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

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES

DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Lettre n°93

Cybercriminalité et blanchiment de capitaux sur internet

Le blanchiment d'argent connaît de nouveaux développements depuis l'avènement d'internet. Le présent article fait le point sur cette cybercriminalité en col blanc.

Dans ce cadre, Internet constitue une source d'inquiétudes, dès lors que l'argent criminel y circule très rapidement, emportant différents risques, comme les risques technologiques, l'anonymat, les limitations à l'accord de licences et au contrôle, les risques géographiques et juridiques, et le risque de transactions (financières) compliquées.

Les criminels disposent ainsi, avec Internet, d'un immense « terrain de jeu » pour y développer leurs activités en profitant d'un avantage incontournable d'invisibilité et d'anonymat. Il y a d'infinies possibilités pour gagner de l'argent sans être confronté à ses victimes. Prenons l'exemple des « attaques informatiques » ou des « cyberattaques ». Il est possible de pénétrer des systèmes numériques publics et privés sans dévoiler son identité ou le lieu de la transaction. Le « phishing » constitue une méthode par laquelle on s'empare du code PIN d'une carte de paiement ou d'une carte de crédit, ou même le code d'accès particulier pour accéder à son compte bancaire ou encore le « pharming ». Pensons également à la « cyber-rançon », où une rançon est demandée, afin d'éviter qu'un système numérique ne soit mis hors service. Enfin, il convient de relever les nombreuses informations détournées par des personnes malveillantes et les cas d'usurpations d'identité qui se multiplient notamment sur les réseaux sociaux. L'espace de la Toile est devenu une infosphère où se multiplient et où cohabitent des données personnelles ou publiques, dont l'origine et la véracité ne sont pas certifiées. Et le nombre d'exemples à citer est innombrable.

En ce qui concerne la cybercriminalité, il y a une économie souterraine qui pourvoit aux besoins d'outils, de marchandises et de services pour commettre le cybercrime, et même pour vendre et acheter des biens et des informations volées. Cela s'appelle le « Dark Net ». Il s'agit d'un environnement économique véritable avec des producteurs, des commerçants de marchandises et de services, des fraudeurs et des clients.

Il y a aussi les jeux et les paris en ligne qui ont connu une explosion exponentielle sur la Toile. Un des problèmes en cette matière consiste à contrôler où se trouve le serveur informatique des jeux (question de compétence de contrôle et juridique). Et ce, sans parler de la « monnaie virtuelle » ? La « monnaie virtuelle », telle qu ele bitcoin, se distingue de la « monnaie électronique », du fait qu'elle est créée par un groupe de personnes (physiques ou morales), et non par un État, ou une union monétaire. Cette monnaie est destinée à comptabiliser, sur un support virtuel, les échanges multilatéraux de biens ou de services au sein du groupe concerné. Il s'agit d'un système non régulé, caractérisé par un facteur d'opacité.

En fait il y a deux éléments essentiels qui différencient les deux systèmes. En premier lieu, la monnaie virtuelle peut être utilisée dans le « cyberspace ». Les transactions ne peuvent pas êtres rattachées à une zone géographique déterminée. Les flux ne sont pas détectables : ces «

monnaies » sont conçues pour exister en dehors du contrôle d'un organe de régulation. Le système peut être fermé (sans convertibilité avec la monnaie officielle) ou ouvert (avec possibilité de convertir les fonds virtuels en monnaie officielle). En second lieu, la monnaie virtuelle permet aussi des transactions totalement anonymes qui peuvent avoir lieu soit directement entre particuliers, soit par l'intermédiaire de prestataires de services. Tous les acteurs opèrent en dehors du secteur traditionnel des services de paiement. Aucun plafond d'utilisation ou plancher d'identification des utilisateurs ne leur est applicable.

L'ensemble de ces nouvelles possibilités qu'offre Internet ont eu, pour corollaire, la création de multiples possibilités d'y blanchir de l'argent. Parmi les méthodes les plus utilisées, il convient de relever l'emploi des « Payable Through Accounts ». Il s'agit ici de comptes bancaires, dont le titulaire a ordonné que, quand un certain solde a été dépassé sur le compte, ce montant soit directement viré sur un ou plusieurs autres comptes (intérieurs ou internationaux). Une autre variante est le « criss-crossing scriptural », par lequel l'argent est transféré mutuellement entre différents comptes en banque à divers noms à l'intérieur et/ou à l'étranger et cela en combinaison avec des transferts d'argent par des firmes de transferts d'argent.

Actuellement les transferts (internationaux) peuvent être exécutés de différentes manières : par les comptes bancaires traditionnels, l'e-monnaie, les services de paiement Internet ou les services de transferts d'argent traditionnels. Indépendamment du mode de payement, toutes ces manières de transférer de l'argent ont leurs propres vulnérabilités en matière de risques de blanchiment de capitaux. Généralement ces transferts internationaux se déroulent dans la deuxième phase du blanchiment : l'empilement.

Des transferts bancaires, des hommes de paille et des mules bancaires sont des méthodes souvent utilisées pour blanchir des avantages patrimoniaux illégaux obtenus par le « phishing ». Afin de cacher son identité, le criminel peut également contacter plusieurs personnes en leur offrant de l'argent pour utiliser leur compte personnel afin d'y effectuer des transactions. Dans de nombreux cas, les hommes de paille ouvrent un nouveau compte personnel à ces fins et quand la transaction en question a été effectuée, ils déclarent que les fonds leur appartiennent. Les fonds sont ensuite transférés à d'autres comptes intérieurs et/ou étrangers ou retirés en liquides. Souvent les liquides sont ensuite envoyés par des services de transferts d'argent à l'étranger. Et ainsi la chaîne du papier est interrompue et le criminel a su effacer ses traces et le lien avec le délit sous-jacent est brouillé.

Le recours à des « shell companies », des sociétés qui n'ont pas d'activités (commerciales), aucun actifs ou obligations financières, sont des structures intéressantes pour les « cyberblanchisseurs ». En effet, ces sociétés disposent de différents comptes bancaires étrangers, souvent situés dans des pays offshore. Ces compagnies sont utilisées comme preuve de paiement pour les banques et permettent ainsi d'effacer la trace de l'argent.

Bien que les nouvelles plateformes de paiement en ligne et les monnaies digitales gagnent de plus en plus en influence dans notre vie quotidienne et environnement social, les cybercriminels et les cyberblanchisseurs dépendent toujours de notre système financier et bancaire traditionnel. Les virements (internationaux) sont toujours rapides et efficaces et généralement utilisés au premier stade du blanchiment de même que la cybercriminalité existe en volant de l'argent des comptes en banques des victimes par des techniques frauduleuses.

En outre, le blanchiment d'argent classique dans les casinos est accompagné du blanchiment dans les jeux et paris en ligne, notamment sur les chevaux, le football, etc.

Les plateformes de jeux et de paris en ligne, qui sont vulnérables pour le blanchiment de capitaux et d'autres crimes financiers par la nature de leurs opérations, peuvent servir comme facilitateurs de blanchiment. Les institutions de jeux sont des commerces très actifs en matière de transactions en liquides qui fournissent une série très large de produits et de services financiers, et qui sont semblables à ceux fournis par des compagnies financières et de services

de transactions financières. En plus, les compagnies de jeux servent à des clients variés et souvent temporaires dont ils ne savent que très peu. Les logiciels fournis par les organisateurs de jeux et de paris en ligne rendent possible de transférer et d'accumuler de grandes sommes d'argent, et déposer et retirer de l'argent gagné par des virements bancaires ou différents systèmes de paiement électroniques.
Profitant de failles juridiques et de faiblesses des moyens de lutte, le crime organisé diversifie ses activités. Pour cela, il recourt à des moyens sophistiqués notamment aux réseaux numériques pour commettre ses méfaits et masquer ses actes illicites, et ce à l'échelle mondiale. Le crime organisé s'affranchit en effet des contraintes géographiques et juridiques pour saisir des opportunités, notamment avec des opérations de blanchiment. Des efforts sont donc attendus concernant les moyens de lutte, en particulier pour améliorer le recueil, la conservation et l'exploitation de la preuve fondée sur des données numériques.
La lutte contre la cyberdélinquance est un défi non seulement pour l'Europe et chacun de ses Etats-membres, mais pour le monde entier. Face aux possibilités infinies offertes par le numérique et aux risques que cela engendre, un dispositif législatif performant et dynamique est indispensable, qui ne cesse pas de s'améliorer et de s'adapter. Aussi le contrôle et la lutte contre la cybercriminalité doivent être continuellement dynamiques et innovantes. Mais dans ce domaine, rien n'est figé et des pistes demeurent à explorer.
https://creobis.eu/blog/2015/08/07/aml/

Blanchiment des capitaux, Nouvelle tendance de la cybercriminalité

Les autorités françaises témoignent du recrutement inquiétant de «mules» sur internet. Des intermédiaires qui réceptionnent puis transfèrent des capitaux via leur compte bancaire en ligne.
Blanchir de l'argent ou transférer des capitaux est une activité en développement sur internet. Les intermédiaires recrutés sont qualifiés de «mules» et peuvent gagner plusieurs milliers d'euros par mois, en toute illégalité.
Il s'agit d'une des grandes tendances 2006 du Panorama de la cybercriminalité, présenté ce 18 janvier par le Club de la sécurité des systèmes d'information français (Clusif). «Les mules sont la version internet des porteurs de valises», explique à *ZDNet.fr* Pascal Lointier, président de l'organisme.
Leur recrutement s'effectue via des spams envoyés en masse. Les messages sont souvent présentés comme des offres d'emploi avec un lien vers un site, qui ressemble à s'y méprendre à celui d'une société respectable (photos de réunions, logos accrocheurs, témoignages de participants...).
L'internaute qui s'y rend se voit proposer de «devenir partenaire» d'une entreprise financière. Il lui est demandé de parler anglais, d'être majeur, d'avoir environ deux heures à consacrer à cette activité par jour et, surtout, de disposer ou d'ouvrir un compte en banque pour effectuer des transactions.

Jusqu'à 3.000 euros par mois de commission

S'il se déclare intéressé, il doit alors surveiller sa messagerie électronique régulièrement afin d'être réactif. Il va recevoir des e-mails lui indiquant qu'une somme d'argent a été versée sur son compte; somme qu'il devra par la suite transférer «à des clients».
Pour cette opération, l'intermédiaire empochera une commission de 5 à 10% des sommes transférées. Jusqu'à 3.000 euros par mois, avancent certaines annonces.

Dans les faits, l'internaute crédule, ou peu scrupuleux, participe à une opération de brouillage de pistes qui permet à l'auteur d'une attaque sur le Net de récupérer de l'argent. Il peut, par exemple, s'agir d'une attaque par phishing qui aura permis de rassembler plusieurs dizaines de milliers de dollars. Plutôt que de recevoir directement l'argent sur son compte, son auteur passe par une ou plusieurs mules, ce qui pourra ralentir d'éventuelles tentatives de suivi des fonds.

«Nous n'avons pas de chiffres précis mais la prolifération de ces intermédiaires recrutés sur le Net nous est confirmée par les services de police et de gendarmerie en France», poursuit Pascal Lointier. Légalement, ils peuvent être poursuivis au pénal pour complicité d'escroquerie et écoper jusqu'à cinq ans de prison.

«Ce phénomène participe d'une tendance plus générale d'une professionnalisation des attaques sur internet avec de plus en plus un appât du gain», conclut le président du Clusif.

Une motivation financière qui avait déjà été observée dans le cadre du panorama 2005 de la cybercriminalité avec la diffusion d'*adware*.

http://www.zdnet.fr/actualites/blanchiment-des-capitaux-nouvelle-tendance-de-la-cybercriminalite-en-2006-39366347.htm

Cybercriminalité et blanchiment d'argent

En ces temps de crise, il est difficile de connaitre si un travail peut engager notre responsabilité pénale ou civile. Depuis 2006, de nombreuses personnes ont été victimes de manipulation et d'escroquerie par les cybercriminels en faisant du blanchiment d'argent.

Ces personnes, ayant reçu par mail (Spam) des offres pour le poste d'agent financier ou de chef de transactions sont plutôt aveuglées par les privilèges offerts par ces postes (rémunération élevée, travail à temps partiel et à domicile) et ne se doutent généralement pas du caractère délictueux de leur mission : accepter des transferts d'argent (sale) sur leurs comptes personnels puis envoyer les sommes via un service de transfert de fonds tel que Western Union vers une adresse d'entreprise située à l'étranger.

L'origine de l'argent sale est souvent le gain de fausses enchères en ligne ou celui d'une attaque de phishing. Les cyberdélinquants ne font que manipuler ces agents pour les transactions financières. Ces agents sont doublement perdants car pour la plupart du cas ils ne sont pas rémunérés comme convenu et feront l'objet d'une poursuite judiciaire pour complicité de blanchiment d'argent lorsque l'infraction principale est découverte.

Notons que ces agents ne sont pas les seuls moyens utilisés par les cybercriminels pour blanchir leur argent. Il y a aussi les salles de poker virtuelles où les joueurs (cybercriminels) sont des adversaires camarades et qui utilisent des coordonnées bancaires volées (phishing). En ce sens, l'acte de blanchiment d'argent sale réside dans le fait de perdre et que les gains sont transférés directement dans des comptes d'autres personnes. Ces dernières peuvent ensuite être payées par une somme envoyée par un service de transfert d'argent (Western Union) pour avoir prêté leurs comptes.

http://www.anti-cybercriminalite.fr/article/cybercriminalit%C3%A9-et-blanchiment-dargent

Cybercriminalité : La diffusion frauduleuse d'adware en forte croissance

Sécurité : Les millions de programmes robots, cachés dans les systèmes des PC, ont largement servi en 2005 à diffuser illégalement des logiciels publicitaires adware. Selon des experts, chaque adware installé peut rapporter à son distributeur jusqu'à 7 centimes d'euros.

Une nouvelle forme de cybercriminalité a sévi en 2005: la diffusion frauduleuse d'*adware*, des programmes parasites qui affichent des pop-up publicitaires non sollicités. C'est l'une des principales observations du Club de la sécurité des systèmes d'information français (Clusif), qui a présenté le 12 janvier son "Panorama de la cybercriminalité 2005".
Pour propager ces programmes, certains internautes peu scrupuleux n'hésitent plus à utiliser massivement des "logiciels robots". C 'est en cela que leur diffusion prend un caractère frauduleux, car l'installation d'un adware doit normalement s'effectuer avec le consentement préalable de l'utilisateur.
Le robot est un programme malveillant qui s'installe discrètement sur des machines pour en prendre le contrôle à distance. Grâce à des robots, un attaquant peu se constituer rapidement une armée de milliers d'ordinateurs "zombies", qui seront autant de cibles que de relais.
«Le robot ouvre une brèche sur l'ordinateur où va être installé un ou plusieurs adwares», explique à *ZDNet* François Paget. Ce chercheur de l'éditeur McAfee France et intervenant pour le Clusif, aujoute que «le système qui héberge le robot peut également être utilisé pour diffuser à son tour l'adware vers d'autres ordinateurs présents sur le voisinage réseau, en exploitant une faille du système d'exploitation.»
François Paget rappelle qu'en 2004, les robots étaient déjà exploités pour diffuser du spam ou lancer des attaques par saturation, de type déni de service distribué (DDoS). Leur utilisation pour la distribution d'adwares est une nouveauté 2005.

