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

100 banques victimes d'un cyberbraquage à 1 milliard de dollars

Selon l'agence de sécurité russe Kaspersky, Interpol et Europol enquêtent sur un gang de cybercriminels baptisé « Carbanak ». Celui-ci s'attaque depuis 2013 à des établissements financiers dans une trentaine de pays dont la France**.**

Finis les braquages dans les agences bancaires. Désormais, les criminels ont recours aux techniques informatiques les plus sophistiquées. Interpol et Europol enquêteraient ainsi sur une vaste opération mondiale de cyberbraquage ayant coûté 1 milliard de dollars à une centaine de banques et d'établissements financiers sur la planète, révèle lundi l'agence de sécurité russe Kaspersky Lab, qui dit collaborer avec les agences internationales.

Selon Kaspersky Lab, ces cyberattaques, débutées en 2013, seraient toujours à l'oeuvre. Elles concernent une trentaine de pays, parmi lesquels la France, la Russie, les Etats-Unis, l'Allemagne, la Chine, l'Ukraine, le Canada, Hong-Kong, Taïwan, la Roumanie, l'Espagne, la Norvège, l'Inde, le Royaume-Uni, la Pologne, le Pakistan, le Népal, le Maroc, l'Islande, l'Irlande, la République Tchèque, la Suisse, le Brésil, la Bulgarie, et l'Australie.

Deux à quatre mois pour infecter la banque

Cette vague de cyberattaques, sans précédent, serait le fait d'un groupe de cybercriminels, en provenance de la Russie, de l'Ukraine, ainsi que de la Chine. Baptisé « Carbanak », celui-ci dérobe directement l'argent dans les caisses des banques en infectant leur réseau interne. Une technique qui prend deux à quatre mois pour porter ses fruits, selon Kaspersky.

Les cybercriminels infectent d'abord l'ordinateur d'un employé de la banque visée à l'aide de la technique dite du « spear phishing » ou hameçonnage - l'employé recevant un mail semblant émaner d'une personne ou d'une entreprise qu'il connaît est invité à cliquer sur un lien par lequel il télécharge en fait un logiciel malveillant. Une fois dans la place, Carbanak infecte l'ensemble du réseau interne de la banque, notamment les ordinateurs des administrateurs chargés de la vidéo surveillance. Les cybercriminels peuvent ainsi surveiller et enregistrer toutes les opérations de transfert à l'oeuvre au sein de la banque, afin d'en imiter les codes.

Transferts d'argent en ligne

Ils procèdent ensuite au retrait d'argent à l'aide de trois méthodes. L'une d'elles consiste à transférer l'argent via des systèmes de paiement en ligne sur des comptes basés, selon Kaspersky, en Chine et en Amérique. Les cybercriminels peuvent aussi agir directement sur les comptes, en falsifiant le solde et en retirant l'excédent sur leur propre compte. Par exemple, si un usager dispose de 1.000 dollars sur son compte, ils

chiffrent virtuellement sa valeur à 10.000 dollars, transfèrent 9.000 dollars sur leur propre compte. L'intéressé, lui, ne soupçonne rien puisqu'il dispose toujours de 1.000 dollars sur son compte.
Enfin, les cybercriminels ont recours aux distributeurs de billets des banques, en déclenchant à distance une sortie de billets à un horaire déterminé. L'un des complices n'a alors plus qu'à attendre la pêche miraculeuse devant le distributeur.
Selon, Sanjay Virmani, directeur du centre sur le crime virtuel à Interpol, « ces attaques révèlent que les criminels sont prêts à exploiter toute vulnérabilité dans n'importe quel système. Cela souligne également qu'aucun secteur ne peut se considérer protégé contre ces attaques et doit constamment revoir ses procédures de sécurité ». 16/02/15
Liens : http://www.lesechos.fr/16/02/2015/lesechos.fr/0204163075897_100-banques-victimes-d-un-cyberbraquage-a-1-milliard-de-dollars.htm

L'incroyable cyber-braquage de la banque centrale du Bangladesh

L'institut monétaire du Bangladesh a perdu près de 100 millions de dollars. La banque centrale a été la cible de pirates informatiques. Histoire d'un casse hors du commun.
Personne n'est épargné par les pirates informatiques, pas même les banques centrales. Celle du Bangladesh en a récemment fait les frais. En effet, des hackers lui ont dérobé 81 millions de dollars, sans avoir eu besoin de creuser le moindre tunnel ou faire exploser un seul bâton de dynamite.

Comment les hackers ont-ils procédé ? Où est l'argent ?

Pour arriver à leurs fins, les pirates ont simplement profité d'un manque de communication entre l'antenne new-yorkaise de la Fed - où la banque centrale bangladaise détient un compte - et l'institut monétaire asiatique. Ils ont envoyé plus de trente demandes un vendredi soir pour transférer au total d'environ 1 milliard de dollars vers des comptes aux Philippines et au Sri Lanka.
Dans un premier temps, la banque centrale américaine n'y a vu que du feu. Les codes utilisés au sein de la messagerie bancaire internationale (SWIFT) étaient corrects et les demandes de transferts d'argent émanaient de serveurs apparemment basés à Dacca, la capitale du Bangladesh.
Néanmoins lors de la cinquième demande, la Fed a mis fin aux transferts après avoir repéré une erreur dans le message. Les hackers avaient mal orthographié le nom du destinataire. Ainsi le virement aurait dû arriver sur le compte de Shalika Fandation au lieu de la Shalika Foundation, raconte le New York Times .
Si une partie de l'argent transféré a été bloqué ou en cours de restitution, 81 millions de dollars ont disparu dans la nature. Selon des officiels du Bangladesh, cet argent arrivé sur des comptes aux Philippines a été blanchi dans plusieurs casinos du pays, rapporte le Wall Street Journal .

Qui est fautif ? Qui sont les hackers ?

Dans un communiqué , la Fed explique que les virements ont été totalement authentifiés, suggérant que la faille de sécurité est plutôt à chercher du côté du Bangladesh. La banque centrale américaine souligne par ailleurs que son système n'a été victime d'aucune faille de sécurité.
Au Bangladesh, le gouverneur de la banque centrale, Atiur Rahman, a été contraint à la démission. Il lui est notamment reproché d'avoir tardé à signaler le vol aux autorités. « J'ai vécu cet événement pratiquement comme une attaque, comme un

séisme. Je n'ai pas compris comment [ce vol] a pu se produire, d'où c'est venu et qui l'a réalisé », a-t-il déclaré.
Quant à l'identité des auteurs du vol, il s'agit encore d'un mystère. Selon l'agence financière Bloomberg , les hackers ont utilisé un code malicieux, un malware, et leur attaque présente des similitudes à celle du gang Carbanak . Ce dernier avait réussi à subtiliser un milliard de dollars à des institutions financières. 19/03
Liens : http://www.lesechos.fr/finance-marches/marches-financiers/021774994706-lincroyable-cyber-braquage-de-la-banque-centrale-du-bangladesh-1208253.php

La Banque du Bangladesh récupère un peu de ses millions dérobés début 2016

Environ 15 millions de dollars sur les 81 dérobés en février dernier par des pirates informatiques, pourraient être restitués à la banque centrale du Bangladesh. L'argent devait être blanchi via des casinos et dans des conditions aussi rocambolesques que le vol lui-même.
C'est une toute petite victoire dans la lutte contre la cyber-criminalité. Deux mois après s'être fait voler l'équivalent de 81 millions de dollars (environ 72 millions d'euros) par des pirates informatiques, la banque centrale du Bengladesh va pouvoir en récupérer une partie : près de 15 millions de dollars, soit environ 18 % de la totalité de la somme qui avait été dérobée en février.
Une première tranche de 4,63 millions de dollars a d'ores et déjà été remise aux autorités de Manille par l'un des suspects, Kam Sin Wong, un Chinois qui travaille pour des casinos philippins et dont le rôle est d'attirer de nouveaux clients dont il organise le séjour. Patron d'une société qui s'appelle Eastern Hawaii Leisure Company, il avait été identifié très vite par les enquêteurs comme l'un des bénéficiaires des fonds dérobés.
Il a affirmé devant une commission sénatoriale philippines qui enquête sur cette affaire, que l'argent lui a été donné en paiement d'une dette. Kam Sin Wong s'est dit, selon la chaîne de télévision locale ABS CBN News, être encore en possession de 10 autres millions de dollars obtenus de la même manière et toujours dans les comptes de sa société. Au total ce serait donc une quinzaine de millions sur 81 qui pourraient revenir dans les caisses de la Banque du Bangladesh.

Une première tranche de 4,63 millions de dollars

Pour l'heure cependant, seulement 4,63 millions de dollars ont effectivement été restitués par Kam Sin Wong est sont entreposés à la banque centrale des Philippines, dans le même coffre qui recèle les bijoux de l'ancienne première dame, Imelda Marcos, saisis et destinés à être vendus.
Des représentants officiels du Bangladesh devraient arriver à Manille ce samedi et définir les modalités de rapatriement des fonds. Dacca espère pouvoir récupérer à terme la totalité de l'argent dérobé.

Une commission d'enquête sénatoriale aux Philippines

Cette restitution, très médiatisée, est sans doute le plus spectaculaire des rebondissements d'une affaire qui captive la presse philippine. Et pour cause, dès début mars, peu après la révélation de ce vol sans précédent, toutes les pistes montraient que c'est sur l'archipel philippin que s'était joué l'essentiel de ce casse sans précédent, tant pour son montant que pour sa mise au point.

Devant l'importance du scandale, le Sénat des Philippines a mis en place une commission d'enquête qui, depuis quelques semaines, a multiplié les auditions. Ce qui permet ainsi de retracer ce qui s'est passé une fois que les 81 millions ont été transférés.

Des comptes dormants créés en 2015

Selon Conseil philippin de lutte contre le blanchiment d'argent, les fonds ont tout d'abord été déposés sur quatre comptes dormants à la Rizal Commercial Banking Corporation (RCB) de Manille. Ils avaient de fait été ouverts en mai 2015 en utilisant de faux permis de conduire et n'avaient pas fonctionné jusqu'en février 2016.

Une fois viré sur ces quatre comptes, l'argent a ensuite été transféré sur un cinquième, ouvert cette fois-ci au nom d'un financier bien réel du pays, William Go, qui affirme ne pas avoir été au courant. L'argent a ensuite transité par Philrem, une société de courtage et de transfert d'argent reconnue qui existe depuis 1990.

La dirigeante de Philrem, Salud Bautista, a déclaré devant la commission sénatoriale, avoir viré les fonds, principalement en liquide, à la demande de la numéro deux de la RCB, Maia Santos Deguito. Celle-ci se défend d'y être pour quelque chose et affirme que se signature a été imitée.

Deux Chinois bénéficiaires des transferts

Les enquêteurs ont déterminé que les bénéficiaires des transferts effectués par Philerm sont d'une part Kam Sin Wong et d'autre part un autre Chinois, Weikang Xu, qui travaille lui aussi pour des casinos de l'archipel philippin. Le premier aurait ainsi reçu, selon Philrem, quelque 21 millions de dollars, tandis que le second aurait perçu 59 millions, dont une trentaine en liquide.

Mais les faits ne sont pas totalement avérés, Kam Sin Wong contredit les déclaration de Salud Bautista et indique en effet ne pas avoir reçu autant d'argent. Et selon lui, Philerm aurait gardé pas moins de 17 millions de dollars. Ce que dément la société.

En tout état de cause, les voleurs avaient parfaitement choisi leurs circuits de blanchiment : d'une part la législation de lutte contre le blanchiment d'argent des Philippines ne couvre pas les casinos. D'autre part, ils ont organisé ces transferts lors du nouvel an chinois, période pendant laquelle les casinos reçoivent traditionnellement d'importantes sommes d'argents de joueurs chinois. Ces transferts auraient, en théorie pu passer inaperçus.

Un cyber-braquage interrompu par une faute d'orthographe

Le 4 février dernier, les cyber-braqueurs ont presque réussi le casse parfait, sans armes ni violence. Profitant d'un manque de communication entre l'antenne new-yorkaise de la Fed - où la banque centrale bangladaise détient un compte - et l'institut monétaire asiatique, les pirates ont envoyé début février 35 ordres de virement un vendredi soir pour transférer au 951 millions de dollars vers des comptes aux Philippines et au Sri Lanka.

Si dans un premier temps, la Fed a répondu aux demandes qui avaient l'apparence d'émaner de Dacca, au cinquième mail elle a mis fin aux transferts après avoir repéré une erreur dans le message : les hackers avaient mal orthographié le nom du destinataire, écrivant "Shalika Fandation" au lieu de la "Shalika Foundation".

Une partie de l'argent a été bloqué, mais 101 millions de dollars ont été transférés, dont une vingtaine a été récupérée dans une banque du Sri-Lanka.

Un vol qui a coûté son poste à Atiur Rahman, le gouverneur de la Banque centrale du Bangladesh.01/04

Liens : http://www.lesechos.fr/finance-marches/marches-financiers/021810870771-la-banque-du-bangladesh-recupere-un-peu-de-ses-millions-derobes-debut-2016-1211093.php

Banque de l'Equateur piratée : 12 millions de dollars dérobés via SWIFT

La banque du Bangladesh n'est pas la seule victime des récents « cyber-hold-up ». Après la récente attaque ayant visé la banque de l'Equateur (12 millions de dollars dérobés), cela ressemble de plus ne plus à une cyberattaque généralisée visant le système bancaire mondial…

Il s'agit là d'une énième cyberattaque de banque, au cours de laquelle les cybercriminels ont directement cible le système SWIFT, utilisé par l'ensemble de l'écosystème financier mondial. La cible : la banque de l'Equateur. Le bilan : 12 millions de dollars dérobés par les pirates informatiques.

Cela devient une évidence que tout le monde peut remarquer : le système bancaire international basé sur SWIFT est bien attaqué, comme le prouvent les récents cyber-casses ayant visé de nombreuses banques de moindre sécurité. Si l'on ajoute ces récents 12 millions volés à une banque équatorienne (Banco del Austro) aux 81 millions de la banque du Bangladesh, cela montre bien l'aspect critique de la situation.

L'attaque de Banco del Austro en Equateur aurait eu lieu en janvier 2015, information révélée par le biais d'un procès intenté par la banque contre Wells Fargo, une banque basée à San Francisco, comme l'a rapporté Reuters.

Voici comment les cyber-criminels ont ciblé ces banques :

- Utilisation de logiciels malveillants sophistiqués pour contourner les systèmes de sécurité locaux de la banque
- Gagner l'accès au réseau de messagerie SWIFT interne
- Envoi de messages frauduleux via SWIFT pour initier les transferts de fonds à partir de comptes vers de plus grandes banques

Pendant plus de dix jours, les pirates ont pu avoir la main sur le système SWIFT d'un employé de la banque, et ainsi, modifier les détails des transactions d'une douzaines de transferts pour un montant total dépassant les 12 millions de dollars, transféré sur des comptes à Hong Kong, Dubaï, New York et Los Angeles.

Durant le procès devant un tribunal de New York, Banco del Austro tient Wells Fargo responsable de ne pas avoir repéré les transactions frauduleuses et a exigé de la banque de lui rembourser le montant total qui lui a été volé. Selon BDA, tout cela aurait pu être évité si les deux organismes avaient partagé de plus amples informations sur SWIFT.

Wells Fargo a bien entendu également riposté et a directement blâmé les faiblesses des politiques et des procédures de sécurité au sein de Banco del Austro, ayant permis le cyber-braquage. Pour Wells Fargo, les transactions ont été bien traitées par rapport aux instructions fournies, reçues via des messages SWIFT authentifiés et donc non repérés comme frauduleux.

Selon les rapports, la cyberattaque est longtemps restée secrète. D'après les divers communiqués sur l'affaire, le brèche n'est pas identifiée et aucun des partis n'a d'explications précises sur le pourquoi du comment…

« *Nous ne savions pas*« , a déclaré SWIFT dans un communiqué. « *Nous avons besoin d'être informés par les clients de ces fraudes si elles se rapportent à nos produits et services afin que nous puissions informer et soutenir la communauté. Nous avons été en contact avec la banque concernée pour obtenir plus d'informations, et nous rappelant les clients de leur obligations de partager ces informations avec nous.*«

Les rapports montrent que la sécurité de SWIFT même n'a pas été violée durant l'attaque, mais que les cybercriminels ont utilisé un logiciel malveillant de pointe pour voler directement les informations d'identification aux employés de la banque et ainsi, couvrir leurs traces.
Le malware en question avait déjà été utilisé lors de l'attaque ayant visé la banque du Bangladesh, et avait permis aux cybercriminels de manipuler à leur guise les journaux d'historique des systèmes et de faire disparaître toute trace des transactions frauduleuses. A suivre. 23 mai 2016
Liens : http://www.undernews.fr/banque-cartes-bancaires/banque-de-lequateur-piratee-12-millions-de-dollars-derobes-via-la-faille-swift.html

Cybercrime : 20 millions £ dérobés via un malware bancaire au Royaume-Uni

Des cybercriminels ont volé près de 20 millions de livres au Royaume-Uni dans des comptes bancaires en utilisant le malware Dridex. L'affaire a été confirmée par l'Agence nationale de la criminalité (NCA).
L'agence nationale de la criminalité (NCA) met en garde les internautes via son compte Twitter contre le logiciel malveillant Drilex, également connu sous le nom de Bugat et Cridex. La chasse est ouverte pour mettre la main sur les cybercriminels à l'origine de l'attaque, et la NCA avoue qu'ils sont techniquement à la pointe. Le montant du préjudice global a déjà atteint près de 20 millions de livres sterling, soit près de 30 millions de dollars ou 27 millions d'euros.
Une arrestation a déjà été réalisée, elle visait Andrey Ghinkul, en Moldavie, qui était déjà recherché pour piratage informatique aux Etats-Unis.
« *Cette forme particulièrement virulente de logiciels malveillants a été développée par des criminels en Europe de l'Est. Elle est capable de récolter les données bancaires en ligne et de dérober efficacement de l'argent à des particuliers et aux entreprises, et ce, à l'échelle mondiale*« , explique la NCA.
Les victimes sont infectées la plupart du temps via des courriels apparemment légitimes. Les institutions financières et les différents systèmes de paiement ont été ciblés. Les utilisateurs de Windows sont les plus à risque. La NCA recommande de s'assurer que les systèmes d'exploitation sont bien à jour et qu'un logiciel antivirus est installé pour se protéger. De plus, le principal conseil reste de ne pas ouvrir les pièces jointes ou cliquer sur des liens non fiables ou suspects.
La *National Cyber Crime Unit* de la NCA a d'ores-et-déjà rendu une grande partie du botnet inoffensif et travaille actuellement sur l'assainissement total du réseau pour protéger les victimes. L'équipe travaille en collaboration avec Europol, la police métropolitaine, le GCHQ, le FBI et les autorités allemandes et moldaves.
« *Les cybercriminels agissent souvent à travers les frontières internationales, mais cette opération témoigne de notre détermination à les arrêter, peu importe où ils se trouvent physiquement*«, déclarele directeur adjoint exécutif du FBI Robert Anderson.
Au Royaume-Uni, les victimes sont invitées à joindre Action Fraud.
Liens : http://www.undernews.fr/banque-cartes-bancaires/cybercrime-20-millions-derobes-via-un-malware-bancaire-au-royaume-uni.html

« La cybercriminalité est la nouvelle menace du XXIe siècle »

Pour riposter aux cyberattaques, les forces de l'ordre sont contraintes de se mettre au niveau techniquement et de développer des outils transnationaux. Aussi, le Complexe mondial pour l'innovation, une forteresse high-tech dédiée à la lutte contre les cybermenaces, vient-il de voir le jour à Singapour. Explications.

Commissaire de police depuis 1976, Mireille Ballestrazzi s'impose, à 61 ans, comme la deuxième femme à occuper le prestigieux poste de directrice générale de la Police judiciaire. Également présidente du comité exécutif d'Interpol, le réseau international des polices, elle décrypte pour *La Tribune* comment les forces de l'ordre françaises, européennes et internationales luttent contre la cybercriminalité. Elle revient aussi sur les missions du tout nouveau Complexe mondial Interpol pour l'innovation de Singapour, une forteresse high-tech consacrée à la lutte contre les cybermenaces.

À l'heure où Internet s'immisce partout, y compris dans nos objets connectés du quotidien, et que le Dark Web monte en puissance, la cybercriminalité s'impose comme « la menace du XXIe siècle » et pose un défi d'une ampleur inégalée aux forces de police.

La Tribune. Avec la numérisation de la société et de l'économie et le développement des nouvelles technologies, les crimes et délits se multiplient dans le cyberespace. Comment les forces de police abordent-elles cette problématique?

