وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م ا 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°92

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

Fintech : Lemon Way sanctionnée pour des failles dans sa lutte contre le financement du terrorisme

L'Autorité de contrôle prudentiel (ACPR) a sanctionné la Fintech à 80.000 euros d'amende. L'établissement de paiement a failli dans la mise en oeuvre des normes de lutte contre le blanchiment d'argent et le financement du terrorisme en 2015.

Le discours de fermeté des autorités financières vis-à-vis des trublions de la finance se traduit désormais dans les faits. En témoigne la sanction infligée à l'établissement de paiement Lemon Way, spécialisé dans la collecte de paiements pour le compte de plateformes de financement participatif et des sites d'e-commerce . La jeune pousse qui vient de passer le cap des 3 millions de clients et qui se revendique « *première Fintech de l'Hexagone en nombre de clients particuliers* » a reçu fin mars un blâme du gendarme bancaire (Autorité de contrôle prudentiel et de résolution - ACPR) assorti d'une amende de 80.000 euros.

Des manquements repérés par le gendarme financier en 2015

Les griefs à l'encontre de la Fintech - spécialisée à l'origine dans le paiement de personnes à personnes et les prestations de paiement pour de opérateurs de bitcoins - sont nombreux. Mais ils se concentrent sur des manquements dans la connaissance de ses clients qui ont été identités mi-2015. « *50 clients n'ont pas été identifiés alors qu'ils ont utilisé les services de paiement de Lemon Way par l'intermédiaire d'un site de financement participatif, les noms et prénoms renseignés étant fantaisistes* », indique le gendarme bancaire dans sa décision rendue publique début avril.

Plus préoccupant, Lemon Way a failli dans la mise en oeuvre des normes de lutte contre le blanchiment d'argent et le financement du terrorisme. « *Les procédures internes de Lemon Way ne prévoient la détection des personnes politiquement exposées que si le montant des opérations dépasse 100.000 euros par an* ». Un niveau bien trop haut pour détecter les comportements suspects puisqu'en 2015, « *le panier moyen des investisseurs français se situe en-dessous de 200 euros par investisseurs* », relève encore l'ACPR.

Les plate-formes de bitcoins concentrent les dossiers douteux

Enfin, aux yeux du régulateur, la Fintech a aussi manqué à ses obligations de déclaration de soupçon à TracFin . Vingt dossiers sont ainsi pointés du doigt : « *14 de ces dossiers concernaient des opérations effectuées pour des montants significatifs, de 20.000 à 190.000 euros ; Lemon Way ne connaissait ni l'origine des fonds utilisés pour l'achat des bitcoins, ni à l'inverse, les circonstances dans lesquelles les clients étaient entrés en possession des bitcoins cédés* ».

Depuis, la Fintech a corrigé le tir, « *elle a interrompu ses relations d'affaires avec plusieurs sites et actualisé ses procédures en matière de déclaration de soupçon* », indique l'ACPR. Mais Lemon Way a aussi fait évoluer son modèle et proscrit les activités de paiement en bitcoin qui étaient « *à l'origine de 80% de ses dossiers douteux* », indique Damien Guermonprez, directeur général de Lemon Way. «*Dans notre grande naïveté nous pensions que faire entrer le bitcoin dans l'économie régulée permettait de mieux le contrôler mais en 2015, notre société ne comptait que 12 personnes et était peu outillée pour gérer ces questions. Aujourd'hui nous sommes sept fois plus nombreux et un quart des effectifs s'occupent de contrôle. C'est notre priorité* », assure Damien Guermonprez.

https://www.lesechos.fr/finance-marches/banque-assurances/0211983758698-fintech-lemon-way-sanctionnee-pour-des-failles-dans-sa-lutte-contre-le-financement-du-terrorisme-2080450.php

Cybercriminalité : Les outils gratuits de piratage sont une porte d'entrée pour les adolescents,

61 % des pirates auraient commencé avant 16 ans.