744 dollars par jour avec 5.000 machines

L'appât du gain est la première motivation de ces actes malveillants, encouragés par la passivité des éditeurs d'adwares, activité tout à fait légal. Pas trop regardants sur les méthodes de distribution de leurs produits, ils ont recours à des «affiliés», un statut ouvert à n'importe quel internaute. Chaque affilié reçoit un identifiant qui lui servira à marquer chaque adware qu'il diffuse; l'éditeur le rétribue en conséquence.
«Ces entreprises ne sont pas complices. Dans la plupart des affaires que nous avons observées, ce sont d'ailleurs elles qui ont porté plainte contre des affiliés peu scrupuleux. Elles cherchent aujourd'hui à redorer leur blason», précise le chercheur de McAfee France.
En août 2005, la société américaine 180solutions a ainsi porté plainte contre des affiliés en Grande-Bretagne, en Australie, au Canada, au Liban, en Slovénie et en Hollande. Pour augmenter leurs gains (entre 7 et 50 cents par installation), ils auraient utilisé plusieurs réseaux de milliers robots. Un réseau de 5.000 machines permet de dégager un revenu de 744 dollars par jour, ou 22.346 dollars par mois, selon le rapport du Clusif.
Autre exemple: en octobre 2005, la police hollandaise a arrêté trois jeunes gens qui avaient pris sous leur contrôle plus de 1,5 million de machines et de serveurs grâce à des robots. Ils sont notamment accusés de diffusion d'adwares.
«D'octobre 2004 à octobre 2005, il y a eu une augmentation de 400% du nombre de robots», poursuit François Paget. De 5 à 10 millions de ces robots peuvent être simultanément en activité sur le web.
Un robot arrive la plupart du temps de la même manière qu'un virus, via un e-mail piégé ou en exploitant une faille de sécurité du système d'exploitation. Toutefois un système correctement "patché" et protégé par un antivirus mis à jour ainsi qu'un pare-feu est «immunisé à 95%», conclut l'expert en sécurité.

http://www.zdnet.fr/actualites/cybercriminalite-2005-la-diffusion-frauduleuse-d-adware-en-forte-croissance-39302880.htm

L'appât du gain est désormais au cœur de la cybercriminalité

Sécurité : Le Club de la sécurité des systèmes d'information français (Clusif) dresse son bilan annuel de la cybercriminalité. Principale observation en 2004: une croissance forte des actes de malveillances et de chantage commandés par des intérêts financiers.

La cybercriminalité se professionnalise de plus en plus. Et l'intention n'est plus simplement de nuire à une image de marque (en défigurant un site ou en répandant un virus), mais de réellement gagner de l'argent. Telle est l'une des principales observations du Club de la sécurité des systèmes d'information français (Clusif), qui a présenté le 13 janvier son «Panorama de la cybercriminalité 2004».

«L'enrichissement et la déstabilisation économique sont les formes de cyberciminalité qui ont connu la plus forte croissance en 2004», résume pour *ZDNet* son président, Pascal Lointier.

Dans son document, le Clusif revient sur divers actes de malveillances tels que le chantage, la demande de rançon et d'extorsion de fond. Des observations, a indiqué son dirigeant, basées sur des informations déjà publiées. L'organisme ne prétend donc pas, dans ce panorama, faire remonter des informations confidentielles (même rendues anonymes) en provenance de ses membres, qui sont pour la plupart des cadres de grandes entreprises.

Parmi les cas cités, celui emblématique de Google, qui a été victime en mars 2004 d'un maître chanteur réclamant 100.000 dollars pour qu'il se tienne tranquille; il menaçait d'utiliser un logiciel qui fausserait le système de paiement des publicités postées sur le célèbre moteur de recherche. L'auteur présumé de ce chantage a été inculpé. C'est d'ailleurs pour cela que l'affaire s'est ébruitée.

Autre cas d'école: celui du japonais Softbank en février 2004, qui s'est dit victime de chantage et d'extorsion de fond. Une somme de 28 millions de dollars lui était réclamée contre la non-divulgation de données personnelles touchant 4,5 millions de clients. Quatre suspects ont été arrêtés au Japon.

La déferlante "adware" et "spyware"

Outre ces chantages, des exemples de déstabilisation économique ont également été évoqués. Notamment celui du vol de bases de données dont a été victime Microsoft en février 2004, concernant du code de Windows 2000 et NT4. En mai, c'est ensuite l'équipementier réseau Cisco Systems qui s'est vu dérober des fichiers sources de son système d'exploitation IOS.

L'appât du gain se manifeste aussi avec la prolifération, en 2004, de programmes espions s'infiltrant dans les PC (comme pour les virus, Windows est l'OS plus souvent visé). Ces fameux "spyware" et en particulier les "adware" (de "ad", publicité) peuvent, par exemple, afficher des pop-up publicitaires sans que l'internaute ne sache d'où il vient. Les auteurs de ces programmes, explique le Clusif, se rémunèrent directement auprès d'annonceurs peu scrupuleux.

Plus de robots que de virus

Dans la même veine, l'année passée a été marquée par l'avènement des "logiciels robots", tels que Botnet ou Spybot, qui s'installent discrètement sur les machines pour permettre d'en prendre le contrôle à distance. Un moyen, par exemple, de lancer des attaques par saturation, de type déni de service distribué (DDoS), via des ordinateur "zombies" qui, compromis grâce à ces robots, sont finalement contrôlés par un groupe d'escrocs. Leur objectif est souvent de relayer du spam.

«Nous sommes persuadés qu'il y a aujourd'hui dans le monde entre 4 et 6 millions de machines infectées par des robots», explique à *ZDNet* François Paget, chercheur antivirus pour l'éditeur McAfee France. «La grande difficulté est que cette menace est difficile à contrer devant le volume de programmes disponibles. Il y a entre 40.000 et 100.000 robots différents actuellement sur le Net», poursuit-il.

Encore une fois, l'utilisation de ces programmes se monnaie: un réseau de 500 robots peut se louer 380 euros, révèle l'étude du Clusif. L'accès exclusif à une seule machine zombie peut se négocier à partir de 0,35 euro par utilisation. Alors qu'une attaque DDoS peut se "vendre", d'après des études d'origine américaines, entre 38 et 750 euros.

Au final, tous ces produits malveillants deviennent plus inquiétants que les virus ou vers informatiques qui circulent sur le Net. «Il y a actuellement 25 à 50 nouveaux robots par jour.

Par ailleurs, il a fallu attendre vingt ans pour avoir 1.500 virus réellement dans la nature. En simplement deux ans, nous avons observé l'apparition de quelque 7.000 adware», indique François Paget. «À la fin des années 90, les logiciels de protection détectaient 70% de virus et 30% d'autres programmes malveillants. Aujourd'hui, c'est l'inverse», conclut le responsable.
http://www.zdnet.fr/actualites/l-appat-du-gain-est-desormais-au-coeur-de-la-cybercriminalite-39198290.htm

La lutte contre la cyber-contrefaçon en quête d'efficacité

Traditionnellement jugée comme une simple infraction, la contrefaçon représente actuellement un vrai défi pour les Etats, les citoyens, l'environnement, et, surtout, pour une économie toujours plus mondialisée. Elle nuit en effet fortement aux entreprises car elle détruit le produit de l'innovation, peut avoir des répercussions dommageables sur l'emploi, et par son caractère non conforme aux normes de sécurité elle cause d'importants préjudices à la santé et la sécurité des consommateurs. En sus, elle nuit à la croissance économique, a un impact négatif sur la fiscalité des gouvernements et, par conséquent, sur le fonctionnement des services publics. Prenant des tournures de plus en plus variées, la contrefaçon est donc l'affaire de tous. Le Rapport « Trade in Counterfeit and Pirated Goods », élaboré conjointement par l'OCDE et l'EUIPO en avril 2016 dans l'objectif de mettre à la disposition des gouvernements un état des lieux rigoureux et mis à jour de la contrefaçon dans le monde, présente d'ailleurs des chiffres préoccupants : la contrefaçon représente 2.5% du commerce mondial, soit un volume d'échange qui s'évalue à 461 milliards de dollars en 2013, et 5% des importations dans l'Union européenne soit un total de 85 milliards d'euros.
L'apparition d'Internet, désormais premier vecteur de distribution des produits de contrefaçon, s'est avérée particulièrement nuisible pour les droits de propriété intellectuelle et a rendu la maîtrise du phénomène encore plus ardue. Il a fragmenté la contrefaçon et a été à l'origine d'une multiplication et d'une diversification des *modus operandi* au service des contrefacteurs. Par ailleurs, internet a contribué à rendre les contrefacteurs invisibles et leur localisation malaisée, et parallèlement, l'interception des produits contrefaisants difficile. Le développement des plateformes de e-commerce telles qu'Amazon ou eBay, et des réseaux sociaux tels que Facebook ou Twitter, a inévitablement propagé le phénomène. Or, l'acquisition de produits contrefaits sur Internet présente des risques plus élevés pour le consommateur. Le contrefacteur peut en effet voler ses données personnelles, lui envoyer des spams, des malwares, débiter indument son compte bancaire, voire usurper son identité. En outre, si la majorité des échanges de contrefaçons se réalisent via Internet, un volume non négligeable d'échanges se fait aussi sur le Darknet (Réseau virtuel privé) et le Deep web (Web invisible). C'est ce qu'a démontré l'affaire « Silk Road » en 2013. Il s'agissait en l'espèce d'un site internet dissimulé dans le Deep web dont l'accès était réservé aux utilisateurs du réseau décentralisé TOR. Ce réseau avait pour caractéristique principale de garantir un anonymat total et une impossibilité de tracer les paiements. D'après le FBI, le site Silk Road était un immense marché noir en ligne sur lequel étaient échangés de multiples produits illicites dont des contrefaçons, des stupéfiants et des armes en très grande quantité par des Bitcoins. Cette monnaie virtuelle a été utilisée par les auteurs de contrefaçon pour s'assurer de préserver leur anonymat et pour garantir la confidentialité des échanges. Pour ce site internet, l'épilogue judiciaire a été particulièrement brutal : l'administrateur du site internet « Silk Road » a été condamné pour association de malfaiteurs au sein d'un trafic de drogue, blanchiment d'argent, trafic de contrefaçon et pour diverses infractions de cybercriminalité.

Bien que de notables efforts ont été déployés sur le plan législatif, notamment par l'adoption de la loi du 21 juin 2004 dite LCEN, de la loi du 12 juin 2009 dite HADOPI, de la loi du 14 mars 2011 dite LOPPSI 2, ou plus récemment de la loi du 11 mars 2014 renforçant la lutte contre la contrefaçon, une forte asymétrie persiste entre l'ampleur des conséquences de la contrefaçon et les moyens de répression. Le Rapport Unifab, nommé « Contrefaçon & Terrorisme », met habilement en exergue l'indéniable lien entre la criminalité organisée, le terrorisme et la contrefaçon. Le directeur d'Interpol Ronald L. Noble et le sénateur français Richard Yung ont, à maintes reprises, attiré l'attention cette relation. Ils ont notamment souligné que l'utilisation privilégiée de la contrefaçon par les organisations terroristes génèrent des profits illicites considérables permettant la prolifération de leurs actes. Il apparait ainsi regrettable que la dernière loi renforçant la lutte contre la contrefaçon précitée n'ait pas pris en considération cette problématique pourtant nettement évoquée par les parlementaires lors des discussions.

Si l'anéantissement total de ce fléau semble quelque peu illusoire, d'aucuns essaient tant bien que mal de proposer des refontes afin de moderniser l'arsenal juridique actuel, notamment sur plan numérique. La lutte passe nécessairement par la mutualisation des efforts entre les titulaires de droits, les forces de police, les magistrats, les autorités douanières, et surtout, les intermédiaires techniques de l'internet. Or, selon le député Philippe Gosselin, les obligations qui pèsent sur les intermédiaires techniques de l'internet, prévoyant un régime de responsabilité atténuée (soit une absence de surveillance générale et de recherche de contenu illicite), n'ont pas produit le résultat escompté. Partant, le 8 janvier 2016, ledit député a présenté un amendement à l'alinéa 3 de l'article 23 du projet de loi pour une République numérique destiné à impliquer davantage les plateformes en ligne dans la lutte. Il porte sur la mise en place d'un « devoir de diligence » à l'égard des plateformes en ligne. Le « devoir de diligence » conduira les plateformes en ligne à prendre « toutes mesures raisonnables, adéquates et proactives afin de protéger les consommateurs et les titulaires de droits de propriété intellectuelle contre la promotion, la commercialisation et la diffusion de produits contrefaisants tels que définis aux articles L521-1, L615-1 et L716-1 du Code de la propriété intellectuelle. » Cette nouvelle obligation devra être calquée sur le modèle du devoir de diligence déjà existant en matière de contenus pédopornographique, de contenus faisant l'apologie ou provoquant au terrorisme, de contenus incitant à la haine ou encore de contenus illégaux de jeux d'argent en ligne. Bien que la Secrétaire d'Etat chargée du Numérique estime que ce « devoir de diligence » n'est qu'un rappel de l'obligation de droit positif de retirer les contenus illicites prévus par l'article 6 de la LCEN, les titulaires de droits se réjouissent de cet amendement en ce qu'il participe à une meilleure protection et à une prise en considération accrue des droits de propriété intellectuelle en France. Ils y voient également une potentielle source d'inspiration pour une future législation prise dans un cadre européen. Le 3 mai 2016, lors de l'examen du projet de loi par le Sénat, cet amendement a été adopté.

Examiné et adopté le 29 juin 2016 par la Commission mixte paritaire, la nouvelle version du projet de loi pour une République numérique n'a pas encore été publiée. Toutefois, la synthèse du projet de loi fait apparaitre que l'article 23, tel qu'adopté par le Sénat, a été maintenu mais modifié par la Commission. Reste à savoir si les membres de la Commission mixte paritaire ont fait le choix de supprimer ou de simplement modifier ce « devoir de diligence » prévu par cet article.

Ces atermoiements législatifs témoignent d'une chose : les réformes sont difficiles à mener et c'est souvent une politique des « petits pas » qui prévaut en la matière. Concomitamment, les réseaux de contrefaçon semblent chaque jour mieux structurés et plus diffus. L'évolution législative relative aux intermédiaires techniques envisagée semble, dès lors, aller dans le bon sens, et ce même si le chemin de la réforme globale semble encore long.

https://www.observatoire-fic.com/la-lutte-contre-la-cyber-contrefacon-en-quete-defficacite-par-betul-iler-ceis/#_ftnref1

Banques et cyber attaques : Etat des lieux des préjudices et des règlementations

Les impacts des cyber attaques peuvent être financiers, atteindre l'image de marque des établissements financiers et entrainer des problématiques de conformités légales et réglementaires…

Le risque de cyber attaques est aujourd'hui nettement supérieur dans le domaine bancaire que dans celui des services ou du commerce. Le préjudice peut s'évaluer par coût de l'actif dérobé (data), par sanctions pénales, s'agissant de vol de données, ou par la détérioration de l'image de marque. Selon l'étude « Cost of Data Breach » publiée par the Ponemon Institute en 2016, le coût moyen d'une fuite par document dans le secteur financier s'élève à 221 $, soit plus que les 158 $ perdus en moyenne par les autres secteurs. En France, la perte de client –churn rate- consécutif à une fuite de donnée a un impact très important sur le coût moyen de l'actif dérobé. Depuis trois ans, notre pays demeure, au niveau international, celui qui a le taux de résiliation client le plus élevé (+4,3%) après une fuite de donnée. Lorsque l'on ramène ce taux au secteur financier, il est de +6.2%, impactant considérablement la réputation et l'image de marque des établissements concernés. En sus des préjudices financiers, liés aux pertes et fuites de données, il convient de rajouter les ressources financières consenties à la réparation du préjudice (recherche des causes, intervention pour mettre fin à l'accident, remplacement des équipements…). Plusieurs facteurs permettent de réduire le coût des fuites de données par actif, notamment le temps de réponse aux incident (-14$/actif), et l'utilisation intensive de technique de chiffrement (-13$/actif).