Mireille Ballestrazzi. La cybercriminalité est clairement la nouvelle menace du xxie siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale. Le cybercrime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières. Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants. Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes « classiques ». Avec la démocratisation de l'accès à Internet et l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début : toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier.

En tant que présidente du comité exécutif d'Interpol, vous avez inauguré, en avril dernier, le Complexe mondial pour l'innovation, situé à Singapour et spécialisé dans la lutte contre la cybercriminalité. C'est l'outil qui manquait pour être à la hauteur de l'enjeu ?

Il est essentiel que la police tente d'avoir une longueur d'avance sur les malfaiteurs. Lutter efficacement contre le crime en général et contre la cybercriminalité en particulier demande la mise en place d'outils globaux. Interpol, dont le siège est à Lyon, remplit déjà cette mission. Il dispose de bases de données massives, sur la pédopornographie par exemple, alimentées par l'ensemble des polices du monde. En revanche, les crimes sur Internet nécessitent une attention particulière. C'est pourquoi les 190 membres d'Interpol ont accepté à une quasi-unanimité l'ouverture de cette nouvelle structure à Singapour. Le Complexe mondial transcende le modèle

traditionnel répressif en matière d'application de la loi, en utilisant toutes les possibilités de l'ère numérique.

Quelles sont ses missions ?

C'est un centre ultramoderne, doté d'ordinateurs de grande capacité. Le choix s'est porté sur Singapour, car Lyon n'avait pas la place pour l'accueillir. Il dispose d'experts et d'équipements à la pointe du progrès, au service de deux grandes missions. D'abord, la recherche autour du développement des nouvelles technologies par les criminels, de manière à fournir aux services de police des outils de riposte adaptés. Ensuite, le Complexe fournit une aide aux enquêteurs du monde entier, via des formations, des échanges d'informations et un renforcement des capacités d'intervention. Il travaille aussi avec d'autres organismes transnationaux comme Europol, le réseau des polices des pays de l'UE. Actuellement, le centre compte 95 personnes, mais l'effectif va monter en puissance pour atteindre 160 employés d'ici à 2018-2019.

Concrètement, comment se passe la collaboration internationale pour lutter contre une cybermenace ?

Prenons l'exemple de la pédopornographie, qui prospère sur Internet. Il existe des sites d'une horreur absolue. Grâce à sa base de données, Interpol peut découvrir un réseau. Mais souvent, l'initiative part d'un pays membre, qui identifie un certain nombre d'adresses IP problématiques et ouvre une enquête judiciaire. Internet étant mondial, les adresses IP concernent souvent plusieurs États. Interpol contacte alors le bureau central d'Interpol dans chaque pays concerné pour mettre en place une coopération internationale. Celle-ci permet de partager les informations et de mener des actions simultanées comme l'arrestation, au même moment et dans plusieurs pays, de plusieurs organisateurs d'un réseau pédopornographique. Il arrive très régulièrement que la police française ou la gendarmerie participe à ce genre d'opérations. De même, la police judiciaire est en lien direct avec Singapour via un commissaire de police qui y est détaché. Nous collaborons aussi avec EC3, la plateforme d'Europol vouée à la cybercriminalité. L'objectif de toutes ces structures est d'être plus efficace sur le terrain mais aussi d'éviter les doublons, car lutter contre la cybercriminalité coûte très cher. Pourquoi faire enquêter plusieurs équipes, séparément, dans différents pays, quand on peut avoir une vision d'ensemble ?

Comment prenez-vous en compte le Dark Web, les tréfonds d'Internet, véritable repère de cybercriminels ?

Nous sommes démunis face au Dark Web. La quasi-totalité de nos actions se concentrent sur le Web ouvert, qui est déjà très large. Le Dark Web est un vrai problème, car les malfaiteurs les plus pointus techniquement l'utilisent de plus en plus pour des actions liées au terrorisme, aux trafics de stupéfiants ou au blanchiment d'argent. Nous sommes démunis, car nous n'avons pas assez d'outils pour l'explorer. Par définition, on ignore ce qui se passe sur le Dark Web, donc il est très difficile de le combattre. Nous échangeons régulièrement avec le FBI pour mesurer la menace du Dark Web et pour mettre au point des outils technologiques qui nous permettront d'identifier les malfaiteurs qui y opèrent.

Quels sont les pays les plus ciblés par les cyberattaques et ceux qui produisent le plus de cybercriminels ?

En volume, l'essentiel de notre action porte sur les escroqueries et les fraudes. Les pays les plus riches sont, logiquement, les plus ciblés par les cybercriminels. Ils en produisent aussi beaucoup, même si les malfaiteurs peuvent provenir de toutes les régions du monde, y compris de pays qui sont moins attaqués, comme l'Afrique de l'Ouest. La filière nigériane, notamment, fournit beaucoup de pirates numériques qui agissent partout.

L'État français a-t-il pris la mesure des enjeux autour de la cybercriminalité ?
Avec les États-Unis et l'Allemagne, la France est l'un des pays précurseurs dans la lutte contre la cybercriminalité. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé en 2001 par le ministère de l'Intérieur. C'est l'une des premières structures au monde. Sa création, qui remonte à avant même le 11-septembre, a fait office de déclic pour mettre en place un vaste réseau international qui garantisse une réponse coordonnée face aux cybermenaces. La France est régulièrement citée en exemple, notamment en Europe, car elle a des enquêteurs d'excellent niveau, spécialisés en criminalité informatique. Ce n'est pas non plus un hasard si le siège d'Interpol se situe à Lyon. À titre de comparaison, la plateforme européenne Europol a vu le jour il y a seulement deux ans.

Comment s'organise la lutte contre la cybercriminalité en France ?
L'action est coordonnée par le ministère de l'Intérieur, où travaille un « Monsieur cybercriminalité », Jean-Yves Latournerie, dont le rôle est de coordonner les différents services. La police et la gendarmerie ont chacune des enquêteurs spécialisés. La police judiciaire dispose aussi d'une division spéciale, la Sous-direction de lutte contre la cybercriminalité (SDLC). Depuis avril 2014, elle remplace et étend l'action de l'Office, créé en 2001. Quatre-vingts policiers et gendarmes de haut niveau y travaillent pour identifier et anticiper les cybermenaces. L'une de leurs missions est de surveiller le Web. C'est un travail extrêmement difficile, moralement, psychologiquement, notamment pour les agents qui effectuent la veille au sujet de la pédopornographie. Globalement, le champ d'action de la SDLC est plus large que celui de l'Office. Elle prend aussi en compte les attaques subies par les entreprises et les particuliers. Auparavant, les PME dont les systèmes informatiques étaient attaqués, par exemple, ne savaient pas vers qui se tourner, car les policiers de base n'ont pas forcément la connaissance suffisante pour traiter ce genre de plainte. La SDLC va alors conseiller les victimes qui se tournent vers elle, mais aussi les policiers, pour leur indiquer les questions qu'ils doivent poser et ce qu'il faut mentionner dans la plainte.

Les policiers de base reçoivent-ils une formation pour comprendre les nouveaux enjeux liés à Internet ?
Nous avons un budget consacré à la formation initiale. De nos jours, il est indispensable que chaque policier ait un minimum de connaissances sur ce qu'est Internet, comment fonctionnent les réseaux sociaux, qui sont les grands opérateurs, ce qu'est la cybercriminalité... De nombreux adolescents sont victimes d'arnaques ou d'agressions sur les réseaux sociaux, et de plus en plus de personnes subissent des fraudes sur Internet, liées notamment à l'e-commerce. Si tous les policiers maîtrisent le b.a.-ba d'Internet, ils sauront mieux réagir et aiguiller les victimes. Pour l'heure, ce n'est pas suffisant mais cela va venir. Nous n'avons jamais assez de moyens, mais la France fait partie des pays les mieux dotés au monde.

Une harmonisation des lois et des pratiques au niveau européen est-elle possible?
Des discussions sont toujours en cours, cela avance doucement. Il est clair que l'échelle nationale n'est pas suffisante, il faut agir au niveau européen et mondial. Nous souhaitons que la Convention de Budapest, rédigée par le Conseil de l'Europe en 2005, soit transposée au niveau mondial. Il s'agit du premier traité définissant les grands principes de la cybercriminalité. Il tente aussi d'harmoniser certaines lois nationales pour améliorer les techniques d'enquêtes en augmentant la coopération entre les nations. C'est un combat de longue haleine, car les pays n'ont pas tous la

même vision de ce qu'est la cybercriminalité et comment il faut la traiter. Il est important de s'organiser, car ce n'est que le début. On entre dans un monde connecté. Demain, il y aura des voitures sans conducteur, par exemple. Cela soulève des questions sur les moyens de prévention et de riposte contre les pirates numériques. Nous sommes dans une course-poursuite permanente pour nous mettre au niveau des cybercriminels, anticiper leurs attaques et utiliser la technologie contre eux. Plus les nouvelles technologies entrent dans notre quotidien, plus les possibilités d'infractions sont grandes, et plus la lutte contre les attaques est complexe

Liens : http://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html

Les mules :
A l'intérieur des opérations de cyber-criminalité

Les experts en sécurité offrent un aperçu de la façon dont les mules sont recrutées, payées et gérées par des cyber-gangs qui cherchent à voler vos données et votre argent.

Les passeurs d'argent recrutés ne sont peut être pas le plus sexy dans le cadre d'une opération de cyber-criminalité, mais ils sont pourtant parmi les points vitaux du trafic. Cela a d'ailleurs été souligné l'année dernière quand le FBI a arrêté des mules liées à un gang accusé du pillage de millions de banques à travers le monde.

Selon *Fortine***t,** les recruteurs de mules font de plus de plus en plus d'efforts en ciblant des pays spécifiques. Par exemple, l'entreprise a trouvé certaines de ces campagnes « localisées »qui ont utilisé des noms de domaine à consonance tels que asia-sitezen.com et australia-resume.com , qui tous deux ont été enregistrés avec le même contact en Russie.

« Les services se déplacent furtivement sur la Toile en changeant de pays et de monnaie en se basant sur la géolocalisation IP des visiteurs. Maintenant, cette méthode est aussi appliquée pour le recrutement des mules », a déclaré *Derek Mank***y,** chef de projet de cyber-sécurité et chercheur sur les menaces chez *Fortinet*. « Ce faisant, il est plus ciblé. L'un des exemples que nous avons vu avait établi une relation avec des banques locales comme une condition préalable. C'est parce que mules doivent généralement ouvrir plusieurs comptes et il est beaucoup plus facile de le faire si vous êtes un client de longue date. »

En ouvrant plusieurs comptes dans plusieurs régions, les cyber-criminels créent une couche de redondance dans leurs opérations, a t-il ajouté.

Dans la plupart des cas, le recrutement est local et cible des pays spécifiques, a déclaré Uri Rivner, chef des nouvelles technologies pour les consommateurs Identity Protection de la division d'EMC de sécurité RSA. Une exception à cela, cependant, est l'Europe, où le SEPA (Single European Payment Area) rend cette initiative moins nécessaire.

« Par exemple, si un fraudeur cible des victimes en Allemagne, ils n'ont pas à recruter des mules de l'Allemagne en raison du SEPA, » déclare Rivner. « Ils ne peuvent virer de l'argent d'une banque allemande à une banque en Lettonie. Selon la loi, il est considéré comme une transaction interne. Aux États-Unis, ce serait comme les banques le traitement des transactions entre les Etats. Les banques américaines devraient être très heureuses de ne pas fonctionner de cette façon en Europe parce qu'en Europe, le problème est beaucoup plus difficile en raison du SEPA. Il est donc plus facile de recruter des mules de n'importe où en Europe.

« Dans de nombreux cas que nous avons étudiés, les opérateurs des mule sont physiquement situés aux États-Unis où ils ont les coordonnateurs locaux des mule dans certains pays, a t-il poursuivi. « Ils gèrent les appels téléphoniques des mules, les questions de soutien, etc. Une chose qui semble être une nouvelle tendance est que de nombreuses mules sont des étudiants qui viennent tout en sachant qu'ils font partie d'une organisation criminelle ou alors qu'ils sont tout simplement stupides. Mais les opérateurs des mules leur promettent du travail aux États-Unis, et ils obtiennent un visa d'étudiant, ils volent aux États-Unis pour étudier et travailler à temps partiel comme une mule. «

Les experts de la sécurité conviennent que les organisations cyber-criminelles se présentent maintenant comme des entreprises de l'underground, une sorte de cyber-monde souterrain. Selon RSA, le nombre de sites Web spécialisés dans le recrutement de mules est passé de 34 en décembre 2007 à 591 en décembre 2009.

Les salaires des mules peuvent varier, avec des offres parfois exagérées par rapport à ce que les mules vont réellement obtenir, explique Manky.

La plupart des paiements, a t-il dit, se présentent sous la forme d'une commission, généralement environ 10 pour cent de chaque transaction. En raison de lois sur le blanchiment d'argent, la plupart des transactions restent sous la barre des $ 10,000 (USD), la moyenne se situant dans les milliers, a t-il ajouté.

« Comme toute relation d'affaire, une mule établie et ayant fait ses preuves aura plus de confiance vis à vis des opérateurs, et recevra donc des transactions plus importantes le plus souvent sur une base plus fréquente; donc ils vont gagner plus que d'autres, » a déclaré Manky.

Une autre façon utilisée par les fraudeurs est le vol en espèces suivit d'une opération de réexpédition, qui est l'endroit où un criminel utilise une carte de crédit volée pour acheter un article en ligne, puis expédié au domicile d'une mule.

« Les opérations avec des mules sont les grandes entreprises. Les cybercriminels recrutent des mules, et ces dernières expédient des marchandises hors du pays, vendent des marchandises sur les sites d'enchères, etc », a déclaré Rivner. C'est beaucoup de travail de contrôler les mules, les recruter et répondre à leurs questions. C'est une main-d'œuvre tout à fait unique. Les opérateurs de mules doivent être plus des managers que des pirates, il est donc logique de séparer les opérations. «

Liens : http://www.undernews.fr/hacking-hacktivisme/les-mules-a-linterieur-des-operations-de-cyber-criminalite.html

Fraude au clic : A l'intérieur du générateur d'or des cybercriminels

Le business de la publicité en ligne brasse des millions. Et quand un malware spécialisé s'y attaque, ça fait très mal. Les auteur du redoutable botnet de fraude au clic « *Redirector.Paco* » font fortune depuis 2014. Bitdefender Labs alerte sur le danger.

Cela fait plus de 2 ans qu'un groupe de cybercriminels génèrent d'incroyables bénéfices sans rien faire grâce à leur outil malveillant d'une extrême performance baptisé *Redirector.Paco*. Son but ? Remplacer les résultats de recherche classiques par ceux d'un programme publicitaire rémunérateur, en l'occurrence celui de Google Adsense. C'est donc là un immense botnet dédié à la fraude massive au clic sponsorisé par injection. On parle ici au bas mot d'un million de victimes dans le monde, autant dire que le détournement de liens vaut de l'or pour les pirates…

Le concept est simple et en même temps ultime : les cybercriminels à l'origine de *Redirector.Paco* ont fait en sorte que le malware qui, une fois installé sur un ordinateur, va remplacer les résultats naturels des moteurs de recherche par des résultats sponsorisés rémunérateurs générés par le programme publicitaire Google Adsense, notamment en modifiant les paramètres de connexion Internet des machines ciblée et ajouter un proxy sur-mesure qui intercepte et filtre l'ensemble du trafic Web (hijack). Pour survivre de manière durable sur les machines infectées, le cheval de Troie va créer de nouvelles clés dans le registre en se faisant passer pour Adobe Flash Player : *Adobe Flash Update* et *Adobe Flash Scheduler*.
Le malware va encore plus loin dans la sophistication pour garantir un taux de succès phénoménal et pour passer inaperçu au sein des systèmes, même via l'utilisation d'une connexion sécurisée SSL/HTTPS. Il ajoute pour cela lors de son installation sur la machine un certificat racine auto-généré capable de générer de faux certificats de sécurité pour les moteurs de recherches. La tromperie vaut des millions d'euros et ils empochent le jackpot !
Et il n'y a pas que les gains qui sont hors-norme. Et pour cause, l'étude révèle un mode de propagation quasi insensé : Pour distribuer massivement leur malware, les cybercriminels ont réussi a l'intégrer à des installateurs légitimes modifiés de programmes de renommée internationale tels que WinRar, YouTube Downloader, Connectify, Stardock Start8 ou encore KMSPico.
D'après l'étude publiée par les laboratoires Bitdefender, les pays les plus touchés seraient l'Inde, la Malaisie, les Etats-Unis, le Brésil, la Grèce, l'Italie mais aussi l'Algérie. Le botnet spécialisé dans la fraude au clic publicitaire gère aujourd'hui les moteurs de recherche populaires tels que Google, Bing et Yahoo, en proposant des clones exacts des pages de résultats respectives
23 mai 2016
Liens : http://www.undernews.fr/hacking-hacktivisme/fraude-au-clic-a-linterieur-du-generateur-dor-des-cybercriminels.html

Le blanchiment des fonds de la cybercriminalité : cryptomarchés et cryptomonnaies

Si le cybercrime devient de plus en plus accessible, les gains – souvent financiers – demeurent difficiles à monétiser lors de leur passage du virtuel vers l'économie réelle et licite. Par contre, les monnaies numériques dont le développement soulève de nombreuses questions tant au niveau de leur utilisation que de la législation, peuvent-elles représenter de nouvelles opportunités pour le cybercriminel ?

L'essor des cryptomonnaies

Lors de cette dernière décennie, les systèmes de monnaies virtuelles se sont non seulement multipliés mais également imposés en tant que véritable devise avec un taux de change de plus en plus intéressant.
Au «cours» actuel, certaines de ces monnaies numériques vont de 2 euros l'unité (Litecoin, BanxShares, SuperNet, etc.) jusqu'à dépasser les 210 euros le Bitcoin qui est devenu l'une des cryptomonnaies les plus populaires et utilisées dans le monde depuis 2009.
Ces nouvelles méthodes de paiement, pensées initialement comme solution alternative et à des fins légales, s'accompagnent de nombreux services facilitant les transactions mais également renforçant l'anonymat de leurs utilisateurs.

Attractivité des devises virtuelles : cible et moyen

Alors que peu de juridictions reconnaissent ces monnaies virtuelles comme de réelles devises, et certains Etats en interdisent leur utilisation (Thaïlande, Russie, etc.), on assiste de plus en plus à l'émergence d'importants réseaux de change (ZipZap, etc.) mais également à l'apparition de distributeurs de monnaie similaires aux traditionnels ATM.
Pour les (cyber)criminels, les disparités légales en la matière, la polyvalence, la popularité et les taux de conversion intéressants font de ces devises virtuelles un moyen efficace d'échapper aux services de paiement traditionnels – déjà régulés – où les risques de détection sont plus importants.
Dès lors, la monnaie virtuelle peut être non seulement une cible de la cybercriminalité (vol, mining, etc.) mais également permettre de réaliser des transactions illicites (marchés noirs, etc.) et de blanchiments grâce à l'anonymat et aux vides juridiques actuels propres à ces devises.

