (l'objet acheté et payé), le revendeur va donner la part due au drop-shipper et celui-ci une fois l'argent reçu va expédier le colis à l'adresse de l'acheteur.
Le revendeur, dans tout ça, conserve tout l'argent qui est au-delà du montant demandé par le carder. Imaginons que le carder en demande 250 € et que la vente s'est finalisée à 564 €, le revendeur empoche donc les 314 € restant. »

Le cashout

Lorsqu'un carder a dérobé des identifiants de cartes bancaires, il lui faut blanchir l'argent. Ces procédés de blanchissements sont appelés cashout. Voici des exemple d'annonces sur des techniques de cashout :

La fraude aux faux-papiers

Des carders se spécialisent aussi dans la falsification de documents, sur une offre un carder nous propose d'accéder à son « catalogue », sécurisé par mot de passe et en suivant ses recommandations :
Vous remarquerez la présence des hologrammes ainsi que la qualité faisant qu'il est très difficile de pouvoir affirmer qu'il s'agit d'un faux. Même les pays de l'est, comme la Pologne, sont touchés.

Après avoir contacté un de ses carders pour en savoir plus sur ce business, celui-ci a montré ses templates éditables. Il s'agit de fichiers .psd, Photoshops éditables. Ainsi les carders peuvent y insérer des noms, photos et même signature.
Il y a aussi de nombreuses templates pour carte bancaires et surtout des papiers d'identité, des permis pour tout les états des États-Unis, quelques pays d'Europe de l'est et les plus grands pays Europe de l'ouest.
Les carders se renseignent aussi sur les méthodes employées par les polices afin de débusquer ces faux-papiers
Ainsi les carders peuvent bypass (dépasser, passer outre) les systèmes de vérifications mis en œuvre par les polices. Ces derniers n'hésitent pas à développer des logiciels pour parfaire leurs faux-papiers, tels que des générateurs de codes barres par exemple ou encore la modification des bandes magnétiques.

Autres fraudes relatives au carding

Voici des captures d'écran de la page d'acceuil d'un Blackmarket vous résumant le « reste » :

Conclusion

A la suite de cette étude nous pouvons conclure sur le fait qu'internet peut donner accès à des trafics pour n'importe qui tels que le trafic d'armes, de drogues, de faux-papiers, de données bancaires etc…
Le fait le plus effrayant est que n'importe qui peut avoir accès aux méthodes, à l'achat et à la vente de ce type de produits.

Liens : http://www.undernews.fr/undernews/reportage-etude-au-coeur-du-carding-et-deepweb.html

Carding
Arrestations à l'Île Maurice

Encore une affaire de carding d'envergure. Cette fois, c'est à l'Île Maurice que deux ressortissants moldaves ont été arrêtés par la Cybercrime Unit du Central Criminal Investigation Department (CCID).
Leur but était clair et simple : récupérer un max de cash à travers des différents distributeurs automatiques de billets de l'île pour blanchir l'argent du piratage. Edgar Patrasco, 24 ans, et Dorin Galearschi, 35 ans, 2 ressortissants moldaves, avaient débarqué à Maurice pour 10 jours, en possession d'une dizaine de cartes de crédit piratées au préjudice de clients chinois, portugais, néerlandais et britanniques.
Ils étaient donc chargé de blanchir l'argent du piratage de cartes bancaires effectué aux quatre coins du monde, et provenant de piratages en ligne (bases de données de sites marchands par exemple) ou physiques (via skimmers). En effet, les cybercriminels n'utilisent en règle générale jamais eux-même les données bancaires volées, afin de réduire les risques, et optent pour l'engagement de mules pour faire le sale boulot à leur place.
La brigade de police Mauricienne spécialisée, le Cybercrime Unit du Central Criminal Investigation Department (CCID) de l'Ile Maurice a été alerté par des banques qui se sont étonnées de la ponction en masse de comptes bancaires de ressortissants étrangers. Il faut dire aussi que des banques étrangères ont prévenues leur homologue Mauricien. les clients en question ne se trouvaient pas sur l'île paradisiaque. A partir de ces informations, ils ont donc pu facilement en déduire que ce sont des clones de CB piratées qui étaient utilisés.

Un "salaire" de 1 000 € pour un max de cash

Après une courte enquête, grandement facilitée par l'étendue limitée de l'île et la multitude de caméras de vidéosurveillance, les deux hommes ont été arrêtés alors qu'ils reprenaient l'avion. Durant 10 jours, ils ont visité les distributeurs de billets, avec des cartes bancaires clonées piratées, dans le but de récupérer un maximum de billets. Il s'avère que ces billets ont été envoyés à un commanditaire encore inconnu dans un pays de l'Est.

Les deux mules ont avoué avoir reçu 1 000 € pour réaliser le coup sur le terrain, ainsi qu'un pourcentage sur la somme qu'ils ont réussi à collecter. Leur voyage et tous leurs frais annexes étaient payés par le commanditaire, ils agissaient donc "tous frais payés". Interpol a ouvert une enquête d'envergure pour tenter d'identifier et d'appréhender la tête pensante de cette affaire.

A noter que ce n'est pas la première fois que ce type de pirates sont arrêtés sur l'île Maurice, c'est un endroit prisé pour ce genre d'opérations semble t-il… Les deux mules étaient des maçons d'après les informations presses.

Liens : http://www.undernews.fr/banque-cartes-bancaires/carding-arrestations-a-lile-maurice.html

Techniques de pirates
Comment les cybercriminels blanchissent l'argent du carding (Cash Out) ?

Blanchir l'argent émanant de la cybercriminalité et plus particulièrement du carding est une affaire hautement risquée. Le processus est lourd, long, coûteux et les intermédiaires ne sont pas fiables. Comment procède les pirates aujourd'hui pour réaliser un Cash Out (Ca$h Out) ?

Les opérations cybercriminelles à grande échelle peuvent permettre de passer outre la plupart des pièges et aux opérations illégales de devenir beaucoup plus rentables et sûres, surtout lorsque les cybercriminels réussissent à dissimuler leurs activités frauduleuses au sein d'entreprises légitimes en cours d'exploitation aux États-Unis. Ils sont de plus en plus nombreux à faire cela.

Un nouveau type de service underground a vu le jour et est commercialisé par et pour des cybercriminels. La réexpédition (par exemple via des mules, ndlr) de marchandise achetée par le biais de cartes bancaires volées (carding) a toujours été la façon la plus courante et populaire pour les pirates informatiques et carders se situant à l'étranger d'encaisser l'argent de leurs actes cybercriminels commis sur le territoire américain ou européen.

Les cyberescrocs s'appuient très souvent sur ce genre de service de réexpédition à l'international pour le déplacement et l'acheminement de matériel électronique et d'autres biens qui sont achetés avec des cartes de crédit piratées, puis expédiés à l'étranger pour être vendus pour de l'argent "cash". De nombreux fraudeurs utilisent des carte bancaires volés pour payer des étiquettes d'expédition de l'US Postal Service et de FedEx (aussi appelées les "étiquettes noires") mais les principaux fournisseurs d'expédition semblent être à même de mieux en mieux à bloquer et intercepter ce type de paquet. La preuve en est, on ne compte plus les plaintes de cybercriminels sur les forums underground spécialisés du Deep Web…

En conséquence, les cybercriminels se tournent de plus en plus vers un service plus fiable : les marques blanches d'expédition qui sont payées avec des comptes bancaires

offshores dédiés exclusivement à la cybercriminalité et financés par l'intermédiaire de sociétés bidon, mais apparemment légitimes aux États-Unis.

Retirer de l'argent cash, le Graal pour tout pirate informatique

Dans le cas d'une violation d'une boutique en ligne qui expose des données bancaires (numéro de carte, date d'expiration et CVV), ces dernières sont généralement utilisées pour acheter de l'équipement électronique à prix élevé dans boutiques en ligne connues pour être "cardable", c'est à dire non regardant sur l'identité de l'acheteur (pas de copie numérique de pièce d'identité demandée par exemple) et proposant l'expédition de la marchandise à une adresse différente de l'adresse de facturation.

Dans le cas des violations sur les moyens de paiements physiques où les attaquants utilisent un logiciel malveillant afin de compromettre les opérations bancaires effectuées en caisse et de recueillir des données qui peuvent être utilisés pour fabriquer de nouvelles cartes, les fraudeurs emploient des équipes annexes spécialisées et équipées techniquement qui utilisent les données dérobées pour créer des cartes contrefaites pour ensuite acheter des marchandises à prix élevé à des grandes surfaces ou voyager.