Les préjudices liés au cyber attaques peuvent aussi s'évaluer en termes de ressources humaines. Au début de l'année 2016 dans l'affaire Swift, le directeur de la banque centrale du Bangladesh a démissionné et trois de ses plus importants collaborateurs sont été simplement licenciés. Mais le préjudice qui reste indéniablement le plus important, car par nature incalculable, reste celui de la réputation et de l'image de marque. Comme le disait à juste titre Warren Buffet, « Il faut 25 ans pour bâtir une réputation et moins de 5 minutes pour la ruiner »

Vers un renforcement des règlementations

Le secteur bancaire est déjà soumis à une grande variété de législations, visant notamment à combattre le blanchiment, la corruption, l'évasion fiscale, les produits dérivés (titres échappant aux contrôles classiques) ou d'autres crimes qui pèsent considérablement sur la santé des états et des populations. La lutte contre la cybercriminalité implique un renforcement des règlementations en termes d'analyse de risques et de protection des données.

1. Accords de Bâle (III du 16 décembre 2010).

Les principes d'agrégation de données et de reporting des risques définis par le Comité de Bâle sur le contrôle bancaire (BCBS 239), intègrent des notions d'indication de l'origine des données et de leur mode de traitement

2. La loi de programmation militaire (LPM) N° 2013-1168

Elle impose à l'ensemble des Organismes d'Importance Vitales (OIV) et notamment les établissements bancaires de cartographier leurs réseaux et de les cloisonner pour éviter la propagation des attaques, d'identifier les systèmes d'information ultra critiques, de déployer des outils de détection des cyber attaques et de signaler les incidents subis.

3. La Directive NIS –Network Security and Information

Approuvée par le Conseil de l'Union et le Parlement Européen, cette directive dont l'entrée en vigueur est prévue en 2018, traite des mesures à mettre en place afin d'assurer un haut niveau de sécurité en matière de réseaux et de systèmes d'information dans l'Europe des 28. Elle vise un renforcement de la coopération stratégique en matière de lutte contre la cybercriminalité entre les États membres, et à sensibiliser les entreprises aux risques d'intrusion et de piratage de leurs réseaux. Les opérateurs concernés- Opérateurs fournissant des services essentiels- devront prendre des mesures préventives, d'ordre technique et opérationnel afin de détecter tout risque concernant la sécurité du réseau informatique, avec obligation de déclaration aux autorités compétentes en cas de piratage, et/ou d'intrusion dans les systèmes informatiques. En France, les OIV sont déjà soumis à cette obligation de reporter aux autorités compétentes toute attaque informatique, auprès de l'ANSSI.

4. Le GDPR -Règlement général européen sur la protection des données

Applicable en 2018, le GDPR, obligera, sanctions à la clé (jusqu'à 4% du CA annuel global), les sociétés du secteur financier à alerter les clients affectés par une fuite de données. L'article 37 du GPDR suggère par ailleurs la nomination, dans l'entreprise d'un délégué à la protection des données –DPD- qui serait à même de comprendre la façon dont les données sont traitées, d'en évaluer les risques, la conformité, la supervision, les choix technologiques… Alors que cette méthodologie d'analyse des risques cyber sécurité orientée « impact d'entreprise » est déjà maîtrisée par le RSSI (ISO27001), le DPD réalisera des analyses de risques orientées « impact sur les personnes ». Une mise en conformité GDPR qui risque donc de poser problème, tant en terme de charge de travail que de compétences requises pour l'analyse des risques.

5. Prestations de Services Essentielles Externalisées (PSEE)

S'agissant d'informatique déportée dans le nuage, et dès lors qu'une banque requiert un service Cloud pour les besoins de ses activités, elle doit vérifier la conformité de ce service aux lois, règles et normes qui s'appliquent à elle. Avec la notion de Prestations de Services Essentielles Externalisées (PSEE), le prestataire ou fournisseur Cloud est soumis à des obligations renforcées de sécurité pour toutes les activités relevant du cœur de métier de la banque et/ou jouant un rôle dans la sécurité des actifs et données bancaires (analyse préalable de risques, plan de continuité d'activité, manuels de procédures, respect du secret bancaire même en cas d'hébergement à l'étranger.). Le renforcement de la règlementation en matière de sécurité bancaire implique aussi l'apparition de catégories spécifiques de préjudices dans les contrats -informations privilégiées, conformité aux PSEE, protection des donnée- avec un nouveau risque, celui de déplacer les plafonds de responsabilité des banques vers leurs prestataires de services.

https://lalettreducloud.com/2017/01/13/comment-les-banques-sarment-face-aux-cyber-attaques-etat-des-lieux-des-prejudices-et-des-reglementations/

Les moyens juridiques de lutte contre la cybercriminalité

Les réseaux numériques sont devenus une composante majeure sur laquelle repose la croissance de nos économies. Pourtant, l'utilisation des réseaux tels l'internet présentent des risques et des vulnérabilités inhérentes à leur nature ouverte et internationale. Ainsi, depuis que l'internet s'est développé dans le grand public, il ne se passe pas une semaine sans que les médias ne rapportent une affaire liée de près ou de loin à l'utilisation frauduleuse des TIC (Technologies de l'Information et de la Communication).

Chacun a en mémoire la récente affaire Yahoo! (Ordonnance de Référé du 20 novembre 2000, TGI Paris), qui a ouvert une brèche dans le principe de territorialité du droit pénal. En effet, le

juge des référés français, a condamné une entreprise américaine, sur le fondement du droit français (article R-645-1 du code pénal), pour des faits (ventes d'objets nazis) commis virtuellement sur le territoire français, à partir du territoire américain.

Pour autant, les activités criminelles liées aux technologies de l'information ne se limitent pas à des actes racistes ou néo-nazis ; en effet, elles peuvent prendre des formes très variées : atteintes aux systèmes d'information et/ou aux données informatisées, attaques de serveur par saturation (spamming), violation du secret des correspondances privées, violation des règles de protection des données personnelles, espionnage industriel ou militaire, contrefaçon de droits de propriété intellectuelle (brevets, marques, dessins, droits d'auteur, …), délits de presse (ex : diffamation), fraude fiscale, fraude à la carte bancaire, blanchiment d'argent, réseaux de pédophiles, usurpation d'identité, organisation de la prostitution, … La liste des infractions est longue ; ces dernières touchent aussi bien l'entreprise et les administrations que les individus.

Par ailleurs, la diffusion de certains virus (ex : Melissa, Iloveyou, Code Red) a causé d'importants dommages aux entreprises et autres organismes publics. Leurs modes de propagation sont divers : e-mail, Web, partage de réseau, etc.

Plus récemment, des activistes se sont livrés à des activités de terrorisme sur les réseaux. A la suite des attentats du 11 septembre 2001, il a été annoncé que les terroristes d'Al-Quaida avaient eu recours aux systèmes de messageries électroniques associés à l'usage de moyens de cryptologie et de stéganographie pour assurer la confidentialité de leurs échanges tendant à la préparation et à l'organisation de leurs attentats.

En tant qu'espace de communication ouvert, l'internet permet la diffusion de tout type d'information sans aucune contrainte géographique. Suivant la loi applicable dans le pays de destination de l'information, cette dernière pourra être considérée comme licite ou illicite, parfois en fonction des principes (variables) de liberté d'expression et de respect de la vie privée.

En matière de criminalité informatique ou de criminalité informatisée (que l'on nomme ensemble usuellement "cybercriminalité"), dès lors que le recours à l'appareil répressif est décidé par la victime ou par le Ministère Public, une réalité classique s'impose : le droit pénal est une des expressions de la souveraineté des États, en fonction de laquelle il possède une dimension territoriale. Or, l'internet s'affranchit de toute contrainte territoriale. En effet, en matière pénale, le juge d'instruction et la police judiciaire recherchent classiquement et principalement à localiser et identifier l'auteur d'une infraction et à préserver les éléments de preuve pour matérialiser l'infraction qui peuvent se trouver sur le territoire d'un autre État.

Le fait d'appréhender des comportements délictueux sur les réseaux se heurte à trois types de contraintes :

• l'anonymat qui peut être organisé sur les réseaux. L'utilisation des services des prestataires de services de certification, tels que la société Certinomis, qui fournissent des certificats électroniques d'identification et de confidentialité, peut jouer un rôle non négligeable en terme de sécurité, et ce d'autant que des obligations légales s'imposent à eux tant pour le recouvrement des clés de chiffrement que pour la lutte contre l'anonymat ;

• la volatilité des informations numériques (possibilité de modifier et de supprimer des éléments de preuve quasi instantanément) ;

• les comportements délictuels qui revêtent souvent un caractère transnational.

Face à ces réalités, une harmonisation internationale du droit et des procédures ainsi qu'une étroite coopération judiciaire sont des conditions sine qua non pour être en mesure de lutter efficacement contre des cybercriminels qui tendent à s'organiser et à agir au niveau planétaire.

Cette harmonisation est devenue une priorité majeure des États qui sont entrés dans la société de l'information, spécialement les États membres du Conseil de l'Europe, conformément aux bases qui ont été définies par le G8. C'est dans cette perspective que la Convention du Conseil

de l'Europe sur la cybercriminalité a été signée le 23 novembre 2001 à Budapest par 33 États, dont les membres de l'Union européenne, les Etats-Unis d'Amérique, le Canada, le Japon et l'Afrique du Sud. Cette Convention présente l'avantage d'énoncer les mesures que les États doivent adopter, mais sans que leur contenu soit précisé. Ceci explique pourquoi, concernant l'harmonisation des sanctions relatives aux attaques visant les systèmes d'information, la Commission européenne vient de publier une proposition de décision cadre le 19 avril 2002.
Lors de la réunion du G8 des 13-14 mai 2002 au Canada, de nouvelles recommandations ont été adoptées sur les crimes de hautes technologies, les crimes informatiques et les moyens de lutte y associés.
Les enjeux juridiques sont à la mesure des pertes financières et des dommages résultant de la cybercriminalité qui ont connu une forte progression, encore accrue, au cours de ces dernières années. Ainsi, du point de vue de l'assurance, si les risques matériels et immatériels (données numérisées) sont assurables en vertu de leur caractère aléatoire, il en va différemment des risques pénaux nés de la commission des infractions relatives à la cybercriminalité. Il n'en demeure pas moins que l'analyse des moyens juridiques de lutte contre la cybercriminalité permet de mettre en relief le contenu de l'arsenal répressif existant.
Envisageons tour à tour les principaux aspects de la lutte contre la cybercriminalité.

La conservation des données de connexion

En vertu de la Convention du Conseil de l'Europe, les États ont l'obligation d'adopter les mesures nécessaires afin de pouvoir enjoindre à une personne ou à une entreprise de conserver certaines données informatiques stockées ou des données de connexion relatives à une infraction pénale, sous le sceau du secret procédural, notamment lorsque ces données risquent de disparaître ou d'être modifiées et de pouvoir les divulguer à l'autorité compétente de l'État partie. De la même manière, les Etats doivent habiliter leurs autorités compétentes à avoir le pouvoir d'enjoindre aux personnes présentes sur leur territoire et aux fournisseurs de services internet à communiquer les informations en leur possession.
La France est intervenue en ce domaine avec la loi du 1er Août 2000 (réformant la loi du 30 septembre 1986 sur la liberté de communication) qui encadre la responsabilité et les obligations des fournisseurs d'accès à l'internet (F.A.I.) et des fournisseurs d'hébergement. Elle leur impose d'identifier leurs clients bénéficiant de services d'accès à l'Internet et leur donne obligation de conserver et de communiquer ces données identifiantes sur réquisition de l'autorité judiciaire. Toutefois elle ne précisait pas combien de temps les F.A.I. avaient l'obligation de conserver ces données, ni ce qu'il convient d'entendre par autorité judiciaire (les demandes d'un O.P.J. semblent a priori exclues). Par ailleurs, les personnes physiques ou morales dont l'activité est d'éditer un service de communication en ligne, autre que des correspondances privées, doivent s'identifier précisément et tenir ces informations à la disposition du public.
De plus, la loi sur la sécurité quotidienne (L.S.Q.) du 15 novembre 2000 impose aux opérateurs de télécommunications la conservation des données de connexion des internautes pendant une durée de un an avec pour finalité de mettre à la disposition des autorités judiciaires des informations nécessaires à l'enquête. Cependant, les modalités de conservation doivent encore être précisées par décret. Ces dispositions législatives figurent dans un Chapitre intitulé : " Dispositions renforçant la lutte contre le terrorisme ". L'article 22 de la loi trace la perspective dans laquelle s'inscrivent les dispositions légales : "Afin de disposer des moyens impérieusement nécessaires à la lutte contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication, les dispositions du présent chapitre sont adoptées pour une durée allant jusqu'au 31 décembre 2003. Le Parlement sera saisi par le Gouvernement, avant cette date, d'un rapport d'évaluation sur l'application de l'ensemble de ces mesures. ". Il convient de préciser, en outre, que la loi de finance rectificative pour 2001

du 28 décembre 2001 a élargi l'accès aux données de connexion auprès des fournisseurs d'accès et des opérateurs de télécommunications, alors que la L.S.Q. réservait cette possibilité aux seuls juges, aux agents des douanes, du fisc et aux enquêteurs de la Commission des Opérations de Bourse (C.O.B.).
La conservation de ces données a pour objectif de permettre l'identification des délinquants et de matérialiser des éléments de preuve des infractions. Néanmoins, ces mesures peuvent s'avérer insuffisantes si l'État en cause ne se dote pas des moyens juridiques appropriés pour procéder à des interceptions légales et aux déchiffrements des messages codés suspects.