Blanchiment d'argent : un processus délicat, de nouvelles solutions

Les cybercrimes ont souvent pour finalité un gain financier. Profiter du butin induit généralement une transaction financière. C'est précisément l'une des étapes les plus dangereuses pour le cybercriminel car le passage du virtuel au réel l'expose inéluctablement aux risques d'être identifié.
La cryptomonnaie combinée aux modes opératoires traditionnels de blanchiment d'argent offre aux (cyber)criminels de nouvelles opportunités d'échapper à la détection et aux poursuites judiciaires :
– Le recours au *commerce électronique licite* : dans le cas de petits larcins virtuels, les cybercriminels opèrent à travers l'achat de produits sur les e-commerces licites notamment via des paiements en monnaie virtuelle. Afin de minimiser la traçabilité, les produits sont acheminés vers des dropzones (intermédiaires logistiques) ou house drop (maison/appartement vides).
– Les *casinos en ligne* : à travers les dépôts/jeux/retraits, le cybercriminel peut transformer sa cryptomonnaie en argent réel mais également blanchir ces fonds en les changeant en gains. De plus, ces casinos/sites de jeux en ligne sont souvent situés dans des pays offshore ou, à tout le moins, bénéficiant d'une législation financière plus légère faisant obstacle à toute remontée d'informations auprès des autorités financières et judiciaires.
– Le recours aux *«mules»* : les transactions bancaires sont souvent risquées puisque plus régulées. Afin de blanchir des gains illicites de manière sécurisée, les cybercriminels recourent le plus souvent aux mules. Ces intermédiaires sont enrôlés – de manière volontaire ou à leur insu (spam, fausses annonces d'emploi, etc.)– et ont pour mission de recevoir le butin illicite et de le transférer par la suite sur plusieurs comptes bancaires afin de blanchir les fonds du commanditaire ; les mules reçoivent en retour une commission significative qui contraste avec le peu de travail qu'ont nécessité ces opérations.
Liens : https://tetedansleguidon.com/2015/11/16/le-blanchiment-des-fonds-de-la-cybercriminalite-cryptomarches-et-cryptomonnaies/

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.
Liens : http://creobis.eu/aml/

Un réseau de blanchiment d'argent par Internet a été démantelé

La plate-forme numérique Liberty Reserve constitue la plus importante fraude financière décelée sur Internet. Ses dirigeants sont accusés d'avoir blanchi 6 milliards de dollars en sept ans.
La justice américaine a dévoilé *« la plus importante »* affaire de blanchiment traitée par les États-Unis. Elle a conduit à l'inculpation de l'émetteur de monnaie numérique Liberty Reserve et de sept de ses responsables. Créée en 2006 et enregistrée au Costa Rica, Liberty Reserve était une plate-forme de paiement électronique, permettant d'envoyer sans trace de l'argent n'importe où dans le monde, en dehors de toute réglementation.
Pour ouvrir un compte, il suffisait de donner, sur Internet, un nom, une date de naissance et une adresse électronique. Les transactions se réalisaient dans une monnaie numérique appelée L.R., du nom du site Liberty Reserve. Ces monnaies virtuelles peuvent s'acheter via des sites Web. Leurs cours varient suivant l'offre et la demande.
Les transactions étaient *« anonymes et impossibles à tracer »*, selon l'accusation. Pour ajouter à l'opacité, les utilisateurs de la plate-forme ne pouvaient pas y virer ou retirer directement des fonds, mais devaient passer par des sites « tiers ». Le site était utilisé dans de nombreux pays dont le Vietnam, le Nigeria, la Chine et les États-Unis.

Serveurs en Suède, en Suisse et au Costa Rica

Liberty Reserve était devenue *« la plaque tournante financière de la cybercriminalité »*, allant du vol d'identité à la pornographie enfantine en passant par le trafic de drogue et la fraude aux cartes bancaires, selon le procureur de Manhattan, Preet Bharara. Elle comptait plus de 1 million d'usagers, dont 200 000 aux États-Unis, qui en sept ans ont passé 55 millions de transactions. *« Presque toutes étaient illégales »*, a-t-il ajouté.
Au total, six milliards de dollars auraient ainsi été blanchis. *« Liberty Reserve était essentiellement une banque au marché noir »*, a déclaré Preet Bharara, ajoutant que ses serveurs, installés en Suède, en Suisse et au Costa Rica avaient été fermés et son nom de domaine saisi.

Le Trésor américain a mis Liberty Reserve à l'index

L'enquête a été menée par les forces de l'ordre de dix-sept pays. Sept responsables de Liberty Reserve ont été inculpés : cinq ont été arrêtés vendredi 24 mai en Espagne, au

Costa Rica et à New York, et deux autres sont toujours recherchés au Costa Rica. Le fondateur de la plate-forme Arthur Budovsky – âgé de 39 ans et habitant aux Pays-Bas – a été arrêté en Espagne, le cofondateur Vladimir Kats, 41 ans, à Brooklyn.
Arthur Budovsky avait déjà été condamné en 2006 à New York pour avoir tenté de lancer une opération similaire, sous le nom de « Gold age ». Il avait en 2011 renoncé à sa nationalité américaine pour devenir costaricain, *« afin d'échapper aux lois américaines »*. Le Trésor américain a mis Liberty Reserve à l'index comme *« une institution dont le but premier est de blanchir de l'argent »*.
Liens : http://www.la-croix.com/Economie/Un-reseau-de-blanchiment-d-argent-par-Internet-a-ete-demantele-2013-05-30-966734

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.
Liens : http://creobis.eu/aml/

Au tribunal de l'Internet : Une société sans pièces ni billets est-elle réaliste ?

Rendue possible grâce aux technologies, une société sans cash est-elle pour autant une bonne idée ? À vous de juger !
Le meilleur des mondes est-il un monde sans cash ? Certains économistes prédisent que, dans une dizaine d'années, nos porte-monnaie disparaîtront, faute d'argent liquide à y stocker. Des pays comme Suède et la Norvège sont déjà très en avance sur la voie des paiements dématérialisés, misant sur le développement exponentiel du paiement sans contact par carte et téléphone mobile. Et les fabricants rivalisent d'imagination sur ce marché prometteur. Google, par exemple, expérimente son nouveau service *Hands free* qui évite au client de sortir son téléphone de sa poche. Il suffit de dire au caissier « Je paye avec Google », de lui communiquer ses initiales et sa photo préenregistrée, et le paiement se réalise via les technologies Wifi et Bluetooth.

Les adeptes d'une société sans pièces ni billets vantent ses multiples avantages, à commencer par la simplicité et la rapidité des transactions. Faute d'avoir à sortir sa carte et à taper son mot de passe, le consommateur est protégé contre le risque d'usurpation de ses données bancaires. En outre, la traçabilité des opérations empêchera le blanchiment d'argent, l'évasion fiscale et le travail dissimulé. La dématérialisation des paiements est, en revanche, un terrain propice aux cyberattaques visant les terminaux de paiement et les serveurs. Et d'ailleurs, en Suède, les fraudes aux paiements électroniques ont été multipliées par deux en 10 ans.

Verrouillage étatique ?

Par ailleurs, du point de vue des libertés, est-il prudent de confier son patrimoine financier à des machines ? Certains experts en doutent, pressentant l'asservissement des individus à une sorte de dictature orwellienne : « La société sans cash qu'on nous promet grâce au numérique donnerait aux décideurs – sans possibilité d'échappatoire pour les particuliers, faute d'avoir assez d'argent liquide – les moyens de contrôler tout le système : pensons au verrouillage des retraits de cash en Grèce », avance le professeur d'économie Henri Bourguinat dans une tribune publiée par le journal *Le Monde* en mars 2016.

La fin de l'argent liquide est-elle une bonne idée ? À vous de juger ! Mais après avoir regardé le 43e épisode de la série Au tribunal de l'Internet ! dans lequel nos deux expertes, Myriam Quemener et Christiane Féral-Schuhl, plaident le « pour » et le « contre » en... trois minutes ! 23/05/2016

Liens : http://www.lepoint.fr/justice-internet/au-tribunal-de-l-internet-une-societe-sans-pieces-ni-billets-est-elle-realiste-23-05-2016-2041285_2081.php

Les nouvelles formes de scam : les mules et le blanchiment

Méthode de nouveaux trafiquants: les scammeurs

Les nouvelles victimes de scam ne sont plus des individus naïfs qui se font soustraire leur argent. Maintenant, ce sont des personnes crédules mêlées à des traffics d'argent.

Bientôt fini le temps du scams 419 où des correspondants soi-disant nigérians arnaquent des personnes naïves et leur soutirent jusqu'à plusieurs dizaines de milliers d'euros ? Il semble que la nouvelle forme de scam soit plus imaginative dans la mesure où le scammeur ne cherche plus à soutirer directement de l'argent à la victime. Il acquiert l'argent par d'autres moyens illégaux (vol de carte bleue, piratage de comptes bancaires ou de comptes paypal, etc…), mais se sert de la victime comme d'une mule.

En matière de trafic de drogue, une mule est une personne qui fait passer la drogue au travers des postes de contrôles. Le trafiquant a donc intérêt à choisir la mule qui semble la plus innocente possible, de manière à ne pas alerter les contrôleurs. De même, il doit cloisonner totalement la mule, qui ne devra pas savoir qui est son commanditaire. En matière de fraudes sur l'Internet, le plus dur n'est pas la fraude elle-même, mais de pouvoir profiter des fruits de la fraude tout en restant intraçable. Or, pour recevoir l'argent ou les colis achetés grâce à une CB volée, il faut une identité et une adresse, tous les deux aisément traçables. C'est ici qu'interviennent les mules, que les scammeurs convainquent d'accepter de recevoir et garder un paquet ou une somme chez eux jusqu'à ce qu'on vienne les récupérer à une date future.

Le principe est le même que pour un scam traditionnel. Le scammeur entre en contact avec une mule potentielle. Il faut noter ici l'apport immense des réseaux sociaux du type Facebook ou Second Life, qui facilitent la tâche des scammeurs, puisque non

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

Les jeux sur Internet favorisent le blanchiment

Dans un rapport, le service central de prévention de la corruption affirme que «le grand banditisme a su tirer profit de l'économie virtuelle», et met en garde l'État sur les risques d'Internet.
Côté statistiques, l'état de la corruption en France n'a pas bougé. Le nombre de jugements prononcés depuis dix ans est quasiment stable : en 2006, une centaine de chefs d'entreprise, élus ou fonctionnaires ont été définitivement condamnés pour corruption active ou passive, pour des scandales remontant souvent à plusieurs années. Le dernier rapport du service central de prévention de la corruption (SCPC), dont Le Figaro a pris connaissance, relève même que ce genre de dossiers ne représente que 0,023 % des «affaires poursuivables» dans les tribunaux de la région parisienne. «Des progrès en terme de détection paraissent envisageables», estime sobrement le magistrat Michel Barrau, chef de cet organisme interministériel crée en 1993 et qui dépend du garde des Sceaux.
Le service central de prévention de la corruption adresse cette année sa principale mise en garde aux partisans de la libéralisation des jeux sur Internet. Nouvelles

formes de fraudes, enquêtes rendues presque impossible par la multiplicité des interlocuteurs… Selon le rapport du SCPC, l'ampleur actuelle des flux suspects est de nature à multiplier les délits de corruption et de blanchiment. Pour la criminalité organisée, décrit le rapport, «il est relativement facile de blanchir des fonds illégaux à partir d'un site de jeu sur Internet». Les casinos virtuels, souvent basés à Malte ou à Gibraltar pour des raisons fiscales, permettent, par exemple, de fournir des gains de jeu officiels à des joueurs ayant misé de l'argent sale. Il s'agit simplement de la version moderne du blanchiment ou du casino utilisé jadis par les mafias italiennes ou new-yorkaises.

Autre grand risque de ces salles de jeu apparues sur Internet : les nouvelles corruptions autour des compétitions sportives. Il s'agit pour un groupe criminel de corrompre joueurs ou entraîneurs afin de truquer les matchs sur lesquels des millions d'euros sont pariés. Le rapport relève que les autorités mondiales du football sont déjà vigilantes sur l'activité des bookmakers, mais «il serait souhaitable que les lobbyistes et les États qui prônent l'ouverture à la concurrence de ce secteur prennent conscience qu'il ne s'agit pas d'une activité économique ordinaire mais d'un secteur danslequel le risque est patent, connu, irréfutable et que le choix de l'absence de contrôle pourrait favoriser la criminalité.»

L'obstacle du secret bancaire

Faisant allusion à l'affaire du cercle Concorde, cercle de jeu parisien fermé il y a tout juste un an avant une série de mise en examen pour association de malfaiteurs, extorsion de fonds et corruption, le rapport du SCPC insiste : «des exemples récents montrent qu'il est difficile de contrôler des jeux installés physiquement sur un territoire. Qu'en sera-il alors, si on y ajoute l'utilisation d'Internet et des paradis fiscaux ?» Sur ce point, la lutte contre les mafias ayant trouvé des débouchés sur les casinos virtuels et les longues enquêtes financières internationales se rejoignent. Elles butent sur les mêmes barrages. Les investigations se heurtent systématiquement à la difficulté de retracer les flux financiers empruntés.

Le juge financier Renaud Van Ruymbeke, intervenant récemment au cours d'un colloque organisé par la société d'avocats Carbonnier Lamaze Rasle, exposait ainsi que «face aux détournements menés par le biais de circuits offshore, il faudrait s'interroger sur des mesures comme la levée du secret bancaire en Suisse, au Liechtenstein, à Gibraltar ou aux îles Caiman, mais on se heurte à des résistances très fortes».

Liens : http://www.lefigaro.fr/actualite-france/2008/11/10/01016-20081110ARTFIG00581-les-jeux-sur-internet-favorisent-le-blanchiment-.php

Espagne: un réseau international de cyberpirates démantelé

Madrid (AFP) - La police espagnole a annoncé vendredi le démantèlement d'un réseau international piratant les messageries électroniques de chefs d'entreprises pour leur soutirer des centaines de milliers d'euros au bénéfice de Nigérians.

"Quarante-quatre personnes ont été détenues: 43 en Espagne et une au Royaume-Uni dont les 17 plus hauts responsables du réseau", a assuré la police dans un communiqué.

Le montant des fonds obtenus frauduleusement allait de 20.000 à 1,8 million d'euros.

"Certains des dirigeants du réseau, d'origine nigériane (...) opéraient en cachant leur véritable identité", a souligné la police.

Interrogé par l'AFP un porte-parole de la police n'a pas été en mesure de préciser la date des arrestations et la nationalité des suspects.
Des perquisitions ont été menées en Espagne et au Royaume-Uni et notamment "dans un local d'un aéroport de Londres où étaient stockées d'importantes quantités d'argent liquide avant leur envoi vers le Nigeria", selon la police.
En Espagne, sept personnes qui dirigeaient un cybercafé de la région de Madrid sont soupçonnées d'avoir organisé les envois hebdomadaires d'argent vers le Nigeria par avion. C'est ainsi que "135.000 euros en billets ont été découverts à l'aéroport de Madrid, dissimulés dans des sacs poubelles cachés parmi des sous-vêtements, dans une valise devant voyager en soute".
L'enquête avait débuté fin 2014 avec la plainte d'un citoyen pakistanais victime d'une escroquerie de 34.000 euros par le piratage de son compte bancaire.
Selon la police le mode opératoire consistait à "pirater les comptes de courrier électronique de dirigeants d'entreprises (...) pour avoir accès à des données confidentielles".
A partir de ces comptes, les "hackers" envoyaient ensuite des courriers aux différents contacts du dirigeant, avant de développer leurs escroqueries.
Parmi les personnes interpellées figurent "de nombreux entrepreneurs espagnols" soupçonnées d'avoir servi à blanchir des fonds. Publié le 06-05-2016
Liens : http://www.sciencesetavenir.fr/high-tech/20160506.AFP4440/espagne-un-reseau-international-de-cyberpirates-demantele.html

Les banques face à la révolution numérique

Après le thème de l'emploi, je vais continuer cette petite série de l'été sur les faux semblants du numérique. Nous allons passer en revue quelques industries ou métiers dont la disparition est parfois annoncée quelque peu prématurément. Exemples retenus : les banques, la télévision et les usines.
A chaque fois, ces industries ont ou font face aux révolutions numériques et font face à de nouvelles formes de concurrence. Leurs réseaux physiques traditionnels sont transformés. Mais elles s'adaptent et ne fléchissent pas pour autant.

Les banques de détail

Les banques de détail ont été particulièrement affectées par l'avènement du numérique et de la mobilité et notamment leurs réseaux d'agence dont on n'a plus besoin comme auparavant ! Il y a dix ans, on pouvait prédire soit la fin des banques traditionnelles, soit de leurs agences de détail. Aujourd'hui, qu'en est-il ? Les banques sont toujours là, tout comme leurs agences de détail, même si leur nombre commence tout seulement à décroitre. Les désintermédiateurs en puissance ne manquent pas mais aucun n'a réellement réussi à déloger les banques. Elles ont plutôt bien résisté au tsunami numérique même si leurs métiers ont été profondément transformés. Et on ne parle même pas des crises financières tout comme des évolutions de la règlementation prudentielle et des ratios de solvabilité (Bâle II & III).
Cela fait longtemps nous pouvons gérer une grande partie de nos transactions financières en ligne dans les banques traditionnelles : obtenir l'état de ses comptes, effectuer des virements immédiats, différés ou réguliers, et même mener différentes transactions financières plus spécialisées. Cela avait même commencé à l'époque glorieuse du Minitel ! Et on peut faire cela surtout tous les écrans, notamment mobiles.

La banque directe

Les réseaux de banques traditionnelles ont aussi lancé leurs offres de banques directes, sans agences : eLCL chez LCL, Agence Directe à la Société Générale, Hello Bank à la BNP-Parisbas, CMUT Direct au Crédit Mutuel, Filbanque au CIC, diverses offres dans les différentes caisses régionales du Crédit Agricole, et aussi AXA Banque (anciennement Banque Directe)
Liens : http://www.oezratty.net/wordpress/2013/banques-revolution-numerique/

Carte visa anonyme sur internet : un mythe ?

L'avènement des banques en ligne sur internet a coïncidé avec l'évolution des moyens de paiement de par le monde : propagation des cartes bancaires, diminution du cash, échanges transfrontaliers via des solutions de type Western Union.
Or, qu'est ce qu'une banque en ligne apporte de fondamentalement nouveau par rapport aux géants du marché type BNP Paribas ?

- La rapidité internationale : pour qu'un virement à l'étranger soit disponible quasi-instantanément. C'est utile en cas de besoin urgent d'argent.
- Le paiement alternatif : pour éviter de donner un numéro de carte de crédit ou un RIB, on peut fournir un identifiant de compte de type « e-wallet » : l'exemple le plus connu est Paypal
- L'anonymat : certaines banques en ligne permettent l'émission de cartes de crédit sans nom, donc anonymes.
- Le multi-devises : certains comptes permettent de convertir instantanément de l'argent d'une devise à l'autre.
- Nous lançons donc une série sur les comptes bancaires du 21ème siècle. Aujourd'hui, nous allons explorer le point de l'anonymat.

Anonyme, c'est à dire ?
Que veut dire être « bancairement » anonyme sur Internet ? Cela dépend par rapport à qui l'on veut être anonyme.
Cela peut être par rapport au marchand ou à l'institution. Vous ne souhaitez pas qu'il connaisse votre no de compte ou votre no de carte bancaire.
Cela peut aussi être vis-à vis de l'état. Vous ne souhaitez pas que certaines entrées d'argent apparaissent sur vos comptes « officiels ».
Enfin 3e cas surtout réservé aux marchands, vous pouvez souhaiter être anonyme par rapport à la réception de paiements sur internet, et donc ne pas leur donner vos coordonnées bancaires réelles
Tout anonymat est relatif
Bien sur, l'anonymat bancaire n'a rien à voir avec l'anonymat tout court. A cause des lois contre le blanchiment, désormais presque toutes les banques et porte-monnaies électroniques demandent des preuves d'identité. Et puis de toute façon, un anonymat bancaire pose toute sa confiance dans le fait que la banque gardera vos informations secrètes : mais lorsqu'on sait que toutes les grosses boites américaines collaborent avec la NSA, il n'y a aucune raison que Paypal et consorts ne collaborent pas avec le fisc ou l'IRS américain. Au moindre doute, vos données personnelles seront dévoilées, et même s'il s'agit du numéro de carte bancaire qui vous a servi à alimenter votre compte « anonyme », il permettra de remonter à votre banque « officielle » et donc jusqu'à vous.

Même dans le cas idéal d'un PMÉ (Porte Monnaie Électronique) sans pièce d'identité et sans numéro de carte bancaire, qui serait alimenté via un autre PMÉ, vous ne serez jamais vraiment anonymes : d'abord parce que, comme avec les histoires de paradis fiscaux, le gouvernement ou l'organisation qui veut vous connaître, peut essayer de remonter le fil de vos PMÉ jusqu'à tomber sur une banque « traditionnelle » d'un pays collaborant, qui filera vos infos personnelles.
Ensuite parce qu'en admettant que les méchants qui vous en veulent butent sur votre PMÉ, vous devrez bien à un moment ou un autre utiliser votre argent. Là encore, soit vous le dépensez uniquement sur des sites internet qui permettent des livraisons anonymes (heu?), soit vous allez retirer de l'argent dans des DAB ou payer avec votre carte de crédit dans des magasins réels. Dans ces trois cas, les méchants pourront vous tracer géographiquement. Il sera un peu plus possible de vous cacher sur internet (en passant par un proxy) mais cela reste imparfait. Quant au réel, à moins de payer une personne pour aller retirer votre argent, les caméras de surveillance et vos habitudes de déplacement permettront de vous attraper « physiquement ».

Pourquoi être anonyme ?

Les raisons d'être bancairement anonyme se déduisent de la liste des interlocuteurs :

- Éviter les risques de piratage, via utilisation d'un numéro de carte différent
- Donner à ses interlocuteurs un numéro de compte différent de son compte principal, afin qu'ils ne puissent pas vous prélever plus que prévu
- Se créer une nouvelle identité pour avoir une carte de crédit et un compte, par exemple pour un interdit bancaire.
- Pouvoir sortir de l'argent gagné par internet, de façon discrète, en liquide ou par des paiements en ligne, avec une autre carte de crédit, sans passer du tout par ses comptes « normaux ».
- Accepter des paiements de l'étranger, dans une autre monnaie
- Convertir facilement de l'argent d'une monnaie à une autre
- Utiliser sa carte d'une autre devise, dans un pays étranger, pour réduire les frais

Comment être anonyme ?