Dans tous les cas envisageable de fraude bancaire, l'un des moyens les plus lucratifs pour les fraudeurs se situant à l'étranger pour encaisser l'argent des cartes de crédit piratées, est d'avoir des produits brevetés expédiés à l'étranger, où l'électronique et autres articles de luxe se vendent généralement un prix beaucoup plus élevé que dans les États-Unis ou en Europe (les derniers iPads et iPhones, par exemple).

L'étape la plus difficile dans tout ce processus est de faire sortir les marchandises des États-Unis ou d'Europe, car un pourcentage élevé de détaillants refusent tout simplement de les transporter vers des pays tels que la Russie et l'Ukraine en raison du taux élevé de fraude dans ces régions.

Traditionnellement, les fraudeurs réussissent à contourner ce type de restriction en se tournant vers des services qui s'appuient sur les « mules » pour procéder à la réexpédition des marchandises. Ces précieux intermédiaires sont recrutés localement pour réexpédier les paquets après avoir reçu la marchandise à leur domicile. Ces mules dédiées à la réexpédition reçoivent plusieurs colis contenant des produits électroniques qui ont été achetés avec des cartes bancaires volées et également des étiquettes prépayées et pré-adressée d'expédition. Ces personnes mal informées que sont les mules sont responsables de s'assurer que les marchandises sont réexpédiées rapidement et avec précision.

Malgré cela, l'année dernière, ce mode de fonctionnement a toutefois rencontré des problèmes, de plus en plus de cybercriminels utilisateurs de services réexpédition ayant rapportés qu'une grande part de leurs paquets ont été interceptés ou annulés. Apparemment, les compagnies maritimes sont de mieux en mieux équipées pour procéder à la détection des étiquettes d'expédition qui sont payées illégalement.

Des services innovants dédiés à la cybercriminalité

Face à ces nouvelles difficultés engendrant de lourds coûts de fonctionnement, la cybercriminalité internationale s'est organisée et a créé des services undergrounds 100% dédiés à leurs activités illégales, permettant de transporter la marchandise à bon port avec un important taux de succès (la livraison est garantie ou remboursée, ndlr).

Aucun nom ne sera cité dans cet article à but purement informatif. Cependant, il faut s'avoir que ces services sont poussés par la criminalité organisée mondiale et difficiles à stopper. De plus, les tarifs sont entre 15 et 20% moins chers que les transporteurs légitimes, permettant des marges maximales aux utilisateurs et ainsi, amplifier leurs profits.

Là encore, la majorité de ces service en marque blanche se trouvent en Russie.

Une façon de récupérer et d'augmenter les gains blanchis

Retirer l'argent volé à un distributeur automatique de billets à l'autre bout du monde via une carte de débit clonée est certes efficace mais il ne donne pas la possibilité au cybercriminel de réinvestir cet argent dans l'achat de biens ou dans toute autre façon de le faire fructifier.

Les réseaux criminels sont reliés pour un maximum d'efficacité. Grâce à ces nouveaux réseaux undergrounds très discret et délocalisés, une autre forme de fraude est née, dont le but est d'extraire le maximum de valeur des activités cybercriminelles.

Liens : https://www.undernews.fr/fiches-pirates/techniques-de-pirates-comment-les-cybercriminels-blanchissent-largent-carding-cashout

Cybercriminalité : Perfect Money s'impose définitivement comme remplaçant de Liberty Reserve

Il y a tellement de façons de transférer de l'argent de manière anonyme sur Internet que le ministère américain de la Justice a déclaré la guerre aux devises virtuelles largement utilisées par les cybercriminels.

Juste après l'opération massive dans 17 pays visant la fermeture de *Liberty Reserve*, plateforme de paiement anonyme ayant permis le blanchiment de 6 milliards de dollars, les cybercriminels ont adoptés une autre devise en ligne appelé *Perfect Money*.

Perfect Money, une autre monnaie numérique privée et indépendante qui a vu le jour afin de répondre à la demande des criminels et des pirates, leur permettant d'acheter et de vendre des malwares anonymement mais aussi très utile aux personnes pratiquant le carding, le business juteux des cartes de crédit volées sur le Black Market au fin fond du Deep Web.

Les fraudeurs ont rapidement migrer vers *Perfect Money*, qui permet aux utilisateurs de transférer facilement de l'argent de manière anonyme en achetant et en échangeant de la monnaie virtuelle contre des dollars, des euros ou encore de l'or.

Ces monnaies virtuelles sont souvent rapprochées de *Bitcoin*, car ce dernier a également été utilisé par les cybercriminels. Nombreux étaient les personnes qui pensaient que Bitcoin serait le remplacement idéal à Liberty Reserve. Bitcoin est une crypto-monnaie, basée sur un modèle de chiffrement open-source, tenant des registres de toutes les transactions de manière assez transparente, mais Bitcoin est également une monnaie anonyme, qui garde la véritable identité d'une personne séparée de son adresse numérique visible.

Depuis que le gouvernement américain a montré un intérêt dans la régulation de Bitcoin et des échanges qui lui permettent de fonctionner, il est devenu une proposition moins attrayante pour les criminels. Du coup, Perfect Money à prit la tête des services utilisés par les pirates informatiques. UnderNews avait par ailleurs réagit très rapidement dans ce sens lors de la fermeture de l'empire Liberty Reserve et ne semble pas s'être trompé…

Liens : https://www.undernews.fr/banque-cartes-bancaires/cybercriminalite-perfect-money-simpose-definitivement-comme-remplacant-de-liberty-reserve.html

Même les geeks se méfient de l'e-monnaie

Jusqu'à l'éclatement de l'affaire Liberty Reserve, cette société américaine de transferts de fonds sur Internet, aujourd'hui soupçonnée de blanchiment d'argent à hauteur de 6 milliards de dollars (4,6 milliards d'euros), peu de gens connaissaient l'existence des monnaies électroniques, ni leur mode de fonctionnement.

En quelques jours, on a découvert la dimension de ces nouveaux instruments monétaires. Dans la foulée ont émergé les noms des champions de ces monnaies virtuelles : Mt. Gox, la "Bourse d'échange" numéro un du circuit, et d'autres aux noms aussi "numériques" (Bitomat, Bitfloor…) que leur monnaie : Bitcoin, Litecoin, SolidCoin, GeistGeld, Ripple, BBQCoin… Ces sociétés ne sont pas qu'américaines : on en trouve à Moscou (WebMoney), au Panama (Perfect Money)… Au Proche-Orient, la plus connue s'appelle cashU. En 2011, quand elle a senti le souffle de la justice dans son dos, Liberty Reserve s'était délocalisée au Costa Rica.

Pour l'anecdote, la première tentative d'acheter des biens sur Internet en "monnaie virtuelle" remonte à 1999, lorsqu'une devise du nom de Flooz fit brièvement son apparition. La prononciation à l'anglaise ("flouze") avait un petit côté provocant et sans équivoque.

Mais si chaque plate-forme de transfert d'argent dispose aujourd'hui de sa propre "monnaie virtuelle", la plus célèbre se nomme Bitcoin, première du genre à s'être imposée. C'était il y a quatre ans seulement. Il n'est vraisemblablement pas anodin que le nom de son ou de ses inventeurs soit lui-même resté jusqu'à ce jour inconnu ! Sotashi Nakamoto, auteur du premier post sur le Web expliquant le fonctionnement de Bitcoin, le 24 mai 2009, s'est révélé n'être qu'un pseudonyme.

Le *New Yorker* a cherché à découvrir son identité, sans succès. Autant prévenir le lecteur peu averti de la mathématique financière, la lecture du texte (*Bitcoin : A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf) est légèrement absconse. Bitcoin a ensuite donné naissance à de multiples autres monnaies qui, toutes, fonctionnent sur un principe identique.

Jetons de casino

Ce ne sont pas de "fausses monnaies" : leur détention n'est pas prohibée, on peut les acheter et les vendre, etc. Leur valeur peut même fluctuer en fonction de l'offre et de la demande de leurs "consommateurs".

Ainsi, le Bitcoin s'échangeait entre 2 et 11 euros en 2011-2012, puis a connu une flambée inouïe, grimpant à 110 euros entre février et début avril 2013, puis à 200 euros en une semaine, avant de s'effondrer à 66 euros. Il a ensuite repris son cours haussier et valait 91 euros lundi 3 juin.

