L'investigation informatisée des fraudes

Yoanna PONS
Auditrice système d'information AUDEA

Noël PONS
Consultant et essayiste

Résumé. – La cybercriminalité est désormais une activité industrialisée. Elle affecte aussi bien la sphère privée que l'économie et l'intelligence économique. Le grand nombre de personnes œuvrant dans ce domaine, l'importance des sommes détournées et des flux devant être protégés, la capacité de manœuvrer au niveau mondial exigent un minimum d'organisation. La criminalité et les mafias en ont naturellement fourni les moyens puisqu'elles utilisaient ce vecteur depuis l'origine. Le caractère généralisé de ces montages nécessite une amélioration constante des paramètres de sécurité car la mondialisation rend les poursuites difficiles.

Mots clés : Hacker – cracker – scam – smurf - cukoo-smurphing - phishing - pharming - botnet - internet protocol - cloud computing

Nous avons choisi dans cet article de traiter de la cybercriminalité et de la recherche de sources lucratives illégitimes. Nous ferons l'inventaire des acteurs œuvrant dans ce domaine, établirons leurs liens avec la grande criminalité, exposerons ensuite les manipulations le plus souvent utilisées puis convierons le lecteur à une ballade parmi les fraudes les plus marquantes dans ce domaine. Pour conclure l'analyse du casse numérique du siècle mettra en évidence certaines failles qui pourraient remettre en cause le principe du *cloud computing*.

I. — QUI SONT LES INTERNAUTES CRIMINELS ?

La cybercriminalité est devenue une affaire de professionnels présentant un très haut niveau intellectuel : études supérieures, docteurs, ingénieurs ce sont

eux qui œuvrent désormais. Ils ont quelque peu détrôné les étudiants en informatique et les amateurs éclairés. Les jeunes « bidouilleurs » sont cependant toujours présents et réalisent des coups remarquables. Les professionnels des fraudes les intègrent très rapidement dans leurs opérations.

Les « hackers » spécialistes des systèmes de sécurité informatique s'intéressent aux failles et certains aident les entreprises à se protége*r*. Avec l'accord du management, ils tentent de s'introduire par effraction dans les réseaux, dans le but d'identifier les failles et de les corriger.

Les « chapeaux noirs », avec des capacités techniques similaires, effectuent les mêmes tentatives, mais dans l'intention de nuire ou dans le but de retirer un gain de leur situation. Ils sont organisés en réseau et travaillent pour des structures criminelles ou pour leur propre compte. Ils tentent de voler des données en masse ou de bloquer les systèmes afin de les monnayer. La toute dernière attaque identifiée affecterait plusieurs dizaines de millions de comptes.

Les pirates informatiques peuvent être classifiés en fonction de leur activité et de leur spécialisation. Ces catégories sont d'ailleurs très fluctuantes car le réseau et les techniques évoluent constamment. Ils se rencontrent d'ailleurs régulièrement à l'occasion de conférences ou de réunions regroupant les meilleurs d'entre eux. Ils s'informent ainsi et échangent leur expérience acquise sur des techniques innovantes ou spécifiques ce qui rend le système particulièrement évolutif.

Les criminels sont classifiés en fonction de leurs comportements :

- les *script kiddies* manipulent les ordinateurs sans avoir aucune idée de la législation et des risques encourus.
- les *kids* un peu plus âgés, plus expérimentés aussi, participent à de multiples forums, à des tests en *live* et financiarisent leur activité par l'achat et la revente de *spams*. Mais le monde est leur terrain de jeu et ils sont très mobiles.
- les « codeurs » plus aguerris, plus expérimentés, programmeurs professionnels, souvent autodidactes, conçoivent et vendent des *bots* sur mesure ou des chevaux de Troie.
- les *drops*, le plus souvent très proches des criminels, sont incontournables dans la cyber-fraude. Leur rôle consiste à accompagner la transformation de l'argent « virtuel » en argent utilisable. Blanchisseurs de talent, ils facilitent les transferts des fonds vers des comptes protégés. Leur activité est rémunérée par leurs propres prélèvements, tout travail méritant salaire, certains ont cependant succombé pour avoir trop prélevé. Ils sont dans la plupart des cas contrôlés par des structures mafieuses et installés dans des pays dans lesquels les délits numériques n'existent pas ou ne sont pas réprimés. En fait un certain nombre de « cyber-paradis » se sont créés.