Les solutions d'anonymat, il n'y en a plus tant que ça. D'abord les PMÉ. Ils répondent à la plupart des besoins d'anonymat, sachant que Paypal est le moins « anonymisé » de tous car il n'offre pas de carte de crédit.

- Entropay permet d'avoir une carte Visa prépayée. Elle peut être au choix virtuelle ou réelle (« plastique »). Mais les moyens de remplissage sont limités : une autre carte de crédit, ou un virement. Pas d'autres PMÉ, ce qui limite l'intérêt. Sinon, on peut recevoir des paiements, et changer de monnaie, comme avec Paypal. Il s'agit donc en gros d'un Paypal en un peu mieux car avec carte de crédit. Les frais sont élevés :
    - 4,95% pour charger de l'argent sur la carte
    - 1,95% pour en recevoir
    - 4,50euros pour décharger
    - des frais pour les virements entre comptes Entropay, etc..
- Skrill est très similaire à Entropay, mais permet d'avoir une Mastercard et non une Visa. Skrill permet aussi, à la manière de Paypal, de payer avec son PMÉ (et non la Mastercard associée) sur un site. Mais ce mode de paiement est encore peu accepté, en comparaison avec Paypal. Les frais sont modérés
    - Mastercard : 1,80 eur pour un retrait à un DAB
    - Mastercard : 2,49% lors d'une conversion de devise
    - Mastercard : 10 euros de frais fixe par an

    - 1,90% pour charger de l'argent par CB sur la carte
    - 2,95eur pour transférer de l'argent de son compte Skrill vers un compte Bancaire ou une autre carte.
    - Envoi d'argent entre pays (concurrent de Western Union) : environ 3,99% (2,99% de frais de change et maximum 1% de frais fixe). Ce qui est malin c'est que le destinataire crée à son tour un compte Skrill et retire ses fonds avec sa Mastercard à lui ou paye avec cette carte.
- Speedcard.com est réalisé par FBME, une banque Chypriote peu regardante sur les détails personnels. Cependant les fonctionnalités sont à peine identiques à Entropay. Les frais restent élevés (l'équivalent de 3 euros par mois, plus des frais par chargement et par retrait). Son avantage était de permettre l'ouverture d'un compte anonyme jusque 500 euros. Mais c'est terminé depuis 2013 on dirait
- Ecopayz est aussi un clone d'Entropay mais il est le premier de notre liste à permettre effectivement de créer un compte sans donner de nom. Son autre avantage est de permettre le chargement depuis de nombreux PMÉ exotiques comme moneta.ru, InstantBank, Sofort… Leur carte mastercard s'appelle « Ecocard », en mode anonyme elle n'est que virtuelle pour des paiements sur internet.

Tous ces PMÉ sont assez restreints en anonymat, à cause des lois sur le blanchiment, mais ils seront utile par exemple pour un joueur de poker en ligne qui se fait payer en dollars US par une site américain et souhaite pouvoir retirer son argent en euros via une carte mastercard

Blanchir du cash

Un autre anonymat peut-être requis pour « blanchir » de l'argent liquide, en le faisant rentrer sur un compte anonyme..

La solution peut-être Ukash. Vous donnez des espèces à un bureau de tabac, en échange vous obtenez une carte de type « carte téléphonique des années 90″.. Son numéro garantit son authenticité et ensuite vous pouvez utiliser votre ukash en ligne : soit sur quelques sites (principalement des casinos, sites de rencontres, etc..) soit pour alimenter un PMÉ comme Neteller. Ensuite Neteller permet d'avoir une Mastercard, et le tour est joué.

Une carte de crédit anonyme ?

Nous avons donc des comptes anonymes, des cartes « alternatives » (mais pas anonymes).. il nous manque dans notre panoplie, une carte vraiment anonyme.

D'après des sites experts, il vaut mieux acheter ces cartes de crédits contre du cash chez un buraliste. En tout cas aux USA, on vous demande uniquement un nom et une adresse, mais elles ne seront jamais vérifiées, à part par les systèmes de paiement américain qui demandent le nom et l'adresse. Il suffit alors de leur donner les mêmes infos pipeau que lors de l'achat. Ce sont en fait souvent des cartes cadeau, avec des montants fixes, et utilisables en ligne car elles ont un no de carte compatible Visa ou Mastercard. Il y a par exemple les cartes de Simon (jusque 500$) ou IDTPrime au UK. Si la carte doit être activée en ligne, pensez bien à passer par un anonymiseur de type « Tor ».

Mais bien sur, une carte qu'il faut charger en cash, il nous en faut une disponible en France, et puis, si possible, une autre qui soit chargeable via un PMÉ.

InstantVCC permet d'acheter des cartes virtuelles, qui donnent aussi un IBAN. Aucune vérification d'identité. Chargement via PerfectMoney, OKPay ou Western Union. Pour 30$, vous aurez une carte valable 3 ans, et top du top, chargeable depuis Paypal. Sortir ses bénéfices internet vers une carte « discrète » pour éviter de faire

transiter l'argent par son compte et alerter le fisc, n'aura jamais été aussi facile. Ces cartes sont liées à des comptes en Pologne et sont limitées à 2500 euros d'utilisation par an. Et attention, les frais de chargement sont élevés : 10%. Le prix de l'anonymat..
Ultimate Anonymity vend des cartes virtuelles limitées à 500$, non rechargeables.
Unitrust Capital vend pour 185$ une carte bancaire offshore. D'autres sites comme PrivacyWorld vendent soi disant des packages clés en main avec comptes et cartes anonymes mais à des prix délirants, 1000, 2000 ou 5000 (!) euros.. à ce prix là, autant vous payer un aller-retour aux Bahamas ou un autre paradis fiscal pour y ouvrir un compte anonyme…
Sur [http://anonymousdebitcards.weebly.com/: site défunt depuis 2015], vous pouvez aussi payer 500$ pour avoir une carte anonyme dans une banque américaine, mais après avoir donné une copie de passeport scannée.. l'anonymat est donc tout relatif, sauf si vous fournissez de faux papiers..
Enfin chez eNumbered.com, un concurrent de Paypal, pour 150$, vous pouvez avoir une carte anonyme. Cette carte vient d'une banque européenne et a une limite de 160$ de retrait par jour. L'intérêt est qu'elle peut être chargée depuis de nombreux PMÉ.
Edit 2015 : ENumbered était apparemment aussi un scam et a arrêté ses opérations
Liens : http://www.rentables.fr/depenser-moins/anonymat-bancaire-sur-internet-un-mythe/

Fraude informatique

La fraude informatique est la variante informatique de l'escroquerie au sens classique du terme. L'escroquerie consiste à soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand quelqu'un utilise à cette fin des moyens de communication modernes, le législateur considère qu'il s'agit également d'escroquerie. Internet permet, dans un délai rapide et à moindres frais, de toucher un grand nombre de victimes.

Pratiques connues

1. Transactions financières

Il vous est peut-être arrivé de recevoir un e-mail vous proposant de grosses sommes d'argent à changer ou à blanchir. L'arnaque consiste à vous faire croire qu'il est possible d'encaisser d'importants bénéfices excédentaires d'une instance soi-disant officielle. Cet e-mail sollicite votre aide : on vous demande de verser de l'argent ou transmettre des documents d'entreprise. En échange, on vous promet une participation aux bénéfices de l'ordre de 20 % ou plus.
Il existe, dans cette catégorie, un autre type de criminalité : le "phishing". Par ce procédé, des criminels reproduisent des sites d'entreprises ou d'organisations connues pour voler des données personnelles, des mots de passe et des sommes d'argent.

2. Loteries ou jeux de hasard

Vous recevez par e-mail un avis vous indiquant que vous avez gagné le gros lot à une loterie ou à un jeu de hasard. Pour recevoir votre prix, vous devez d'abord verser une somme d'argent.
Les loteries officielles ne fonctionnent pas de cette manière : vous ne pouvez recevoir un prix qu'après avoir acheté un billet de loterie, un billet à gratter ou un bulletin de loto. La loterie ne prend jamais contact avec le gagnant : ce dernier doit en prendre l'initiative.
Parier n'est pas punissable. En revanche, exploiter des jeux de hasard sans une autorisation de la Commission des jeux de hasard l'est effectivement. Selon la loi sur

les jeux de hasard, il est interdit en Belgique d'exploiter des jeux de hasard ou des établissements de jeux de hasard, sous quelque forme, dans quelque lieu et de quelque manière que ce soit. Seul un nombre d'établissements défini par le législateur peuvent organiser des jeux de hasard. Cela signifie donc que les casinos et les jeux d'argent en ligne sont toujours illégaux en Belgique.

3. Héritages

Vous recevez par courriel un avis d'un soi-disant organe officiel étranger ou d'un soi-disant "notaire" étranger. Ce message précise qu'après de longues recherches, on a pu vous identifier comme étant le (seul) héritier d'une personne très riche récemment décédée. Mais attention : pour pouvoir recueillir l'héritage, vous devez d'abord verser une somme d'argent, destinée soi-disant à régler tous les frais administratifs. Vous comprenez dès lors qu'il ne s'agit pas ici d'un vrai notaire, mais bien d'escrocs qui en veulent à votre argent.

4. Investissements exotiques

Vous recevez par e-mail des propositions (malveillantes) d'investissements dans des projets exotiques, avec promesses de gains astronomiques à la clé. Bien entendu, il s'agit ici encore de fraude.

5. Passeports, visas, documents, …

Les escrocs tentent aussi de jouer sur vos sentiments. Dans certains e-mails par exemple, on vous demande de verser de l'argent pour quelqu'un qui a besoin de toute urgence d'un passeport, d'un visa ou d'un autre document officiel. Pour vous apitoyer, l'e-mail décrit avec force détails les conditions de vie déplorables d'un pays situé à l'autre bout du monde. L'argent que vous devriez verser servirait à payer l'intermédiaire chargé de délivrer le document. Il va de soi que vous ne verrez jamais cette personne et que vous aurez tout simplement perdu votre argent …

6. Achats sur Internet

On peut acheter à peu près tout sur Internet. Mais tous les vendeurs ne sont pas fiables. Certains, surtout à l'étranger, ne livrent pas les biens achetés et payés.

7. Ventes sur Internet

Vous placez une annonce sur Internet dans le but de vendre quelque chose. Une personne ou une entreprise accepte l'offre sans même discuter le prix demandé. L'escroc peut alors procéder de différentes manières : il vous donne un chèque sans provision, vous demande de verser une garantie sur un compte à l'étranger …

Liens :

http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/fraude_informatique

Criminalité informatique

Les ordinateurs font partie intégrante de la vie des citoyens et des entreprises. Internet est devenu l'un des moyens les plus importants d'information et de communication.

Le revers de l'impact grandissant de l'informatique est que la criminalité informatique devient à la fois de plus en plus rentable et peut causer toujours plus de dégâts. Un virus informatique relativement simple peut rapidement entraîner une perte économique de plusieurs millions d'euros.

Cette évolution s'explique, en grande partie, par les caractéristiques d'Internet :

- Le réseau Internet est immatériel : les actions ne sont pas vraiment tangibles mais occasionnent de réels préjudices ou dégâts.
- Il est mondial : les frontières disparaissent.

- Tout se produit en temps réel : les résultats se font sentir instantanément.

La loi décrit quatre nouveaux délits relatifs à la criminalité informatique :

- le faux en informatique
- la fraude informatique
- la manipulation de données
- le "hacking"

Liens : http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique

"hacking"

Hacking est une notion très vague. Même les informaticiens ne tombent pas d'accord sur la signification exacte du mot. Hacking consiste à pénétrer illégalement dans un système informatique. Cette "effraction" implique généralement une intention frauduleuse. Mais établir involontairement une connexion et la maintenir volontairement est également considéré comme du piratage. Même pirater un système informatique qui n'est pas ou à peine sécurisé est punissable.

Dans l'évaluation de hacking, la loi distingue les 'insiders' des 'outsiders'. Les insiders sont des personnes qui ont une autorisation d'accès, mais qui outrepassent cette autorisation. Ces personnes ne sont punissables que si leur piratage cache une intention de nuire ou une intention frauduleuse. Pour les 'outsiders', cette restriction n'existe pas : ils sont dans tous les cas passibles de sanctions, même s'ils s'introduisent dans un système avec "de bonnes intentions".

Il est interdit de collecter ou d'offrir - contre rétribution ou non - des données permettant des violations informatiques. Cette interdiction vise surtout à juguler le commerce de codes d'accès et de 'hacking tools'.

Les pirates informatiques utilisent parfois un grand nombre "d'ordinateurs zombies". Il s'agit d'ordinateurs individuels ou de sociétés mal protégés et infectés par un "cheval de Troie". Le cheval de Troie est un programme qui permet à un malfaiteur de prendre le contrôle d'un ordinateur relié à Internet et de l'utiliser. Votre ordinateur peut lui aussi être intégré dans un tel réseau. Le pirate a ainsi le contrôle total sur votre ordinateur et a accès à vos données.

Protégez votre ordinateur contre le piratage, car une fois que quelqu'un y a accès, tout est possible : le pirate peut non seulement fureter à sa guise mais également utiliser votre ordinateur à des fins illégales ou détruire vos fichiers.

Liens http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/hacking

Faux en informatique

Constituer un faux en informatique consiste à modifier ou à effacer des données d'un système informatique ou à modifier l'utilisation de ces données, de manière à entraîner également la modification de leur portée juridique.

Cette notion a été introduite pour mettre fin aux problèmes que suscitait la notion de "faux en écriture" appliquée aux données informatiques. Des exemples de faux en informatique sont la falsification de cartes de crédit, de moyens de paiement numériques, de signatures électroniques.

Liens :
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/faux_en_informatique

Escroquerie sur Internet

Lors d'une escroquerie sur internet, l'imposteur change délibérément des données électroniques pour soutirer de l'argent. L'escroquerie sur internet ressemble très fort à la fraude sur internet mais dans ce dernier cas, l'imposteur ne manipule pas des données mais bien des personnes.
Quelques exemples d'escroquerie sur internet :

- l'utilisation d'une carte de crédit volée pour retirer de l'argent à un distributeur automatique
- le dépassement illicite du crédit octroyé par une carte de crédit
- l'installation ou la modification de programmes dans le système d'autrui afin d'obtenir régulièrement des paiements par l'intermédiaire de ces programmes

Liens :
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/escroquerie_sur_internet

Blanchiment des capitaux, nouvelle tendance de la cybercriminalité

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

Blanchiment d'argent : La cybercriminalité en plein recrutement

Profitant de la crise financière et du sentiment d'insécurité l'accompagnant, les cybercriminels recherchent des « mules »
Profitant de la crise financière et du sentiment d'insécurité l'accompagnant, les cybercriminels recherchent des « mules », intermédiaires pour des opérations de blanchiment d'argent. Les laboratoires de sécurité G DATA alertent les internautes d'une montée en flèche des spams de recrutement depuis le début de l'année.

La crise financière, un contexte idéal

« En période de crise financière, la tentation pourrait difficilement être plus grande : de l'argent rapide et facile. Avec de telles offres, les cybercriminels tentent aujourd'hui de recruter massivement les destinataires d'emails comme supposés agents financiers. Celui qui mord à l'hameçon devient un blanchisseur d'argent et donc un complice, avec toutes les conséquences déplaisantes que cela implique, telles des poursuites judiciaires», explique Ralf Benzmüller, directeur des laboratoires de sécurité G DATA.

Un emploi de rêve

L'opportunité d'embauche proposée dans ces emails est plus qu'alléchante : travailler comme agent financier ou chef de transaction, pour quelques heures par semaine seulement et à partir de son domicile, contre une rémunération élevée. L'activité de la « mule » consiste à accepter des transferts d'argent sur son compte personnel. La victime utilise ensuite les services de transfert de fonds comme la Western Union pour envoyer l'argent vers une supposée adresse d'entreprise, en Europe de l'Est le plus souvent. L' « employé » conserve un certain pourcentage sur le montant du transfert, généralement entre 3% et 5%, comme commission pour le service.

L'arnaque

Le transfert entrant a pour origine des fausses enchères en ligne ou des transactions effectuées de manière illégales par des attaques de phishing réussies. Les criminels utilisent l' « agent » comme simple blanchisseur d'argent. Une fois que l'argent est en

route vers le compte étranger, la victime escroquée précédemment n'a quasiment plus aucune chance de récupérer son argent.Lorsque la fraude est découverte, ce sont les blanchisseurs d'argent insouciants qui reçoivent les demandes de dommages et intérêt ou les lettres de l'accusation.
Les experts des laboratoires de sécurité de G DATA déconseillent expressément de répondre à ce type d'offres d'emploi et recommandent aux destinataires d'effacer les mails correspondants sans même les lire.
Liens : https://www.gdata.fr/espace-presse/communiques/article/1091-blanchiment-dargent-la-cy

Focus sur la lutte contre la fraude documentaire liée au blanchiment d'argent

Les avancées spectaculaires en matière de technologie informatique et de communication offre une large gamme de possibilités, avantages, inconvénients et risques. Des réseaux d'ordinateurs et de télécommunications (Internet) augmentent l'efficacité des services et améliorent la vie quotidienne. L'utilisation de ces technologies comporte également de nouveaux dangers, non seulement pour notre vie privée et nos libertés, mais également lors de nos transactions financières.
Afin de répondre de manière appropriée à la lutte contre la fraude documentaire, qui va souvent de pair avec des infractions pénales plus graves, ce qui affecte encore plus notre société, les acteurs financiers (banques, compagnies d'assurances et de cartes de crédit,… mais également d'autres acteurs du circuit économique comme les sociétés commerciales,…) doivent se munir de moyens de détection et de contrôle sophistiqués et adéquats. Acquérir une attitude critique et disposer de connaissances actualisées sur la fraude (documentaire) par leurs membres du personnel sont d'autres facteurs-clé. Via une approche professionnelle de scepticisme, nous devons être capables de reconnaître et de détecter les indicateurs et les typologies de tentatives de contrefaçon et de falsification.
Les pratiques et le mode opératoire des contrefacteurs ont évolués avec l'actuel progrès technique exponentiel, ce qui gêne énormément la détection et la prévention. A titre d'exemple, le "spear phishing", où les escrocs contactent des administrateurs de sociétés par mail ciblé grâce aux informations récoltées sur Internet et les réseaux sociaux (social engineering).
La fraude documentaire (passeports ou factures falsifié(e)s) vise souvent à soutenir d'autres crimes (escroqueries, blanchiment, financement du terrorisme, …). Il est essentiel que les acteurs des services financiers soient bien informés sur ses différents aspects et typologies. Primordial est de savoir quels sont les outils de lutte contre ces délits (fraude) afin de réagir de la manière la plus propice.
Lors du blanchiment de capitaux, le but final est de dissimuler l'origine de l'argent criminel. Une des techniques pratiquées est la fraude documentaire afin de cacher le lien entre le délit sous-jacent et l'auteur. Dans ce sens, la fraude documentaire peut être considérée comme une des typologies afin de détecter le blanchiment.
Par ailleurs, il est capital d'acquérir des connaissances sur les documents qui sont susceptibles d'être falsifiés. Les questions suivantes doivent être posées: qui, quand, comment? Une fois que des faux documents ont été détectés; quelle procédure doit être suivie?
L'objectif de cette formation est d'apprendre comment adopter une attitude professionnelle de scepticisme, ce qui inclut entre autres: accepter que la fraude

(documentaire) puisse exister, développer un esprit critique et faire une évaluation pertinente en cas de preuves potentielles. Suivre une telle formation est donc fondamentale si vous voulez pouvoir déceler une fraude et disposer d'une vigilance professionnelle.

Liens : https://www.febelfin-academy.be/fr/actu/detail/focus-sur-la-lutte-contre-la-fraude-documentaire-liee-au-blanchiment-d-argent

Phishing

De quoi s'agit-il ?

Le terme Phishing (ou hameçonnage) désigne l'envoi par des criminels de courriels ou de messages texte (SMS) provenant prétendument d'entreprises, d'institutions financières ou d'organes officiels. Il arrive aussi que le destinataire de ces messages soit renvoyé à un site web falsifié, offrant toutes les apparences du site original.

Le but principal des escrocs consiste à soutirer des données d'identification (nom d'utilisateur et mot de passe) pour un compte (compte E-mail, accès e-banking, site d'enchère en ligne) pour ensuite y accéder à la place de la victime.