L'organe principal de lutte contre les crimes organisés au Royaume-Uni en l'occurrence la National Crime Agency (NCA) a publié son rapport intitulé *Pathways into Cybercrime* et dans lequel il met en évidence la montée en puissance des adolescents dans le domaine de la cybercriminalité. Dans son rapport, la National Crime Agency tire la sonnette d'alarme sur le fait que les nombreux outils gratuits de piratage (les services de DDOS, les chevaux de Troie, etc.) qui sont disponibles sur Internet constituent une véritable porte d'entrée pour les adolescents dans la cybercriminalité. Cette situation est également accentuée par le fait que beaucoup de ces outils sont disponibles sur des forums de modding ou de jeux avec souvent des liens qui pointent vers des tutoriels qui facilitent leur prise en main. L'utilisation de ces outils de piratage ne demande pas souvent des compétences techniques très pointues. « *La barrière des compétences pour intégrer le domaine de la cybercriminalité est*

aujourd'hui très faible. Les outils de piratage, qui pour être utilisés ne nécessitent pas une expertise technique assez avancée, sont disponibles soit gratuitement, soit à faible coût pour les utilisateurs. Beaucoup de ces outils illégaux sont annoncés ouvertement sur des forums de piratage ou de jeux, et les tutoriels vidéo ou bien didacticiels sur la façon de les utiliser étape par étape sont facilement accessibles sur la toile », a déclaré la National Crime Agency.
Selon la National Crime Agency, au Royaume-Uni, près de 61 % des pirates informatiques ont commencé à commettre des forfaits à l'âge de 16 ans. Il ajoute que durant l'année 2015, les résultats des enquêtes menées par l'unité spéciale de lutte contre la cybercriminalité au Royaume-Uni à savoir la National Cyber Crime Unit (NCCU) ont montré que la moyenne d'âge des suspects et des pirates informatiques qui ont été mis aux arrêts est de 17 ans. Au même moment, l'âge moyen des pirates arrêtés dans des affaires de trafics de médicaments est de 37 ans, alors que celui des pirates impliqués dans des affaires relatives à la cybercriminalité économique est de 39 ans.
La NCA soutient également dans son rapport que le gain financier n'est pas nécessairement l'élément qui motive les jeunes pirates. Ces derniers seraient également motivés par le besoin de renforcer leur réputation au sein de la communauté dans laquelle ils évoluent ; à cela s'ajoute l'anonymat sur Internet que les outils de piratage sont censés leur garantir.
Le rapport fait également état de l'absence d'une application de la loi au Royaume-Uni et que la plupart des jeunes qui sont impliqués dans des actes relatifs à la cybercriminalité ignorent que ce qu'ils font rentre dans le cadre de l'illégalité. « *Un membre d'un groupe de pirate qui a vendu des outils DDoS et des services de botnet a déclaré à la police qu'un avertissement de l'application de la loi l'aurait empêché d'exercer cette activité* », a affirmé la National Crime Agency. Cette dernière précise que son rapport est basé sur des entretiens avec des jeunes cybercriminels afin de connaître le pourquoi ils sont entrés dans la cybercriminalité.
La NCA conclut en affirmant que l'objectif visé à travers cette enquête était de comprendre les voies que les délinquants prennent et d'identifier les points d'intervention les plus efficaces pour les détourner vers le droit chemin.
https://www.developpez.com/actu/131646/Cybercriminalite-les-outils-gratuits-de-piratage-sont-une-porte-d-entree-pour-les-adolescents-61-pourcent-des-pirates-auraient-commence-avant-16-ans/

Jeux illicites : plus de 200 millions d'euros blanchis via des sociétés basées en Auvergne

La justice a mis au jour un circuit de blanchiment d'argent de plus de 200 millions d'euros lié à des jeux en ligne illicites et impliquant plusieurs sociétés en France, a indiqué vendredi le parquet national financier.
L'argent provenait de comptes de particuliers américains qui misaient sur des plateformes illicites de paris en ligne et "a atterri depuis 2009 dans plusieurs sociétés d'un particulier en Auvergne", a précisé une source proche de l'enquête.
Les sommes étaient ensuite envoyées dans divers pays de l'Union européenne (Danemark, Allemagne, Estonie, Lettonie, Lituanie) et des centres financiers offshore basés à Hong-Kong et Singapour, selon le communiqué du parquet national financier (PNF) qui évalue la fraude pour le fisc français à plus de trois millions d'euros.
L'affaire a démarré en 2013 quand des banques de Clermont-Ferrand ont remarqué le train de vie inhabituel d'un de leurs clients. Tracfin, la cellule anti-blanchiment de Bercy, avait alors émis un signalement et le parquet de Clermont-Ferrand s'était saisi de l'affaire avant de transmettre le dossier en 2015 au PNF vu l'ampleur des sommes en jeu.
Les enquêteurs français, en collaboration avec Europol et Eurojust (l'unité de coopération judiciaire européenne), ont mené une quinzaine de perquisitions dans plusieurs pays

européens et ont saisi des avoirs et des biens d'un montant de 3,5 millions d'euros, dont plusieurs voitures de luxe et divers biens immobiliers appartenant au suspect.