L'accès aux contenus des messages : Interceptions de sécurité et déchiffrement des données codées

Les autorités compétentes des Etats parties à la Convention sur la cybercriminalité pourront collecter les données de connexion et intercepter les données relatives au contenu directement ou en contraignant les fournisseurs de services internet (ex : le système Carnivor du F.B.I. aux U.S.A.).
Le libellé de la Convention permettra à chaque pays d'adapter un système d'interception à sa législation interne.
Pour ce qui est de la France, l'autorité judiciaire a déjà la possibilité de procéder par voie de réquisition auprès des opérateurs téléphoniques qui ont l'obligation de fournir les données de connexion (la prestation est facturée environ 90 €). En ce qui concerne le contenu des communications, c'est le régime classique sur les écoutes téléphoniques (procédure judiciaire) et les interceptions de sécurité (procédure administrative) qui a vocation à s'appliquer, sans qu' il y ait besoin de profonde modification (loi du 10 juillet 1991). C'est en ce sens que la L.S.Q. a anticipé l'adoption de la Convention. Un nouvel article 11-1 a été introduit dans la loi du 10 juillet 1991, aux termes duquel les autorités judiciaires pourront avoir accès aux conventions de chiffrement des données chiffrées du présumé délinquant par l'entremise des prestataires de services de cryptologie.
En outre, d'une part, la L.S.Q. introduit plusieurs articles dans le code de procédure pénale afin de permettre aux magistrats (du parquet, de l'instruction et de la juridiction de jugement) d'ordonner le déchiffrement des données. D'autre part, elle établit une nouvelle incrimination avec l'introduction de l'article 434-15-2 dans le code pénal : toute personne qui a connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, a l'obligation de remettre ladite convention aux autorités ou de la mettre en œuvre. En cas de défaut d'exécution, des peines de prisons et d'amende sont prévues. Ces nouvelles dispositions doivent interpeller les assureurs auxquels s'imposera l'obligation de limiter leur garantie à certains coûts liés à la reconstitution des clés de chiffrement des clients des prestataires qu'ils assurent.

1. L'harmonisation des infractions

Les États parties à la Convention s'engagent à adopter en conformité avec leur droit interne des législations qui définissent un certain nombre d'infractions ainsi que leur tentative de commission, tout en laissant aux États une marge d'adaptation plus ou moins large selon les faits visés. En droit français, ces incriminations reprennent globalement la substance de la loi Godfrain du 5 janvier 1988 (articles 323-1 à 323-7 du code pénal). Les États doivent prendre les mesures nécessaires pour que les infractions visées soient sanctionnées par des "sanctions effectives, proportionnées et dissuasives y compris la privation de liberté". Ils doivent adopter des législations incriminant les infractions suivantes : Infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.
Sont ainsi incriminés l'accès illégal, les interceptions illégales, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et les abus de dispositifs informatiques permettant la commission d'infractions.

2. Falsifications et fraudes informatiques

Sont ici visées les modifications, altérations de données informatiques lorsqu'elles sont utilisées aux fins de paraître légales ou authentiques, ainsi que toute atteinte au fonctionnement d'un système informatique dans l'intention d'obtenir sans droit un bénéfice économique quelconque.

3. Pornographie enfantine

Sont incriminées toutes les productions, mises à disposition, diffusions, ou détention d'images de pornographie enfantine concernant des mineurs de 18 ans, voire de 16 ans en fonction du droit interne de chaque État. Cette disposition, particulièrement attendue par le grand public, revêt un caractère plus symbolique, qu'une nécessité purement juridique. En effet, rares sont les États qui n'ont pas légiféré ou qui n'ont pas de règles de prohibition en matière de protection des mineurs. A la vérité, la difficulté tient davantage à la non application par certains États de leur propre législation pour des raisons de corruption ou de politique pénale laissant apparaître, de fait, une certaine permissivité ou tout au moins une inertie judiciaire. C'est en réalité la différence entre les seuils de la majorité qui risque de poser des difficultés, notamment pour les pays qui opèrent une distinction entre la majorité civile et la majorité sexuelle.

4. Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Les atteintes aux droits protégés en vertu notamment des droits nationaux ou du Traité de l'OMPI sur le droit d'auteur (entrée en vigueur le 6 mars 2002) ou de la Convention de Berne (1886) doivent être réprimées. Le texte de la Convention prévoit ainsi un durcissement de la protection des droits de propriété intellectuelle par le fait que les atteintes seront systématiquement sanctionnées sur le plan pénal.

Du point de vue français, cela ne bouleversera pas l'ordre juridique puisque l'actuelle victime d'une atteinte à un droit de propriété intellectuelle (contrefaçon) a le choix entre la voie civile à vocation purement indemnitaire, et la voie pénale à vocation répressive et indemnitaire par constitution de partie civile. En revanche, pour ce qui est des droits voisins (droits connexes dans la Convention), il faudra procéder à des ajustements législatifs. Pour d'autre pays, il s'agira de modifier substantiellement l'état actuel de leur droit.

La responsabilité pénale des personnes morales

Cette responsabilité peut être pénale, civile ou administrative lorsque les faits définis dans la Convention ont été commis par une personne physique ayant le pouvoir d'engager ou de représenter la personne morale ou lorsqu'elle exerce sur elle un contrôle. Elle doit être établie indépendamment de la responsabilité pénale des personnes physiques ayant commis les faits. En droit français, il est possible d'engager la responsabilité pénale d'une personne morale, sous la condition que le législateur l'ait prévu.

Les procédures et perquisitions

Les Etats parties à la Convention ont l'obligation d'habiliter leurs administrations respectives à perquisitionner les systèmes informatiques, à saisir des données et à imposer aux personnes concernées de fournir les données en leur possession, de conserver les données " vulnérables " ou de les faire conserver par les personnes concernées.

Les mesures prévues par la Convention sont applicables en droit interne à toutes les enquêtes et procédures pénales relatives aux infractions définies dans la Convention ainsi qu'à toute infraction commises au moyen d'un système informatique ou pour la collecte de preuves électroniques concernant une infraction pénale quelconque. Cette précaution vise à permettre une souplesse procédurale afin de rendre applicable la coopération procédurale lorsque l'enquête nécessite des investigations sur des moyens informatiques. La mise en œuvre des procédures doit être proportionnée avec la nature des circonstances de l'infraction et s'inscrire dans la conformité de l'ordre juridique interne et respecter les libertés fondamentales et les droits de l'homme.

Les autorités compétentes d'un Etat doivent pouvoir perquisitionner et saisir les informations relatives à une infraction liée à l'utilisation de l'informatique. La question des perquisitions à distance et transfrontalières dans des systèmes informatiques implantés dans un Etat partie, à partir d'un autre Etat a été abordée, mais aucune position commune n'a pu être adoptée, ni aucune mesure technique envisagée concrètement. Cette position était défendue par les Etats-Unis qui préfèreraient voir en lieu et place du système de coopération judiciaire et d'entre aide, instaurer une véritable " cyberpolice " internationale qui se jouerait des frontières. A cette omission volontaire, plusieurs raisons : la souveraineté des Etats est directement atteinte par de telles pratiques, et la plupart des Etats demeurent réticents à dévoiler qu'ils disposent déjà d'un arsenal technologique leur permettant d'opérer ce type de "visites" dans des systèmes d'information étrangers sans laisser de traces …

En ce qui concerne la France, les dispositions pénales permettent déjà de saisir tout type d'information dans le cadre d'une enquête judiciaire. Néanmoins, le législateur prévoit dans le projet de loi sur la société de l'information (LSI) de modifier les articles 56 et 97 du code de procédure pénale en complétant le concept de "documents" par celui de "données informatiques" et le concept de "pièces" par celui d' "informations " et en organisant la saisie ou la copie des données informatiques.

En conclusion, nous observerons que pour mettre en œuvre cet arsenal pénal international, la Convention pose un principe général de coopération. La Convention du Conseil de l'Europe prévoit que les traités et accords internationaux de coopération en matière pénale, seront applicables aux infractions et procédures définies dans le corps du texte de la Convention. Il est certain que les Etats qui n'ont pas de retard technologique, ou qui chercheront à utiliser la Convention à des fins de politique interne, mettront les moyens matériels et humains en place. Mais d'autres pays, même s'ils sont partie à la Convention, - a fortiori s'ils ne le sont pas - demeureront, faute de moyens suffisants, de parfaits paradis informationnels que ne manqueront pas d'utiliser les professionnels du crime organisé sur les réseaux, tout en ayant acquis une respectabilité d'apparence en matière de lutte contre la cybercriminalité. Dans la mesure où les risques sont identifiés et que les parades existent en droit français notamment, il reste à les prendre en considération dans la pratique de l'assurance des ressources informatiques et des réseaux.

http://www.caprioli-avocats.com/publications/50-securite-de-linformation/78-moyens-juridique

Le G7 promet d'en faire plus contre les cyberattaques

Les ministres des Finances du G7 ont promis samedi à Bari, dans le sud-est de l'Italie, de renforcer la cybersécurité au moment où elle est battue en brèche, après une réunion qui a aussi permis de briser un peu la glace avec les Etats-Unis.

La discussion des ministres et des gouverneurs des banques centrales du G7 est intervenue samedi, précisément au moment où une partie de la planète était victime d'une série de cyberattaques, qui ont sérieusement perturbé les hôpitaux britanniques ou paralysé des usines automobiles du groupe Renault en France.

Ces attaques sont un "rappel de l'importance de la cybersécurité et de la nécessité de se concentrer sur ce problème", a indiqué samedi devant la presse le secrétaire américain au Trésor, Steven Mnuchin.

Son homologue italien, Pier Carlo Padoan, hôte de cette réunion, s'est même autorisé à plaisanter en affirmant s'être concerté avec les auteurs de ces attaques pour prouver l'importance du sujet à l'agenda de ce G7.

Plus sérieusement, le gouverneur de la Banque d'Italie, Ignazio Visco, a assuré de son côté qu'elles n'avaient pas affecté le sytème financier international.
Dans une déclaration commune, les pays du G7 (Etats-Unis, Japon, Allemagne, France, Grande-Bretagne, Italie et Canada) ont affirmé reconnaître la "menace croissante" que représente la cybercrimainalité pour leurs économies et promis de trouver des réponses.
Le sujet sera notamment évoqué dans deux semaines à Taormina, en Sicile, à l'occasion d'un sommet des chefs d'Etat et de gouvernement du G7, a promis M. Padoan.
Il s'agit en attendant de demander aux experts de procéder à une évaluation précise des capacités en matière de sécurité informatique, pour mieux préparer la riposte, a indiqué de son côté le gouverneur de la Banque de France, François Villeroy de Galhau.
Les grands argentiers du G7 ont aussi promis d'en faire plus pour lutter contre le financement du terrorisme, l'évasion ou l'optimisation fiscale.
Et sur ces sujets, toutes les délégations ont été "très fermement unis", y compris celle des Etats-Unis, a assuré le ministre français des Finances Michel Sapin.
http://www.lanouvellerepublique.fr/France-Monde/Actualite/Politique/n/Contenus/Articles/2017/05/13/le-G7-promet-d-en-faire-plus-contre-les-cyberattaques-3098555

Le GABAC dénonce les risques que la finance mobile fait courir à l'Afrique centrale

Selon le Groupe d'action contre le blanchiment d'argent en Afrique centrale (GABAC), pour cause d'asymétries d'information, les activités de la finance mobile en Afrique centrale sont sujettes à plusieurs manquements. Car, la variété d'acteurs répertoriés dans cette chaine d'activités (banque, opérateur, agent, marchand, client utilisateur final), n'appréhendent pas tous de la même manière, les risques liés au blanchissement de capitaux et au financement du terrorisme.
L'institution fustige surtout l'attitude des banques, pourtant directement liées aux organismes de régulation, qui ne sont pas toujours bien équipées pour assurer la conformité des activités de la finance mobile chez les opérateurs.
Il y va également de leurs agents qui sont souvent peu ou pas avertis, du potentiel d'utilisation frauduleuse de la monnaie électronique, et ne sont pas à même d'effectuer un véritable contrôle de l'identité des usagers. A titre d'exemple, déplore l'institution en charge de la lutte contre le blanchiment d'argent, *« à la souscription, la photocopie de la pièce d'identité suffit, il n'y a donc pas de moyen de contrôle de son authenticité.»*, indique-t-elle.
En outre, poursuit le GABAC, la volatilité des capitaux, d'un acteur à l'autre, échappe également au contrôle des institutions. Le GABAC regrette aussi le relatif *« vide juridique »* dans l'espace CEMAC en comparaison avec la zone CEDEAO, en matière de régulation. L'institution fait savoir à cet effet que les règlements ne comportent pas de réelles obligations contraignantes, ni de mentions sur les rapports entre établissements de crédit et partenaires (contrôle de l'origine des fonds, des objets des transactions, des destinations etc.). En général, *« les textes ne sont pas encore en phase avec les objectifs de prévention de blanchiment d'argent et de transactions financières, car il n'y a pas eu d'évaluation portant sur le sujet en Afrique centrale ».*
Dans ce cadre, pour pallier les limites du dispositif réglementaire, dont le règlement N°01/11/CEMAC/UMAC/CM du 18 septembre 2011 constitue la base, et les vulnérabilités liées à l'utilisation de la monnaie électronique, ce dispositif a été complété en 2016, par un règlement portant sur la prévention et la répression du blanchiment des capitaux et du

financement du terrorisme en Afrique centrale (règlement n°01/CEMAC/UMAC/CM du 16 avril 2016).
Ce texte prévoit ainsi l'adoption de diligences telles que la connaissance de la clientèle, des relations d'affaires du client, le contrôle des transactions et l'obligation de déclaration de soupçon aux agences nationales d'investigation financière.
http://www.investiraucameroun.com/finance/0905-8877-le-gabac-denonce-les-risques-que-la-finance-mobile-fait-courir-a-l-afrique-centrale

Une surveillance des monnaies virtuelles afin de combattre le blanchiment et le terrorisme

Communiqué de presse de la commission Commerce extérieur/international / Affaires économiques et monétaires du Parlement Européen – 26 mai 2016 **:** « La Commission européenne devrait mettre en place un groupe de travail pour superviser les monnaies virtuelles, comme le Bitcoin, afin de prévenir leur usage dans le cadre d'activités de blanchiment et de financement du terrorisme, a déclaré le Parlement dans une résolution non contraignante votée ce jeudi. »
« Le texte rédigé par Jakob von Weizsäcker (S&D, DE) suggère que la Commission développe une expertise relative à la technologie des monnaies virtuelles, et recommande une législation. Il met cependant en garde contre une régulation excessive d'une technologie qui peut offrir des opportunités significatives pour les consommateurs et l'économie.
"Afin d'éviter d'étouffer l'innovation, nous préférons une surveillance de précaution plutôt que la régulation préventive. Cependant, les innovations dans le domaine des TIC peuvent se répandre très rapidement et devenir systémiques. C'est pourquoi nous appelons la Commission à établir un groupe de travail pour surveiller activement la façon dont la technologie évolue et proposer la régulation adéquate si le besoin s'en fait sentir", a déclaré M. Von Weizsäcker.
La Commission examine des propositions pour intégrer les plateformes d'échange de monnaies virtuelles dans le cadre de la directive existante contre le blanchiment, qui sera prochainement mise à jour. Ces propositions prévoient l'obligation faite aux plateformes de mettre fin à l'anonymat lors d'un transfert d'une monnaie réelle à une monnaie virtuelle. Les régulateurs craignent en effet que le système existant ne facilite le blanchiment et les activités d'organisations terroristes.
La résolution du Parlement fut adoptée par 542 voix pour, 51 contre et 11 abstentions. »
https://bitcoin.fr/une-surveillance-des-monnaies-virtuelles-afin-de-combattre-le-blanchiment-et-le-terrorisme/