A titre d'exemple :

Dans un premier temps, l'escroc se procure un accès à votre compte de messagerie ou à votre ordinateur, éventuellement via votre réseau local sans fil (wireless local area network). Lorsqu'il juge l'occasion favorable, il se fait passer pour l'interlocuteur (qu'il soit banquier, policier ou autre) avec lequel vous venez de communiquer par courriel, en vous adressant un message à l'aide d'une adresse électronique similaire à celle de votre interlocuteur original. Il tente ensuite par cette usurpation d'identité de vous amener à lui communiquer des informations sensibles ou à vous les faire enregistrer sur un site web falsifié.

Que faire en cas de sollicitation ?

Ne répondez en aucun cas à ce type de courriels, pas même pour exprimer votre refus. Effacer immédiatement le message et ses annexes.

Nos conseils :

- Méfiez-vous des courriels non sollicités dans lesquels on vous demande de fournir sur-le-champ des renseignements personnels ou financiers
- En cas de doute sur un courriel ou un site web, ne cliquez pas sur les liens indiqués mais passez par vos favoris ou entrez l'adresse web manuellement
- Ne révélez aucune donnée sensible telle que mot de passe, nom d'utilisateur ou numéro de carte de crédit par courriel
- Mettez régulièrement à jour vos antivirus et autres systèmes d'exploitation afin de protéger votre ordinateur
- Vérifiez régulièrement vos relevés bancaires et de cartes de crédit pour vous assurer de la légitimité des transactions y figurant
- En cas de soupçon d'escroquerie, veuillez en informer la police judiciaire de votre canton de domicile ou le Service de coordination de la lutte contre la criminalité sur Internet SCOCI

Liens :

https://www.fedpol.admin.ch/fedpol/fr/home/aktuell/warnungen/phishing.html

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

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

L'arnaque de la fausse offre d'emploi

Ces fausses offres d'emploi consistent à vous faire travailler au blanchiment d'argent sale, et si vous acceptez vous risquez tout bonnement d'aller en prison.

Voici une autre arnaque très répandue dans le monde des offres d'emploi : le blanchiment d'argent sale ou de biens volés, par des particuliers qui ne se doutent de rien et croient effectuer un travail comme un autre.

Exemple de faux emplois les plus utilisés

Il existe pas mal de combines différentes, en voici deux :

Pour éviter les autres, restez éloignés des offres d'emploi trop alléchantes ou trop rémunératrices si vous n'avez pas les qualifications correspondantes. En ces temps difficiles les gros salaires ne s'obtiennent pas à la première offre d'emploi venue sur internet…Méfiez-vous des choses qui brillent trop, il s'agit certainement de fausses offres d'emploi.

1) On vous demande d'ouvrir un compte puis de fournir ce numéro de compte. Sur ce compte on vous enverra de très grosses sommes d'argent (provenant de la drogue, vente d'arme, prostitution etc …) et on vous proposera d'en conserver une partie

(1000 euros pour 100.000 par exemple) puis de renvoyer les 99.000 restants sur un autre compte.
Voilà, simple comme bonjour, vous allez gagner de très grosses sommes très facilement un peu à la manière d'un trader confirmé ! Sauf que … vous allez finir en prison !!
2) Autre technique : Il s'agit là d'une méthode visant plus particulièrement les portails de jobs étudiants.
Voici l'histoire de cet étudiant qui a bien failli accepter une fausse offre d'emploi :
« Bonjour,
En cherchant un emploi étudiant sur le site www.studentjob.fr, j'ai postulé à une annonce d'emploi en tant que client mystère avec Mr ANDRE AUBERT.
Après plusieurs échanges par mails, on m'annonce que je suis retenue pour le poste et je reçois plusieurs jours après une lettre d'ordre de mission.
Quelle ne fut pas ma surprise en découvrant pour 3000 € de travellers chèques dont 300 € qui me sont destinés!
La lettre dit de changer ces chèques contre du cash à la banque et de se rendre dans une agence Western Union pour effectuer un transfert à DANIEL SLATER à Londres. Sous couvert d'analyser le service proposé par l'agence.
Cela paraît énorme mais j'ai tout de même failli me faire avoir! car la banque accepte les chèques sur le moment, donc on pense que tout est OK.
J'en ai parlé autour de moi, une personne qui avait vécu la même histoire m'a averti : Au bout d'un mois la banque se rend compte que les chèques sont volés, donc on vous débite la somme de votre compte. Mais comme le cash a déjà été envoyé la somme reste à vos frais. J'ai donc failli m'endetter de 2700 € alors que je le rappelle je suis étudiante! »
Ici on est plus dans un cas de recel de biens bancaires falsifiés. Idem, on vous fait miroiter un salaire assez élevé pour un soi-disant travail parfaitement normal. Cependant même s'il s'agit d'une fausse offre d'emploi, quand la banque se retournera contre vous c'est vous qui payerez les pots cassés car vous avez encaissé une partie de ces chèques pour votre compte.
Encore une recommandation, restez éloignés de toutes ces offres d'émir bloqués dans leur pays avec des milliards, qui ont des difficultés à conserver leur argent après je ne sais quel retournement politique dans leur pays et qui sont prêts à vous léguer leur fortune.
Ils vous demanderont bien sûr au dernier moment d'envoyer un paiement par Western Union (1000€?) pour couvrir les frais du transfert des millions qui vous attendent. Ne le faites surtout pas c'est une arnaque !
Evidemment une fois les 1000 euros reçus, adieu vos rêves de millionnaire, vous ne toucherez pas un centime. Le père noël n'existe pas rappelons-le encore une fois, même à des adultes.
Liens : http://www.web-arnaque.com/particulier-a-particulier/fausse-offre-d-emploi/

Pris en flagrant délit : Les meilleures arrestations de cybercriminels du mois

Nous continuons d'observer comment les organismes d'application de la loi dans le monde combattent la cybercriminalité. Ils continuent d'emprisonner les pirates – qu'il s'agisse de crimes mineurs comme le piratage de comptes Facebook ou de crimes majeurs, comme le blanchiment de 6 milliards de dollars. Mais une étoile brille dans

la constellation des derniers succès de la police : ils ont réussi à arrêter un gang impliqué dans le piratage et dans un trafic de drogue. Le partenariat entre les experts de la loi et ceux de la sécurité fait ses preuves !

60 secondes chrono

Une histoire digne du cinéma a eu lieu aux Pays-Bas et en Belgique. La police a arrêté 7 contrebandiers hollandais et 2 pirates informatiques belges qui ont été recrutés par ces 7 contrebandiers. Les trafiquants de drogue hollandais ont décidé d'intercepter un cargo qui transportait plus de 2 tonnes de cocaïne et d'héroïne et se dirigeait vers Rotterdam. Pour cela, ils ont embauché des pirates qui se sont infiltrés dans les serveurs de la compagnie du bateau et ont changé la destination du cargo pour Antwerp en Belgique. Bien que le piratage en lui-même se soit bien déroulé, la manipulation a été remarquée par le département de la sécurité qui a immédiatement contacté la police. Quand les trafiquants de drogue sont arrivés pour accueillir le cargo, ils ont également trouvé une unité spéciale de la police.

Comment voler un million

Quinze compagnies du secteur financier ont été victimes d'un gang basé aux États-Unis et en Ukraine qui a réussi à leur voler près de 15 millions de dollars. Parmi les victimes : Citibank, JP Morgan Chase et PayPal, pour n'en citer que quelques-unes.

Les suspects ont piraté les serveurs des banques, puis se sont infiltrés dans les informations sécurisés de leurs clients et ont transféré l'argent des comptes bancaires légitimes vers des cartes de débit prépayées. Les « encaisseurs » situés aux États-Unis ont vidé les comptes via des distributeurs automatiques et en réalisant de faux achats. Les officiers fédéraux ont inculpé huit membres d'un gang, mais les deux leaders du réseau, Oleksiv Sharapka et Leonid Yanovitsky sont toujours introuvables, ils se cacheraient actuellement en Ukraine.

Un autodidacte vole 46800€

Un individu ayant abandonné le lycée et sans aucune formation en technologie a été arrêté à Moscou, en Russie. Ayant lui-même étudié les forums souterrains, ce jeune de 19 ans a diffusé un malware capable de voler les identifiants de systèmes de paiement en ligne. Il a ensuite utilisé les identifiants volés pour transférer l'argent sur son compte. Il a gagné prêt de 2 millions de roubles (environ 46800€) de cette façon. Ce qu'il ne savait pas c'est que ce crime est passible de poursuites judiciaires pour fraude et qu'il peut être condamné à 5 ans de prison.

Liberté d'expression et assignation à résidence

Un pirate canadien qui a réalisé une attaque cybernétique contre le site du gouvernement du Québec a été arrêté à son domicile ce mois-ci. Un ancien employé de la Chambre des communes a probablement utilisé ses connaissances pour attaquer le système. Un juge a déclaré qu'il ne s'agissait pas d'une revendication politique, mais qu'on ne trouvait pas non plus de raison économique derrière ce crime. Il s'agit peut-être d'une forme d'expression personnelle qui vaudra tout de même au pirate une assignation à résidence de huit mois.

Cyber-harcèlement

Un pirate de 34 ans originaire de Morgan City, en Louisiane, a piraté le compte Facebook d'une femme. Il en a ensuite changé le mot de passe et a posté des menaces et des commentaires négatifs sur sa page. La police a été rapide et a arrêté le suspect quelques jours seulement après que la victime ait déposé plainte pour harcèlement sur un réseau social.

Trafic de cartes bancaires volées

L'un des plus grands forums spécialisés en vente de cartes bancaires volées a été fermé grâce aux efforts de représentants de la loi américains, britanniques et

vietnamiens. Le FBI affirme que le forum Mattfeuter a vendu plus de 1 million de numéros de cartes bancaires, et les criminels auraient gagné plus de 220 millions de dollars. Certains utilisateurs du forum ont été arrêtés au Royaume-Uni, et le fondateur de ce « business », Van Tien Tu a été arrêté au Vietnam. Nous ne connaissons pas la loi vietnamienne, mais les cybercriminels ayant participé à cette fraude encourent près de 30 ans de prison aux États-Unis.

Stop au blanchissement d'argent

Les autorités américaines ont réussi à saisir des domaines associés au système de paiement Liberty Reserve, une société accusée d'avoir participé à une affaire de blanchissement d'argent et d'avoir créé une entreprise de transfert financier sans aucune autorisation.

Liberty Reserve est devenu l'un des outils favoris des cybercriminels pour transférer de l'argent car il est anonyme – les opérateurs du système n'ont pris aucunes mesures pour vérifier l'identité de leurs clients, et ont fourni des outils permettant de renforcer cet anonymat : l'envoyeur peut cacher ses identifiants et transférer de l'argent via des services d'échange externes. Selon les procureurs, la compagnie aurait aidé à blanchir plus de 6 milliards de dollars et dispose de plus d'un millions de clients fidèles.

Liens : https://blog.kaspersky.fr/pris-en-flagrant-delit-les-meilleures-arrestations-de-cybercriminels-du-mois/1196/

Cybercriminalité : quels enjeux pour les économies souterraines ?

A l'occasion de la sortie de son dernier numéro, *Lumières sur les économies souterraines*, la revue *Regards Croisés sur l'Économie* a organisé, le 26 mars dernier, une soirée-débat sur le thème de la cybercriminalité. Cette soirée a été l'occasion de présenter l'organisation et le fonctionnement des économies parallèles alimentées par les cybercriminels, encore peu connues et pourtant en pleine expansion. Différentes questions ont été abordées : qui sont les acteurs en jeu dans les marchés de la cybercriminalité ? Quel est le coût de la cybercriminalité pour l'économie réelle ? En quoi son développement modifie les formes que prennent les économies souterraines pré-existantes ? La cybercriminalité a-t-elle fait émerger une forme spécifique d'économie souterraine ? Quelles sont les mesures et les moyens disponibles pour lutter contre ces formes de cybercriminalité tout en préservant les libertés numériques individuelles ?

Jérôme Saiz, Information Security Analyst

Jérôme Saiz commence par une brève présentation de la place qu'a prise internet dans nos sociétés : plus d'un tiers de la population mondiale y a aujourd'hui accès, et en 2020, six fois plus d'objets que d'hommes seront connectés à Internet. L'espace internet fournit ainsi un nouveau terrain favorable pour les activités criminelles. La cybercriminalité représente un véritable marché mettant en jeu des agents spécifiques. Ces criminels de la toile créent des écosystèmes avec leurs propres règles, jargons et coutumes. Il distingue trois types d'acteurs sur ce marché :

- le pirate isolé : il correspond à l'internaute qui se livre seul à une activité pirate (par exemple en profitant d'outils de piratage développés par d'autres, faciles d'accès et simples d'utilisation). les groupes criminels présents seulement sur le réseau internet : ces groupes sont très structurés et centralisés, chacun de ses membres ayant une fonction bien précise. Il décrit les fonctions-clé suivantes :

le codeur qui est en charge de faire « les codes malveillants » ; le hacker qui pénètre et vole les codes bancaires ; le cardeur qui revend les numéros de cartes bancaires ; la mule qui blanchit de l'argent. Enfin, le « manager » se charge de trouver des organisations de spécialistes et de recruter parmi eux. Ces membres n'interagissent entre eux que par internet, sans jamais se rencontrer physiquement. Certains de ces groupes sont suffisamment organisés pour gérer toute la chaine de la cybercriminalité (revente de biens illégaux, encaissement et blanchissement d'argent, etc).

- les groupes criminels traditionnels : dans le contexte du développement d'internet, les groupes criminels traditionnels (mafias, gangs) ont récemment commencé à exploiter ce nouveau support pour mener leurs actions. Ces groupes tirent différemment profit de cet outil, soit en recrutant en interne des spécialistes de la cybercriminalité, soit en « louant » des experts, ou encore en contraignant certains spécialistes à travailler pour eux par l'usage de la force. Il cite l'exemple du Mexique où des pirates du Net ont été récemment kidnappés par ces groupes criminels traditionnels.

80% des infractions sur Internet sont commises par des groupes. Par ailleurs, Internet permet aux deux types de groupes cités précédemment de collaborer. En ce sens, on assiste à une reconfiguration des activités de l'économie souterraine. \\

Jérome Saiz fournit ensuite des exemples de pratiques concrètes d'activités cybercriminelles, les sites sur lesquels se déroulent ces activités et les biens qui s'y échangent. Ces activités se déroulent sur des forums référencés sur Google où des pirates tentent de proposer des biens ou des services illégaux, sur les Internet Relay Chat (Protocole de communication textuelle sur internet), ou encore sur le marché noir en ligne non répertorié par les moteurs de recherches traditionnels et seulement accessible grâce à des réseaux d'anonymisation. On peut citer l'exemple de Silk Road qui était un marché noir de produits illégaux qui utilise le réseau Tor pour assurer l'anonymat des acheteurs et vendeurs, ainsi qu'une monnaie électronique, le Bitcoin dont la possession n'est pas nominative. Sur ce marché, on peut y échanger des numéros de cartes bancaires (contenu intact de la piste magnétique de la carte bancaire), des comptes bancaires ou Paypal, etc. Les acheteurs de ces numéros vont ensuite répliquer les cartes en questions.

Ces marchés de la cybercriminalité sont très rentables. Jérôme Saiz nous livre quelques estimations : selon l'United Nations Office on Drugs and Crime, le vol d'identité rapporterait à lui seul 1 milliards de dollars par an ; selon le Center for Strategic and International Studies (étude de juillet 2013), la seule fraude en ligne chez les marchands représenterait 3,5 milliards de dollars et le poids du cybercrime se situerait entre 300 milliards et 600 milliards par an. Enfin une étude du Ponemon Institute sur un échantillon de 60 entreprises américaine publiée en 2013 évalue e coût moyen du cyber-crime à 11,6 millions de dollars par an. Ces activités cybercriminelles représentent selon lui le plus grand transfert de ressources de tous les temps.

Fabien Cozic, consultant en cybercriminalité

Fabien Cozic souligne une évolution des modes d'organisation cybercriminelle. Dans les années 1980, des cybercriminels isolés cherchaient la performance. Kevin Mitnik par exemple est très connu pour avoir piraté très jeune les réseaux de sociétés de télécommunications aux Etats-Unis. Aujourd'hui, on a plutôt affaire à des professionnels qui veulent faire prospérer leurs activités dans le temps long.

L'essentiel des victimes sont issues des petites et moyennes entreprises (PME) car ce sont les plus grandes détentrices de brevets et les plus grands fournisseurs de services.

Le hacker peut retirer de ses attaques un transfert monétaire immédiat mais aussi des savoir-faire ou de l'information sur les stratégies économiques des entreprises visées. Ces attaques relèvent alors de l'espionnage industriel. Pour s'attaquer aux entreprises du CAC 40, les cybercriminels attaquent « par rebonds », c'est-à-dire qu'ils s'attaquent aux sous-traitants dans un premier temps. Ils y visent une personne stratégique en particulier, la surveillent et lui soutirent les informations qui leur permettront de remonter vers la grosse entreprise cible.
Fabien Cozic distingue différents types d'attaques :

- le vol de données qui est opéré par des logiciels malveillants. La récente attaque contre la troisième chaîne de distribution américaine « Target » est un cas d'école. Les attaquants ont installé des malwares (Logiciels malveillants) sur les terminaux de paiement, qui ont extrait les informations bancaires de la mémoire vive des caisses enregistreuses. Les substitutions de terminaux de paiement par des appareils identiques équipés d'un système d'émission par bluetooth et d'un skimmer qui capte les données bancaires sont de plus en plus courantes dans les commerces en France.
- l'usurpation d'identité mise au point grâce à l'information recueillie sur les réseaux sociaux et dans les organigrammes mis en ligne. Le phishing (Arnaque visant à soutirer de l'argent à des particuliers en se faisant passer par mail pour un tiers de confiance (la banque de la victime par exemple).) ou les arnaques aux faux ordres de virement en sont des exemples.
- le chantage avec menace de mise à plat de serveur d'entreprise ou de parcelles de data center par un malware ou un botnet (Réseau de programmes connectés à internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches).

Comment s'en prémunir ? Il faut se fournir en pare-feu et de sécuriser ses informations sur les réseaux sociaux. On parle d' « hygiène informatique ». Et la métaphore ne s'arrête pas là puisque les épidémiologistes s'inspirent des modes de contamination informatique pour modéliser la propagation des maladies.
En conclusion, Fabien Cozic précise bien que la dimension technique de ces infractions n'est ni le mal ni le remède, c'est bien le facteur humain qui est à la racine de ces actes criminels.

Myriam Quenemer, magistrate

Myriam Quenemer commence par se livrer à un exercice de définition. La cybercriminalité recouvre tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent. La commission européenne y distingue trois formes d'infractions : les infractions propres aux réseaux électroniques de type piratage ; les infractions qui reprennent les formes traditionnelles de criminalité et les infractions qui consistent à diffuser des contenus illicites (pédopornographie, racisme).
La délinquance se déplace en parallèle de l'action humaine : elle est devenue numérique. En réponse à cela, la justice doit se doter de nouveaux modes d'investigation. Trois caractéristiques propres à la cybercriminalité posent problème : combattre ces infractions nécessite des compétences techniques, beaucoup d'infractions sont extraterritoriales, et enfin les délits se multiplient car le passage à l'acte est beaucoup plus facile dans un espace numérique qui distance l'agresseur de la victime.
Quelle est la traduction juridique de ces modes opératoires ? La loi informatique et libertés de 1978 est la première à donner un cadre au traitement de données nominatives, en créant notamment la Commission Nationale de l'Informatique et des

Libertés (CNIL). Sur ces questions, le droit pénal évolue ensuite sous l'impulsion du développement du crime organisé et du terrorisme. En 2001, la loi relative à la sécurité quotidienne permet de conserver les données de trafic jusqu'à un an, i.e. les données permettant d'identifier toute utilisation des réseaux de communication. Une série de lois votées en 2004 font des données informatiques un objet de réquisition et désignent des juridictions spécialisées. Enfin en 2011, la loi LOPSI II définit le délit d'usurpation d'identité sur internet au terme d'un long débat sur le \textit*phishing* et permet d'intercepter le réseau internet dans le cadre d'une enquête. La convention de Budapest d'août 2011 est le premier traité international en matière de lutte contre la cybercriminalité. Son principal objectif, énoncé dans le préambule, est de poursuivre « une politique pénale commune destinée à protéger la société contre le cyber-crime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale ».

Cependant, Myriam Quenemer regrette l'absence d'une réelle politique publique et pénale globale. Des lacunes législatives subsistent : le vol d'éléments immatériels n'est pas explicitement traité dans la loi et certaines infractions déjà complexes à définir comme le blanchiment ou la traite des êtres humains sont complexes à caractériser lorsqu'elles sont commises via les réseaux numériques. D'autre part, les données sur le phénomène sont encore approximatives. Une réelle coopération public / privé doit se mettre en place pour avoir une vue d'ensemble du phénomène.