Communiqué de presse du Parquet national financier - "Une enquête préliminaire suivie par le parquet national financier depuis septembre 2015 a permis de mettre au jour un vaste et complexe circuit de blanchiment dans 6 Etats membres de l'Union Européenne (Danemark, Allemagne, Estonie, Espagne, Lettonie, Lituanie) et dans des centres financiers offshore extra- européens (Hong-Kong, Singapour). Un signalement de la cellule française de renseignements financiers TRACFIN et une plainte de la Direction générale des finances Publiques sont à l'origine de cette enquête, confiée à la Direction centrale de la police judiciaire (co-saisine de la Brigade nationale de répression de la délinquance fiscale et du Service régional de police judiciaire de Clermont-Ferrand). Elle a pour objectif, sous l'égide d'EUROJUST et d'EUROPOL, en concertation avec les magistrats et enquêteurs des pays sollicités, de démanteler un important réseau de blanchiment faisant apparaître deux types d'infractions : d'une part le blanchiment, depuis la France, de délits susceptibles d'être liés à des jeux en ligne illicites, d'autre part la fraude fiscale supposée avoir été réalisée à cette occasion. A ce stade des investigations, les délits porteraient sur la conversion illicite, depuis 2009, de plus de 200 millions d'euros et sur une fraude fiscale évaluée à 3 millions d'euros éludés d'impôt sur le revenu."

http://www.lamontagne.fr/clermont-ferrand/justice/2017/03/17/jeux-illicites-plus-de-200-millions-d-euros-blanchis-via-des-societes-basees-en-auvergne_12326136.html

Paiements électroniques : Un filon pour le blanchiment d'argent

Cartes prépayées, paiements électroniques, monnaie virtuelle : autant de moyens qui constituent un risque de blanchiment d'argent et requièrent toute la vigilance de Tracfin.

Les cartes de paiement prépayées, qui s'utilisent comme des cartes bancaires classiques sans l'obligation d'avoir un compte associé, et qui peuvent se recharger à souhait : voilà l'objet de la surveillance de Tracfin, la cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme. Mais Tracfin est également sur le qui-vive en ce qui concerne les paiements électroniques et les monnaies virtuelles.

"La combinaison des différents nouveaux moyens de paiement peut permettre la mise en place d'un circuit parallèle de flux financiers fonctionnant en dehors du secteur financier traditionnel", lit-on dans le rapport d'activité 2011 de Tracfin.

Anonymat de la monnaie électronique

Et si ces moyens de paiement attirent autant l'attention de la lutte anti-blanchiment, c'est d'abord par leur mode de distribution. En effet, les cartes prépayées sont par exemple disponibles chez les buralistes ou les maisons de la presse, sans qu'une connaissance du client ne soit exigée, et sont payables en espèces.

"Il reste possible, compte tenu des caractéristiques des distributeurs de monnaie électronique, que l'identification et la vérification d'identité du client reste douteuse, même au-delà du double seuil de 250 et 2500 euros. [...] Le moyen de paiement étant attaché au porteur, rien ne garantit que l'acheteur de la carte prépayée soit son utilisateur final", relève Tracfin.

L'institution donne ainsi l'exemple de marchands d'or qui avaient mis en place un système pour contourner l'interdiction des opérations d'achat/vente d'or en espèces, et ce, via l'achat de cartes prépayées en paiement de l'or.

Une traçabilité complexe

Les modes de paiement électronique présentent également d'autres risques : la difficulté de contrôler les flux transfrontaliers de capitaux. "Compte tenu des montants peu élevés

nécessaires à la commission d'attentats terroristes et à l'anonymat de la monnaie électronique, ces instruments présentent un risque élevé en matière de financement du terrorisme".
Les transactions électroniques sont par ailleurs difficiles à tracer, d'autant plus que les réseaux de distribution de ce type de paiement ne font généralement pas partie du circuit financier et acceptent mal d'être surveillés.
Quant à la monnaie virtuelle, elle présente aussi une frontière poreuse favorable au blanchiment d'argent : elle est principalement utilisée sur Internet sur des systèmes de paiements alternatifs comme les Facebook Credits ou les "bitcoins". Selon Tracfin, elles "constituent potentiellement un risque élevé compte tenu de l'opacité qui entoure leur existence et leur fonctionnement, ainsi que de l'absence complète de régulation des acteurs qui animent ce marché".
Les investigations menées par Tracfin peuvent aussi achopper sur la rapidité de ces transactions : "Les évolutions technologiques vont, par ailleurs, dans le sens de transactions de plus en plus rapides. Cette rapidité des flux complique considérablement le contrôle et peut empêcher la saisie et le gel des fonds délictuels".
Tracfin a également identifié un risque concernant les opérations de financement peu intermédiées, comme le micro-crédit, pour lesquelles l'origine et la destination des fonds font encore peu l'objet d'attentions.