Pour sûr, on sent dans ces variations un fumet spéculatif prononcé. Surtout, ces monnaies n'ont de valeur qu'en circuit fermé, un peu comme des jetons de casino. Elles sont "virtuelles", car sans autre valeur d'usage, comme les jetons, que d'être échangeables contre des devises réelles.

Sont-elles obligatoirement source de trafic ? Pas sûr. Aux Etats-Unis, les sociétés de transfert, pour éviter d'être instrumentalisées "à l'insu de leur plein gré" par des criminels, se disent favorables à une réglementation si elle n'empiète pas sur leur fonctionnement. Ainsi, contrairement au "LR", la monnaie de Liberty Reserve, la traçabilité de chaque Bitcoin est supposée acquise.

Son principal promoteur, la société Mt. Gox, assure exiger une preuve tangible d'identité et de résidence du client avant d'autoriser une transaction et tenir un registre public de tous ses transferts de fonds. Le problème est que ce n'est pas le cas des

autres, et que Mt.Gox est lui-même soupçonné… d'avoir développé des filiales pour se soustraire à sa propre règle.
C'est vraisemblablement parce qu'elles avaient suspecté la propension des promoteurs de ces monnaies et de beaucoup de leurs utilisateurs à y avoir recours pour dissimuler des transactions douteuses que des organisations plutôt favorables au numérique ont progressivement tourné le dos aux monnaies virtuelles.
Ainsi de WikiLeaks, qui n'accepte plus les dons en monnaie virtuelle. Ou de Facebook. En 2009, le réseau social a offert à ses membres d'utiliser des "Facebook Credits", mais coupa rapidement court à cette pratique
Liens : http://www.lemonde.fr/economie/article/2013/06/04/meme-les-geeks-se-mefient-de-l-e-monnaie_3423395_3234.html

Banque centrale du Bangladesh : Un cyber-casse de 80 millions de dollars

Il s'agit de l'un des plus grosses affaires cybercriminelles portant sur des faux ordres de virements bancaires. Une erreur de frappe lors d'un virement bancaire frauduleux a permis d'empêcher le vol de près d'un milliard de dollars et de mettre en évidence de précédentes fraudes s'élevant à 80 millions de dollars.
Les responsables de la banque centrale du Bangladesh affirment que les pirates informatiques ont réussi à voler plus de 80 millions de dollars avant d'être repérés. L'identité des cybercriminels impliqués dans cette affaire n'est toujours pas connue. Le piratage bancaire réalisé est de haut vol, puisque les pirates sont parvenus à s'introduire au sein du système de transfert et de paiement de la banque. Ils ont ensuite envoyé près de trois douzaines de demandes de virement à la Federal Reserve Bank de New York, vers des entités en Philippines et au Sri Lanka.
Au bout de 4 requêtes exécutées avec succès, les voleurs ont réussi à détourner et dérober un total de 81 millions vers les Philippines. Mais voila, la cinquième requête de virement d'un montant de 20 millions de dollars était erronée et mal orthographiée, ce qui a attiré l'attention de l'organisme bancaire en charge de réaliser le transfert, la Deutch. En effet en lieu et place de *Shakila Foundation,* les pirates ont écrit *Shakila Fandation*… La Deutch a alors contacté les autorités de la banque centrale du Bangladesh pour demander des clarifications et la transaction a été annulée.
De plus, le nombre inhabituel de demandes de transfert vers des entités privées a alerté les autorités de la Federal Reserver Bank de New York qui ont à leur tour contacté la banque centrale du Bangladesh pour le leur signaler. En somme, c'est près de 870 millions de dollars qui ont été sauvésde justesse ! Notons que les fraudes bancaires de ce genre ont fait beaucoup de dégâts dans le milieu bancaire au cours de ces deux dernières années, comme le dénonce la société de sécurité russe Kapersky, qui avance que des bandes de cybercriminels internationaux ont réussi à voler plus d'un milliard de dollars dans une centaine d'institutions financières à travers le monde.
La banque centrale du Bangladesh a déclaré avoir récupéré une partie de l'argent qui a été volé et travaille en collaboration avec les autorités philippines de lutte contre le blanchiment d'argent pour essayer de récupérer le reste. Un fonctionnaire de la banque affirme que les autorités font allusion à la transaction qui était destinée à l'ONG au Sri Lanka.
Ces attaques contre les banques démontrent que la menace de cybercriminelle pèse sur le monde et touche même les réseaux informatiques les plus sécurisés au monde.

Cela pose également la question de savoir comment font ces pirates pour trouver des failles dans de tels systèmes. Plus d'un mois après l'incident, la banque centrale du Bangladesh est toujours sur la trace des malfrats sans avoir réussi pour le moment à retracer l'argent volé. La banque travaille également à renforcer son système de sécurité en identifiant les failles qui ont permis aux pirates de s'y infiltrer. D'après des experts en sécurité interrogés sur la question, les auteurs du vol avaient une connaissance approfondie du fonctionnement interne de la banque. Quant aux autorités, ils blâment la banque fédérale américaine de n'avoir pas arrêté les opérations plus tôt, le ministre des Finances du pays envisage même une poursuite contre la banque fédérale pour récupérer l'argent. 13 mars 2016

Liens : https://www.undernews.fr/banque-cartes-bancaires/banque-centrale-du-bangladesh-un-cyber-casse-de-80-millions-de-dollars.html

Les pratiques de blanchiment d'argent via les sites de trading en ligne

Le trading en ligne est devenu de nos jours un phénomène qui prend de plus en plus d'ampleur. En effet, l'investissement en bourse a connu un essor considérable depuis sa dématérialisation. De ce fait, tout le monde peut investir sur les marchés financiers avec internet ou même un téléphone mobile et autres tablettes. Cependant**,** cette dématérialisation a favorisé une pratique illégale : le blanchiment d'argent via les sites de trading en ligne. L'essor de cette pratique est du à de nombreux facteurs. Dans ce billet, je vais vous donner un aperçu de ces pratiques qui existent dans le trading en ligne.

L'implantation des brokers dans les paradis fiscaux

Cela est le plus grand facteur qui favorise le blanchiment d'argent via le trading en ligne. En effet, la plupart des courtiers se sont implantés dans des paradis fiscaux afin de bénéficier d'impositions fiscales peu élevées et ainsi faire de plus grands profits. Cependant, en se basant sur ces paradis fiscaux, les brokers bénéficient aussi de certains avantages pouvant leur permettre de ne pas dévoiler les informations financières à l'institution fiscale. En plus de cela, la facilité d'accès via internet, la dématérialisation du contact entre le client et le courtier et la rapidité des opérations électroniques font que le blanchiment d'argent est un fléau qui sévit fortement sur les marchés financiers. Ces derniers éléments cités rendent difficile l'identification de l'investisseur et le suivi des comptes et des transactions par les institutions financières. De plus, puisque qu'il n'y a plus d'intervention humaine susceptible de contribuer à la détection d'opérations suspectes ou inhabituelles, le blanchiment d'argent se fait de plus en plus via le trading en ligne et est devenu un casse-tête pour les autorités fiscales qui ont du mal à détecteur ceux qui le font.

Comment se passe le blanchiment d'argent via le trading en ligne ?

La diversité du nombre d'instruments financiers disponibles avec l'investissement en ligne a fait que le blanchiment d'argent a pris une considérable ampleur. En effet, les marchés boursiers ainsi que ceux des produits dérivés permettent aux blanchisseurs de fonds de mettre en place des stratagèmes de plus en plus sophistiqués. Par exemple, un courtier se voit donner la possibilité de laver de l'argent à travers des transactions parfaitement légales et cela sans avoir recours à des manipulations de données. La technique la plus courante est celle qui consiste à vendre et à acheter deux contrats futurs. Ainsi, l'investisseur gagnera avec l'un et perdra avec l'autre quelque soit l'évolution du cours du sous-jacent. En attribuant les gains à un compte et en

assignant les pertes à un autre dans lequel l'argent sale a été déposé, le courtier blanchit ainsi de l'argent sans enfreindre la loi. Ce procédé est possible avec plusieurs produits financiers dérivés tels que la vente de Put et l'achat de call simultanés ou toute autre combinaison qui permet d'obtenir un gain et une perte. Ces moyens semblent être très efficaces car la volatilité des marchés peut rendre ces gains tout à fait normaux rendant ainsi la détection difficile. Aussi, pour ne pas éveiller de soupçons avec leur compte qui gagne, ces blanchisseurs attribuent les gains à un à un troisième compte et les pertes au compte détenant l'argent blanchi ce qui fait que ce dernier ne sera pas toujours « gagnant » et n'éveillerait ainsi aucune suspicion.