Rodolphe Durand, professeur à HEC

Rodolphe Durand ouvre la discussion en proposant une réflexion plus générale sur les organisations pirates. Selon lui, leur essor est à relier aux évolutions du capitalisme moderne. Tout au long de l'histoire, ces organisations ont émergé en réaction à la volonté des Etats de détenir le monopole de certains territoires (monopole de ressources, dans la définition des normes, etc). Ces pirates ont alors cherché à conquérir de nouveaux espaces de libertés au sein même de ces territoires.

Il revient ainsi sur l'histoire des premiers pirates qui date de la découverte de l'Amérique : à cette époque, les monarchies européennes revendiquaient les routes maritimes commerciales qu'ils avaient « découvertes ». Ainsi, certains marins alors exploités par la marine marchande ont cherché à s'organiser en s'unissant à des groupes établis sur les côtes américaines afin de récuser ce droit de propriété affirmé par les Etats européens. L'argument principal contre ces monopoles était la légitimité d'un commerce maritime ouvert à tous. Les Etats finissent par entendre cet argument en créant les eaux internationales. De nouvelles formes de pirateries se sont ensuite succédées, dans ces périodes de révolutions territoriales liées aux mutations du capitalisme : on peut penser aux radios pirates qui se sont opposées au monopole des ondes par la BBC au milieu du XX^{e} siècle ; aujourd'hui, à la piraterie internet avec Wikileaks, Anonymous, MegaUpload qui contestent le pouvoir de marché de Google ou Microsoft ; ou encore la piraterie génétique avec le développement de sites comme Do It Yourself Bio gérés par des « biohackers » capables d'assembler des séquences d'ADN synthétiques. Rodolphe Durand explique qu'une piraterie de l'espace apparaîtra probablement.

Il opère ensuite une distinction entre l'organisation pirate et l'organisation mafieuse, chacune d'entre elles ayant un rapport différent aux territoires, à un niveau local et global. En effet, l'organisation pirate est illégitime à un niveau local et prolifère plus la souveraineté étatique est forte puisque son but est d'entrer en contestation avec celle-ci. Toutefois, s'il existe ce qu'il appelle un « consensus normatif global » (au delà de l'échelle nationale), l'organisation périclite. A l'inverse, la mafia est illégale mais détient une certaine légitimité locale ; si la souveraineté locale est forte, la mafia

périclite. L'organisation mafieuse, à l'inverse de l'organisation pirate, cherche davantage à s'infiltrer dans l'Etat.
Pour conclure, il évoque le complexe triptyque que forment l'Etat, les entreprises et les organisations pirates, chacun d'entre eux interagissant et ayant des frontières relativement floues. Le capitalisme marchand est profondément lié à la notion d'Etat souverain. Selon lui, l'Etat crée des normes marchandes que les entreprises traditionnelles peuvent suivre pour s'implanter mais qui sont contestées par les pirates. Ainsi, ces derniers recréent toujours les frontières de l'Etat qui finit par prendre en compte ces revendications en adoptant de nouvelles lois sur le territoire en question. Rodolphe Durand conclut en expliquant que les cyberpirates ne sont pas contre le capitalisme : ils luttent davantage contre les monopoles (d'entreprises, d'Etat) et sont en ce sens de fervents défenseurs de la concurrence et de la liberté économique sur des territoires considérés comme un bien commun.

Débat

Les intervenants notent un décloisonnement croissant des activités criminelles. Le blanchiment d'argent par le biais des monnaies virtuelles est typiquement utilisé par les trafiquants d'armes, de stupéfiants ou même par les terroristes. Les armes en pièces détachées sont échangées sur internet. Le trafic de données bancaires peut être lié au terrorisme. Les modes d'investigation doivent s'adapter en conséquence note Myriam Quenemer. Ainsi la collaboration des douanes, des sites internet et des postes est nécessaire.
La mobilisation contre la cybercriminalité se fait à plusieurs niveaux. Jérome Saiz signale que les banques rachètent parfois les codes volés de cartes bancaires aux criminels pour en comprendre les failles. Myriam Quenemer rappelle l'importance de la coopération internationale en soulignant la création récente du centre européen de lutte contre la cybercriminalité (EC3). Enfin Fabien Cozic nous parle de la « phishing initiative », plateforme sur laquelle les internautes sont invités à signaler les adresses de sites de phishing.
Concernant l'interception, Jérome Saiz et Myriam Quenemer insistent sur la différence entre le champ judiciaire et le champ administratif. Des logiciels permettent maintenant de faire des liens entre certaines transactions, certains appels ou échanges de données et des activités criminelles. En cela, la preuve sera de plus en plus numérique. Mais les interceptions judiciaires sont encadrées par les juges et sont soumises à des lois restrictives. Myriam Quenemer cite la loi sur la géolocalisation judiciaire du 1er mars 2014 à titre d'exemple. Les interceptions administratives sont elles gérées par une commission et leur réalisation est soumise à l'accord du Premier Ministre. La loi de programmation militaire votée en décembre dernier multiplie les intervenants capables de demander des accès administratifs aux données personnelles.
La loi qui permet de conserver les données de trafic jusqu'à un an a suscité des réactions du public y voyant une violation des libertés individuelles. Myriam Quenemer répond que ces données ont permis de faire aboutir un certain nombre d'affaires et que la perquisition peut être en un sens plus « intrusive » que le bornage qui consiste à récupérer des données a posteriori et non en temps réel comme le fait la géolocalisation. C'est une question de modèle de société, il s'agit de trouver le bon équilibre entre une justice qui se donne les moyens d'investigation, y compris sur ces nouveaux champs, et une surveillance accrue et abusive des citoyens.

Liens : http://www.rce-revue.com/?Cybercriminalite-quels-enjeux-pour,641

Divergence de vues sur l'utilité d'autres conventions internationales pour combattre les formes nouvelles de criminalité, dont celle sur Internet

Doha, Qatar, 17 avril - Le débat que le treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale a tenu aujourd'hui, à Doha, sur les « approches globales et équilibrées contre les formes nouvelles et émergentes de criminalité organisée » s'est résumé à une question: les conventions des Nations Unies suffisent-elles pour triompher de la cybercriminalité, du trafic de biens culturels et d'espèces sauvages, ou de la contrefaçon?

Les interventions de l'Inde et du Japon ont illustré à elles seules la divergence des points de vue. Peut-on vraiment combattre une cybercriminalité en constante mutation avec des instruments datant d'il y a plus de 10 ans? a douté le représentant indien. La Convention des Nations Unies contre la criminalité transnationale organisée, dite Convention de Palerme, et celle contre la cybercriminalité, dite Convention de Budapest, ont été adoptées respectivement en 2000 et en 2001. Le défi n'est pas l'absence d'instrument juridique mais bien les lacunes des législations et des procédures pénales, au niveau national, a tranché le représentant japonais.

Ces 10 dernières années, la situation a évolué*****: la cybercriminalité comprend, par exemple, les infractions dans lesquelles les données informatiques sont l'objet de l'infraction-même mais aussi celles dans lesquelles ils ne sont que les moyens par lesquels elle est commise. La criminalité environnementale quant à elle couvre à la fois le braconnage et des infractions nouvelles, comme celles liées à l'échange des droits d'émission de carbone et à la gestion de l'eau. L'Internet se prêtant bien à une coordination plus large entre individus d'une zone géographique très étendue, un nombre beaucoup plus important de groupes criminels organisés ont émergé.

Faut-il de nouvelles conventions? Non, a répondu la représentante de la Norvège. Les conventions contre les stupéfiants, contre la criminalité transnationale organisée et contre la corruption couvrent déjà toutes les formes de crimes. Leur potentiel doit être pleinement exploité pour les formes anciennes et nouvelles des crimes. Il ne sert à rien, a insisté la représentante, de développer de nouveaux instruments, conventions et protocoles, alors que nous ne mettons en œuvre ni ne respectons ceux dont nous disposons. Les organisations criminelles sont efficaces, créatives et modernes. Utilisons les mêmes armes: efficacité, suffisance des ressources et outils technologiques, a encouragé la représentante. Parlant en particulier de la cybercriminalité, son homologue du Japon a estimé que le défi n'est pas l'absence d'instrument juridique mais bien les lacunes dans les législations nationales qui ne couvrent toujours pas la cybercriminalité et dans les procédures pénales qui limitent le travail de la police, des procureurs et des autorités judiciaires compétentes et ne facilitent pas non plus la coopération entre États. Identifions les besoins et renforçons « concrètement» l'assistance technique souhaitée par les instruments existants.

Il faut en effet, a reconnu la représentante de la Suisse, doter les tribunaux et les autorités de poursuite pénale et de contrôle des moyens nécessaires pour leur permettre de réagir avec la même flexibilité que les groupes criminels. Au niveau international, des procédures simples et accélérées sont nécessaires pour que la police puisse échanger des informations avec des États partenaires et réagir en temps utile à des signalements en provenance de l'étranger. « Une législation efficace, une prévention ciblée, des autorités de poursuite pénale efficaces, bien formées et

équipées, et une coopération non bureaucratique entre les différentes autorités et institutions, telle est la combinaison qui peut nous permettre de faire face de manière adéquate et rapide aux formes de criminalité les plus diverses », a tranché la représentante.

La déléguée suisse n'a pas caché que pour son pays, la Convention des Nations Unies contre la criminalité transnationale organisée n'offre qu'une base juridique « limitée » pour poursuivre les nouvelles formes de criminalité. Il n'est pas judicieux, a-t-elle jugé, de rattacher ces nouvelles formes à l'élément constitutif de la criminalité organisée. Un nouveau cadre juridique multilatéral devient donc « crucial », en a conclu le représentant du Brésil, soutenu par son homologue de la Chine. La réponse juridique doit se concentrer sur les outils de la coopération internationale car « les moyens traditionnelles de cette coopération ont montré leurs limites ». Compte tenu du lien entre cybercriminalité et terrorisme, il devient de plus en difficile de voir l'efficacité des instruments existants, a ajouté le représentant de l'Iraq. « La cybercriminalité profite de l'absence d'un instrument international efficace, a prévenu, à son tour, celui de la Tunisie. Les anciens criminels s'étant modernisés, nous devons nous montrer plus intelligents qu'eux, a alerté le représentant du Maroc.

Peut-on vraiment combattre une criminalité en constante mutation avec des instruments de plus de 10 ans? a douté son homologue de l'Inde. Non, il en faut de nouveaux, a répondu le représentant du Pakistan, soutenu par son homologue de l'Afrique du Sud, au nom du Groupe des États d'Afrique. Envisageons au moins une révision, a suggéré celui de l'Iran.

Mais en quoi la **Convention de Budapest sur la cybercriminalité** aurait-elle perdu de sa légitimité? s'est interrogé le représentant de l'Allemagne. Face à « la démocratisation de la cybercriminalité et la délinquance sans frontière », cette Convention est la clef, a estimé son homologue de la France. Ratifiée par 45 États dont un nombre important de non-membres du Conseil de l'Europe, c'est l'instrument de référence qui permet l'entraide judiciaire. Élaborer une nouvelle convention, a poursuivi son homologue de l'Allemagne, exigerait un processus de plusieurs années et des ressources énormes, sans rien à apporter de nouveau. Concentrons-nous plutôt sur une meilleure application de la Convention, en offrant, par exemple, aux personnels concernés une bonne formation et en renforçant la coopération internationale. Si l'on peut toujours améliorer cette coopération, a commenté la représentante de l'Australie, il faut reconnaître que l'instrument actuel s'est révélé efficace, à la fois pour criminaliser les délits dans le cyberspace et plus important encore, pour faciliter une coopération rapide entre les forces de l'ordre. La Convention serait encore plus efficace si tous les États y adhéraient, a souligné la représentante.

Pour renforcer la coopération internationale, a commenté, à son tour, la représentante du Canada, il faut veiller à l'harmonisation des différentes législations et à la fourniture aux pays en développement des capacités juridiques et techniques nécessaires. Le représentant du Conseil de l'Europe a insisté sur les programmes d'assistance mis en œuvre par son organisation. Mais le problème, a estimé le représentant de la Fédération de Russie, est que la Convention a oublié de consacrer « le droit souverain des États » à mener leurs propres enquêtes. Le problème est aussi que son article 37 dispose que « le Comité des ministres du Conseil de l'Europe peut, après avoir consulté les États contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout État non membre du Conseil à adhérer à la Convention. La décision est prise à l'unanimité des représentants des États contractants ». C'est donc que la Convention n'a pas vocation à être universelle et

que les restrictions à son universalisation prouvent la nécessité d'un autre traité, a argué le représentant du Conseil des ministres de l'intérieur des pays arabes.
La vision du Congrès doit être de promouvoir un Internet libre, ouvert et sûr, a estimé le représentant des Pays-Bas, s'opposant, à son tour, à la négociation d'un nouvel instrument qui retarderait, a-t-il prévenu, la réponse de la communauté internationale à la nécessité « immédiate » de renforcer les formes existantes de coopération et l'adoption des nouvelles législations nationales dont les pays discutent en ce moment.
Il a appelé les gouvernements à ouvrir la lutte contre la cybercriminalité au secteur privé, à la communauté technologique, au monde universitaire et à la société civile.
Le représentant est revenu sur le futur « Forum mondial de la cyberexpertise », une initiative pour le renforcement des capacités, qui facilitera le partage des expériences, des évaluations et des meilleures pratiques, identifiera les lacunes dans les capacités et mobilisera des ressources et des expertises additionnelles. Le forum sera pragmatique, orienté vers l'action, flexible et fondé sur une participation volontaire.
Le représentant de la Tunisie a confirmé la nécessité d'une aide au renforcement des capacités.
Le **trafic des biens culturels** n'a pas été oublié au cours des discussions, le problème le plus « cuisant » étant en Syrie et en Iraq, comme l'a souligné le représentant de l'Allemagne. Il faut, a-t-il dit, travailler ensemble pour sensibiliser à ce problème qui est devenu le troisième crime mondial après le trafic de drogues et d'armes et qui alimente le terrorisme. Nous devons renforcer la coopération entre Interpol, l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), l'Office des Nations Unies contre la drogue et le crime (ONUDC) et les autres organisations internationales pertinentes, a ajouté le représentant allemand avant que son homologue de l'Égypte ne fasse part de la demande des États africains pour un nouvel instrument sur la protection du patrimoine culturel ou au moins un protocole additionnel à la Convention contre la criminalité transnationale organisée.
Après que le représentant de la Chine eut appuyé cette proposition, la représentante du Canada a prôné, au contraire, une application plus efficace des instruments existants dont « Les Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et d'autres infractions connexes », adoptés l'an dernier par l'Assemblée générale de l'ONU. Le cadre international actuel est largement suffisant, a acquiescé le représentant de la France, en rappelant les dispositions de la Convention contre la criminalité transnationale organisée et celle de l'UNESCO de 1970 concernant « les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels ». Mettons l'accent sur l'évaluation de la mise en œuvre, l'échange des bonnes pratiques, l'assistance technique et la coopération douanière, a encouragé le représentant français, soutenu par son homologue de l'Italie laquelle aide l'ONUDC à préparer un outil technique.
Son homologue du Viet Nam a annoncé l'organisation en 2016, dans son pays, de la troisième Conférence sur le **commerce illicite des espèces sauvages**. Dans ce cadre, le représentant de l'Indonésie a voulu que la pêche illégale, qui génère 23 milliards de dollars, soit reconnue comme une forme émergente de criminalité transnationale pour, a-t-il dit, renforcer la prévention et la lutte contre ce fléau. Il faut faire le lien, a renchéri le représentant du Pérou, entre exploitation illégale des ressources naturelles, corruption et blanchiment d'argent. Il faut des normes internationales « spécifiques » pour traiter de ces problèmes de manière « globale et équilibrée », a-t-il dit, soutenu par le représentant de la Fédération de Russie. Ici aussi, la représentante du Canada a rappelé qu'il existe déjà une série d'instruments et de processus internationaux dont

l'incontournable Convention contre la criminalité organisée et les nombreux autres accords multilatéraux négociés sous l'égide du Programme des Nations Unies pour l'environnement (PNUE). Il y a aussi la Convention sur le droit de la mer, a ajouté le représentant de l'Espagne. Évitons les doubles emplois et concentrons-nous sur les mécanismes qui existent déjà et sur lesquels des experts travaillent, a insisté le représentant, s'opposant à son homologue de l'Équateur qui a insisté sur l'élaboration d'un quatrième protocole à la Convention de Palerme.

Les **crimes environnementaux**, a plaidé la représentante d'« Environmental Investigation Agency (EIA) » sont traités, en ce moment, dans une myriade de cadres juridiques. C'est leur diversité qui est un des principaux obstacles à une réponse mondiale cohérente. Elle a encouragé les États à discuter des différentes options possibles avec des juristes et des experts des services de police, de la conservation et d'autres secteurs, y compris les ministères de l'intérieur et de la justice, et à réfléchir aux instruments spécifiques qui devraient être créés.

Le représentant de l'Inde est intervenu sur la question des **contrefaçons**. Il s'est étonné que l'ONUDC soit en train d'élaborer des dispositions législatives types contre le trafic illicite de médicaments frauduleux, alors que cette question relèverait naturellement de l'Organisation mondiale de la Santé (OMS). Médicaments frauduleux, contrefaits ou falsifiés? De quoi parle-t-on? s'est impatienté le représentant devant une question « aussi sensible ». Son homologue de la France l'a renvoyé à la « Déclaration politique »**** adoptée au premier jour du Congrès, et qui parle de la détermination des États à s'attaquer à la « contrefaçon de marchandises de marque ». Son homologue de l'Italie a d'ailleurs regretté ce libellé, arguant que la « contrefaçon de marchandises de marque » ne représente qu'une infime partie du phénomène. Il a alerté sur la faiblesse de l'entraide judiciaire et remercié, comme son homologue français, l'ONUDC qui s'efforce de mettre en œuvre la résolution 20/6 de la Commission pour la prévention du crime établissant le lien entre « médicaments frauduleux et trafic transnational organisé ».

Beaucoup de pays, dont l'Australie, ont longuement parlé de leur lutte contre le **terrorisme**, classé également dans les formes nouvelles et émergentes de criminalité.

Le représentant l'Organisation de la coopération islamique (OCI) a réclamé une définition internationale de ce fléau. On ne peut, a-t-il plaidé, combattre cette criminalité sans en connaître les contours, sans parler des causes. Le terrorisme est devenu un crime organisé et collectif, faisant naître des menaces « complexes et extrêmement dangereuses », avec un recours aux technologies modernes et à des armes meurtrières. « La coopération internationale devient inévitable. »

Haïti, la Tunisie, la Thaïlande, le Pérou, l'Équateur, El Salvador, Oman, le Koweït, le Qatar et les États-Unis ont aussi pris la parole. Le représentant américain s'est opposé à tout nouvel instrument juridique international, tout comme son homologue de l'Union européenne. 17 avril 2015

Liens : http://www.un.org/press/fr/2015/soccp365.doc.htm

La FINMA simplifie les relations d'affaires par internet

L'identification de clients bancaires électroniquement sera désormais possible, a décidé la FINMA.

L'autorité fédérale de surveillance des marchés financiers (FINMA) adapte ses règles pour permettre de nouer électroniquement des relations d'affaires. Un intermédiaire

financier pourra établir une relation commerciale par vidéo et en ligne sous certaines conditions.
«La FINMA donne ainsi la même valeur à une identification des partenaires contractuels par ce moyen qu'à une rencontre en personne», annonce lundi le gendarme financier helvétique dans un communiqué. D'autres formes d'identification en ligne doivent désormais également être possibles, estime-t-il.

Identification en ligne

Alors que cela était jusqu'à présent exigé, une attestation d'authenticité numérique d'une copie d'un document d'identité ne devra plus être obligatoirement émise et transmise à l'intermédiaire financier sous forme physique. Elle pourra être établie par le biais d'une identification en ligne.
De même, la déclaration indiquant les ayants droit économiques ne devra plus nécessairement être signée de manière manuscrite et transmise physiquement à l'intermédiaire financier.