Pour lutter contre les ransomwares, il faut encadrer le bitcoin

Le ransomware est une vraie vérole. Et F-Secure le confirme en expliquant que son modèle économique doit notamment sa viabilité et sa rentabilité à l'existence du BitCoin qui alimente la cyber criminalité. Et le Laboratoire F-Secure de mettre en garde les gouvernements pour qu'ils se décident enfin à éliminer ce mode de transactions anonymes.
D'après le Rapport F-Secure sur la Cyber Sécurité 2017, on comptait, en 2012, une seule famille de ransomware connue. En 2015, ce nombre atteignait 35, pour exploser en 2016, avec 193 familles identifiées. Les entreprises chinoises ont investi des sommes colossales

dans des fermes de serveurs web, s'assurant ainsi le monopole de la monnaie virtuelle. Résultat : 42% des transactions mondiales de Bitcoins menées l'année dernière ont eu lieu sur les places d'échanges chinoises, d'après une étude du New York Times. Sean Sullivan, Security Advisor chez F-Secure, a même constaté que le Shanghai Composite Index, l'un des principaux indicateurs financiers du pays, s'alignait parfois sur l'index Bitcoin.
« *L'amélioration de la technologie Blockchain offre une meilleure visibilité sur leur marché, explique le spécialiste. Les autorités chinoises ont peu d'intérêt à voir le marché du Bitcoin s'enrayer. Le gouvernement américain, à l'inverse, ne semble pas vouloir participer à la légitimation de cette monnaie virtuelle.* » La Commission boursière américaine (SEC) a d'ailleurs rejeté en mars dernier la création d'un fond d'échange Bitcoin, en raison de « *préoccupations relatives aux pratiques et activités frauduleuses ayant lieu sur ce marché* ».
Les autorités américaines et européennes pourraient porter un coup d'arrêt au Bitcoin avec une mesure relativement simple. « *Il serait possible d'exiger une adresse physique pour tout compte d'échange Bitcoin* », explique Sean Sullivan. Á l'heure actuelle, il ne faut que quelques minutes pour ouvrir un compte Bitcoin sur un marché tiers. Avec cette nouvelle mesure, un code d'activation serait envoyé par courrier à l'utilisateur pour que celui-ci puisse créer son compte. Cette contrainte ne concernerait pas les attaques menées depuis la Russie ou la Chine, mais elle réduirait considérablement leur rentabilité.
« *Les marchés n'apprécieraient pas du tout. Mais au vu des centaines de millions de dollars extorqués chaque trimestre, cela semble s'imposer* » confirme Sean Sullivan. « *Sans mesure destinée à combattre le Bitcoin, le développement exponentiel des familles de ransomware semble inévitable.* »
Moralité : les gouvernements doivent réagir dès aujourd'hui pour proposer une réponse aux monnaies virtuelles, car les choses vont devenir de plus en plus complexes.
http://www.infodsi.com/articles/168795/lutter-contre-ransomwares-faut-mieux-encadrer-bitcoin.html

Local ou virtuel, l'argent change de visage

Du léman au bitcoin, de la micro-monnaie purement régionale à sa version cryptée et intraçable, les formes de paiement évoluent. Décryptage.
Bitcoin, bilur (gagée sur le pétrole), Ethereum, Zcash ou encore à une échelle locale le léman et le farinet… Les monnaies alternatives n'ont cessé de se multiplier au cours des dernières années. Qu'est-ce qui explique un tel engouement? Décryptage.
Soutien à l'économie locale
«Favoriser les circuits courts et promouvoir l'économie locale». C'est l'argument clé à l'origine des initiatives de micromonnaie qui se multiplient actuellement en Suisse. De Genève au Tessin en s'arrêtant par le Chablais ou le Gros-de-Vaud, tous semblent vouloir leur monnaie locale. En Valais, par exemple, le lancement du farinet est prévu pour le 13 mai. A l'origine de ce projet, l'envie de «relocaliser tout ce qui peut l'être, notamment dans l'alimentaire, et être moins dépendant des ressources étrangères».
Le léman est certainement le projet aujourd'hui le plus abouti étant donné que son lancement remonte au mois de septembre 2015. Moins de deux ans plus tard, quelque 400 sociétés acceptent d'être payées avec cette monnaie. En tout, cela représente 110'000 francs de contrepartie déposée à la Banque Alternative Suisse. «Un succès plus grand que prévu», selon Jean Rossiaud, président de l'association Monnaie Léman
Le léman est aujourd'hui disponible dans six «bureaux de change». L'objectif est de développer son réseau pour atteindre la cinquantaine d'endroits où il serait possible de s'en pourvoir. A noter que la monnaie valdo-genevoise aura son pendant numérique, le e-léman.

«Une forme de bitcoin, mais sans la spéculation», selon son président.

Une forte spéculation

Si les promoteurs de monnaies locales cherchent à éviter toute spéculation – le léman, par exemple, n'est pas convertible –, la donne est différente pour les nombreuses monnaies virtuelles apparues ces dernières années.

Prenez le bitcoin, cette pionnière des devises virtuelles. Depuis son lancement, en 2009, son cours n'a cessé de jouer au yo-yo. Ces derniers jours, il enchaîne les records. Sa valeur a ainsi dépassé mardi les 1800 dollars le bitcoin. A titre de comparaison, l'or terminait la journée à 1220 dollars l'once. Selon un classement réalisé par Coinmarketcap.com, la capitalisation boursière de la célèbre crypto-monnaie frôlerait les 30 milliards de dollars (voir infographie).

L'engouement pour ces alternatives monétaires ne semble pas prêt à s'interrompre, puisque de nouvelles venues continuent d'arriver sur le marché, à l'exemple du Zcash depuis l'automne dernier. Sa valeur a d'ailleurs connu un parcours aussi chaotique que le bitcoin avec une valeur qui n'a cessé de passer d'un extrême à l'autre. Après avoir frôlé les 1000 dollars, la valeur du Zcash est retombée à moins de 100 dollars.

Crypto-monnaie et criminalité

Contrairement aux monnaies locales, qui ont plutôt bonne presse, l'image du public sur les crypto-monnaies reste plutôt négative. Le plus souvent anonymes, voire pour certaines intraçables, elles sont très souvent assimilées aux trafiquants actifs notamment sur le Darknet, face cachée d'Internet. Echappant aux régulations classiques des banques centrales (émettrices des monnaies traditionnelles), les crypto-devises serviraient notamment à blanchir de l'argent, à acquérir n'importe quel type de produits illégaux, à financer le terrorisme, voire même à servir de moyen simplifiant l'évasion fiscale. Aux Etats-Unis, une enquête menée par les agents de l'IRS (fisc américain) est par exemple en cours suite à de tels soupçons.

En Suisse, les autorités ne savent pas trop comment se positionner face à l'émergence de ces monnaies virtuelles. En juin 2014, un rapport concluait qu'il s'agissait d'un «phénomène marginal» et qu'il n'était pas nécessaire de légiférer. «Le Conseil fédéral entend néanmoins suivre de près l'évolution de la situation, afin de distinguer en temps utile l'apparition d'une telle nécessité.» Selon le Secrétariat d'Etat aux questions financières internationales, la position officielle n'a pas changé depuis, la surveillance de ce domaine relève de la FINMA.

Des coûts moins élevés

La question des coûts en jeu entre également dans la balance et contribue au succès de ces monnaies alternatives. Le comité du léman a ainsi imaginé le Lemanex pour permettre à une société en manque provisoire de liquidités par exemple de prendre un crédit à taux zéro.

L'intérêt financier est d'ailleurs le même pour les crypto-monnaies. «Elles sont moins coûteuses à utiliser en comparaison des prestations offertes par les acteurs traditionnels comme PayPal ou MasterCard», explique Arturo Bris, professeur de finance à l'IMD. Certains sont d'ailleurs convaincus qu'une monnaie comme le bitcoin débouchera sur une réduction drastique des coûts liés aux transactions, à l'exemple de Daniel Haudenschild, partenaire chez EY. Ce dernier évoquait dans une chronique parue dans Le Temps les fortes incitations financières en jeu, à commencer par «le caractère captif des transactions par carte de paiement».

Les Suisses restent fortement attachés à l'argent sous forme liquide

Mercredi matin, la Banque nationale suisse présente son tout nouveau billet de 20 francs. Dès le 17 mai, il rejoindra son grand frère vert dans les porte-monnaie… pour autant que les Suisses en utilisent encore. Face aux moyens de paiement digitaux à l'exemple de Paymit ou de Twint, aux 16 millions de cartes qui circulent dans le pays et aux crypto-monnaies qui se multiplient de plus en plus, l'avenir de l'argent sous forme liquide se pose.

Fin avril, la banque Mirabaud organisait une table ronde consacrée à cette thématique et concluait prudemment que les deux systèmes de paiement (cash et mobile) devraient être

amenés à se côtoyer. En tout cas durant encore un certain laps de temps. D'autres osent être plus affirmatifs, à l'exemple du CEO de la Deutsche Bank, John Cryan, qui affirmait à Davos il y a un an que l'argent physique n'existerait plus d'ici un laps de temps de dix ans. Pour le patron allemand, «il est quelque chose de terriblement inefficace et cher». Dans un bouquin paru l'année dernière, The Curse of Cash (La malédiction de l'argent liquide), l'économiste de Harvard, Kenneth Rogoff, abondait dans ce sens. «Un pays sans liquidités est une idée dont le temps est venu», affirme-t-il. Les statistiques actuelles leur donnent toutefois tort. Une récente enquête de MasterCard contredit en effet tous ceux qui imaginent la mort prochaine et surtout rapide de l'argent liquide. D'après l'émetteur de cartes de crédit, 85% des transactions des consommateurs du globe se font en cash.
En ce qui concerne la Suisse, la masse de monnaie en circulation augmenterait de manière constante d'année en année. D'après Cashless, une communauté regroupant les prestataires de cartes bancaires, seulement 23% des personnes interrogées lors d'un sondage seraient prêtes à renoncer définitivement aux pièces de monnaie et billets de banque.
Sur le long terme toutefois, la technologie pourrait finir par changer la donne et mettre bel et bien un terme à l'attachement des Suisses pour leur monnaie. Les smartphones et les montres sont en effet en train de s'imposer plus rapidement que prévu en Suisse comme porte-monnaie électroniques. Biberonnée au paiement mobile sans contact, la prochaine génération pourrait ainsi sonner le glas des bonnes vieilles coupures. (24 heures)
Créé: 10.05.2017
http://www.24heures.ch/vaud-regions/local-virtuel-argent-change-visage/story/30131897

L'ether,
Cette monnaie virtuelle qui veut rivaliser avec le bitcoin

Dans le monde, 90.000 comptes ont déjà été ouverts dans cette crypto-monnaie. Elle peut servir en ce moment à Paris à acheter les créations de jeunes artistes réunis dans une exposition conçue pour faire aussi œuvre de pédagogie.
C'est un programmeur canadien de 23 ans, Vitalik Buterin, passionné par le bitcoin, qui l'a inventée... L'ether est une monnaie virtuelle née seulement fin 2015, d'une technologie blockchain baptisée Ethereum et confiée à une fondation en Suisse. C'est un système proche de celui qui a permis l'essor du bitcoin, mais aussi une invention prise au sérieux. Microsoft, JP Morgan ou encore Intel se sont regroupés en mars dernier pour développer l'usage très prometteur d'Ethereum.
Moins sulfureuse que son grand frère, qui est, lui, très en vogue sur le «dark Web» (les activités illégales sur Internet), l'ether est l'unité de compte, la monnaie d'Ethereum. Cette blockchain crée sept ethers toutes les cinq minutes. Mais sur certains sites Internet, elle s'échange bel et bien contre des euros sonnants et trébuchants... à un cours très capricieux, comme celui du bitcoin, qui a connu plusieurs krachs financiers.

Un ether vaut 45 euros, mais le cours est volatil

Aujourd'hui, un ether (ETH) vaut environ 60 euros contre une dizaine d'euros il y a quelques mois. Le cours, qui dépend de l'offre et de la demande, est particulièrement volatil. Ouvrir un compte en ethers -90.000 ont été ouverts dans le monde-, y transférer des euros ou des dollars (par carte ou virement) pour acheter la crypto-monnaie, ou encore apprendre à se méfier des commissions de change (parfois 10% du montant converti) n'est pas si simple.
Pour faire connaître cette nouvelle monnaie qui veut changer les codes, de jeunes artistes ont donc accepté de participer à une exposition, à Paris, où leurs œuvres ne s'achèteront qu'en ether, jusqu'au 9 juin. À La Compagnie, dans le Xe arrondissement - un de ces lieux qui fleurissent dans la capitale pour promouvoir le coworking, héberger des start-up, et surfer sur

l'innovation-, à côté des photos, toiles et œuvres numériques de ces jeunes artistes, un coin pédagogique fournit les explications nécessaires aux acheteurs tentés par ces œuvres dont les prix, autour de 10 à 50 ethers, restent encore raisonnables. Et qui sont prêts à payer dans une monnaie numérique.
«C'est une première mondiale. L'ether fait son entrée dans le monde réel en permettant l'acquisition d'œuvres d'art»» raconte Christophe Pouilly, organisateur de l'événement, avec le soutien d'Ethereum France, l'association sans but lucratif qui veut démocratiser dans l'Hexagone la blockchain Ethereum.
http://www.lefigaro.fr/conjoncture/2017/05/03/20002-20170503ARTFIG00007-l-ether-cette-monnaie-virtuelle-qui-veut-rivaliser-avec-le-bitcoin.php

Le Bitcoin menacé par le Bilur ?

C'est l'une des premières alternatives au Bitcoin. Indexé sur la valeur du pétrole, la monnaie virtuelle « Bilur » pourrait bien séduire les utilisateurs encore réticents vis-à-vis des fluctuations incessantes des devises numériques.
Récemment introduite par la société londonienne R FinTech à Genève, la nouvelle monnaie virtuelle « Bilur » se positionne comme une alternative viable au Bitcoin, la célèbre crypto-monnaie qui avait autant séduit à ses débuts qu'elle n'avait essuyé de revers. Si les deux devises ne dépendant d'aucune banque centrale, le nouvel arrivant « Bilur » se base sur un réseau peer-to-peer en blockchain et possède la particularité d'être indexé sur le cours du pétrole, une première dans le monde des crypto-monnaies.
Afin de rattacher sa valeur à celle du pétrole, c'est près d'un million de barils stockés au Texas qui ont été achetés par R FinTech. Un Bilur correspond à peu de choses près à une tonne de pétrole, soit environ 6,5 barils. « Si on tient compte du prix moyen du baril de Brent depuis le début de l'année, un bilur vaut 356,45 dollars (326 euros). », explique la revue Challenges. L'idée étant d'acquérir davantage de pétrole à mesure que la nouvelle monnaie se développe.
Garanti par un bien physique, le « Bilur » reste difficile à contrôler, notamment en ce qui concerne les équivalences entre quantité de pétrole et nombre de « Bilurs » en circulation. De même, difficile de savoir si cette alternative s'avère être plus sécurisée que les autres devises numériques, souvent remises en cause pour leurs cours volatiles. Toutefois, le fait que le « Bilur » se base sur un bien physique et tangible pourrait contribuer à rassurer certains utilisateurs, déjà initiés à la monnaie virtuelle.
« Nous restons une crypto-monnaie, nous ne faisons que la soutenir avec quelque chose de réel », a expliqué Usama al Ali, directeur du développement de R Fintech**.**
http://www.ladn.eu/tech-a-suivre/blockchain/le-bitcoin-menace-par-le-bilur/

Une nouvelle monnaie virtuelle s'attaque au bitcoin

Une nouvelle monnaie virtuelle a été lancée mardi à Genève, avec pour ambition de concurrencer le bitcoin en adossant sa valeur sur les cours du pétrole, une première dans le secteur en développement des cryptomonnaies.
La devise, baptisée «bilur» et créée par la société londonienne R FinTech, vise à offrir une option alternative aux utilisateurs hésitants devant les fluctuations sauvages des monnaies numériques.