Les dispositions prises par les autorités de régulations pour contrecarrer ce phénomène.

Pour remédier à ces pratiques, les autorités de régulations telles que l'AMF ont pris un certain nombre de dispositions visant à sauvegarder les investissements des particuliers et à les protéger contre certaines arnaques. De ce fait, l'AMF procède à une vérification régulière des brokers autorisés à exercer sur le territoire français. Ces courtiers sont ceux qui disposent d'une licence de régulation de la part de cette autorité ce qui fait montre de leur fiabilité et de leur sérieux. En délivrant cette licence de régulation, l'AMF s'assure d'abord de la régularité des transactions financières qui se font à travers les interfaces de ces brokers mais aussi de la fiabilité du courtier. Ainsi, en s'impliquant sur le trading en ligne, l'autorité des marchés financiers s'engage dans une lutte contre le blanchiment d'argent et les arnaques financières. Trader Bankster – Jordan Belfort *par CyberPeople*

Conclusion

Le blanchiment d'argent via l'investissement en ligne est bien présent mais, avec l'effort des autorités, cette pratique pourrait bien prendre du plomb dans les ailes. En effet, l'AMF, en publiant régulièrement sa liste noire de brokers en ligne, montre au trader les courtiers qui sont susceptibles d'avoir recours à ces pratiques. De ce fait, pour un investissement sûr et fiable, je vous conseille de choisir un courtier détenant une licence de la part de l'AMF

Liens : http://boursebinaire.fr/les-pratiques-blanchiment-d-argent-via-les-sites-trading-en-ligne.html

Pourquoi les sites de trading sont-ils tous basés à chypre ?

Je n'ai de cesse de vous le répéter, Lorsque vous choisissez un broker, assurez-vous de ne pas souscrire un compte chez un courtier basé à l'étranger. L'AMF conseille de se méfier des sites proposant aux investisseurs français des services de trading en dehors de toute autorisation, cette information est disponible sur la liste noire des brokers sans autorisation publiée chaque mois sur le site web de l'Autorité des Marchés Financiers. Vous ne le savez sans doute pas, mais une grande quantité de sociétés de courtage de devises (Forex) et/ou de CFD ou encore d'options binaires sont basées à Chypre. Cette concentration s'explique par la réglementation et la fiscalité particulièrement favorable qui a permis à l'île disputée par la Grèce et la Turquie d'attirer un grand nombre d'acteur sur le marché du trading en ligne, en pleine expansion depuis une décennie. Chypre à réintégré il y a peu les listes de surveillance de l'OCDE, elle l'avait quitté au début des années 2000, mais la perspective d'intégrer l'Union européenne l'a obligée à revoir sa stratégie de lutte contre les pratiques de blanchiment d'argent et la délinquance en col blanc. Cette

volonté politique a conduit à la naissance en 2003 de son autorité de marché, la CySEC, la Cyprus Securities and Exchange Commission. Depuis 2009 le rôle de cette autorité de régulation des marchés est aussi de lutter contre les sites irréguliers œuvrant sans licence d'investissement suite à sa réintégration sur la liste blanche de l'OCDE en 2009. Toutefois la fiscalité de la République de Chypre avec un taux d'imposition sur les sociétés de 10% seulement explique pourquoi les sites de trading sont-ils tous basés à chypre.

Pour l'AMF avec un broker non régulé « Le risque est au bout du clic ».

Les publicités aussi agressives que mensongère qui envahissent le web telles que « Gagnez 3 000 EUR par jour». « Devenez tradeur ». « La fortune en un mois ». Cachent souvent la présence d'escrocs en col blanc. Le grand banditisme est aussi présent sur les activités financières, comme vous avez pu vous en rendre compte si vous avez vu le JT de 13 heures de France 2, si tel n'est pas le cas, vous pouvez revoir le sujet consacré aux arnaques du trading en ligne sur notre site Bourse binaire. Ce phénomène en pleine accélération a poussé le Gendarme de la Bourse en France à siffler la fin de la récréation et à sévir, bien que les moyens de lutte passent avant tout par la prévention. L'AMF a donc lancé une campagne de communication afin de prévenir les particuliers un peu trop crédules, dont le slogan est « Le risque est au bout du clic ». Une campagne de prévention qui intervient après son étude menée durant 4 ans entre 2009 et 2012. Près de 13500 traders particuliers se sont vus perdre 175 millions d'Euros, soit une perte moyenne de 10 000 euros par personne, autre chiffre édifiant 9 personne sur 10 s'est retrouvée ruinée. Le schéma classique de la perte initiale que l'on souhaite effacer en réinvestissant pousse les plus désespérés à une perte moyenne dépassant les 25 000 euros.

Pourquoi vous devez absolument trader avec un broker régulé

La régulation vous met à l'abri de nombreuses déconvenues, sans pour autant être une assurance tout risque. En effet la justice française avec toute sa bonne volonté peut parfois se heurter à des blocages administratifs. Et ce d'autant plus si vous avez fait le choix d'ouvrir un compte avec un broker même régulé mais qui se trouve en réalité dans un paradis fiscal permettant l'anonymat des sociétés. Dans ce cas vous pouvez vous préparer à un véritable parcours du combattant car il ne vous restera comme maigre espoir de porter plainte auprès des autorités locales, de trouver un avocat sur place, et espérer des institutions judiciaires du paradis fiscal qu'elles veuillent bien enquêter sur des entreprises écran derrière lesquelles se cache peut-être la Mafia.

Conclusion

Bien que le tableau dépeint puisse paraitre très sombre, il ne faut pas pour autant céder à la panique, mais garder les pieds sur terre, croire que l'on peut s'enrichir en quelques minutes sans efforts relève de l'utopie si ce n'est de la psychiatrie. Le trading n'est pas une activité facile et à la portée de tous, tout comme les brokers ne sont pas tous des arnaqueurs. Inlassablement je vous conseille de ne trader qu'avec un courtier régulé et qui ne figure pas sur la liste noire de l'AMF. Vous devez aussi une fois ces précautions prises, prendre le soin de lire en détail les CGU du site, des clauses telles que l'impossibilité de retirer son argent sans avoir une pénalité de 30% ou bien l'obligation de trader 26 jours dans le mois alors qu'un mois boursier compte au mieux 22 jours, doivent vous mettre la puce à l'oreille.

Liens : http://boursebinaire.fr/les-sites-trading-bases-chypre.html

Coup dur pour la finance participative

Une plateforme de prêts participatifs entre particuliers et entreprises frauduleuses ruine 900 000 épargnants en escroquant 7 milliards d'euros, ça se passe en Chine, mais ne croyez pas que cela n'arrive qu'aux autres. La faillite de la start-up de crowdfunding Ezubao est un avertissement des risques pesant sur ce segment de la finance grise (shadow banking). Explications de Deontofi.com

Se passer des banques qui ne font pas leur travail de financement de l'économie, en mettant directement en relation les épargnants et les emprunteurs, ou les entreprises en manque de capitaux. C'est la belle idée du crowdfunding, le financement participatif, ou financement par la foule, rendue possible par l'explosion des réseaux sociaux et l'émergence de l'internet collaboratif. Mieux qu'un financement bancaire, le financement participatif rendrait tout le monde heureux : les emprunteurs ayant accès à des crédits moins coûteux et surtout moins contraignants en terme de démarches, justificatifs, sélection et garanties de remboursement; les particuliers obtenant une meilleure rentabilité de leur épargne en la mettant au service de l'économie réelle, le tout simplement grâce à ces plateformes dont la petite commission est bien inférieure à la marge d'intérêt et aux frais dont se gavent les banques.

Plus besoin de banques ! L'idée est séduisante et bénéficie d'un capital de sympathie indiscutable vis-à-vis du public enthousiaste. Qu'on en juge : 1,5 million de Français auraient prêté 85,2 millions d'euros, investi 24,3 millions d'euros ou soutenu un projet avec 23,7 millions d'euros de dons (dont 20 millions « avec récompense » c'est-à-dire contre un produit ou service), dans le cadre d'opérations de crowdfunding au premier semestre 2015, soit deux fois plus qu'au premier semestre 2014, selon le dernier baromètre de l'association Financement Participatif France.