Chiffres clés de Tracfin en 2011 (évolution par rapport à 2010)

24 000 demandes d'information reçues.
26 091 actes d'investigations (+72.6%).
Montants moyens par déclarations : inférieurs à 500 000 euros dans 90% des cas, dont plus de la moitié est inférieure à 50 000 euros.
Moyens de paiement les plus couramment déclarés : 8100 informations sur des espèces, 6700 sur des virements, 4140 sur des chèques.
http://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/20120822trib000715627/paiements-electroniques-un-filon-pour-le-blanchiment-d-argent.html

Bitcoin : monnaie dangereuse mais technologie vertueuse ?

Un rapport publié mercredi par le Conseil économique, social et environnemental (CESE) dénonce l'utilisation du Bitcoin à des fins "douteuses". En cause : l'absence de transparence et de traçabilité de cette monnaie virtuelle. Pour autant, l'institution estime intéressante la technologie de cryptage.
Fiable, le Bitcoin ? Le Conseil Économique, Social et Environnemental (CESE) a tranché dans un rapport publié mercredi 15 avril. Le Bitcoin, qui représente "*90% de l'activité*" monétaire virtuelle, ainsi que les 500 autres monnaies de ce type "*doivent faire preuve de transparence et de traçabilité*" et être soumise à "*un cadre réglementaire*", préconise l'organisation.

Problème de confiance et de transparence

La devise, émise selon un algorithme et indépendante des banques centrales, permet l'achat de biens ou des services auprès de toute personne ou société qui l'accepte comme mode de paiement. Ce système rend "*impossible*" d'associer des personnes à des transactions, observe le CESE. Il "*permet tout type de parades*", y compris les opérations "*douteuses, voire illégales* [ainsi que] *le blanchiment d'argent"*.
"*Une monnaie, à l'instar du Bitcoin qui met l'anonymat total en tête de gondole*" pose "*un problème majeur*", a alerté Pierre-Antoine Gailly, rapporteur de l'étude consacrée aux enjeux des nouvelles monnaies lors de sa présentation à la presse.

"*Aujourd'hui le Bitcoin ne répond pas du tout aux besoins d'une monnaie transparente et confiante*", a-t-il ajouté.
Le site internet Silk Road, surnommé "l'eBay de la drogue", l'utilisait par exemple comme monnaie d'échange jusqu'à sa fermeture par les autorités américaines en 2013. L'an dernier, des enquêteurs d'Europol ont également identifié pour la première fois un site qui vendait de la pédopornographie exclusivement contre des bitcoins.

Extrême volatilité et manque de fiabilité des plateformes

Le CESE pointe par ailleurs la grande volatilité de cette monnaie dont la valorisation "*a évoluée entre 1 dollar et 1163 dollars au plus haut*" depuis sa création, indique le rapport.
D'autre part, "*les acteurs proposant ces nouvelles solutions* [monétaires] *ne sont pas régulés*" selon les normes existantes, souligne le CESE. Les risques pour les utilisateurs de bitcoin "*de ne pas récupérer le montant*" d'une transaction augmentent en conséquence.
Le Bitcoin s'est en effet bâti une réputation sulfureuse en raison de son manque de fiabilité, notamment après la faillite de la plateforme d'échanges de Bitcoin MtGox en 2014, qui avait mystérieusement perdu des centaines de milliers de bitcoins et le piratage de plusieurs autres au cours des derniers mois. Face à ce manque de fiabilité, quelques acteurs, dont les frères Winklevoss -connus notamment pour avoir revendiqué l'invention de Facebook-, travaillent sur l'ouverture de plateformes d'échanges hautement sécurisées.