Prévu pour mars

De telles mesures visaient à lutter contre le blanchiment d'argent et le financement du terrorisme. Ces dispositions devant tenir compte de la numérisation croissante des prestations financières, la FINMA adapte, dans une nouvelle circulaire, les obligations de diligence propres à la réglementation en matière de blanchiment d'argent.
Une audition relative à cette circulaire sur l'«identification par vidéo et en ligne» a été lancée. Elle dure jusqu'au 18 janvier prochain. L'entrée en vigueur de la circulaire devrait se faire en mars 2016. (ats/nxp). 21.12.2015,

CEO swindle : 43 personnes arrêtées dans un vaste réseau de piratage

La police espagnole et britannique a mis fin, vendredi 6 mai, à un vaste réseau de pirates informatiques spécialisés dans le CEO swindle. 43 personnes impliquées et des millions d'euros détournés.
Sept dirigeants de cybercafé de Madrid et 36 autres personnes ont été arrêtées par les autorités Espagnoles et Britanniques, vendredi 6 mai. Elles sont accusées d'avoir détourné des millions d'euros dans plusieurs arnaques informatiques montées à partir de comptes mails piratés. Du CEO swindle. L'affaire a débuté en 2014, à la suite d'une plainte d'un homme d'affaire Pakistanais. Des intrus lui avaient volé 34 000 euros.

CEO swindle

Les voleurs exploitaient les informations privées interceptées dans les comptes électroniques des dirigeants ciblés. Lors des perquisitions, un lieu étonnant a été visité par les policiers, celui d'un local situé prêt de l'aéroport de Londres. Plusieurs dizaines de milliers d'euros, en liquide, y avaient été cachés. A Madrid, un sac replis de billets a été découvert dans une valise placée en soute. 135.000 euros !
Selon le communiqué de presse de la police Espagnole, le mode opératoire consistait à « ***pirater les comptes mails de dirigeants d'entreprises*** (…) ***pour avoir accès aux données confidentielles***« . Les pirates faisaient ensuite chanter les patrons. Un piratage informatique qui est d'autant plus intéressant qu'il a été découvert que « ***de nombreux chefs de sociétés espagnoles*** » sont soupçonnés d'avoir exploité les pirates pour permettre de blanchir des fonds qu'ils souhaitaient cacher au fisc.
L'argent détourné était envoyé, en liquide, au Nigeria. 07 mai 2016.
Liens : http://www.zataz.com/ceo-swindle-arrestation-pirate-scam/#axzz49k7KuR67

SWIFT étend sa solution Sanctions Screening afin de filtrer tous les formats de transactions financières

Le service hébergé offre un outil simple et économique permettant de se conformer à la réglementation en matière de sanctions**.**

SWIFT annonce l'extension de son service Sanctions Screening permettant de filtrer tous les messages utilisés pour les transactions financières, indépendamment du format ou du réseau financier utilisé. Les utilisateurs peuvent dorénavant filtrer tous les formats de transactions, y compris SEPA et Fedwire, ainsi que les transactions effectuées sur d'autres réseaux que le réseau SWIFT. Le service étendu offre également une plus grande flexibilité et une meilleure intégration dans le back office, répondant ainsi aux besoins des banques de taille moyenne et aussi des utilisateurs qui ont des activités et des exigences opérationnelles plus complexes.

SWIFT a développé Sanctions Screening pour les institutions qui recherchent une solution hébergée proposant le filtrage en temps réel des messages sur la base des listes de sanctions internationales. La solution Sanctions Screening de SWIFT allie un moteur sophistiqué de filtrage et de mise à jour de listes de sanctions à la sécurité et la fiabilité de SWIFT. Les transactions peuvent être filtrées par rapport à plus de 30 listes majeures de sanctions, notamment les listes de l'OFAC (Etats-Unis), de HM Treasury (Royaume Uni), de l'Union Européenne et de l'autorité monétaire de Hong Kong. SWIFT effectue les mises à jour des listes de sanctions, sans frais supplémentaire, éliminant ainsi une source majeure de coûts et de risques pour les clients.

«Nous utilisons Sanctions Screening depuis 2012. Ce service est un élément essentiel de notre programme de conformité, et il offre une véritable tranquillité d'esprit » indique Christine Coffin, Head of Back Office, CPoR Devises. « Nous avons testé le service étendu de SWIFT et sommes vraiment satisfaits de pouvoir dorénavant compter sur Sanctions Screening pour les paiements SEPA.»

«Dans le monde actuel, les banques ont besoin de renforcer leurs systèmes AML/CFT avec des outils automatisés en temps réel, qui permettent un contrôle efficace », déclare Ramiro Uribe Aleman, Chief Compliance Officer of Banco Economico, Bolivie. « Nous avons choisi d'intégrer le service Sanctions Screening de SWIFT à notre procédure d'envoi et de réception des virements électroniques. Nous sommes convaincus que cette application fournie par SWIFT va grandement contribuer à une conformité à la réglementation relative aux sanctions.»

«Sanctions Screening est un service centralisé qui rend le filtrage des transactions simple et économique, même pour les petites institutions » ajoute Nicolas Stuckens, Head of Sanctions Compliance Services, SWIFT. « Etendre ce service est une étape naturelle pour SWIFT, en ligne avec notre vision : répondre aux besoins du secteur en matière d'évolution de la conformité à la réglementation contre la criminalité financière.»

Sanctions Screening a été introduit par SWIFT en 2012 et a été la première offre du portefeuille de solutions de conformité contre la criminalité financière de SWIFT. Près de 300 institutions dans 97 pays ont souscrit au service, y compris 15 banques centrales.

Pour plus d'informations sur Sanctions Screening, consultez swift.com/sanctionsscreening.

A propos de SWIFT's financial crime compliance services portfolio
Le Service Compliance de SWIFT gère un portefeuille croissant de solutions innovantes contre la criminalité financière dans le domaine des sanctions, comme Know Your Customer (KYC) et Lutte anti-blanchiment (LAB). Développé en collaboration avec la communauté financière, ce portefeuille inclut Sanctions Screening, une solution de filtrage standard et Sanctions Testing, qui aide les banques à maximiser l'efficacité de leur conformité aux sanctions. Ce portefeuille comprend également Compliance Analytics, un outil de business intelligence qui aide les banques à faire face aux risques de la criminalité financière en tirant parti de leurs données de trafic SWIFT; et le Registre KYC, un utilitaire centralisé de collecte et de distribution des informations standards exigées par les banques dans le cadre de leurs processus de diligence raisonnable. swift.com/complianceservices.
À propos de SWIFT
SWIFT est une société coopérative qui permet aux membres de son réseau d'échanger des informations financières standardisées et automatisées de manière sûre et fiable, et, ainsi, réduire les coûts, limiter les risques opérationnels et supprimer des processus opérationnels inefficaces. Plus de 10 500 organismes bancaires, établissements financiers, institutions et entreprises, dans 215 pays, bénéficient des produits et services ainsi que de l'expertise SWIFT et de sa plate-forme de communication sécurisée, unique au monde. SWIFT assure l'échange sécurisé de données propriétaires en garantissant confidentialité et intégrité. SWIFT facilite également le rapprochement des acteurs de la communauté financière pour élaborer ensemble les pratiques de marché, définir des standards et envisager des solutions aux questions d'intérêt commun. En utilisant SWIFT, les clients peuvent bénéficier d'un large panel de solutions métier et optimiser la gestion des flux financiers. swift.com
Liens : http://www.finyear.com/SWIFT-etend-sa-solution-Sanctions-Screening-afin-de-filtrer-tous-les-formats-de-transactions-financieres_a31631.html

Arnaque Western Union : Les différents scénarios possibles

L'arnaque Western Union ainsi que d'autres arnaques de ce type et provenant de Côte d'Ivoire sont très nombreuses, et même en augmentation ces derniers mois. Si vous avez déjà vécu ce genre d'arnaques, vous aviez probablement eu affaire à l'une citées dans cet article.

L'arnaque au client mystère (Secret Shopper)

Vous êtes contacté soudainement (souvent en anglais ou dans un français catastrophique) par un individu qui vous propose de faire une mission en tant que « client mystère ». Vous recevez des « *traveller chèques* » (chèques de voyage) d'un montant important avoisinant généralement le millier d'euros et quelques semaines plus tard, vous apprenez qu'ils ont été refusés par votre banque car ils ont été contrefaits ou volés.

Entre temps, vous avez bien entendu reversé une rémunération de quelques centaines d'euros et viré le montant restant à une personne X ou Y. Ce montant, vous ne le reverrez jamais en plus de ne pas recevoir votre rémunération… Dans ce cas là, il est primordial de prendre contact avec la société émettrice des travellers chèques afin de vérifier le numéro de série, cela prend 5 minutes et vous pourrez les jeter à la poubelle directement sans vous faire arnaquer.

L'arnaque aux sentiments

Les cyber-escrocs créent des faux comptes sur des sites de rencontre, ou sur les réseaux sociaux en utilisant des photos d'hommes ou de femmes récupérées sur internet. Leur but est d'entretenir pendant des semaines voir des mois des conversations sentimentales avec des internautes.

Les cibles sont souvent choisies, c'est-à-dire des personnes qui sont déjà affaiblies sentimentalement au moment de la rencontre. À un moment donné, ils solliciteront leur victime pour l'achat d'un billet d'avion leur permettant de leur rendre visite, pour l'achat de quelques nuitées à l'hôtel, pour aider un proche tombé soudainement malade ou victime d'un accident, etc. Les raisons ne manquent pas, les seules limites sont la capacité d'imagination de l'escroc !

Ces arnaqueurs qui se font appeler « ***brouteurs*** » en Côte d'Ivoire maîtrisent très bien la langue française ainsi que les outils informatiques, dont les logiciels webcam truqués et de retouches d'images. Les excuses données par la suite sont très bancales, on apprend qu'ils se sont fait arrêter à l'aéroport car leurs vaccinations n'étaient pas à jour, ou car un autre phénomène « imprévisible » est arrivé. Dans ce cas, il n'y a que la vivacité d'esprit et la perspicacité qui peut empêcher de tomber dans le panneau. Ne pas être trop crédule, surtout sur le Net avec des total inconnus.

L'arnaque à l'héritage

Il s'agit en général de prétendus fonds (des dizaines de milliers d'euros) qui se trouveraient bloqués dans une certaine banque au nom d'un certain héritier ne pouvant récupérer son avoir sans l'intervention d'un tiers. Les escrocs manient là encore très bien la langue française et font douter les internautes en utilisant des noms réels et des adresses mail qui semblent légitimes.

Les escrocs récupèrent ensuite vos coordonnées bancaires ou vous font payer plusieurs « frais de dossier » ou douaniers en cascade. Les motifs donnés sont très variés, il peut s'agir d'une personne atteinte d'une grave maladie ou décédée, d'un objet qui n'a pas pu être livré, etc. Avec une simple recherche Google sur le mail de l'escroc, vous tombez généralement sur des résultats probants.

Les arnaques Le Bon Coin

Ces arnaques prennent plusieurs formes mais ont habituellement toutes un point commun : une offre excessivement alléchante. Certains escrocs répondent à vos annonces en indiquant être un acheteur résidant en Côte d'Ivoire. Ils demandent l'expédition de votre objet (souvent de véhicules) depuis la France à vos frais avec promesse de règlement dès réception, ou en demandant vos coordonnées bancaires pour un prétendu « paiement ».

D'autres escrocs vendaient sur Le Bon Coin des objets en demandant un paiement par mandat-cash, bien-sûr les acheteurs ne recevaient jamais leur commande. Faîtes également attention avec votre numéro de téléphone, lorsque vous initiez une conversation de ce type, vous risque d'être inondé d'appels et de SMS toute la journée

L'arnaque à la loterie

L'une des plus populaires, et sûrement l'une des moins efficaces à présent. Les mails finissent en grande majorité dans les dossiers spam et ne sont pas convaincants. L'un des derniers en date était plutôt marrant, à savoir une « Loterie Microsoft » accompagnée de photos de Bill Gates, vous annonçant que vous êtes l'heureux gagnant de plusieurs dizaines de milliers d'euros. Fake !

L'arnaque Skype (anciennement MSN)

Votre contact réel se fait pirater et l'escroc se sert du compte pour demander de l'aide, notamment pour l'achat d'un objet ou le paiement d'un loyer.

L'arnaque au remboursement

Pour vous faire croire que l'on va vous aider, on vous propose des faux sites et fausses adresses mail à contacter, tout en cherchant à vous arnaquer une deuxième fois.
Ne croyez absolument pas les sites qui vous proposent de vous aider ou de vous rembourser, pareil pour les adresses mail du type « interpole-service-anti-arnaque@hotmail.etc ». A noter qu'il y a eu plusieurs commentaires de ce type postés sur UnderNews depuis un an, la plupart modérés.
Les seules vraies adresses et sites se trouvent à la fin de cet article.

D'autres arnaques plus techniques

Le phishing ou hameçonnage, vous recevez un mail provenant soi-disant de *PayPal* ou de votre banque vous demandant de mettre à jour vos informations. Plus dangereux encore, un faux mail de paiement PayPal en réponse à la vente d'un objet en ligne sur un site de petites annonces : vous envoyez alors l'objet en pensant avoir été payé mais il n'en ai rien ! Pensez à vérifier systématiquement dans votre compte PayPal que la somme a bien été véritablement versée (ne surtout pas accorder de l'importance aux mails reçus).
Cette arnaque est très utilisée sur Le Bon Coin ou eBay et fait énormément de victimes en France. Un reportage au journal de 20H a d'ailleurs été diffusé juste après les fêtes pour avertir des risques.

Et le pire dans tout ça ?

Beaucoup de victimes arnaquées ne portent pas plainte, car elles se sentent embarrassées d'être tombées dans le piège.
Celles qui portent plainte ne revoient tout de même pas leur argent ou objet car la police française ne prend pas souvent (jamais ?) le temps de faire les démarches. Les escrocs se trouvent à l'étranger et sont, pour la plupart du temps, intouchables.

Comment éviter ces arnaques ?

Ne faîtes d'une manière générale absolument pas confiance aux annonces de ce type, et restez vigilent et informés. Ne répondez pas aux mails lorsqu'ils sont alléchants ou vous demandent vos identifiants et/ou informations bancaires.
Utilisez TinEye sur les images des réseaux sociaux et annonces pour savoir si l'image a été récupérée sur Internet ou non.

Comment récupérer votre argent ?

Telle est la question. L'arnaque western union (ou toute autre arnaque de ce type) est compliquée à traiter pour les autorités.
Voici la plateforme pour la lutte contre la cybercriminalité en côte d'ivoire http://cybercrime.interieur.gouv.ci/. Vous pouvez également envoyer un courriel à cybercrime@interieur.gouv.ci.
Vous pouvez bien-sûr déposer plainte en France, ce qui est d'ailleurs le seul choix possible pour que vous puissiez obtenir une réponse favorable, à condition que la justice française décide de poursuivre son enquête en Côte d'Ivoire, le consulat transmettra alors la commission rogatoire internationale aux autorités ivoiriennes.
Si vous déposez plainte en Côte d'Ivoire, vous vous exposez à des frais de déplacement élevés, alors que la probabilité de récupérer vos fonds reste toujours extrêmement faible, pour ne pas dire nulle.

Liens : https://www.undernews.fr/reseau-securite/arnaque-western-union-les-differents-scenarios-possibles.html

Etats-Unis :
Un site de monnaie virtuelle démantelé pour blanchiment d'argent

La justice américaine a mis fin au site de monnaie virtuelle Liberty Reserve, un service utilisé par un million de personnes. Ce serait l'une des plus grosses plateformes de blanchiment d'argent démantelée au monde.

Mardi 28 mai, la justice américaine a affirmé avoir mis fin à ce qu'elle appelle la plus grosse opération de blanchiment d'argent du monde, effectupar l'intérmédiaire de Liberty Reserve, un site internet de monnaie numérique virtuelle. Il aurait permis le blanchiment de six milliards de dollars, soit près de cinq milliards d'euros.

Transformer des dollars en argent virtuel sans contrôle

Sur Liberty Reserve, les internautes pouvaient déposer les sommes qu'ils voulaient anonymement, et de nombreux criminels en ont profité. Le système était simple: il suffisait de s'inscrire en donnant juste un nom que personne ne vérifie. En clair, un faux nom.

Les utilisateurs pouvaient ensuite envoyer 10.000 dollars bien réels qui seront convertis en monnaie numérique. Avec cette monnaie numérique, ils pouvaient acheter n'importe quoi, pour le revendre ensuite et racheter à nouveau. Une fois le business fini, les internautes n'avez plus qu'à reconvertir leur monnaie numérique en dollars sonnants et trébuchants.

Un million d'utilisateurs, cinq milliards d'euros

Pour la justice américaine, le blanchiment d'argent criminel était le fonds de commerce de Liberty Reserve, issu de la fraude à la carte bancaire jusqu'à la pornographie infantile, en passant par le piratage informatique. Un million de personnes utilisaient ce site dans le monde dont 200.000 aux Etats-Unis.

Les sites de monnaie numérique, comme le Bitcoin, remportent un succès grandissant et le gouvernement américain précise qu'il ne s'oppose pas à toute forme d'argent virtuel. Mais il explique que le risque de blanchiment est toujours élevé et que l'impunité et l'anonymat, même sur Internet, ont leurs limites

Liens : http://bfmbusiness.bfmtv.com/entreprise/etats-unis-un-site-monnaie-virtuelle-demantele-blanchiment-d-argent-525010.html

9000€ en faux billets pour un adolescent de 14 ans

Parce qu'il s'est cru plus malin que les autres, un adolescent risque de finir entre 4 murs pour avoir écoulé 9000€ de faux billets acheté dans le black market.

Imaginez la tête des parents. Découvrir que leur adorable adolescent n'est rien d'autre qu'un petit voyou du numérique. Un cas rare ? Malheureusement non. La rédaction de zataz.com en rencontre de plus en plus. Le dernier cas en date, un collégien de 14 ans. Arrêté par la police après une alerte de la proviseur de son établissement scolaire. La responsable du collège avait été alertée par des élèves.

L'histoire est simple. Le « môme » avait d'abord mis en place un phishing, un hameçonnage de données en diffusant de faux courriels aux couleurs de NetFlix. Une fois les données des « pigeons » en main, le malveillant a cherché un moyen de blanchir les données volées. Bilan, direction le blackmarket. En revendant les données bancaires, l'adolescent a été payé en bitcoins. Monnaie virtuelle et décentralisée qui

lui a offert l'occasion d'acquérir, ensuite, des faux billets de 20€. Plus de 400 billets qu'il s'est fait livrer, par la poste.

Votre ado : ange ou démon sur la toile ?

Sans vouloir transformer les parents en vicieux petits espions, il est conseillé de comprendre comment un simple adolescent peut mal finir. Il ne faut pas tomber dans la paranoïa. Heureusement, la majorité des internautes ne sont pas des voyous 2.0, et ils n'ont pas envie de le devenir. Mais comprendre comment agit un « pirate » de ce genre peut éviter de voir débarquer au domicile familial « *Les amis du petit déjeuner*«. Pour rappel, la contrefacteur de monnaie peut finir avec 10 ans de prison dans les jambes.

Malin, malin et demi

Ce collégien de 14 ans a d'abord eu l'idée de créer des hameçonnages. Pour cela, ses visites dans certains « forums » dédiés au piratage informatique lui on offert de quoi réaliser ce genre d'attaque. Un kit phishing Netflix qu'il est possible de trouver sur la toile gratuitement. Ensuite, contacter des internautes, au hasard, via des adresses électroniques glanées, si et là. Les pigeons ne tardent pas à tomber.

Une fois les données volées en main, le pirate a besoin de les blanchir et d'en extraire le plus rapidement possible l'argent qu'elles peuvent contenir. De l'argent sous forme de numéros de cartes bancaires, d'identités, de numéros de téléphones, … L'adolescent contrefacteur va trouver dans le blackmarket des moyens de se faire de la monnaie. Du moins de la monnaie virtuelle. Dans le blackmarket, les paiements se font dorénavant en monnaie dématérialisée, sous forme de Bitcoins ou autres billets 2.0. L'adolescent a donc revendu ses informations volées. Elles lui seront payées en Bitcoins qu'il a ensuite exploité en achetant des faux billets de 20 euros. Billets suffisamment bien réalisés pour être utilisés dans les commerces, à hauteur de 9000€.

Tout ceci n'est malheureusement pas de la science fiction et peut se faire en quelques minutes. Bref, parents, sans vouloir vous transformer en vicieux petits espions, il est conseillé de comprendre comment un simple adolescent, peut mal finir, avant qu'il ne soit trop tard

Liens : http://www.zataz.com/9000e-en-faux-billets-pour-un-adolescent-de-14-ans/#axzz4A3JYqryt

Un code malveillant dans un système de lecture de CB

Le groupe de restaurant Pizza & Pub Village informe ses clients d'une attaque informatique. Un code malveillant a été injecté dans des lecteurs de cartes bancaires (POS).

Le site DataSecurityBreach révèle un piratage informatique particulièrement intéressant. Le groupe de restauration Village Pizza & Pub vient d'informer ses clients d'une intrusion dans son système informatique. Un logiciel espion a été introduit dans le système de paiement par carte bancaire des restaurants. Un cheval de Troie installé à partir de l'outil de TransformPOS, un fabriquant de lecteurs de CB. TransformPOS a assuré que la cause de l'incident avait été identifiée et résolue.