Le facilitateur en dernière place, au demeurant essentiel, des activités criminelles dans ce domaine est le « mulet » ou « stroumphs » ou « smurf ». Présents dans la plupart des montages, il s'agit de particuliers, personnes physiques n'ayant pas de lien permanent apparent avec la criminalité qui sont utilisés pour transporter des objets illicites (armes, drogue, numéraire) ou pour transférer des fonds structurés en respectant les principes du fractionnement. Parfois à leur insu, ils sont recrutés par e-mail pour transférer les fonds contre rémunération. Pour le recruter, le pirate abuse un internaute qui se rend ainsi complice de fraude, vol, détournement ou blanchiment d'argent passible de poursuites. Ces mules permettent de fractionner les envois ou les transferts et, en multipliant les transferts, noient les pistes de contrôle. Elles passent le plus souvent par la case prison et protègent de ce fait les autres passeurs. De fait, le grand nombre de personnes engagées dans ces opérations ne permet pas de poursuivre et de sanctionner l'ensemble des participants ce qui explique la pérennité du système.

Les cibles des criminels sont en majeure partie constituées, malgré quelques attaques réalisées dans un but publicitaire, de dirigeants, de cadres d'entreprises moyennes ou encore de filiales de multinationales. Au cours de leurs attaques ils procèdent de la manière suivante :
1-Ils choisissent d'abord la typologie de fraude qui doit être utilisée, en général les manipulations sont camouflées sous les identifiants falsifiés de collègues, donc sous des noms existants[1].
2-Ils siphonnent des identifiants ce qui permet de les utiliser de manière ludique ou avec des mails alarmistes.
3-Ils anonymisent ces travaux afin de rendre difficiles les recherches et la sécurisation des opérations.
4-Ils vendent les informations à des groupes organisés qui les distribuent, un peu à la manière de la gestion des otages par les groupes terroristes.
5-Ils organisent les transferts de fonds et le blanchiment qui les accompagne.

La cybercriminalité est très largement utilisée par le crime organisé car des sommes colossales sont en jeu. De nombreux groupes criminels ont très vite compris que l'anonymat et la liberté que procure internet facilitent la corruption, les fraudes, les détournements et le blanchiment d'argent sans risque. Nous constatons sur internet une réelle industrialisation des montages cornaquée par les criminels qui permet la réalisation de profits immenses

1 Il est fréquent d'obtenir les mêmes résultats en laissant en évidence une clé USB en apparence perdue, sa première utilisation fait entrer le virus qu'elle cachait dans le système. Il semblerait que l'attaque des systèmes d'une centrale iranienne se soit produite de cette façon.

accompagnés de risques minimes. Ce phénomène est constaté dans pratiquement tous les continents avec une priorité pour l'Afrique, les pays de l'Est et les pays d'Asie. Dans ces contrées, pays de mafias et triades le basculement a été aisé et rapide.

II. — LES TYPOLOGIES DES CYBER-FRAUDES

Les manipulations présentes sur internet sont très nombreuses et très variées, mais finalement on ne rencontre que peu de montages réellement novateurs, la plupart d'entre elles sont composées par de vieilles escroqueries remises au goût du jour.

Le *spamming*[2], envoi massif et automatique de messages électroniques non sollicités, les *spams* sont généralement adressés à des fins publicitaires. Les pourriels composent une partie conséquente du trafic qui pourrait être évaluée à plus de 80 % du trafic total, 16 milliards de *spams* seraient envoyés chaque jour en Europe. S'ils sont utilisés pour frauder, ils diffusent des incitations à visiter des sites piégés à partir desquels il sera possible de propager des virus ou des chevaux de Troie afin de capturer des informations confidentielles. Du fait de la mise en place de contrôles les cybercriminels ont développé désormais une pratique assez ingénieuse, appelée *drive by download*, ou « téléchargements cachés » réalisés à l'insu de l'utilisateur au cours d'un téléchargement ou de la consultation d'un site web ou de sa messagerie.