Utiliser la technologie de cryptage à d'autres fins

Pour le CESE, il est donc nécessaire de "*mettre en place un cadre légal international de régulation*" des monnaies virtuelles du genre. L'institution compte particulièrement sur l'entente entre États pour "*harmoniser leurs pratiques*" afin de lutter "*contre le blanchiment et le financement du terrorisme*". En juin 2014, Tracfin, la cellule anti-blanchiment du ministère des Finances, avait déjà invité les pouvoirs publics à encadrer l'utilisation des monnaies virtuelles, renforcer leur régulation et travailler au suivi des risques qu'elles génèrent.
"*Pour autant, la technologie de cryptologie qu'il y a derrière le bitcoin n'est pas à jeter*", a estimé Pierre-Antoine Gailly. Elle pourrait notamment être utilisée dans le "*transfert de documentations*", conclut-il.
http://www.latribune.fr/entreprises-finance/banques-finance/bitcoin-monnaie-dangereuse-mais-technologie-vertueuse-469259.html

La Russie pourrait autoriser le Bitcoin en 2018

Alors que les crypto-monnaies étaient interdites en Russie depuis 2014, le gouvernement de Vladimir Poutine serait en train de revoir son jugement.
Légaliser le Bitcoin pour mieux le contrôler ? L'hypothèse a été avancée ce mardi dans *Bloomberg* par Alexey Moiseev, ministre adjoint russe des Finances. En accord avec la Banque centrale, le pays pourrait autoriser le Bitcoin et les crypto-monnaies en 2018. Objectif affiché : renforcer sa lutte contre le blanchiment d'argent. *"L'Etat doit savoir à chaque instant qui se situe des deux côtés de la chaîne financière"*, assure Alexey Moiseev. *"Lorsqu'il y a une transaction, les personnes qui la facilite devraient pouvoir comprendre à qui ils ont acheté et à qui ils vendent, tout comme les opérations bancaires"*, poursuit-il.

Le Bitcoin accusé de faciliter le blanchiment d'argent

Réputé pour l'anonymat de ses transactions, le Bitcoin a été perçu par la Russie comme un moyen de faciliter des activités criminelles. Car cette monnaie virtuelle s'échange sans passer par l'intermédiaire de banque ou de sociétés tierces de paiement en ligne, comme PayPal. En 2014, la Russie a justifié son interdiction des crypto-monnaies en invoquant une lutte contre le blanchiment d'argent et le financement du terrorisme. En avril dernier, le pays est allé plus loin. Le ministre des Finances envisageait de punir les utilisateurs de crypto-monnaies avec

une amende pouvant aller jusqu'à 38.000 dollars et 7 ans de prison, rapportait alors *Bloomberg*.
http://www.latribune.fr/entreprises-finance/banques-finance/la-russie-pourrait-autoriser-le-bitcoin-en-2018-684929.html

Dixième congres des nations unies pour la prévention du crime et le traitement des délinquants

Lutter contre la criminalité sur le Net

Au cours des dernières années, l'Internet a connu une croissance explosive. Comparés aux quelque 26 millions d'utilisateurs dénombrés en 1995, ce sont aujourd'hui plus de 200 millions de personnes qui communiquent, font leurs achats, payent leurs factures, font du commerce et consultent même leur médecin sur Internet.
Alors que l'Internet connaissait une grande expansion, le crime en ligne augmentait également. Les cyber-criminels, comme on les appelle, ont largement envahi ou envahiront le monde virtuel, commettant des délits, tels qu'utilisation de codes d'accès confidentiels, piratage, fraude, sabotage informatique, trafic de drogue, commerce pornographique à caractère pédophile et "cyber-harcèlement".
Les criminels informatiques sont aussi variés que les différentes formes de crime qu'ils pratiquent. Il peut aussi bien s'agir d'étudiants, de terroristes ou de membres du crime organisé. En ce qui concerne la criminalité économique, telle que la fraude ou le vol d'informations, ce sont les employés à domicile qui représentent la catégorie la plus importante, tenue responsable de 90% de ces délits, selon le Manuel des Nations Unies sur la prévention et le contrôle de la criminalité informatique.
Les cyber-criminels sont à même de traverser, à toute allure, les frontières en passant inaperçus, cachés derrière d'innombrables "liens" ou en disparaissant tout simplement sans laisser de trace écrite. Ils peuvent faire passer des communications par le biais de "refuges de données" ou y dissimuler les preuves de leurs délits, les pays ne disposent pas des lois ou du savoir-faire nécessaires pour les retrouver.
Dans un effort tendant à réduire cette menace croissante, un atelier spécial sera organisé lors du Dixième congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, à Vienne, du 10 au 17 avril. L'atelier, organisé par l'Institut asiatique et extrême-oriental des Nations Unies pour la prévention du crime et le traitement des délinquants (UNAFEI), basé à Tokyo, et placé sous les auspices du Centre des Nations Unies pour la prévention internationale du crime (CPIC) se concentrera sur la coopération mondiale en matière d'enquêtes sur le crime informatique et de sa poursuite.
"Cet atelier doit servir pour les pays de forum de partage d'informations sur des domaines ayant trait aux techniques d'investigation et aux lois informatiques. Il mettra en présence une grande diversité d'expériences, de savoirs-faire et d'approches relatives à ce problème", déclarait Christopher Ram, responsable de la prévention du crime (crime informatique) au CPIC.