«C'est la première cryptomonnaie avec une vraie valeur», a déclaré Ignacio M. Ozcariz, PDG de la société, lors d'une conférence de presse.
Pour le lancement de cette monnaie, R FinTech et ses partenaires ont acheté un million de barils de pétrole, stockés au Texas. À chaque bilur correspond la valeur d'une tonne - soit 6,5 barils - au cours du jour, qui s'établit actuellement à 356 dollars US.
«Au fur et à mesure du développement du bilur, davantage de pétrole sera acquis, ses réserves stockées se chiffrant en milliards de barils», précise le communiqué de presse.
Contrairement aux devises physiques telles que l'euro ou le dollar, les cryptomonnaies comme le bitcoin ne dépendent d'aucune banque centrale: elles sont générées par des milliers d'ordinateurs dans le monde (un processus baptisé «minage»), et se vendent et s'achètent en ligne.
Le bitcoin, au cours très volatil, est accepté comme moyen de paiement par de nombreux sites internet et même certains commerçants physiques. Ses détracteurs lui reprochent toutefois de manquer de transparence et d'être l'instrument de trafics illégaux.
Le cours du bitcoin a atteint récemment un plus haut de 1400 dollars alors qu'il ne valait que quelques cents lors de son lancement en 2009.
Bilur vise à séduire une clientèle attirée par une monnaie virtuelle, mais qui se sentirait plus rassurée si elle était garantie par des biens tangibles, comme l'étalon or par exemple.
«Nous restons une cryptomonnaie, nous ne faisons que la soutenir avec quelque chose de réel», a expliqué Usama al Ali, directeur du développement de R Fintech.
La société se rétribuera en prélevant 0,01% par jour sur le montant détenu par l'investisseur, ce qui correspond à un peu plus de 3% par an.
Bilur signifie «chaîne» en basque, une allusion à la technologie Blockchain (chaîne de blocs) utilisée dans les cryptomonnaies, a précisé la société.
La société a choisi de lancer sa monnaie à Genève, car c'est «une des premières places mondiales pour le négoce et le financement du commerce international, notamment le pétrole».
http://www.lapresse.ca/techno/201705/02/01-5093912-une-nouvelle-monnaie-virtuelle-sattaque-au-bitcoin.php

Le bilur,
Une nouvelle monnaie virtuelle pour concurrencer le bitcoin

Le bilur, une nouvelle monnaie virtuelle, vient d'être lancée à Genève pour concurrencer le bitcoin. Sa valeur est adossée sur celle du pétrole. Mais cette indexation sur le cours du pétrole n'est pas synonyme d'absence de risque.
Et si vous payiez en bilur? Inutile de chercher la Bilurie sur une carte, ce pays n'existe pas. Mais le bilur, nouvelle monnaie virtuelle lancée hier à Genève, existe bel et bien. Il a été créé par une société londonienne, R Fintech comme alternative au bitcoin. S'il est le plus connu, le bitcoin n'est pas la seule la monnaie virtuelle. Peercoin, Namecoin, Litecoin sont d'autres monnaies virtuelles inspirées et similaires au bitcoin.
Le bilur est intrinsèquement différent. Le site R Fintech PLC indique que le bilur est une monnaie numérique, fondée sur un réseau de pair à pair en blockchain. A la différence des autres monnaies virtuelles, le bilur est indexé sur le pétrole. 1 bilur vaut une TEP (tonne équivalent pétrole), soit 6,481 barils de Brent. Si on tient compte du prix moyen du baril de Brent depuis le début de l'année, un bilur vaut 356,45 dollars (326 euros). Pour attacher la valeur du bilur à celle du pétrole, R Fintech a acheté un million de barils de pétrole, stockés au Texas. " Au fur et à mesure du développement du bilur, davantage de pétrole sera acquis, ses réserves stockées se chiffrant en milliards de barils ", indique le communiqué. Le bilur,

tout comme le bitcoin, ne dépend pas d'une banque centrale, mais il est garanti par un bien physique, un peu comme les premiers billets de banque reposait sur la quantité d'or détenue par l'Etat émetteur de la monnaie. Le bilur remplace " l'étalon or " par un étalon-pétrole. " Il est très difficile de créer un lien entre un bilur et un objet physique, explique Alexandre David, directeur des produits chez Eureka Certification. On ne peut pas contrôler a priori que la quantité de pétrole physique correspond au nombre de bilurs en circulation. "

Aucune garantie

Toutefois, comme aucune banque n'assure la contrepartie, il est difficile d'avoir la moindre garantie que le bilur offre une meilleure sécurité que le bitcoin. Il est vrai que bitcoin repose sur l'inviolabilité supposée de la blockchain et sur le fait que la masse monétaire atteindra un maximum de 21 millions d'unités. Théoriquement, la garantie pétrole offerte par le bilur devrait offrir une plus grande sécurité. Mais faute d'un organisme responsable, il n'est pas facile de comprendre qui interviendrait en cas de faillite du bilur.

Techniquement, le bilur repose sur la blockchain d'Ethereum, concurrente du bitcoin. Ce protocole utilise l'éther comme unité de compte, surtout utilisé pour payer les contrats intelligents. Il est soutenu notamment par Microsoft, Intel, JP Morgan Chase et d'autres banques. Mais le soutien de ces banques ne porte que sur l'aspect technologique d'Ethereum. Il n'a aucune valeur juridique ou financière. En outre, le protocole d'échange du bitcoin est totalement décentralisé alors que ce n'est pas le cas chez Ethereum. « L'environnement d'Ethereum apporte plus de facilité à la création de nouveaux services comme le bilur, précise Alexandre David, mais ces nouveaux systèmes sont en réalité centralisés, ce qui permet à une entreprise de se rémunérer sur les transactions. »

Un montage complexe

R Fintech PLC est une société britannique qui a installé des bureaux à Genève pour le lancement du bilur. Officiellement, elle a voulu se rapprocher des « meilleurs experts mondiaux des domaines que touche principalement bilur, les instruments financiers et les actifs énergétiques. » De fait, bilur est un ETF (exchange traded fund) un fonds indiciel coté. Les années 2000 ont vu fleurir nombre de produits financiers complexes, indexés sur des biens physiques. Certains, indexés sur des prêts immobiliers américains, ont été associés à crise de 2008. « Dans le cas du bilur, conclut Alexandre David, il faudrait pouvoir vérifier le livre blanc qui explique comment fonctionne le système et scruter le code. Mais pour l'instant il est très difficile d'auditer qui est derrière l'opération. ». Le 04.05.2017.

https://www.challenges.fr/high-tech/le-bilur-une-nouvelle-monnaie-virtuelle-pour-concurrencer-le-bitcoin_471032

Zcash la-nouvelle-monnaie-virtuelle-qui-monte

Lancé il y a sept mois, le Zcash, dernière née des monnaies virtuelles, connaît un succès inattendu, en raison de l'anonymat conféré à ses utilisateurs, mais cette opacité risque de rendre difficile son intégration dans le système financier.

Au lendemain de son lancement en octobre dernier, le cours du Zcash s'est envolé sur les plateformes d'échanges au point d'atteindre les 1.000 dollars l'unité, rivalisant ainsi avec le Bitcoin, pionnière des devises virtuelles créée en 2009. Elle fait maintenant partie des dix monnaies virtuelles les plus utilisées.

Si son cours s'est replié depuis, cette monnaie continue de susciter l'intérêt et a été adoptée par des consommateurs russes, chinois, vénézuéliens et dès ce 4 mai par les Sud-Africains. Les Brésiliens, eux, en usent déjà pour régler leurs factures d'électricité, leurs impôts et achats.

Pour faire son trou dans la galaxie des devises virtuelles, le Zcash se vante de "protéger la vie privée", ignorant ainsi la transparence exigée par les autorités qui veulent éviter que ces

monnaies électroniques servent à financer les activités criminelles telles blanchir l'argent sale, financer le terrorisme, l'évasion fiscale et la fraude.
Il s'appuie sur une technologie baptisée zk-Snark, permettant d'effectuer des transactions sans laisser de trace. Les données sont cryptées, mais les utilisateurs sont libres de s'affranchir de cet anonymat.

Piratage et contrefaçon

Si d'autres monnaies virtuelles (Dash et Monero) offrent la discrétion, Zcash va plus loin dans ce sens que le vendeur d'un bien ne peut pas refuser une vente quelle que soit la provenance de l'argent de l'acheteur. C'est tout le contraire du Bitcoin, dont la technologie blockchain permet d'enregistrer les moindres détails d'une transaction de sorte qu'il est possible d'identifier les utilisateurs car chacun d'eux dispose d'une adresse composée de lettres et de chiffres.
"On n'a pas toujours besoin d'exposer ses communications à des inconnus sur internet", défend Zooko Wilcox, PDG de Zcash Electric Coin Company, la société américaine gérant le Zcash. Il espère que la discrétion rattachée au Zcash pourra vaincre les réticences des entreprises à l'adopter comme alternative fiable aux monnaies contrôlées par les gouvernements.
Jonathan Levin, cofondateur de Chainalysis, une start-up aidant les banques et les autorités à traquer l'origine et la destination des fonds transitant par les monnaies virtuelles, doute que le Zcash puisse s'imposer dans le système financier classique.
"Il est difficile pour les institutions financières d'intégrer ce type de cryptomonnaies parce que l'information sur l'origine des fonds est très difficile à vérifier", déclare-t-il à l'AFP.
Les institutions financières traditionnelles ont commencé à s'intéresser au Bitcoin et plus particulièrement à sa technologie, la blockchain, seulement après la fermeture fin 2013 de Silk Road, un site internet qui permettait de régler les transactions en Bitcoins mais qui était devenu une plateforme d'échange de la drogue.
"Personne n'a encore utilisé le Zcash à des fins criminelles", défend Zooko Wilcox, tout en reconnaissant que "toutes les technologies peuvent être détournées".
M. Wilcox, qui affirme avoir le soutien d'un ancien procureur fédéral américain pour attester de la fiabilité du Zcash, a tenu en novembre une réunion virtuelle avec les autorités canadiennes et américaines pour les familiariser au Zcash. Leur réaction a été, affirme-t-il, "très pragmatique".
Le Zcash n'est par ailleurs pas à l'abri d'une attaque informatique ni protégé de contrefaçon, à l'instar de l'attaque informatique survenue en juin dernier contre la monnaie virtuelle Ethereum via sa plateforme DAO. Quelque 50 millions de dollars avaient été volés.
"Un hacker peut créer une fausse technologie zk-Snark" parce que des "incertitudes demeurent sur la solidité des paramètres de cryptographie", estime dans un blog Peter Todd, expert en monnaies virtuelles.
Consciente de ces risques, Zcash Electric, qui a levé 3 millions de dollars auprès de fonds, rémunère des hackers pour trouver des failles au Zcash, répond Zooko Wilcox.
Jusqu'à 21 millions de Zcash devraient être créés, dont 10% sont promis aux actionnaires de la société Zcash Electric (fondateurs, employés, investisseurs ...). AFP / 04 mai 2017.
https://www.romandie.com/news/Zcash-la-nouvelle-monnaie-virtuelle-qui-monte/793030.rom

Lutte contre les transactions financières illicites : La transparence et l'éthique comme parade

L'Amicale des inspecteurs des impôts et des domaines du Sénégal (Aiids) a organisé, vendredi, un diner-débat dont le thème était : « Transactions financières illicites : défis

normatifs et gestion des risques. » Au cours des échanges, il est ressorti que pour lutter contre les transactions financières illicites, la transparence et l'éthique demeurent les seuls gages de succès.

« Transactions financières illicites : défis normatifs et gestion des risques ». Ce thème a été au centre des échanges lors du diner-débat de l'Amicale des inspecteurs des Impôts et des Domaines du Sénégal (Aiids), organisé vendredi. D'éminents spécialistes ont fait des communications pointues sur cette problématique « complexe ». Dans son exposé aux allures d'un cours magistral, le Pr Abdallah Cissé, enseignant en droit des Affaires a mis l'accent sur le mécanisme opératoire des transactions financières illicites, le cadre juridique de la régulation et la gestion des risques liés à ces flux financiers. Pour le premier point, il a indiqué que les transactions financières illicites se situent à la frontière entre le licite et l'illicite. Selon lui, « il faut traiter la question avec beaucoup de rigueur, de minutie, de délicatesse et sous l'angle de la conformité pour éviter l'amalgame». En d'autres termes, il faut regarder d'un côté le licite et le transparent et de l'autre l'illicite et l'opacité pour retrouver des transactions financières illicites.

Dans la lutte contre ces flux financiers, le Pr Cissé a suggéré d'intégrer les « approches financière, économico-juridiques, de conformité, de politique criminelle et gestion de risque et de renforcer des systèmes de gouvernance et de management public ». « Il est nécessaire qu'il y ait un véritable leadership qui promeut l'éthique dans les transactions financières illicites car ; aujourd'hui, on dirige par l'exemple », a affirmé M. Cissé. Il estime que le Sénégal doit accorder une place de choix à la transparence, légiférer pour l'accès à l'information publique, élaborer une charte éthique dans les administrations et combiner le droit civil et commercial dans la lutte contre la corruption.

Systématisation et Rationalisation des stratégies de négociation

S'agissant de la gestion des risques, le Pr Cissé a indiqué qu'il faut l'identifier, l'apprécier et l'analyser. L'identification requiert, a-t-il rappelé, de la vigilance, en insistant sur la nécessité de disposer d'une bonne réglementation et d'un observatoire. Le conférencier a également plaidé pour une systématisation et une rationalisation des stratégies de négociation du Sénégal sur le plan international. Pour l'Agent judiciaire de l'État, Antoine Félix Diome, il a souligné que les acteurs empruntent toujours « l'apparence de la légalité et de la conformité ». « Ce sont des gens très ingénieux et organisés qui ont des relais là où il faut. Pour atteindre des résultats, il va falloir une synergie », a-t-il soutenu.

De son côté, le directeur de la Législation, des études et du contentieux, Amadou Abdoulaye Badiane, a insisté sur le contexte, les enjeux, les techniques et pratiques d'érosion de la base d'imposition utilisées dans les transactions financières illicites. Il a regretté le fait que les pays en développement subissent souvent de fortes pressions pour attirer les investisseurs par le jeu des incitations fiscales, avant de plaider le renforcement des capacités de l'administration fiscale.

Auparavant, la présidente de l'Amicale des inspecteurs des Impôts et des Domaines du Sénégal, Ndèye Aïssatou Ndao, a indiqué que les pays africains en développement auraient perdu plus de 1.000 milliards de dollars américains à cause des flux financiers illicites, ces 50 dernières années. Selon elle, le montant est l'équivalent de l'aide publique au développement reçue sur la même période. Pour limiter les pertes de recettes fiscales, elle a souhaité l'adoption de lois, de règlements et de politiques qui encouragent les transactions financières transparentes. Il importe, à son avis, de renforcer les capacités techniques des acteurs chargés d'appliquer ces lois et règlements.