Les *spams* diffusent la célèbre « arnaque à la nigériane » ou fraude 4-1-9[3] qui a pour objectif d'abuser de la crédulité des internautes en utilisant les messageries électroniques pour leur soutirer de l'argent. Cette tromperie repose sur un envoi de mails visant à faire croire à la victime que l'expéditeur possède une importante somme d'argent comme des fonds à placer à l'étranger suite à un changement de contexte politique. Il leur fait part de son besoin d'utiliser un compte existant pour transférer cet argent. Évidemment les données du compte fourni sont immédiatement pillées. Pour crédibiliser le scénario, les fraudeurs mettent en place de faux sites bancaires qui usurpent l'identité d'établissements internationaux. Ces derniers visent à faire croire aux victimes que l'argent promis existe réellement.

Cette escroquerie est très ancienne dans son principe d'utilisation, d'aucuns en situent l'origine dans les célèbres lettres dites de la « princesse espagnole » détenue par les Turcs, elle épouserait celui qui paierait sa rançon, très pratiquées au cours du XVII^e^ siècle, ont suivi les « lettres de Jérusalem » décrites par Vidocq au XIX^e^ siècle. Elles sont devenues dans les années soixante les lettres d'un ancien ministre corrompu et qui aurait détourné cinquante millions de dollars puis se sont installées sur internet.

2 Le terme proviendrait du mot utilisé dans un sketch des Monty Python, célèbres comiques britanniques, parodiant une publicité radiophonique pour le « SPAM », un jambon épicé, pendant laquelle le terme était utilisé de manière récurrente.

3 En référence à l'article du code pénal nigérian pénalisant cette pratique.

Les réseaux sociaux sont actuellement très utilisés dans la diffusion des *scams* nigérians. L'e-mail de *scam* est envoyé sous la forme d'une invitation à être rajouté au réseau social d'un autre utilisateur. Cette forme est plus dangereuse que les précédentes, car les utilisateurs font une grande confiance à ces supports.

Une autre activité lucrative consiste à proposer à des internautes de participer à des transferts de fonds, en se comportant comme un mulet. Cette pratique appelée *cukoo smurphing* permet de fractionner le transfert de fonds et d'échapper ainsi à la surveillance des banques en ne transférant que des valeurs unitaires inférieures au seuil de contrôle.

Exemple de *cukoo smurphing* : Pour rendre presque indétectable l'intégration de sommes détournées par *phishing*, les criminels avaient recruté par *spamming* de nombreux complices qui prêtaient leur compte bancaire contre rémunération. La valeur des sommes qui transitait dans chacun des postes était calculée en fonction des flux moyens dans les comptes. De cette manière chacun des nombreux comptes utilisés (entre six et huit mille) avait vu passer des valeurs unitaires approchant les 17 000 euros.

Les cyber-délinquants envoient par exemple des e-mails proposant de devenir le collaborateur d'une soi-disant Société Financière Internationale. Parfois, un pseudo-contrat de travail est joint pour rendre l'offre plus crédible. Il est indiqué à l'internaute qu'il recevra des fonds sur son compte bancaire et le rôle de la mule consistera à sortir ces fonds et à les transférer vers un autre compte et donc de servir d'intermédiaire en percevant une commission pouvant aller jusqu'à 3 000 euros par mois. Le cyber-escroc utilise donc un compte tiers pour faire transiter cet argent d'origine frauduleuse et le transfèrer dans un autre pays.

L'Internet a aussi permis un développement considérable des pratiques « d'agiotage » ou de création de « bouilloires ». La multiplication des sites financiers et des forums accroît considérablement le risque de manipulation des cours. On a constaté une double évolution, une dérégulation d'abord, puis la possibilité pour l'utilisateur d'agir directement sur le marché, ce qui a ouvert en grand les portes aux manipulations. Ainsi, les spécialistes ont identifié un certain nombre de « web-manipulations » :

L'agiotage, *pump and dump stock fraud online* : il s'agit de diffuser des informations inexactes, qu'elles soient positives ou négatives dans des bulletins internet, pour faire varier la valeur.