Piratage, sabotage et harcèlement

Le piratage de sites confidentiels, grâce à des techniques sophistiquées permettant d'imiter les codes d'accès ou de contourner les dispositifs de sécurité, est devenu un cyber-délit de plus en plus répandu. Une fois qu'ils ont obtenu un accès, les pirates peuvent "injecter" des virus, envoyer des messages injurieux ou voler des données précieuses, y compris des informations sur les cartes de crédit et des documents confidentiels sur les sociétés.
Les services secrets américains estimaient récemment que les consommateurs perdent environ 500 millions de dollars par an du fait des vols de cartes de crédit ou de la récupération en ligne d'informations sur les cartes, commis par les pirates. Ces codes de cartes peuvent être

vendus pour des n négli fa utilisent des programmes spéciaux pour les les ba que le crédit ou bancaires, note le Manuel de l'O

D'autres cyber- tent les urs vantage économique sur leurs concurren menace nm des fins d'extorsion. Les délinquants tra nées ou rat u bien encore utilisent ce que l'on a sites" o "v er complètement les stèmes ou ées d'u virus informatiques passaien ordinate es "infectées" sont rd'hui se ux et essages e-mail ou ogra par d'I

e la prem tion d'extorsion n virus. E la recherche médicale a été ba étru e des s de données s ve 'soigné er-hard à l'e-m er des messages s person s. On viron 200000 f ées chaque n dan e qu'elle publia stalking: Enf bility On-line World. habitante d'Am dant p ieurs années par inconnu qui men le faire circuler son adre eau, raconte Mme Je

s délinquants se sont discussion" ternet pour dénicher des r exe le, gagnent, confiance des enfants, dans la v réelle po d'eux ou les enlever. éricain, la p ophil progression sur Intern

En plus de s'attaquer vent ouvrir leurs p res sites web pour escroque vices illégaux, t rmes, drogues, médicam s pornograp gne, a dr seau Internet CyberCop Holdi avertissement c commission fi e page web un des voiture du cli cule n'était pas ve 90 jours.

Plusieurs v ıs été vendues d imparti, n nnonces pour leur arge " a fermé dep

Attrap

Comm ssait, de nom des nouv que le piratage. Ils les exi peines pour délits tra vandalisme et s'a monde virtuel.

S xemple, a récemment amendé so les délits , CMA). Selon CNET Singapor les ecourues sont aujourd'hui plus ur quiconque trafique des "ordinateurs protégés" - les individus liés à la sécurité na ne ux banques et aux services financi u'aux urgences et à la fonction pub e, cela s'applique aussi à l'accès à ntiels, à la modification, à l'utilisation ou l'interception de matériel inform

Certains pays disposent de groupes spécialisés dans la recherche des cyber-criminels. Le Service des enquêtes spéciales de l'armée de l'air américaine est un des plus anciens, il fut créé en 1978. Composé de responsables chargés du respect de la loi disposant de formations informatiques très poussées, le groupe des enquêteurs informatiques australiens est un autre organe de ce type. Le groupe australien rassemble des preuves et les communique aux institutions pertinentes chargées du respect de la loi du pays où le délit a été commis.

En dépit de ces efforts, les responsables du respect de la loi sont encore confrontés à de nombreux problèmes. Le problème majeur étant notamment que de tels délits traversent facilement les frontières, ce qui fait des procédures d'enquête sur les délinquants, de même que de leurs poursuites et de l'application de leurs peines, de vrais casse-têtes juridiques et législatifs. Et, une fois qu'un délinquant a été repéré, les responsables doivent décider de l'extrader pour un procès qui se tiendra ailleurs ou de transférer les preuves, et quelques fois les témoins, à l'endroit où les délits ont été commis.