Sur le plan international, a-t-elle relevé, il est nécessaire d'intensifier la coopération entre les États pour une plus grande transparence aussi bien dans les pays d'origine que ceux de destination des flux financiers.

http://www.lesoleil.sn/2016-03-22-23-21-32/item/63841-lutte-contre-les-transactions-financieres-illicites-la-transparence-et-l-ethique-comme-parade.html

Des hackers volent l'équivalent de 50 millions de dollars en monnaie virtuelle

Le fonds d'investissement victime de ce piratage a perdu un tiers de ses avoirs en "ether", une monnaie numérique concurrente du bitcoin.

Des pirates informatiques ont dérobé l'équivalent de plus de 50 millions de dollars de monnaie numérique à un fonds d'investissement expérimental justement créé pour prouver la fiabilité de ces crypto-monnaies, selon le *New York Times* samedi. La somme a été volée à la DAO (Decentralized Autonomous Organization), un fonds d'investissement qui avait collecté l'argent en ether, une monnaie numérique concurrente du bitcoin. Grâce à un projet de financement participatif, la DAO était parvenue à lever 150 millions de dollars afin de prouver l'invulnérabilité de cette technologie. Avec ce vol, elle a donc perdu un tiers de ses avoirs, un gros coup dur pour ce projet.

La technologie sur laquelle sont basées ces nouvelles monnaies dématérialisées est le « Blockchain », de plus en plus en vogue dans le monde de la finance où elle pourrait un jour trouver une utilité. Apparu en 2009 avec les monnaies virtuelles, le « Blockchain » est un code informatique généré par un logiciel de cryptage qui permet de transcrire des opérations financières effectuées en crypto-monnaies. Il permet de faire circuler l'argent aussi librement que les données sur Internet, un potentiel que veulent exploiter les établissements financiers. Toutefois, les informaticiens ont mis l'accent ces derniers mois sur les vulnérabilités des codes utilisés par le projet DAO, selon le *New York Times*.

Le cours de l'ether en chute libre

Vendredi, ses programmeurs hésitaient à simplement modifier leur code : cela leur permettrait de récupérer leur argent mais, ce faisant, ils renieraient le principe même qui conduit leur projet. « Je reconnais qu'il y a de solides arguments qui vont dans les deux sens, et il y aura de fortes oppositions, peu importe la direction que nous allons prendre », a reconnu sur le réseau social Reddit Vitalik Buterin, fondateur et programmeur du projet ether.

Le vol a en tout cas fait plonger le cours de l'ether vendredi. De la même manière, le bitcoin avait été sérieusement dévalorisé début 2014 quand Mt Gox, une des principales plateformes d'échange utilisant cette monnaie virtuelle, a fait faillite. Le patron de cette société, basée au Japon, avait alors expliqué avoir été victime d'une attaque informatique qui aurait entraîné in fine le vol ou la disparition d'une fortune en bitcoins. Source AFP

http://www.lepoint.fr/high-tech-internet/des-hackers-volent-l-equivalent-de-50-millions-de-dollars-en-monnaie-virtuelle-18-06-2016-2047800_47.php

Cybercriminalité. 9 000 serveurs infectés découverts par Interpol en Asie

Une opération contre la cybercriminalité menée par Interpol et les polices de sept pays d'Asie du Sud-Est a permis de mettre au jour près de 9 000 serveurs infectés par des virus, rapporte ce lundi Interpol.

« Cette opération a aidé les participants à identifier et à répondre à différents types de cybercriminalité auxquels ces pays ne s'étaient pas attaqués », a expliqué Francis Chan, chef

de l'unité de la police hongkongaise chargée de la lutte contre le cybercrime et président du groupe de travail Europe-Asie d'Interpol consacré à la cybercriminalité.
Plusieurs types de logiciels malveillants ont été repérés, certains utilisés pour obtenir des rançons en échange de données, d'autres commettants des attaques de déni de service ou diffusant des spams.
L'opération a également permis de voir que près de 270 sites internet étaient infectés par un logiciel malveillant, dont plusieurs sites gouvernementaux ayant pu contenir des données personnelles.
http://www.ouest-france.fr/monde/organismes-internationaux/interpol/cybercriminalite-9-000-serveurs-infectes-decouverts-par-interpol-en-asie-4947871

Interpol identifie près de 9000 serveurs infectieux en Asie

Les milliers de serveurs identifiés par Interpol peuvent servir à distribuer des malwares, des ransomwares ou lancer des attaques DDoS, notamment.
Ce pourrait être un gros coup prochainement porté à la cybercriminalité. Interpol a annoncé avoir identifié quelque 8800 serveurs de Commande et Contrôle (CC) répartis sur huit pays d'Asie du Sud-Est. Ces machines à la solde de pirates peuvent être utilisées pour lancer des attaques massives par déni de service (DDoS), des campagnes de spam/phishing, servir de centre de téléchargement de malwares, propager des ransomwares, etc.

270 sites piratés

Plus précisément, ces serveurs ont été créés à partir de près de 270 sites web infectés par du code malveillant exploitant une vulnérabilité dans la conception des sites, indique l'organisation internationale de lutte contre la criminalité dans son communiqué. Des sites gouvernementaux, qui détiennent potentiellement des données personnelles de citoyens, font partie des victimes, ajoute l'institution dont l'enquête a été confiée à la division IGCI (Interpol Global Complex for Innovation) dédiée aux technologies informatiques.
A titre d'illustration, Interpol déclare avoir notamment identifié des opérateurs de phishing, dont un affiche des liens vers le Nigeria. Un autre, basé en Indonésie, vend des kits d'hameçonnage sur le Darknet et a même posté des modes d'emploi de ses outils sous formes de vidéos Youtube. L'enquête se poursuit sur les activités des serveurs CC, ajoute l'organisation policière.

23 rapports

Interpol souligne l'importance de la coopération internationale, ainsi que celle avec des entreprises privées, pour mener à bien ce type d'enquête. Les informations ont ainsi été remontées suite à des enquêtes effectuées localement en Indonésie, Malaisie, Birmanie, Philippines, Singapour, Thaïlande et Vietnam. La Chine a également contribué à l'effort en fournissant des renseignements. Et des experts d'entreprises privées (Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet et Palo Alto Networks) ont aidé Interpol à préparer les repérages. *« Le partage d'information a été la base du succès de cette opération »,* explique Noboru Nakatani, responsable de l'IGCI, qui y voit un facteur essentiel dans l'efficacité de la coopération à long terme et dans l'activité quotidienne de contre la cybercriminalité.
Un travail de longue haleine qu'Interpol se garde de détailler. D'autant que l'opération n'est pas terminée. Il reste à mettre fin à l'exploitation de ces quelque 9000 serveurs infectés toujours en service, le rôle de l'organisation anti-criminelle s'étant pour l'instant limité au travail d'enquête. Un travail qui est concrétisé par la rédaction de 23 rapports détaillant les activités illégales constatées et suggérant les actions à prendre en conséquence. Actions qui ressortent désormais de la seule volonté des autorités nationales des pays concernés.

http://www.silicon.fr/interpol-identifie-9000-serveurs-infectieux-asie-173079.html

Interpol s'entraîne à combattre le darknet

L'organisation internationale de police criminelle crée son propre darknet, sa crypto-monnaie et ses marchés souterrains. Le but : former des policiers appelés à combattre le crime organisé.

Du 27 au 31 juillet 2015, des policiers de onze pays (France, Pays-Bas, Suède, Finlande, Ghana, Sri Lanka, Singapour, Indonésie, Hong Kong, Japon et Australie) ont été invités par Interpol à suivre une formation centrée sur le darknet, réseau privé accessible via un réseau superposé comme Tor ou I2P.

Le programme a été concocté par le nouveau Complexe mondial Interpol pour l'innovation (CMII) de Singapour et l'Organisation néerlandaise pour la recherche scientifique appliquée **(**TNO). Pour l'occasion, le Cyber Research Lab d'Interpol a créé son propre darknet privé, sa crypto-monnaie et ses places de marché souterraines, recréant ainsi le même type d'environnement virtuel qu'utilisent les cybercriminels – et bien d'autres – pour échapper à la détection.

Platforme privilégiée du crime organisé

« Le darknet devient la plateforme de transaction préférée des individus et des réseaux du crime organisé pour mener des activités illicites, les crypto-monnaies étant le moyen privilégié pour payer ces services », a déclaré Madan Oberoi, directeur de l'unité Cyber Innovation d'Interpol. *« La formation spécialisée fournie par Interpol donne aux forces de l'ordre les outils nécessaires pour mener des actions bien réelles ciblant les criminels dans le monde virtuel. »* Le temps de la formation, les participants jouent les vendeurs, les acheteurs ou les administrateurs pour mieux comprendre les stratégies à l'oeuvre.

Une prochaine session est prévue à Bruxelles, en novembre 2015. Cette initiative d'Interpol fait suite à l'opération internationale de police Onymous menée contre plus de 400 services du darknet, dont Silk Road 2, vendant des marchandises illégales.

http://www.silicon.fr/interpol-entraine-combattre-darknet-123139.html

Hornet,
Un réseau d'anonymisation à la mode Tor en haut débit

Des chercheurs ont mis au point un outil d'anonymisation du trafic similaire à Tor, baptisé Hornet. Il reprend les éléments de sécurisation de son homologue, mais avec des débits beaucoup plus élevés.

Traduit en français par « frelon », le terme anglais « hornet » a d'autres acceptions. Illustration en sécurité IT : une équipe de chercheurs basée entre Londres et Zurich l'utilise tout en capitales (HORNET**)**, comme acronyme pour « High-speed Onion Routing at the NETwork layer »).

Derrière cette appellation se cache une technologie **d'**anonymisation du trafic sur les réseaux informatiques. Sa particularité : elle associe le haut niveau de sécurité d'une solution comme Tor aux performances de protocoles tels que LAP et Dovetail.

Les expérimentations menées sur un routeur logiciel d'une capacité maximale de 120 Gbit/s ont permis de transmettre des données à un débit de 93,5 Gbit/s ; soit près de 12 Go à la seconde. De quoi satisfaire très largement des activités comme la navigation Internet et la messagerie instantanée.

C'est précisément à ces usages que se destine HORNET, le principal objectif étant de protéger les utilisateurs contre les tentatives d'écoute, y compris celles qui émanent d'entités dotées d'une grande force de frappe – typiquement, les agences de renseignement.
Le timing de publication du rapport (document PDF de 15 pages daté du 21 juillet 2015) est idéal si l'on considère d'une part que la conscience du public à l'égard du cyber-espionnage s'éveille au fil des révélations d'Edward Snowden. Et de l'autre, que de nombreux États légifèrent actuellement pour renforcer leurs pouvoirs en la matière.

Du Tor amélioré ?

En termes de sécurité, HORNET est dit résistant aux attaques passives. Ses créateurs se sont notamment assurés qu'un tiers cherchant à écouter du trafic ne puisse pas déterminer d'où provient la communication, ni quelle est sa destination (concept baptisé « end-to-end unlinkability » en anglais »).
Parmi les autres garanties évoquées, l'impossibilité pour des tiers de modifier les en-têtes de paquets sans être détectés ou encore de faire le lien entre différentes sessions de connexion.
Sur le volet des performances, le défi est le suivant : comment accélérer la transmission de données sachant alors que la nature même des protocoles d'anonymisation, avec leurs opérations de chiffrement répétées, ne s'y prête pas ?
A l'instar de Tor, HORNET chiffre les données par cryptographie symétrique en s'appuyant de façon aléatoire sur les différents nœuds (serveurs, passerelles) qui composent le réseau. Mais il traite différemment les informations de routage au niveau des nœuds intermédiaires (ceux situés entre le client et le serveur), de sorte qu'ils peuvent rediriger plus rapidement le trafic.
Les chercheurs pointent aussi du doigt les limites de Tor en matière de montée en charge. Pour résoudre ce problème, le protocole HORNET, tout comme LAP et Dovetail, ne se superpose pas à la couche réseau : il s'y intègre, souligne ITespresso.
A défaut de tests plus poussés par la communauté, on restera prudent sur l'avancée concrète que représente HORNET. Non sans se demander si les réseaux exploités commercialement proposeront un jour l'anonymisation du trafic par défaut…
http://www.silicon.fr/hornet-un-reseau-danonymisation-a-la-mode-tor-en-haut-debit-122583.html

Renseignement : Le Royaume-Uni réessaye de légiférer

Le Communications Data Bill, qui doit réformer la surveillance au Royaume-Uni, devrait faire l'objet d'une nouvelle présentation cet automne devant le Parlement.
Se dirige-t-on vers l'entrée en vigueur, à l'horizon 2016, d'une loi sur le renseignement au Royaume-Uni ? Présenté pour la première fois au Parlement en 2012 par la secrétaire d'État à l'Intérieur Theresa May, le Communications Data Bill – document PDF, 123 pages – est encore, à l'heure actuelle, un projet de loi. Ses défenseurs ont déjà essuyé plusieurs échecs, notamment un blocage en 2013 par les libéraux-démocrates.
Le postulat est le suivant : depuis des années, les services de police et de renseignement s'appuient sur les communications électroniques pour lutter contre la criminalité et le terrorisme. Mais avec l'émergence de nouvelles technologies, il est devenu plus difficile d'accéder à ces données. Au sens de « Communications Data », il convient plutôt de parler de métadonnées. Par opposition au contenu même des communications, il s'agit d'éléments annexes, généralement contextuels. Non seulement à propos de l'utilisateur du service (nom, adresse…), mais aussi sur la communication en elle-même : heure, durée, localisation, etc.

Pour le moment, au Royaume-Uni, toute organisation est tenue de conserver les données qu'elle produit et/ou traite, uniquement si son activité en dépend. Les autres informations, tout particulièrement les communications des utilisateurs chez les opérateurs télécoms et fournisseurs de services Internet, ne sont pas soumises à des exigences de conservation.
Ces exigences pourraient être durcies sous le régime du Communications Data Bill, le texte devant faciliter la disponibilité des métadonnées tout en clarifiant les procédures d'obtention par les autorités compétentes, selon ITespresso.
Ce qui impliquera la modification de plusieurs lois, dont le Regulation Investigatory Power Act 2000 (partie 1, chapitre 2), lequel définit les pouvoirs des organes publics pour mener des opérations de surveillance et intercepter des communications dans le pays.