Les fausses révélations, *posting false inside information*, qui se présentent comme des indiscrétions internes à la structure visée. Il s'agit le plus souvent de faux rapports d'audit.

Les fausses informations, il s'agit d'informations inexactes ou purement fictives, qui sont introduites dans une documentation officielle et largement

distribuées dans les forums et par des pourriels déstabilisants, postés dans des boîtes judicieusement choisies.

Le *boiler room online* qui consiste à mélanger les montages précédents pour escroquer les « pigeons ».

L'escroquerie par petites annonces qui propose des produits sans existence, des contrefaçons ou encore des escroqueries au transport et à la livraison des produits.

Les demandes d'envoi d'argent par mandat cash urgent à partir d'un e-mail détourné par exemple, qui sont très fréquents après la tenue de colloques ou de conférences internationales, très propices à l'échange de mails entre participants.

Les détournements de données à partir de sites de rencontre.

L'ensemble des entourloupes décrites ci-dessus peut être décliné sur l'Internet avec un niveau de réussite bien plus élevé que celui obtenu par des montages classiques. Certains réseaux mafieux ont utilisé ces types de manipulations de manière très efficace au détriment d'entités trop crédules lors de la crise des valeurs technologiques.

L'une des activités frauduleuses les plus lucratives est l'« hameçonnage » des internautes. Ce procédé permet de se faire communiquer les données bancaires au prétexte de vérification ou de sécurisation en se faisant passer pour une banque ou une société connue. Le *phishing* et le *pharming* sont deux techniques permettant de faire croire aux victimes qu'elles se trouvent sur un site web sécurisé, leur banque par exemple, alors qu'elles sont en fait sur un site web factice où leurs informations bancaires vont leur être dérobées. La première utilise le spam pour attirer leur victime sur un site contrefait. La seconde consiste à rediriger les victimes vers un faux site web alors qu'elles ont bien tapé une adresse web correcte dans leur navigateur. La manipulation consiste à modifier les données du serveur DNS (*domain name system*) et à dérouter l'utilisateur vers un site pourri.

Les banques, premières cibles des cyber-escrocs, ont installé de solides protections sans cesse mises à jour, c'est donc vers les détenteurs de compte, moins protégés, que se dirigent les attaques. Ces attaques permettraient de récupérer jusqu'à 400 fois la mise initiale[4]. Ces attaques sont en forte progression, mais les entreprises ne communiquent pas sur ce point, à l'exception de certains cas particuliers.

Désormais, on assiste aussi à l'exploitation des réseaux sociaux comme Facebook ou Linkedln par des cyber-criminels. Ces réseaux, qui concentrent une quantité phénoménale d'informations personnelles, permettent de rassembler suffisamment d'éléments pour se substituer à l'identité des utilisateurs. Le détournement de l'identité d'un individu, la récupération d'éléments

4 Selon Guillaume Lovet, *Mag Secure* n° 18 « Les chiffres de la cybercriminalité ».

à caractère personnel vont ensuite leur servir pour se faire passer pour un autre afin de commettre des délits, des achats avec des moyens de paiement usurpés.

Ce « business parallèle » est difficilement mesurable mais il ne cesse de se développer depuis plusieurs années, ce qui démontre l'existence « d'un marché ». Ce type d'arnaque joue sur la curiosité, la naïveté ou l'appât du gain des internautes. Le client est informé qu'il ne faut jamais laisser ses coordonnées sur le réseau. Il est le principal artisan de sa sécurité. Par ailleurs, les procédés évoluent et sont de plus en plus rusés, des cyberdélinquants font en effet du prosélytisme en matière de sécurité. Ainsi, de récents courriels frauduleux, très convaincants, mettent en garde les clients de banques contre le filoutage, rappelant que les banques ne demanderont jamais de détails sur un compte par courriel et les invitant à signaler tout message suspect. Mis en confiance par ces avertissements, le client va être tenté de cliquer pour signaler le site et c'est alors que la victime va être redirigée vers un site frauduleux.

3. – LE VOYAGE AU PAYS DES MERVEILLES... DE LA DÉLINQUANCE

Nous présentons ici quelques cas plus ou moins récents et démontrons ainsi la variété des montages possibles. Cela met en évidence la difficulté des poursuites et la marge dont disposent les criminels dans ce secteur.