En 1992, des pirates européens ont attaqué un centre informatique californien. L'enquête policière fut bloquée du fait d'un manque de "cocriminalité" -des lois identiques interdisant dans les deux pays de telles pratiques- qui a entravé la coopération officielle, selon le Département américain de la justice. Finalement, la police du pays d'origine des pirates a offert son aide, mais peu de temps après le piratage a cessé, la piste s'est refroidie et le dossier a été fermé.

De la même manière, le Service d'enquêtes criminelles et le Bureau fédéral d'enquêtes américains ont suivi la piste d'un autre pirate jusque dans un pays d'Amérique latine. Le pirate volait des fichiers contenant des mots de passe et modifiait les fichiers d'accès de certains systèmes informatiques militaires, universitaires et privés. Nombre d'entre eux contenaient des études confidentielles sur les satellites, la radiation et la recherche sur l'énergie.

Les responsables du respect de la loi de ce pays sud-américain se mirent en quête de l'appartement du pirate et y saisirent son matériel informatique, au titre de violations potentielles de la loi nationale. Mais aucun accord d'extradition ne liait les deux pays en matière de crime informatique, bien que de telles dispositions existaient entre eux dans le domaine de la criminalité traditionnelle. En fin de comptes, le cas fut résolu, mais uniquement parce que le pirate avait accepté, en échange d'une réduction de peine, de plaider coupable aux Etats-Unis.

Détruire, dissimuler les preuves

Il n'est pas difficile pour les délinquants de faire disparaître les preuves en les modifiant, les effaçant ou les déplaçant. Cela constitue un autre obstacle majeur aux poursuites des cyber-criminels. Si les responsables du respect de la loi sont moins rapides que les délinquants, la plupart des preuves disparaissent. Ou bien les données auront été encryptées; une technique de plus en plus courante visant à protéger les personnes comme les affaires sur les réseaux informatiques.

L'encryptage peut gêner les enquêtes criminelles, mais si les responsables du respect de la loi parviennent à disposer d'un savoir technique trop important, ce sont les libertés individuelles des personnes qui pourraient en souffrir. Le commerce électronique défend l'idée selon laquelle le respect de la liberté est essentiel pour motiver la confiance des consommateurs sur le marché Internet, tandis que les groupes de défense des droits de l'homme réclament une protection concernant les quantités de données personnelles aujourd'hui stockées électroniquement.

Les commerciaux mettent également l'accent sur le fait que l'information est susceptible de tomber en de mauvaises mains, en particulier dans les pays corrompus, dans les cas où les gouvernements auraient accès aux messages encryptés. " Si les gouvernements disposent des clés pour encrypter les messages, cela signifie que des personnes non autorisées, extérieures

au gouvernement, peuvent les obtenir et s'en servir,", déclarait le PDG d'une grande société nord-américaine spécialisée dans la sécurité.

Stopper le crime mondial

Les défis qu'affrontent les responsables du respect de la loi, à travers le monde, mettent en évidence le besoin urgent d'une coopération mondiale, en matière d'actualisation des législations nationales, des techniques d'enquête, de l'assistance légale et de l'extradition, afin de suivre le rythme des cyber-criminels. Certains efforts ont déjà été déployés.

Le Manuel de l'ONU de 1997 engage vivement les nations à harmoniser leurs lois et à coopérer pour lutter contre ce problème. Le European Working Party on Information Technology Crime (EWPITC, le Groupe de travail européen sur les informations relatives au crime technologique) a publié un manuel sur le crime informatique, qui dresse la liste des législations pertinentes dans chaque pays et décrit les techniques d'enquête, de même que les moyens de chercher et de sécuriser le matériel électronique.

Le European Institute for Anti-Virus Research (EICAR, l'Institut européen de recherche pour la lutte contre les virus) regroupe le monde universitaire, l'industrie et les médias, de même que des experts techniques en dispositifs de sécurité, des spécialistes du respect de la loi et des organisations privées de protection pour lutter contre les virus informatiques ou chevaux de Troie. L'Institut travaille également dans le domaine de la lutte contre la fraude et l'exploitation de données personnelles.

En 1997, les pays du G-8 ont adopté une stratégie pionnière de lutte contre le crime technologique de pointe. Le groupe s'est entendu pour développer des moyens de repérer rapidement les attaques informatiques et d'identifier les pirates, en utilisant des liens vidéo pour procéder aux auditions de témoins transfrontaliers et s'entraider dans le domaine de la formation et des équipements. Il a également décidé de se joindre à l'industrie concernant la mise en place d'instituts à même de sécuriser les technologies informatiques, développer des systèmes d'information pour stopper les délits sur le réseau, rechercher les délinquants et rassembler les preuves.