Le retour de la boîte noire

Le Communications Data Bill rencontre encore une farouche opposition, y compris dans la classe politique, dont la méfiance s'est illustrée dernièrement par le rejet de l'initiative de plusieurs sénateurs qui avaient tenté de faire ajouter le texte au Counter-Terrorism and Security Bill.
Plusieurs volets du texte cristallisent les tensions. Non seulement le fait que les entreprises devraient conserver pendant 12 mois toutes les données produites et traitées par leurs soins (e-mails, appels, navigation web…), qu'elles en aient ou non besoin pour développer leur activité. Mais aussi et surtout la notion du « Deep Packet Inspection » (DPI).
Cette dernière se retrouve dans le projet de loi sur le renseignement en France : elle consiste en l'installation, chez les fournisseurs de services, de « boîtes noires », dispositifs censés être placés sur les réseaux pour détecter, via des algorithmes, des comportements suspects.
A en croire les services britanniques, ces « boîtes noires » ne seraient utilisées que si une entreprise refuse de fournir les données. Elles seraient en outre déjà activement exploitées chez de nombreux fournisseurs de services, en remplacement d'un système centralisé dont la mise en place aurait échoué il y a quelques années.
Connu sous le sobriquet «Snoopers' Charter» (que l'on peut traduire par «loi des fouineurs »), le Communications Data Bill pourrait faire l'objet d'une nouvelle présentation devant le Parlement à l'automne. A condition de dissiper les craintes de nombreux élus sur la question du croisement des données.
Les associations de défense des libertés civiles à l'ère numérique (Big Brother Watch, Liberty, Open Rights Group) s'inquiètent aussi des abus éventuellement associés à cette démarche. Elles redoutent qu'une « énorme base de données » soit constituée… et qu'elle représente une mine pour les pirates informatiques, qu'ils soient ou non à la solde d'États.
Dresser ainsi des profils précis d'individus pose aussi la question de la protection des sources journalistiques et des lanceurs d'alertes. L'opinion publique n'y est pas insensible : selon un sondage YouGov, seuls 12 % des Britanniques perçoivent un réel bénéfice au Communications Data Act.
http://www.silicon.fr/renseignement-le-royaume-uni-reessaye-de-legiferer-121719.html

Payer une rançon pour récupérer ses données informatiques : une escroquerie qui prend de l'ampleur

Attention, soyez prudents et attentifs! De nouveaux problèmes informatiques sont en train de se répandre petit à petit sur vos écrans... Dans ce cas-ci, vous pouvez recevoir un mail, et en cliquant sur le lien, toutes vos données sont rendues inaccessibles. Et pour les récupérer, vous allez devoir payer une rançon. C'est une escroquerie qui arrive de plus en plus souvent, et qui

prend de l'importance dans notre pays. Il y a eu 275 victimes fin 2015 et 6261 fin 2016. Il est donc grand temps de se méfier!
La méthode de contamination va toujours s'appuyer sur deux éléments : notre inquiétude ou notre curiosité. L'idée étant évidemment de nous pousser à cliquer. Ce mail que beaucoup de gens ont reçu contient un lien Dropbox et le lien se termine par une extension zip. C'est donc un fichier compressé. Lorsqu'on clique pour l'ouvrir, le virus va alors s'installer.
Ou alors c'est un message provenant d'une structure connue comme bpost et qui vous explique qu'un colis a été présenté à votre adresse et qu'il n'a pas pu être livré. On vous invite ensuite à suivre un lien.

Un processus qui se déclenche après avoir cliqué sur un lien

Toutes vos données vont être cryptées et un compte à rebours va apparaître, vous expliquant que pour récupérer vos données, vous allez devoir payer une rançon. Nombreux sont ceux qui, paniqués, vont payer. Sauf qu'ils ne recevront jamais la clé promise...
Le problème de cette criminalité, c'est qu'elle a un caractère international très marqué et qu'il n'est pas toujours évident de se procurer les outils permettant de récupérer les données qui ont été cryptées.

"No More Ramson"

Il existe le projet "No More Ramson", qui est une initiative de l'unité spécialisée en criminalité informatique de la police néerlandaise, mais aussi de son équivalent au sein d'Europol. Et ce projet est mené avec deux sociétés spécialisées en sécurité informatique. L'objectif est clairement d'aider les victimes de ces logiciels rançonneurs à récupérer leurs données chiffrées sans avoir à payer de rançons aux délinquants.
La police belge a récemment rejoint le projet afin de permettre de communiquer les situations rencontrées par des victimes de notre pays mais aussi de pouvoir informer ces victimes de l'existence de solutions.
Comme il est aussi plus facile de prévenir la menace que d'y répondre une fois que l'ordinateur est infecté, le projet vise également à éduquer les utilisateurs sur la façon dont fonctionnent les logiciels rançonneurs et quelles contre-mesures ils peuvent adopter pour empêcher les attaques. En plus de ces conseils de prévention, le site met à votre disposition une multitude d'outils qui vous permettront peut-être de récupérer vos précieuses données ...

Conservez les supports touchés et faites régulièrement des sauvegardes

Les recherches autour des logiciels utilisés sont constantes et donc, si vous êtes victime de cette forme de criminalité numérique, conservez les supports qui ont été touchés car il n'est pas impossible qu'une bonne nouvelle puisse vous parvenir dans quelques mois. Veillez également à effectuer régulièrement des sauvegardes de toutes vos données, mais surtout, ne laissez pas le disque connecté en permanence car, dans ce type d'attaque, le virus va aussi toucher les supports externes!
https://www.rtbf.be/info/societe/onpdp/detail_payer-une-rancon-pour-recuperer-ses-donnees-informatiques-une-escroquerie-qui-prend-de-l-ampleur?id=9595385

WannaCrypt : Un outil de déchiffrement est en cours de conception

La riposte s'organise face à WannaCrypt. Alors que la propagation du rançongiciel (ou ransomware) a pu être stoppée par hasard, les autorités et les sociétés de sécurité informatique travaillent désormais sur un outil permettant de déchiffrer les fichiers et les dossiers qui ont été verrouillés.
L'attaque a été fulgurante vendredi 12 mai. Le rançongiciel WannaCrypt (aussi connu sous d'autres noms comme WannaCry et WanaCrypt0r) a en l'espace d'un week-end réussi à se

propager dans le monde entier, faisant 200 000 victimes réparties dans 150 pays. Jamais un logiciel malveillant de cette nature ne s'était diffusée de la sorte. Mais aujourd'hui, la riposte s'organise.

Cité par la BBC, le porte-parole d'Europol a déclaré qu'un outil de déchiffrement était en cours de conception pour permettre aux personnes, entreprises et administrations qui sont affectées par WannaCrypt. Rappelons que ce programme verrouille des fichiers et des dossiers dans l'ordinateur et demande ensuite à son propriétaire de payer une rançon pour y avoir de nouveau accès. En théorie.

Le 13 mai, Europol indiquait déjà dans un communiqué de presse que son centre européen de cybercrime (EC3, pour European Cybercrime Centre) était « *en train de travailler en étroite collaboration avec les unités de lutte contre cybercriminalité des pays touchés et les principaux partenaires de l'industrie pour atténuer la menace et venir en aide aux victimes* ».

A priori, l'outil de déchiffrement sera diffusé sur No More Ransom quand il sera prêt. Il s'agit d'une plateforme lancée l'an dernier par Europol, Intel Security, la police des Pays-Bas et Kaspersky Lab pour favoriser la coopération entre les forces de l'ordre et les entreprises du secteur privé — principalement celles fournissant des logiciels antivirus — pour apporter une réponse unifiée face aux rançongiciels.

On peut supposer que la propagation de WannaCrypt va donner un formidable coup d'accélérateur à la notoriété et aux moyens à disposition de No More Ransom, qui peut d'ores et déjà s'appuyer sur une collection déjà étendue d'outils capables de neutraliser divers de ces logiciels malveillants en cas d'infection et sur de nombreux contributeurs, avec l'arrivée de partenaires supplémentaires.

Repéré en premier lorsqu'il a infecté des hôpitaux britanniques, WannaCrypt s'est par la suite propagé à toute vitesse dans le monde entier. Face à cette menace, il existe des parades, à commencer par faire des sauvegardes très régulières sur des supports amovibles et par maintenir son système d'exploitation à jour. L'affaire a également posé la question du rôle trouble du gouvernement américain.

http://www.numerama.com/tech/258017-wannacrypt-un-outil-de-dechiffrement-est-en-cours-de-conception.html

Ransomware WannaCrypt : un chercheur aurait trouvé comment ralentir sa propagation

Par accident, un chercher en sécurité informatique a réussi à ralentir la diffusion du rançongiciel "Wannacrypt", selon plusieurs médias dont Le Monde et The Guardian. Ce ransomware s'est diffusé dans plusieurs dizaines de pays, organisations et entreprises en quelques heures, créant la surprise et le désordre dans certains cas.

Ce chercheur, connu sous le nom de MalwareTech sur Twitter, a en fait découvert ce qui semble être un mécanisme de sécurité dans le code du virus, qui aurait été intégré par les développeurs du ransomware afin d'arrêter sa propagation en cas de problèmes.

En analysant le code, MalwareTech a découvert que le virus devait se connecter à une adresse internet lors de sa diffusion. Si le site répondait qu'il était inaccessible, alors le rançongiciel pouvait se propager. Comme le nom de domaine de ce site était à vendre, le chercheur l'a acheté, donc il a été rendu disponible lors de la connexion.

La condition d'inaccessibilité n'étant plus remplie pour le virus, celui-ci ne continue plus sa propagation. Mais les ordinateurs infectés sont toujours bloqués, l'arrêt de l'expansion du virus ne permettant pas l'accès aux données déjà cryptées. MalwareTech explique plus en détails sa démarche sur son site internet.

https://www.rtbf.be/info/medias/detail_ransomware-wannacrypt-un-chercheur-aurait-trouve-comment-ralentir-sa-propagation?id=9604967

La lutte contre la cybercriminalité : Les premières décisions de la justice sénégalaise

Depuis 2008, le Sénégal s'est engagé résolument sur la voie de la lutte contre la cybercriminalité, c'est-à-dire toutes les infractions commises par l'entremise des outils technologiques. En effet, à cette date, une vaste réforme a permis de doter notre pays d'un ensemble de textes de lois, notamment la loi n° 2008 – 11 du 25 janvier 2008 portant sur la cybercriminalité. Aujourd'hui, l'application de ce texte a été à l'origine de plusieurs décisions prononcées par les juridictions sénégalaises. Voici brièvement commenter les toutes premières décisions inédites.

Ayant pris conscience qu'un nombre grandissant de délinquants utilisent désormais les nouvelles technologies pour commettre leur forfait et n'attendent plus leurs victimes, à l'instar des agresseurs dakarois, au coin des rues, les autorités ont mis à la disposition des enquêteurs et des magistrats des outils et des mécanismes qui règlementent et régulent l'activité cybercriminelle. L'utilisation des Technologies de l'Information et de la Communication (TIC) implique, cela va de soit, des risques. Plus la dépendance aux nouvelles technologies augmente, plus le degré de vulnérabilité des utilisateurs est élevé. Mais, est-ce une raison de renoncer à des droits universellement reconnus. La réponse des magistrats sénégalais, après un travail très professionnel de nos enquêteurs, confirme le contraire.

Dans le jugement n° 3375 du 29 juillet 2009, le Tribunal Régional Hors Classe de Dakar a statué sur une tentative d'escroquerie par le biais d'un système informatique. En l'espèce, il s'agissait de condamner les agissements d'une personne, qui utilisant les nouvelles technologies (un site web et des SMS), proposait des relations sexuelles en contrepartie d'une offre d'emploi. Ce jugement met en évidence la question de l'escroquerie de service et exclut les « relations sexuelles » du champ d'application des services visés par l'article 379 bis du Code pénal. Cette décision fait partie des toutes premières applications de la loi sur la cybercriminalité.

La question du respect de la confidentialité sur internet étant de plus en plus importante, le Tribunal Régional Hors Classe de Dakar a prononcé un jugement relatif au secret des affaires. Dans la décision n° 4241/ 09 du 18 septembre 2009, le juge a condamné un prévenu pour avoir accédé frauduleusement à tout ou partie d'un système informatique. En l'espèce, il est reproché au prévenu d'avoir accédé à l'ordinateur d'un collègue et d'envoyer dans sa propre boîte électronique une copie de données de nature commerciale. En application de l'article 431-8 de la loi sur la cybercriminalité, le juge, pour condamner le prévenu à trois mois d'emprisonnement assorti du sursis, soulève l'absence d'une autorisation du propriétaire de l'ordinateur. Ce constat matérialise le caractère frauduleux de tout accès à un système informatique sans autorisation du responsable. Toujours, dans la même affaire, le prévenu, poursuivi également pour entrave au fonctionnement d'un système informatique, a été relaxé au motif que « le simple changement d'un mot de passe sur un ordinateur n'est pas de nature à caractériser le délit d'entrave qui suppose l'accomplissement d'actes tendant à la paralysie effective du système d'information ». Ce qui n'était pas le cas dans cette affaire. Dans ce jugement, le juge assimile d'une part un ordinateur isolé à un système informatique et d'autre part procède à une conceptualisation des notions « d'accès » ou « d'entrave » au fonctionnement du système informatique.

Par ailleurs, l'escroquerie sur Internet étant le sport favori des cybercriminels, ce délit a été jugé dans l'affaire en date du 21 janvier 2010 par les magistrats du Tribunal Régional Hors

Classe de Dakar en application de l'article 431-16 de la loi sur la cybercriminalité. C'est l'affaire du réseau anglophone de cybercriminels démantelé en 2009 par les éléments de la Division des investigations criminelles. Ces cyber bandits émettaient à partir de leurs boîtes électroniques des messages faisant état, entre autres, de transactions financières fictives ou d'appels de détresse provenant de prétendus héritiers voulant sauver leur fortune ». Il s'agit d'un exemple de l'arnaque, communément appelée par les spécialistes, la « fraude 419 » ou le « scam 419 » qui consiste à abuser de la crédulité de certaines personnes, attirées par l'appât d'un gain facile, pour leur soutirer de l'argent. La dénomination 4-1-9 vient du numéro de l'article du code pénal nigérian sanctionnant ce type de fraude. Dans cette affaire, le juge, relaxant les prévenus uniquement sur ce délit, précise que « l'infraction d'escroquerie via internet n'était consommée que si l'auteur avait reçu un avantage ». Ce que l'enquête n'avait pas établi. Aussi, la tentative d'escroquerie sur Internet n'a pas été prévue dans la loi sur la cybercriminalité. Dès lors, ce manquement doit être corrigé lors des prochaines réformes de ce texte. Cependant, l'application de l'article 431-14 de la loi sur la cybercriminalité aux mêmes faits aurait permis, peut être, de condamner les prévenus « pour avoir produit ou fabriqué un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales ».

Enfin, dans une autre affaire jugée le même jour, à savoir, le 21 janvier 2010, les mêmes juges ont poursuivi un prévenu pour avoir accédé, grâce à des cartes bancaires dupliquées, aux terminaux de paiement électronique d'une grande banque de la place. Cet accès frauduleux à un système informatique, en application de l'article 431-8 de la loi sur la cybercriminalité, sera sanctionné par un emprisonnement de cinq ans ferme et une amende de 500 000 FCFA à l'encontre de l'auteur des faits.

En définitive, la cybercriminalité est désormais une réalité sous nos tropiques et sous de nombreuses facettes. Le travail des magistrats, ainsi que celui des policiers et gendarmes, commence à porter ses fruits. Il est encourageant de voir que le Sénégal est entré de plain pied dans la société de l'information et arrive à répondre aux défis rencontrés. Toutefois, pour être plus efficace contre cette cible mouvante et transfrontalière, il faut, en plus des actions actuelles au niveau national (pourquoi pas la mise en place d'un service spécialisé avec des policiers, gendarmes et magistrats), une réponse internationale à la menace tout aussi internationale. A cet effet, l'adhésion du Sénégal, à la Convention de Budapest de 2001 sur la cybercriminalité, le seul instrument international en la matière, est une piste à explorer par nos autorités afin de bénéficier d'une coopération policière et judiciaire au delà de nos frontières.

http://www.pressafrik.com/La-lutte-contre-la-cybercriminalite-les-premieres-decisions-de-la-justice-senegalaise_a40664.html