Les montages liés aux e-chantages[5] ou aux extorsions en ligne font florès sur le net. Ils sont conçus à partir d'une méthodologie simple qui consiste à repérer les structures fragiles, et à menacer de bloquer le site, ou à le bloquer. Si l'entreprise ne paye pas elle ne pourra pas travailler pendant une période plus ou moins longue qui dépendra de son *backup* et de sa capacité à débloquer (décoder) les données.

Exemple *: Une petite structure commercialise des produits sur Internet, elle reçoit un email menaçant. Si elle ne paye pas 10 000 dollars à l'aide d'une fausse facture, son site sera attaqué. La structure ne prête aucune attention au mail, peu après son serveur « plante », ce qui entraîne des pertes considérables. Un second mail est reçu qui porte le montant à 40 000 dollars. En cas de non-paiement la compagnie risque encore des pertes. En revanche, si elle paie, on lui offre généreusement une protection pendant un an. Après avoir fait le calcul, la compagnie paie.*

La liste des chantages & Co est impressionnante :

- Un fournisseur d'Internet japonais a dû verser 28 millions de dollars : en échange les données personnelles de ses clients n'ont pas été divulguées.
  Le coût final de l'opération est évalué à 36 millions de dollars.

5 Voir sur ce sujet *Cols blancs et mains sales - économie criminelle mode d'emploi,* Noël Pons, éditions Odile Jacob, 2006.

- Des pirates russes ont pris le contrôle en 2003 d'une société hébergeant les données de casinos en ligne. Une rançon a été demandée contre la « livraison » de clé chiffrée seule utile pour reprendre le contrôle des serveurs, 75 000 $ auraient été perdus chaque jour pendant cette période.
- En mars 2004, les vingt sites de paris en ligne ont fait l'objet de trente-trois attaques en quinze jours. Certains ont confirmé avoir été victimes d'attaques qui ont paralysé les serveurs la veille du Cheltenham festival, une course hippique à l'occasion de laquelle les paris sont particulièrement importants.
- Trois jeunes Russes avaient racketté des *bookmakers* anglais, les compagnies agressées auraient accepté de payer 40 000 dollars chacune. C'est à la suite d'une enquête conjointe entre les polices anglaises et russes qu'ils ont été pris.
- La veille de l'ouverture des jeux olympiques d'Athènes, certains sites de prise de paris ont été bloqués, et ces derniers ont fait l'objet d'un chantage, ces sites ont été ré-ouverts juste avant la cérémonie d'ouverture... Les pratiques de sabotage prennent différentes formes, l'attaque bloquante du site est privilégiée dans les périodes proches d'un événement important. On pense en priorité à des événements sportifs, mais ce n'est pas toujours le cas. Certains rapportent que l'élection du pape a été l'occasion de fructueux paris illégaux, alors... Dans d'autres cas c'est le code de programmation qui est modifié ou encore des joueurs qui sont spoliés comme dans les cas de phishing.
- Un concepteur de logiciels de jeu pour Internet a reconnu en septembre 2004 avoir fait l'objet d'une attaque au cours de laquelle un pirate a, après s'être introduit dans le serveur, modifié les jeux de dés et les machines à sous de manière à ce qu'aucun joueur ne perde. 140 parieurs ont remporté des gains à hauteur de 1,9 millions d'euros. L'entreprise a payé les gains car aucun des gagnants n'était complice de l'opération.

L'opération Mariposa recouvre pour sa part tous les ingrédients relatifs à l'activité criminelle dans le secteur informatique et permet de prendre conscience de sa réactivité dans ce domaine.

Une importante fraude informatique a été identifiée par la Guardia Civil espagnole, en collaboration avec le FBI, son nom de code était « Mariposa »[6]. Trois hommes dans le but de détourner des données confidentielles avaient infiltré 13 millions d'ordinateurs. Le *botnet*[7] était constitué d'ordinateurs « zombies » qui après avoir été « vérolés » par des virus, étaient contrôlés à

6 Papillon, en espagnol.

7 Un *botnet* est composé par un ensemble de *bots* informatiques qui effectuent des tâches automatisées et qui sont reliés entre eux.

distance par les pirates. Ces derniers les activaient soit pour générer des escroqueries, soit pour réaliser des attaques de terrorisme informatique.