Le G-8 a, à présent, mis en place des groupes de contact auxquels peuvent s'adresser les responsables du respect de la loi, 24 heures sur 24, sept jours sur sept. Ces groupes activent une enquête menée par un autre pays en fournissant des informations essentielles ou en aidant par le biais de procédures légales, telles qu'auditions de témoins ou regroupement des données informatiques, servant de preuves.

L'obstacle majeur à la mise en place au niveau international d'une stratégie du type de celle du G-8 est que certains pays ne disposent pas d'un savoir-faire technique ou d'une législation qui permettraient aux responsables du respect de la loi de rechercher rapidement les preuves dans le domaine électronique avant qu'elles ne se perdent ou de les déplacer dans un lieu où les délinquants sont mis à l'épreuve.

Réseau : les méchants

Espionnage industriel

Les pirates peuvent entreprendre des opérations sophistiquées d'espionnage pour des sociétés ou à leur compte, en copiant des données commerciales confidentielles, allant des stratégies marketing aux renseignements techniques ou sur des produits.

Sabotage des systèmes

Des attaques, tel les que le "bombardement de courriers", sont à même d'envoyer de façon répétitive des messages à une même adresse e-mail ou sur un même site Internet, empêchant les utilisateurs légitimes d'y accéder. Le flux d'e-mails est susceptible de surcharger le compte personnel du receveur et de détruire le système dans son ensemble. Une pratique si dangereusement préjudiciable n'est pourtant pas nécessairement illégale.

Sabotage de données et vandalisme

Les intrus accèdent aux sites Internet ou aux bases de données, endommageant, effaçant ou modifiant les données, altérant les données elles-mêmes et causant davantage de tort dans les cas où les données sont ensuite utilisées à d'autres fins.

" Pêcheurs ", " découvreurs " de codes d'accès

Les trafiquants trompent souvent les nouveaux utilisateurs ou les moins expérimentés en se faisant passer pour des responsables du respect de la loi ou des employés de leur service de connexion à Internet. Les "découvreurs" de code d'accès utilisent des logiciels pour découvrir l'identité des utilisateurs des codes d'accès, qui leur servira ensuite à se cacher sous leur nom et à commettre d'autres délits, qui peuvent aller de l'utilisation de systèmes informatiques confidentiels à des fins de crime économique, au vandalisme ou à des actes terroristes.

Parodie

Les individus qui pratiquent la parodie ont recours à diverses techniques qui leur permettent de déguiser un ordinateur afin que celui-ci prenne, électroniquement, l'apparence d'un autre ordinateur. Ils peuvent ainsi accéder à un système dont l'utilisation est normalement limitée et commettre des délits. Le pirate bien connu, Kevin Mitnick, a eu recours à cette technique de la parodie, en 1996, pour accéder à l'ordinateur personnel de l'expert en sécurité, Toutomu Shimomura, et communiqua ensuite, sur Internet, de précieuses données sécuritaires.

Pornographie à caractère pédophile

La circulation de documents pornographiques à caractère pédophile à travers le monde par le biais de l'Internet est en plein essor. Au cours des cinq dernières années, les inculpations, dans un pays d'Amérique du Nord, pour circulation ou possession de documents pornographiques à caractère pédophile sont passées de 100 à 400 par an. Le problème se trouve exacerbé par les nouvelles technologies, telles que l'encryptage, qui peut être utilisé pour dissimuler la transmission ou le stockage de documents pornographiques ou d'autres matériaux " choquants".

Les jeux d'argent

Les jeux d'argent électroniques ont augmenté tandis que le commerce fournissait des moyens de contracter des crédits ou de transférer des fonds par Internet. Des problèmes ont vu le jour dans des pays où les jeux d'argent sont interdits ou dans les pays où le jeu ne peut se pratiquer sans licence. On ne peut garantir aux joueurs aucune partialité, étant donné les contraintes techniques et juridiques de contrôle du jeu.

Fraude

Des offres frauduleuses ont déjà été faites à des consommateurs dans différents secteurs du commerce électronique, tels que l'achat et la vente d'action ou d'obligation ou l'achat et la vente d'équipements informatiques.

Blanchiment d'argent

On pense que le commerce électronique est susceptible d'offrir de nouvelles opportunités au transfert électronique de biens et d'argent utilisé pour blanchir l'argent sale, surtout s'il est possible de dissimuler les transactions.

http://www.un.org/french/events/10thcongress/2088hf.htm