Il faut dire que le financement participatif, qui était longtemps hors-la-loi au regard des réglementations financières, a bénéficié d'une réglementation allégée légalisant et facilitant son développement, comme Deontofi.com l'avait évoqué dès 2014.

« En France, l'ordonnance du 30 Mai 2014 et le décret du 16 septembre 2014 relatifs au financement participatif ont régulé le secteur du prêt et de l'investissement participatifs en instaurant deux statuts spécifiques (intermédiaire en financement participatif pour le prêt et conseiller en investissements participatifs pour l'investissement) qui permettent aux plates-formes respectant la législation de bénéficier d'un label. Le gouvernement a ainsi à plusieurs reprises affiché sa volonté de faire de la France le pays leader du crowdfunding, qui rencontre en effet particulièrement de succès dans l'Hexagone », explique ainsi le ministère de l'écologie, du développement durable et de l'énergie sur son site Internet.

Difficile dans ces conditions de mettre en garde les épargnants contre les risques d'arnaques au crowdfunding, sans passer pour un ringard réac défendant le pré-carré des banques. Les lecteurs de Deontofi.com savent bien que ce site d'information n'est pas complaisant avec les lobbies bancaires.

Le problème est que le crowdfunding, sous son visage sympathique, est aussi un boulevard facilitant l'accès de nombreux escrocs à l'épargne publique. Il suffit de s'inventer un projet écolo, ou techno, ou d'entrepreneuriat social dans la tendance du moment, ou au contraire miser sur l'appât du gain avec un mirage immobilier ou n'importe quel château en Espagne, pour convaincre les épargnants confiants de donner leurs économies en échange d'une promesse de rendement élevé pour couronner le tout.

La recette est d'une banalité aussi affligeante qu'efficace, car c'est bien la même qui a permis à la plateforme de financement participatif chinoise Ezubao de collecter 7 milliards d'euros auprès de 900 000 épargnants, en leur promettant des taux d'intérêt entre 9% et 14,5% sur des prêts à d'improbables entreprises fictives.
Près d'un million d'épargnants ne reverront jamais leur argent
L'arrestation du fondateur d'Ezubao, le jeune Ding Ning (34 ans) et d'une vingtaine de ses employés, à Pékin dimanche 29 janvier 2016, a révélé au monde que tout était faux. La start-up était devenue leader chinois du financement participatif en dix-huit mois, à grand renfort de publicités, en engloutissant l'épargne de ses derniers pigeons pour entretenir l'illusion de rentabilité promise aux pigeons précédents dont le capital ne serait jamais remboursable. Quand cette spirale n'a plus trouvé assez de pigeons pour s'entretenir, elle s'est écroulée.
C'est ce qu'on appelle un système d'épargne pyramidal, ou encore système de Ponzi, redevenu célèbre au XXIème Siècle grâce aux prouesses de Bernard Madoff, incontestable recordman de l'escroquerie pyramidale.
Encore une fois, Deontofi.com n'est évidemment pas opposé aux vertus du crowdfunding. D'ailleurs, qui peut l'être ? Mais notre devoir est de mettre en garde les épargnants sur les risques de déceptions liées aux espoirs qu'ils fondent sur le financement participatif, car beaucoup ne reverront jamais leur argent ni même les intérêts ou formidables gains promis.
Liens : https://deontofi.com/coup-dur-pour-la-finance-participative-900-000-epargnants-floues/

Les sites de trading Forex interdits en France, et ceux qui devraient l'être !

Les arnaques au Forex prospèrent ! Les nombreux témoignages de lecteurs sur les forums de Deontofi en témoignent. Entre les escrocs usurpant l'identité de soi-disant autorités boursières pour essorer une seconde fois leurs proies, et la nouvelle offensive de sites autorisés mais infréquentables, Deontofi.com publie la mise à jour des sites interdits et renouvelle son alerte : ne donnez jamais votre téléphone ou numéro de carte à un site de trading !
Plus 23% ! Ce n'est pas le gain promis par les escrocs du Forex, mais l'augmentation de leur nombre estimé. La liste des dangereux sites de trading interdits en France, que le gendarme boursier vient de mettre à jour, compte 188 sites à proscrire impérativement ! Ils n'ont pas le droit de démarcher les clients français, mais le droit est le cadet de leur souci puisqu'ils sont officiellement considérés comme hors d'atteinte des autorités financières françaises : elles n'ont pas le pouvoir de les arrêter, encore moins d'indemniser leurs victimes**.**
Comparée à la liste de 153 sites interdits, publiée par l'Autorité des marchés financiers (AMF), il y a moins de trois mois, la recrudescence annoncée de ces supports d'arnaques est donc de 23%**.** Et sans doute d'une plus grande ampleur. Car de nombreux opérateurs ne figurant pas sur cette liste de sites de trading interdits, dont les publicités s'étalent sur le web, sont aussi infréquentables.
D'abord, tous les sites interdits ne sont pas dans cette liste, et pour cause : il s'en crée tous les jours. Il suffit d'enregistrer un nom de domaine sur Internet, parasitant vaguement une marque financière ou une autorité familière aux épargnants (lire liste ci-dessous), pour en piéger quelques uns dans ces filets, avec l'aide de mercenaires du

démarchage téléphonique**,** experts en harcèlement pour extorquer leur numéro de carte bancaire aux épargnants naïfs**.**
Comme l'écrit un lecteur de Deontofi : « Pourquoi l'AMF ne publie pas une liste des sites autorisés, au lieu de publier une liste des sites non autorisés qui ne sert à rien, à moins que tout site qui n'est pas sur la liste soit autorisé, ce qui n'a pas l'air d'être le cas **»**… Pas si simple, car il y a aussi une quantité astronomique de sites absolument infréquentables qui ne sont pas interdits en France**,** même s'ils n'ont obtenu aucun agrément direct du gendarme boursier français. C'est la magie du « passeport européen » !
Pour dévaliser des épargnants français, rien de tel qu'une image de sérieux avec des références rassurantes, pour mettre en confiance les proies. Certains sites revendiquent ainsi le label de **«** 1er courtier régulé en France et en Europe **»**, avec un éventail impressionnant d'agréments « AMF, Banque de France, et MiFid (Markets in Financial instruments directive, ou directive sur les marchés d'instruments financiers - MIF- en français) ».
Que valent ces agréments pour les épargnants ? Du vent**.** Car ces opérateurs sont installés dans des pays à la réputation bien méritée de Far West financiers, même quand ils sont à l'Est, comme Chypre, ou au Sud, comme Gibraltar. Vous croyez que les institutions financières agréés par la CySEC (la « securities and exchange commission » de Chypre, un oxymore !) se préoccupent de la protection des épargnants ou des obligations de **l**utte anti-blanchiment ? Pas nous. Or, cet agrément de la CySEC est un sésame pour l'Europe, car il est légalement considéré comme équivalent à un agrément par l'AMF ! Le passeport européen est certainement une bonne chose pour favoriser la concurrence bénéfique aux consommateurs. Malheureusement, il favorise le foisonnement des arnaques financières transfrontalières, en toute impunité**.**
C'est l'opinion de Deontofi.com. Les gendarmes boursiers, fonctionnaires ou diplomates n'ont pas le droit de le dire, car ce serait politiquement incorrect au regard des principes européens de libre concurrence et de liberté d'établissement. Mais quand un site de trading chypriote exploite son passeport européen pour mettre en avant ses agréments « français », cette seule supercherie doit vous alerter, car il n'a pas été agréé par les autorités françaises : elles sont forcées à l'autoriser par la loi européenne, ce qui est bien différent.
Comble du piège de mauvais goût, dans lequel tombent facilement les joueurs à la recherche de « bons tuyaux » et autres astuces frelatées pour s'enrichir, certaines publicités utilisent le même boniment que les marchands d'élixirs et régimes minceurs. « Interdit aux USA » ! Voici l'argument massue pour séduire leurs proies. Et pourquoi pas un robot qui gagne en Bourse à tous les coups tant qu'on y est ? C'est vraiment prendre les consommateurs pour des enfants**.**
Ces fables n'existent pas. Aucun professionnel des marchés, aucun scientifique, aucun chercheur académique n'a jamais prouvé qu'une quelconque méthode ou robot permettait de prédire le yo-yo des marchés. Il y a beaucoup de beaux parleurs, mais cela fait plus de vingt-cinq ans que j'attends les preuves… Quant à être interdit aux Etats-Unis, cela n'a jamais été un indice de qualité ou d'honnêteté.
Site « démo », documentations, formations ou autres services gratuits, tout n'est qu'un prétexte pour vous harponner et ne plus vous lâcher**.** Pire que les sectes, ces insectes du trading guettent le moindre mouvement sur leur toile pour vous rouler, vous endormir, et vous assécher**.**
Alors soyez prudents : Ne donnez jamais votre téléphone ou numéro de carte à un site de trading !