Pendant ce temps, en France…

L'Observatoire national de la délinquance et des réponses pénales (ONDRP) a indiqué que plus de 800.000 ménages Français se sont déclarés victimes d'une escroquerie bancaire en 4 ans. Un chiffre tiré de plaintes, entre 2011 et 2014. D'après cette étude, 35% des escroqueries sont inférieures ou égal à 100 €. 25%, entre 301 et 1000 €. 17% sont supérieures à 1000€. Près de 8 ménages escroqués sur 10 ont été

remboursés. 12% de l'argent volé est récupéré par le pirate via un distributeur de billets (donc du skimming qui a permis de cloner la carte, NDR). 60% est récupéré via un achat direct sur la toile. 17 % des cas, le pirate a recours à un autre type de blanchiment. Les cas sont multiples, ZATAZ.COM a déjà pu repérer des rechargements de crédit téléphoniques ; des placements dans des casinos douteux ; des achats de comptes sur des sites pornographiques qui sont revendus… Une étude très (trop) généraliste pour que le publique comprenne véritablement le danger, les possibilités de fuites et comment véritablement se protéger.

Comment se protéger ?

Votre carte bancaire ne doit jamais quitter votre regard lors d'un achat en boutique, un paiement dans un restaurant. Protégez votre carte dans un étui qui empêchera l'interception NFC sans votre accord. Retournez TOUJOURS le lecteur de carte bancaire qui vous est présenté par un commerçant. Est-ce que les visses ont été abimées ? Y-a-t-il un autocollant qui protège le boitier, nous avons eu des cas ou les commerçants s'étaient fait subtiliser leur lecteur de CB, remplacé par une version pirate. Sur Internet, bannissez l'utilisation de votre vraie CB. Demandez à votre banque le moyen qu'elle a mis pour vous permettre de générer une carte bancaire unique, pour un achat, un montant. Le Crédit Mutuel du Nord, par exemple, propose la *PayWeb Card*. Votre commerçant est payé, et si par on ne sait quel hasard il se fait voler le numéro de carte bancaire que vous avez fourni, le pirate ne pourra rien en faire et votre argent est protégé.

Dernier détail, ne perdez jamais du regard votre téléphone portable. Le clonage de votre puce peut permettre à un pirate de valider des achats via un SMS de validation de votre banque en se faisant passer pour votre téléphone.

Bref, n'oubliez jamais que pour les pirates informatiques nous ne sommes que des portes monnaie sur pattes et qu'ils ne manquent pas d'imagination pour mettre la main sur des données bancaires

Liens : http://www.zataz.com/un-code-malveillant-dans-un-systeme-de-lecture-de-cb/#axzz4A3JYqryt

Des guichets automatiques privés pour blanchir l'argent sale

Trois ans après que l'Autorité des marchés financiers (AMF) eut promis de se pencher sur le blanchiment d'argent à travers les guichets automatiques privés, elle n'a toujours pas réussi à contrôler la totalité de cette industrie, rapporte TVA Nouvelles**.**

En 2013, une loi censée faire le ménage dans ce secteur avait été édictée. Or, le Bureau d'enquête de TVA a constaté que « de très nombreux guichets privés ATM, dont plusieurs situés dans des bars, des dépanneurs et des restaurants, continuent d'être opérés au Québec sans afficher la vignette obligatoire de l'AMF ».

Présence du logo de l'AMF

Cette vignette signale que les billets fournis aux clients sont « propres » et que les machines qui les distribuent « sont exploitées par des entreprises légitimes, et non par des organisations souhaitant y laver leur argent sale », précise la chaîne d'information. Autrement dit, lorsque le logo de l'AMF est absent, cela signifie que le fonctionnement du guichet échappe à tout contrôle officiel.

« Si le logo n'est pas visible, la personne qui a le guichet est en infraction avec la loi », confirme à TVA le porte-parole de l'AMF, Sylvain Théberge, qui précise que l'Autorité continuera à faire son travail d'inspection et de vérification.

Selon lui, 94 % des guichets ATM impliqués dans le processus d'accréditation, soit 3 420 machines, ont à ce jour obtenu leur permis (et devraient donc afficher le fameux logo) et il n'en resterait qu'un peu plus d'une centaine en attente de le recevoir.

Jusqu'à 25 000 $ par mois

Toutefois, souligne TVA, ces chiffres ne tiennent pas compte des guichets ATM en exploitation qui ne sont pas engagés dans le processus avec l'Autorité, qui avoue ignorer le nombre de machines que cela représente.

« Il est de la responsabilité des exploitants de nous informer de la présence des guichets », justifie Sylvain Théberge.

Si l'on en croit « une source bien informée » reprise par la chaîne d'information, les appareils privés peuvent non seulement servir à blanchir de l'argent, mais, à cinq dollars par transaction, certains rapporteraient à leurs propriétaires jusqu'à 25 000 dollars par mois. 28 avril 2016

Liens : http://www.conseiller.ca/nouvelles/des-guichets-automatiques-prives-pour-blanchir-largent-sale-58436

Quel est le prix de vos données sur le black market ?

Les cybermenaces se multiplient et avec elles, les acteurs profitant des cyberattaques perpétrées aussi bien contre des entreprises (multinationales ou PME) que des particuliers. Le Saint Graal ? Les données personnelles revendues ensuite sur le black market pour mener d'autres attaques ou escroqueries. Les experts de G Data ont infiltré le marché noir pour comprendre son écosystème.

Dans les tréfonds du dark web, les marchés noirs pullulent, chacun leur petit nom (Silk Road Reloaded, Angora, Pandora, etc.), leurs habitués et *spécialités*. Grâce à eux, vous pouvez acheter ou vendre à peu près tout ce qu'internet compte d'illicite : armes, drogues, faux papiers, données personnelles, tueur à gages, logiciels malveillants, etc.

Récemment, le tenancier de Silk Road, autrement dénommé « l'eBay de la drogue », a été condamné à la prison à vie (deux fois), reconnu coupable, entre autres, de blanchiment d'argent, trafic de stupéfiants et piratage informatique.

Les experts de G Data, éditeur international de solutions de sécurité informatique dont la société sise à Bochum a été créée en 1985, ont infiltré le black market afin de comprendre son écosystème, ce qui s'y échange, quels produits et services y sont vendus et à quel prix ?

Quoi ? Faux papiers, armes, drogues, logiciels malveillants, exploit kit, virus, payés en monnaie virtuelle, dont la plus connue est le Bitcoin (1 bitcoin = 238$).

Qui ? Des cybercriminels donc. S'il y a encore quelques années, seuls les plus aguerris s'y retrouvaient pour échanger leur butin afin de mener des opérations entre eux, force est de constater que le profil du cybercriminel à changer puisque, comme expliqué précédemment, tout s'achète sur le black market, même les services d'un autre. Ainsi, sans grandes compétences, on peut s'allouer les services d'un développeur de *malwares*, puis d'un hébergeur, etc. et mener sa propre opération.

Le marché noir est le terrain tout choisi des alliances de compétences entre différents cybercriminels. Bonus : il offre un service après-vente, si un numéro de carte bancaire acheté ne fonctionne pas, il vous en sera délivré un autre, par exemple. Les réputations des vendeurs et des acheteurs sont très importantes, le marché noir marchant sur la confiance des produits, vendeurs, mais aussi acheteurs. C'est la limite

de l'enquête des experts de G Data, ils n'ont rien acheté, n'ont pas construit leur réputation et n'ont pas pu accéder à certains forums privés où il faut être invité.
Tarifs ? Très abordables selon ce que vous souhaitez acheter et les produits les plus recherchés sont les données personnelles : adresse email, compte email, numéro de carte bleue, identité complète.
– Services
Peut aller de 70€ pour l'installation d'un programme malveillant à 100€ pour une attaque DDoS, parfois *loué* à l'heure (entre 10€ et 200€/h d'attaque), 5€ le spam, 20€ le kit d'hameçonnage (ou *phishing*) et 5 000€ l'installation d'un Bot.
– Produits
Logiciels malveillants (Ransomware/Crypter,Exploits).
Tutoriels : gratuit, cadeau de bienvenue.
Faux papiers (1 000$ la carte d'identité, 2 500$ le passeport et 1 150$ le permis de conduire), armes (Desert Eagle IMI, 44, 1250$), drogues, carding et skimming (pour escroquerie et piratage de CB)
Données personnelles : 75€ le million d'emails (ou 0,000075$ l'adresse), 20€ les 40 000 comptes emails, 50€ la CB française volée ou le compte Paypal, 70€ l'identité complète (ou fullz) d'une personne. Les faibles prix s'expliquent aisément par l'offre très abondante. Autrement dit, plus la quantité de données personnelles subtilisées est importante, plus important sera le gain pour le cybercriminel.
Les données personnelles sont les plus prisées et peut-être aussi les plus facilement récupérables : avec elles, c'est la porte ouverte sur votre vie privée et numérique : email, compte email, accès compte réseaux sociaux, usurpation d'identité, achats frauduleux sur internet, fausse carte de crédit, etc. On dénombre 2600 cas par mois, 80% sont des escroqueries et 22% des arnaques à la carte bancaire.
Les Botnet sont de plus en plus utilisés, pour mener des campagnes de spam, stocker des données illégales, mener des attaques DDoS, accéder à un compte Steam, etc. Le botnet est un réseau de *bot* (robot) informatiques, qu'on appelle aussi réseau de machines zombies car plusieurs ordinateurs sont infectés par un virus dormant. Pour mener une attaque de spam, *phishing* ou DDoS, le groupe ou la personne qui contrôle le botnet réveille son réseau d'ordinateurs infectés.
Comme nous l'a expliqué Eric Freyssinet, conseiller du préfet en charge de la lutte contre les cybermenaces au Ministère de l'Intérieur, le Botnet requiert plusieurs compétentes qu'une seule personne ne peut souvent pas réunir et coûte généralement plusieurs milliers d'euros à la personne qui souhaite le constituer et l'utiliser. Les données récoltées grâce à lui, *rentabiliseront* son investissement, une fois revendues sur le black market, mais bénéficieront aussi aux autres acteurs du marché noir, comme les gestionnaires d'infrastructures,acheteurs de données collectées, blanchisseurs d'argent sale, etc.
Pour Eric Freyssinet, l'avenir des Botnet se sont les objets connectés qui, une fois piratés, peuvent donner accès aux serveurs où sont connectés ces objets. Mais également les terminaux de point de vente, de plus en plus ciblés (notamment aux États-Unis).
Leur rapidité de diffusion et d'adaptation (notamment du pays dans lequel le botnet est déployé) en fait des armes redoutables et difficilement traçables. Le temps de l'enquête, l'attaque est terminée depuis longtemps. Cependant, des victoires sont à relever : Blackshade, dont l'enquête a donné lieu à un important coup de filet international, l'auteur de Gameover Zeus, identifié, mais toujours en fuite (le FBI offre 3 millions de dollars pour sa capture) ou le développeur de Blackhole arrêté en 2013.

On en le dira jamais assez une bonne protection (antivirus complet, qui comprend un pare-feu, quand un pare-feu ne comprend pas d'antivirus) est de mise et surtout une grande vigilance. Si les logiciels malveillants ou autres botnet exploitent des failles existantes, ils profitent également de la méconnaissance et l'imprudence de l'internaute lambda, qui même avec un mot de passe à rallonge, ne peut rien faire face à ça.
Liens : http://www.journaldugeek.com/2015/06/09/prix-donnees-black-market/

Escroquerie à la carte bancaire : huit Moldaves écroués

Huit Moldaves ont été mis en examen et écroués pour avoir piraté des distributeurs automatiques de billets dans la Loire, le Calvados, les Alpes-Maritimes et en région parisienne.
Âgés de 25 ans à 40 ans, les suspects ont été mis en examen pour "escroquerie en bande organisée" par un juge d'instruction de la Loire, où leurs agissements avaient été repérés pour la première fois à l'été 2015. Leur interpellation est intervenue en deux phases, en novembre dans l'Essonne pour quatre d'entre eux, et le 30 mars en Seine-Saint-Denis pour le reste de la bande.
"Lors des perquisitions, nous avons retrouvé près d'une vingtaine de cartes bleues contrefaites, des lecteurs pour les ré-encoder avec les coordonnées bancaires volées", a précisé à l'AFP la commissaire divisionnaire Judicaële Ruby, cheffe de la section économique et financière de la Direction interrégionale de la police judiciaire de Lyon, évoquant des équipes "particulièrement organisées".
Sur les distributeurs de billets, les malfrats utilisaient la technique du "skimming" qui consiste à recueillir les coordonnées des cartes bancaires à l'aide d'un dispositif électronique collé sur le lecteur de carte ou installé sur la machinerie interne de l'appareil.
Une micro-caméra, cachée dans un faux plafond de la machine ou dans une fausse paroi latérale, filmait les clients en train de faire leurs codes secrets. Ils ré-encodaient ensuite de fausses cartes avec les données volées, selon la même source. "D'autres suspects ont été identifiés et sont actuellement en fuite", a précisé Mme Ruby.
Le montant du préjudice pour les victimes n'a pas été précisé. 8 Avril 2016
Liens : http://www.lyonpremiere.com/Escroquerie-a-la-carte-bancaire-huit-Moldaves-ecroues_a12391.html

2 millions de dollars dérobés via des skimmers Bluetooth implantés dans des stations services aux USA

Les cybercriminels exploitent toutes les technologies pour faire de l'argent et le Bluetooth ne semble pas être épargné. Un énorme vol de cartes de crédit dans des stations services US a été commis via des skimmers Bluetooth.

13 hommes sont soupçonnés et accusés d'avoir dérobés des milliers d'informations bancaires, en utilisant des skimmers Bluetooth implantés dans des stations service dans le sud des États-Unis. Les informations de cartes de crédit volées leur auraient permis de récupérer plus de 2 millions de dollars via les ATM (les codes PIN des clients ont été aussi enregistrés et l'argent était retiré en cash à des distributeurs automatiques de billets à Manhattan).
Les dispositifs de skimming ont été installés à l'intérieur des machines, de façon indétectable aux gens qui ont payé aux pompes automatiques et les appareils étaient équipés en Bluetooth, de sorte qu'il n'y a pas besoin d'un accès physique pour récupérer les données volées.
Entre mars 2012 et mars 2013, les suspects ont utilisé des fausses cartes bancaires ré-encodées pour retirer de l'argent à partir de distributeurs automatiques de billets, puis déposés l'argent volé dans divers comptes bancaires à New York, en Californie ou encore au Nevada. Une énorme affaire de fraude bancaire en somme…
« Chacune des transactions était moins d'un montant de $10 000. Elles auraient été structurées de manière à éviter toutes les exigences de déclaration des transactions en espèces imposées par la loi et à déguiser la nature, la propriété et le contrôle des produits de la criminalité des accusés. Du 26 mars 2012, à 28 mars 2013, les cybercriminels sont accusés du blanchiment d'environ 2,1 millions de dollars ».
Les quatre principaux accusés sur les 13 – Garegin Spasrtalyan, 40 ans, Aram Martirosian, 34 ans , Hayk Dzhandzhapanyan, 40 ans, et Davit Kudugulyan, 42 ans – sont considérés comme les organisateurs et sont accusés de vol, de blanchiment d'argent et de la possession d'instruments de falsification et de contrefaçon. Les autres criminels sont chargés de deux chefs d'accusation : vol et blanchiment d'argent.
Ils risquent tous plusieurs années de prison ferme et de gros dédommagements… affaire à suivre.
Liens : http://www.undernews.fr/hacking-hacktivisme/2-millions-de-dollars-derobes-via-des-skimmers-bluetooth-implantes-dans-des-stations-services-aux-usa.html

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

Nouveau coup de filet pour Europol qui s'est allié avec la Police financière italienne. 10 membres présumés d'un groupe de cybercriminels ont été arrêtés et inculpés pour arnaques en ligne, fraude bancaire et blanchiment d'argent.
La Police financière italienne (Guardia di Finanza) a arrêté plus de 10 personnes soupçonnées de faire partie d'une organisation criminelle internationale. Le groupe aurait blanchi de plus de 2,5 millions d'euros provenant d'escroqueries en ligne (scams) et fait face à des accusations de fraude et de blanchiment d'argent. L'opération a été menée en collaboration avec Euopol, qui vient de publier un communiqué.
L'opération a impliqué la coopération entre la police italienne, Europol et le Federal Bureau of Investigation (FBI). Des dizaines d'entreprises ont été touchées par ces cyberattaques sophistiquées visant à détourner les données des entreprises victimes et d'échanger ces informations contre des paiements par virement bancaire.
Beaucoup d'entreprises ont donc transféré d'importantes sommes d'argent aux cybercriminels. Des centaines de personnes ont également été affectées par des

escroqueries en ligne où les fraudeurs ont créés de faux profils sur des sites de rencontres et ont convaincu des gens de leur envoyer de l'argent.
Selon les enquêteurs, le groupe a fondé un large réseau international dans le but de procéder à des retraits d'argent liquide dans le monde entier. 32 personnes sont encore activement recherchées dans le cadre de ce "*bank run*" d'envergure.
Liens : http://www.undernews.fr/hacking-hacktivisme/italie-arrestation-dun-groupe-de-cybercriminels-international-scam-blanchiment-dargent.html

Skimming : Le "gang des Bulgares" devant la justice française

Le procès dit des "Bulgares" doit s'ouvrir mercredi 9 octobre 2013 au tribunal correctionnel de Dijon. Huit personnes de nationalité bulgare comparaissent pour escroquerie en bande organisée, contrefaçon de moyens de paiement et blanchiment aggravé.
Les huit prévenus avaient été mis en examen pour avoir piraté des distributeurs automatiques de billets (DAB) grâce à la méthode du skimming. Les criminels piégeaient les DAB avec un dispositif spécial dans le but de copier les bandes magnétiques et apposaient un faux clavier par dessus le vrai pavé numérique pour récupérer les codes secrets des carte bleues des utilisateurs des distributeurs automatiques de billets. Un système qui permet par la suite aux malfaiteurs de produire de "vraies-fausses" cartes bancaires et d'effectuer des retraits partout dans le monde : une fois les informations bancaires recueillies, il leur restait à ré-encoder les cartes, qui étaient utilisées à l'étranger afin que les victimes ne se rendent pas immédiatement compte des ponctions d'argent sur leur compte.
Un total de 1,2 million d'euros de préjudice estimé
Dans cette affaire, les malfaiteurs ont sévi en Bourgogne, mais aussi un peu partout dans le nord de la France. Le préjudice serait d'1.2 million d'euros. Plus de 3 500 cartes bleues auraient été piratées par ce gang. Des retraits qui ont été effectués dans une vingtaine de pays, on imagine facilement que les cartes de crédit ainsi piratées étaient revendues au plus offrant via le Black Market et des sites undergrounds spécialisés dédiés dans le carding.
L'affaire ne date pas d'hier : les deux premiers membres du gang ont été interpellés à Auxerre 2011. Les autres arrestations ont suivi dans le nord de la France après une longue enquête diligentée par la brigade de recherches de Dijon en 2012. La tête du réseau a été arrêtée à Sofia en Bulgarie, puis extradée en France en attendant le procès.
Pas d'information sur le nombre présumé de victimes en France pour l'instant.
Liens : http://www.undernews.fr/hacking-hacktivisme/skimming-le-gang-des-bulgares-devant-la-justice-francaise.html

Pirates sans frontières

Mercredi dernier, la plus grosse équipe de skimming de ces deux dernières années est tombée… entre les mains des enquêteurs la SR de Pau qui la pistait depuis des mois.

Le skimming ? C'est le piratage des distributeurs automatiques de billets et les interpellés n'y allaient pas de main morte ; sur 500 DAB piratés en France en 2015, ils en ont "tapé" près de 400.
A sa tête, trois "cerveaux" : un Italien qui fabriquait les skimmers, un ingénieur basque, et une femme qui gérait les mules chargées de rapporter l'argent de Thailande ou des USA (à raison de 9000 et quelques euros pour chacune, la limite légale en cash), pays où étaient utilisées les cartes avec la France et le Pérou. L'organisation était bien rôdée : certains posaient les skimmers puis envoyaient les données à l'informaticien qui les traitaient, avant de les expédier aux sous-équipes réparties dans les différents pays qui ré-encodaient des cartes vierges et débitaient. Enfin, le blanchiment des sommes en France se faisaient notamment via des tickets gagnants de la Française des jeux achetés avec un bonus à de complaisants joueurs. 24/05/2016
Liens : http://www.metronews.fr/blog/mafia/2016/05/24/pirates-sans-frontieres/