Liens : https://deontofi.com/les-sites-de-trading-forex-interdits-en-france-et-ceux-qui-devraient-letre/

L'enquête du Tribunal de Paris sur les escrocs d'Internet

François Molins, procureur de la République du Tribunal de Grande instance de Paris, expose l'offensive judiciaire contre les escrocs du Forex, lors de la conférence commune des autorités (AMF-ACPR-Parquet du Tribunal-DGCCRF) contre le fléau des arnaques sur Internet.

Deontofi.com livre ici le script de l'intervention de François Molins, procureur de la République du Tribunal de Paris, reconstitué sur la base des notes prises lors de la présentation commune des autorités financières, administratives et judiciaires, réunis au siège de l'Autorité des marchés financiers le 31 mars 2016. Les formulations exactes peuvent avoir été légèrement différentes, mais l'essentiel des informations et l'esprit de cette présentation sont conformes aux notes de l'auteur.

François Molins, procureur de la République du Tribunal de Paris :

Les escrocs du trading sont très bien organisés pour brouiller les pistes, ils utilisent faux noms, appellent depuis des call centers à l'étranger affichant des numéros de téléphone français, utilisant de fausses adresses IP pour leurs communications électroniques, en vue de réaliser des escroqueries de masse, en s'appuyant sur la publicité en ligne que le législateurs pourrait interdire, comme le projet de loi Sapin II le prévoit.

On voit de plus en plus d'usurpation d'identité des autorités, avec des faux noms et des faux documents. Bien évidemment une demande d'argent ne peut pas venir d'une quelconque autorité ni institution. Cela conduit évidemment à aggraver des situations personnelles ou familiales difficiles.

Les arnaques du Forex relèvent de l'escroquerie organisée, et je pèse mes mots, car ils opèrent en réseaux et s'appuient sur un mécanisme de blanchiment à grande échelle.

Les escrocs ouvrent des comptes dans des banques ou auprès de services de paiement dans des pays coopératifs dans l'Union européenne, puis virent immédiatement l'argent reçu vers d'autres pays étrangers non coopératifs.

L'objet ou l'effet de ces circuits est de faciliter le détournement, et en plus d'entraver l'action de la police et de la justice pour semer les enquêteurs et les obliger à recourir à une coopération internationale qui est toujours longue et difficile.

Face à ces escrocs, le parquet a tissé des liens avec l'AMF qui est souvent la première contactée par les victimes, avec l'ACPR qui dispose d'une expertise précieuse en matière de circuits financiers, et avec la DGCCRF, dont le réseau permet un repérage.

Au total, les escroqueries du Forex et des options binaires ont rapporté plus de 4 milliards d'euros, ce qui est supérieur a l'escroquerie sur la taxe carbone, selon une estimation à partir des dossiers que nous traitons.

La vigilance est de mise. Elle est plus que jamais nécessaire, car la perspective de ne jamais récupérer son argent est quasi certaine.

Cette semaine, nous avons mené 15 interrogatoires d'individus impliqués dans ces affaires, et 5 perquisitions ont eu lieu en Israël grâce à la coopération de la police israélienne que je remercie chaleureusement.

Cette enquête met en lumière les méthodes opératoires en bande organisée, des circuits de blanchiment à grande échelle, depuis des centres d'appels avec des dizaines de démarcheurs.

Il faut aussi redoubler de vigilance contre les escroqueries aux faux virements, sur lesquelles enquête la section cybercriminelle de la police. Les « fauvir » (pour faux virement), encore appelées arnaques au faux président, peuvent aller de quelques centaines de milliers d'euros à des millions d'euros. La société victime remet des fonds qu'elle n'aurait pas dû verser, grâce à des manœuvres d'escrocs opérant selon un scénario très sophistiqué, qui se concrétise par une histoire pour obtenir la remise de fonds et prendre la fuite.

Il y a d'abord un stade d'ingénierie sociale, quitte à s'introduire dans le réseau informatique ou pirater l'organisation avec des virus pour accéder à un maximum d'information sur l'entreprise. Puis ils passent à l'attaque avec de fausses identité pour solliciter un virement urgent toujours ultraconfidentiel, sous prétexte de préparer une OPA secrète, de régler une rançon rapidement, payer une taxe en retard discrètement, etc.

Les escrocs s'insinuent dans le lien commercial, après des piratages de mails, pour solliciter un faux virement vers l'étranger. On estime le préjudice supérieur à 500 millions d'euros depuis 2010, en France.

Il faut faire preuve d'une plus grande vigilance pour s'assurer de l'identité des destinataires. Il est nécessaire de déposer plainte extrêmement rapidement et de prévenir aussi vite sa banque. Nous avons une approche pragmatique pour tenter de récupérer les fonds détournés, mais avec la volatilité des circuits financiers, il faut une étroite collaboration internationale, ce qui rend les choses toujours difficiles.

La France est le pays le plus touché, même si ces escroqueries s'étendent dans d'autres pays. La meilleure arme est la sensibilisation.

Il est toujours plus intéressant de prévenir que de poursuivre et punir.

Nous devons faire appel au bon sens du public pour ne pas confier son argent à l'aveugle.

– Pourquoi la France ? interroge un journaliste.

– François Molins : C'est toujours difficile de savoir, mais je pense que cela peut être lié à des individus bien connus dont la base arrière est en Israël et qui avaient déjà été reconnus coupables d'escroqueries passées.

Liens : https://deontofi.com/lenquete-du-tribunal-de-paris-sur-les-escrocs-dinternet/

Faux virements histoire du pionnier de l'arnaque

Gilbert Chikli, inventeur de la juteuse escroquerie aux faux ordres de virement, est jugé demain à Paris avec dix-sept complices.

C'est le procès d'un présumé escroc international de très haut vol qui s'ouvre demain devant le tribunal correctionnel de Paris. Gilbert Chikli, 49 ans, sera jugé, avec 17 autres prévenus, pour une improbable série de près d'une cinquantaine d'escroqueries et tentatives, commises entre 2005 et 2006, au préjudice de banques et de grandes sociétés françaises.

Une arnaque, jusqu'alors jamais vue, dite « au président », ou encore aux faux ordres de virement internationaux (Fovi). Gilbert Chikli, qui se qualifie lui-même de « roi de la déballe (NDLR : argumentaire) », est soupçonné de s'être fait passer pour le PDG de groupes ciblés avant d'ordonner à de simples employés le virement d'importantes sommes vers des comptes bancaires à l'étranger.

Le précurseur de ce type de détournements de fonds a vu réapparaître son mode opératoire en 2011. Aujourd'hui, près de 700 sociétés en ont été victimes pour un préjudice évalué à plus de 350 M€…
Le plus « beau » coup réalisé par Gilbert Chikli reste, peut-être, son tout premier. Le 25 juillet 2005, la directrice d'une agence de la Poste, dans le Ier arrondissement à Paris, est contactée par un homme prétendant être le directeur général de sa banque. Ce dernier lui précise qu'elle va être sollicitée par un agent des services secrets et qu'elle doit coopérer à une enquête confidentielle portant sur « le blanchiment de capitaux destinés à financer des actes terroristes ». Absorbée par le bagout de son interlocuteur, la banquière suit aveuglément ses indications. Il lui demande de réunir 358 000 €, puis de se rendre dans un café place de la Nation.
S'ensuit une scène digne d'un film d'espionnage : la victime reçoit l'ordre de descendre dans les toilettes puis de s'y enfermer. Quelques minutes plus tard, elle entrouvre la porte, après avoir entendu une femme prononcer le mot de passe — « brevet » — puis lui tend la sacoche renfermant les fonds sortis des caisses de sa banque… Après avoir compris qu'elle avait été abusée, la directrice dépose rapidement plainte.
Saisis des investigations, les enquêteurs du premier district de police judiciaire (DPJ) ne tardent pas à découvrir que l'habile scénario a été reproduit à de nombreuses reprises avec plus ou moins de succès. D'autres agences de la Poste mais aussi de la Caisse d'épargne, de la Bred, de la Barclays, du LCL, du Crédit agricole, ainsi que des entreprises telles qu'Accor, Adidas, les Galeries Lafayette, De Dietrich, Disneyland Paris, Thomson, Alstom et les Pages jaunes ont, tour à tour, été ciblées par un certain Paul Ricard, du ministère de la Défense, ou bien encore par M. Brouillard, d'Interpol…
En tout, près de 6 M€ sont ainsi « récupérés » par Gilbert Chikli — qui a toujours agi depuis Israël — avant d'être déposés sur des comptes en Chine. De quoi largement financer son mariage princier auquel participent près de 700 invités. Au cours d'une conversation avec un enquêteur, l'escroc présumé s'est vanté de « la facilité avec laquelle il avait fait faire de telles choses à des banquiers ». L'homme s'était également présenté devant les caméras d'une télé française, en avril 2010, comme un « joueur sur une scène ». Un jeu qui lui avait procuré « une certaine adrénaline et jouissance », ajoutant qu'il avait d'une certaine façon « gagné au Loto » en composant les numéros de téléphone des sociétés et des banques victimes. Gilbert Chikli avait encore assuré « être prêt à refaire ses déballes »…
Après plusieurs mois en prison en France, il avait rejeté la responsabilité de ces arnaques sur deux de ses complices, assurant avoir été contraint de le faire pour rembourser des dettes de jeu. Remis en liberté fin 2009, Gilbert Chikli a ensuite pris la fuite en Israël. Un pays qu'il ne semble pas devoir quitter pour assister à son procès demain… February 19, 2016. Source : leparisien.fr
Liens : http://www.scandalix.com/france/faux-virements-histoire-du-pionnier-de-larnaque-au-president/

La CENTIF démasque une étudiante dont les virements d'argent dépassent un milliard

La Cellule de Traitement des Informations Financières (CENTIF), a révélé une histoire de blanchiment de capitaux. Les activités de la cellule ont démasqué une étudiante sénégalaise vivante à l'étranger.

L'étudiante dont l'identité a été rayée dans le rapport séjourne régulièrement dans un pays étranger, alors qu'une partie de sa famille réside ici à Dakar. Elle est titulaire d'un compte d'épargne dans les livres d'une banque réputée dakaroise. Jusque-là tout est normal. Mais sur une période de quatre mois (4) mois, le compte reçoit par plusieurs versements en espèces effectuées par différentes personnes pour un montant cumulé de plus de 100 millions de F CFA. L'argent est envoyé par le canal d'un système de transfert d'argent international. Au débit, le compte a enregistré deux opérations de 10 millions de F CFA. Un an après l'ouverture du compte, la banque reçoit un virement d'une contre-valeur de plus d'un milliard de F CFA ordonné par une société installée dans un pays tiers.

Ainsi, la banque interpelle l'étudiante une première fois sur la provenance de ses biens. Cette dernière explique dans un premier temps que l'argent provient de la cession de la maison de sa mère. Puis dans un élan ultime de justification, elle tente un coup de poker gagnant, qui va s'avérer navrant par la suite, renseigne « l'Observateur ». Elle indique que les fonds sont le produit de la vente d'un tableau d'art (une peinture célèbre) faite par son père artiste- peintre qui réside dans le pays étranger ou elle fait ses études. A l'appui cette dernière produit un document intitulé : « Facture de vente » portant cession d'un tableau de peinture datant de 1923 et signé de l'artiste- sculpteur peintre mondialement connu.

L'importance des sommes versées sur le compte bancaire de cette étudiante sans activité connue, a conduit la banque à avertir les agents de la CENTIF. Dans son rapport 2013, la Cellule enquête pour découvrir que les justifications de l'étudiante sont douteuses. « Le donneur d'ordre du transfert d'un milliard de F CFA est une société spécialisée dans le conseil en acquisition et en transport d'objet d'art, régulièrement inscrite au registre du commerce. Le document facture de vente produit n'est ni authentique ni conforme aux usages d'un montage réalisé par l'utilisation de l'entête d'un expert. En plus, l'œuvre réalisée est plutôt une sculpture réalisée en 1920 par un autre artiste et non celui indiqué par l'étudiante », sert le rapport de la CENTIF. C'est ainsi que l'autorité judiciaire a été saisie pour une infraction de blanchiment de capitaux

Liens : http://abidjantv.net/economie/la-centif-demasque-une-etudiante-dont-les-virements-dargent-depassent-un-milliard/

L'escroquerie au faux ordre de virement international

Bien que l'escroquerie au faux ordre de virement international (F.O.VI.), appelée également « arnaque au président » soit connue depuis 2011, elle n'a pas perdu de son ampleur et de nombreuses entreprises françaises (allant des plus prestigieuses du CAC 40 aux PME) demeurent toujours victimes de cette pratique criminelle. La Pologne est souvent utilisée comme premier lieu de transit des fonds détournés.

Mode opératoire

De quoi s'agit-il ? Un individu se fait passer pour un haut dirigeant d'une entreprise et demande généralement à un employé de son service comptable ou financier d'effecteur en urgence un virement bancaire international en vue d'une transaction hautement confidentielle (par exemple pour acquérir des parts de marché, éviter un redressement fiscal, etc.). Ce comportement constitue un exemple de délit d'escroquerie par usage d'une fausse qualité et par emploi de manœuvres frauduleuses sanctionné par l'article 313-1 du Code pénal de 5 ans d'emprisonnement

et de 375 000 euros d'amande. En Pologne, la même infraction est sanctionnée de 8 ans d'emprisonnement (article 286 du Code pénal polonais).
Comment se fait-il que ces demandes soient satisfaites sans qu'on puisse s'apercevoir de l'arnaque ?
Les criminels préparent longuement l'opération. Ils étudient l'organigramme de l'entreprise en utilisant les informations qu'ils trouvent sur Internet ou celles publiées directement par l'entreprise, leur permettant ainsi d'intercepter la signature du dirigeant figurant sur des documents officiels. La phase « d'ingénierie sociale » peut être bien plus poussée et il arrive parfois que les escrocs vont jusqu'à introduire un complice au sein même de l'entreprise cible pour mieux connaître son fonctionnement. Après ces préparations minutieuses, les criminels passent à l'acte et demandent par e-mail ou par téléphone à l'employé « sélectionné » d'effectuer un (ou plusieurs) virement bancaire :
Les e-mails peuvent être envoyés de l'adresse e-mail usurpée du dirigeant qui donne prétendument l'ordre. Le plus souvent toutefois les escrocs créent une adresse e-mail si proche que le destinataire croit en toute bonne foi qu'il s'agit d'une adresse authentique.
Dans le cas des arnaques opérées directement par téléphone, la fraude semble plus simple à démasquer. Toutefois, la personne qui appelle sait imiter la voix, la façon de parler du dirigeant pour lequel elle se fait passer, connaissant ses mots ou expressions préférées de sorte qu'au final il est tout aussi facile de se laisser abuser.
Il existe plusieurs variantes d'escroquerie au faux virement, quelques exemples :

- des individus se font passer pour des fournisseurs (bailleur par exemple) et communiquent un changement de domiciliation bancaire sur lequel l'entreprise effectuera désormais ses paiements,
- des « techniciens » viennent de mettre à jour le logiciel de la banque et demandent un « virement d'essai » pour effectuer un test,
- le dirigeant mène une acquisition totalement confidentielle au sein même de son entreprise, raison pour laquelle il demande à la personne choisie dans l'entreprise de ne révéler l'opération à personne d'autre …

La destination finale de ces virements est fréquemment la Chine ou Israël, mais le premier virement est, pour ne pas éveiller les soupçons, fréquemment réalisé à destination d'un pays de l'Union Européenne dans lequel il est aisé d'ouvrir un compte bancaire, par exemple en Pologne pour les cas qui nous intéressent.

Lorsque les fonds transitent par la Pologne

Que faire lorsqu'on s'aperçoit que l'on a été victime de cette arnaque ?
Les premiers jours, voire les premières heures, sont primordiales. Ce n'est pas sans raison que ces escroqueries sont fréquemment initiées les vendredi après-midi ou la veille d'une fête ou d'un pont. Avant que l'entreprise touchée ne s'aperçoive qu'elle a été victime d'une fraude, les malfaiteurs ont souvent eu suffisamment de temps pour faire disparaître les fonds.
En tout état de cause, dès que l'entreprise a connaissance de l'attaque, elle doit agir immédiatement. Ainsi, il est essentiel d'avertir non seulement sa banque en France mais également la banque polonaise destinataire du virement indu.
Il arrive ainsi heureusement que les fonds n'ont pas encore intégralement disparu dans la nature et que tout ou partie de la somme est susceptible d'être récupérée.
En France, sur la base de l'article L.133-18 2 du Code monétaire et financier, la banque rembourse en cas de fraude signalée la somme du virement qui, en principe, était instantané et irrévocable. Toutefois, en pratique, on ne dispose que d'un délai de

3 ou 4 heures durant lesquelles il est possible de récupérer l'argent. Ainsi, il est conseillé de bloquer au même temps le compte rebond.
En Pologne, une banque suspectant que des fonds proviennent d'une origine criminelle a la possibilité de bloquer un compte durant 72 heures sans qu'aucune autorisation judiciaire de saisie ne soit requise (article 106a de la loi bancaire polonaise du 29 août 1997). Ce blocage n'étant toutefois pas systématique, l'entreprise victime a tout intérêt à contacter rapidement un cabinet d'avocats spécialisé qui saura mettre la banque en face de ses responsabilités et déposera dans la foulée plainte auprès du Procureur local sur le fondement de l'article 16 de la loi polonaise du 16 octobre 2000 sur la lutte contre le blanchiment d'argent et le financement du terrorisme.
A l'issue de ces démarches, il sera plus aisé d'obtenir une autorisation du Procureur polonais visant à prolonger le blocage du compte suspect au-delà des 72 heures initiales.
Le rôle de l'avocat se poursuivra, notamment, par l'assistance du Procureur polonais dans ses contacts avec son homologue français qui aura été également saisi, ce qui accélère significativement l'enquête dans les deux pays, le temps étant un facteur clé dans ce type d'affaires.
En parallèle, il est également possible de mettre en cause la responsabilité de la banque française qui aurait négligé son obligation de vigilance imposée par l'article L.561-10-2 du Code monétaire et financier au regard de la lutte contre le blanchiment des capitaux. Dernière mise à jour : 6 avril 2016
Liens : http://www.village-justice.com/articles/escroquerie-president-filiere,20489.html

Le protocole bancaire SWIFT victime de cyber fraude

Sécurité : Suite à la récente cyber attaque la Banque du Bangladesh, l'organisme SWIFT vient de reconnaître que son logiciel a été utilisé pour cacher des preuves de transferts frauduleux.
Cette révélation intervient alors que les autorités du Bangladesh continuent leur enquête sur le vol de 81 millions de dollars en février dernier. Le transfert litigieux a transité d'un compte de la Banque du Bangladesh vers la New York Federal Reserve Bank. Un des enquêteurs, Mohammad Shah Alam, du Forensic Training Institute du Bangladesh, a déclaré à Reuters que la Banque du Bangladesh était une cible facile pour les cybercriminels car il n'y avait pas de pare-feu et que par ailleurs des commutateurs d'entrée de gamme étaient utilisés pour connecter les systèmes informatiques de la banque à SWIFT.
5 paiements frauduleux sur 35 ont été autorisés
Les chercheurs en cyber-sécurité qui travaillent sur ce hold-up ont expliqué le mois dernier qu'un logiciel malveillant avait été installé sur les systèmes informatiques de la Banque du Bangladesh. Ce malware a permis aux attaquants de se dissimuler avant de prendre l'argent. Un rapport interne de la Banque du Bangladesh mentionne que la Réserve Fédérale a été négligente : elle a validé les fausses transactions. Le rapport parle de «faute majeure». Il indique également que 5 paiements frauduleux sur 35 ont été autorisés (pour un total de 951 millions de dollars), et que des entités situées aux Philippines et au Sri Lanka ont reçu une partie des fonds volés. Et c'est une faute

d'orthographe commise par les cybercriminels qui a empêché 20 autres millions de dollars de disparaître en plus des comptes de la Banque du Bangladesh.
Ce vol a provoqué la démission du responsable de la Banque du Bangladesh, Atiur Rahman, 64 ans. Il n'avait pas jugé bon d'informer le ministre des finances du Bangladesh, A M A Muhith, de l'incident. Ce dernier avait appris cet évènement dans la presse étrangère.
SWIFT a reconnu que l'attaque incluait la modification des logiciels SWIFT sur les ordinateurs de la banque pour dissimuler les preuves de transferts frauduleux. "SWIFT est au courant d'un certain nombre d'incidents de cyber récents dans lesquels des personnes malveillantes dans l'entreprise, ou des pirates externes, ont réussi à envoyer des messages SWIFT depuis les back-offices, PC ou postes de travail des institutions financières connectées au réseau SWIFT" avertit l'organisme dans une message d'avertissement à ses clients.
L'avertissement, émit par SWIFT via une alerte confidentielle envoyée sur son réseau lundi, ne donne ni le nom des victimes ou le montant des sommes dérobées. SWIFT a également publié une mise à jour de sécurité pour le logiciel que les banques utilisent pour accéder à son réseau.

SWIFT : 3 000 institutions financières, 11 000 banques

Cette mise à jour doit sécuriser son système vis à vis du malware que les chercheurs de BAE Systems soupçonnent avoir été utilisé dans le hold-up de la Banque du Bangladesh. Les preuves collectées par BAE suggèrent que les pirates ont manipulé le logiciel Alliance Access de SWIFT, que les banques utilisent pour s'interfacer avec la plate-forme de messagerie de SWIFT, afin de brouiller les pistes. BAE a cependant mentionné ne pas pouvoir expliquer comment les commandes frauduleuses ont été créés et poussés à travers le système. SWIFT a cependant fourni des éléments sur la façon dont tout cela est arrivé. L'organisme explique que le modus operandi était similaire dans toutes les opérations frauduleuses. Les agresseurs ont obtenu des informations d'identification valides et ont pu créer et approuver des messages SWIFT.
SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une coopérative détenue par 3 000 institutions financières. Sa plate-forme de messagerie est utilisé par 11 000 banques et autres institutions à travers le monde et est considéré comme un pilier du système financier mondial. SWIFT a dit aux clients que la mise à jour de sécurité doit être installée avant le 12 mai.
26 Avril 2016.

Liens : http://www.zdnet.fr/actualites/le-protocole-bancaire-swift-victime-de-cyber-fraude-39836064.htm

Swift : Le réseau banquier international fait face à une grosse attaque de hackers

Selon une lettre que Swift s'apprête à envoyer vendredi à ses utilisateurs, les méthodes de ces hackers présentent des similitudes avec l'attaque qui avait permis en février à des malfaiteurs de dérober 81 millions de dollars sur un compte de la Banque centrale du Bangladesh auprès de la Réserve fédérale à New York.
Le FBI soupçonne que les malfaiteurs de février avaient bénéficié de complicités internes, avait affirmé mardi le Wall Street Journal.

Le même jour, des hauts représentants de la Réserve fédérale de New York, de la Banque du Bangladesh et du système de paiement international Swift, se sont rencontrés à Bâle, en Suisse, pour discuter de cette fraude cybernétique.
L'attaque menée contre Swift -Society for Worldwide Interbank Financial Telecommunication- montre une véritable tentative pour obtenir un accès à ce système indispensable pour le fonctionnement du monde financier international, selon le texte que s'apprête à publier Swift, cité par le New York Times et le Wall Street Journal.
Cette fois-ci, l'attaque visait une banque commerciale dont elle ne donne pas le nom, et dont les malfaiteurs ont réussi à s'approprier les codes pour envoyer des messages au nom de la banque.
En février, des messages semblant provenir de la Banque du Bangladesh avaient ordonné le transfert vers différents comptes aux Philippines de 81 millions de dollars.
Les méthodes utilisées par les hackers dans ces deux cas « montrent clairement une connaissance approfondie et sophistiquée des opérations de ce type dans les banques visées », selon la lettre de Swift, toujours citée par les journaux. Mai 13, 2016
Source: RTLInternational
Liens : http://www.koldanews.com/2016/05/13/swift-le-reseau-banquier-international-fait-face-a-une-grosse-attaque-de-hackers-a539130.html