Ce réseau aurait contrôlé ces ordinateurs dans pratiquement tous les pays du monde, et dans un grand nombre d'entreprises et de banques. Les organisateurs se faisaient appeler le DDP-Team, pour « Dias De Pesadillas Team »[8].

Une fois les ordinateurs infectés et transformés en « zombies », les informaticiens pouvaient les manipuler à leur guise et explorer leur contenu. Ils recherchaient en particulier des informations sur les comptes bancaires, les identifiants, les mots de passe et numéros de cartes bancaires.

Les logiciels malveillants installés à distance étaient sans cesse modifiés et améliorés échappant ainsi aux antivirus les plus coriaces.

Ils se faisaient payer par leurs « clients » pour envoyer des bordées de spams sur toutes les adresses récupérées depuis les ordinateurs piratés. Ces informations personnelles (coordonnées bancaires, postales, etc.) étaient ensuite revendues. Ces derniers pouvaient aussi insérer des publicités sur les sites web administrés par les ordinateurs piratés, à un prix sans commune mesure avec celui du marché. Le chiffrage des sommes circulant dans ce business n'a pas été possible mais leurs revenus provenaient apparemment exclusivement de leurs activités illégales.

Mais la prime de l'inventivité résidait dans le blanchiment de l'argent récolté. L'une des méthodes du trio pour blanchir ces sommes consistait à jouer au poker en ligne. Ils recrutaient des joueurs, ces derniers perdaient systématiquement les parties mais ne payaient jamais les sommes perdues. Les pertes étaient couvertes par les fonds provenant des opérations citées ci-dessus, elles étaient donc blanchies.

Une fois découverts ils ont par ailleurs lancé une « importante attaque informatique » contre ceux qui les avaient identifiés.

Le réseau « Mariposa » a été rendu inactif le 23 décembre 2009 mais à ce jour les ordinateurs pourraient encore être infectés, la prise de contrôle du réseau et sa réactivation est donc toujours possible. Finalement l'identité de celui qui a conçu la fraude demeure un mystère.

Comme autrefois autour du Nasdaq[9] lors de la création de la bulle des valeurs technologiques, les criminels se sont intéressés à la bourse des quotas carbones.

On ne peut que s'extasier sur la manière dont a été traitée l'installation du marché du carbone, faisant suite aux accords de Kyoto de 1997. L'idée n'était pas sotte, elle consistait en l'identification des gros pollueurs, l'affectation d'un quota d'émission à chacun d'entre eux, puis, lorsque leur activité dépassait le quota, les amener à racheter les droits à polluer excédant la base fixée. En fait, ce principe cohérent en apparence stabilise les volumes de pollution par l'achat

8 L'équipe des journées de cauchemar.

9 Le *NASDAQ*, est le sigle de National Association of Securities Dealers Automated Quotations.

des droits à polluer des pays pauvres. Les États distribuant dans un premier temps ces permis de polluer.

Un nouveau marché a donc été créé, Le SCEQE[10] est un mécanisme de l'Union européenne complètement immatériel dont les opérations d'achats et de ventes sont elles-mêmes dématérialisées.

C'est sur cette construction que se sont installés les carrousels. Le carrousel TVA est une vieille fraude consistant à détourner des crédits de TVA sur la base de documents falsifiés, de sociétés écrans et d'échanges intra-communautaires. Connue depuis fort longtemps, cette pratique, difficile à identifier et à poursuivre par ailleurs, constitue l'une des ressources les plus appréciées de la criminalité européenne. Ce montage caméléon est toujours pratiqué, mais il ne cesse d'évoluer en s'adaptant à la situation économique et aux modes. Il a été utilisé dès 2006 pour détourner le mécanisme des permis négociables sur le marché des droits à polluer. La criminalité a ainsi organisé un carrousel autour des « quota-carbone » en créant un flux de fausses facturations.

Les principes de ce carrousel sont, encore une fois, relativement simples, ils sont fondés sur le détournement de la TVA qui accompagne la défaillance d'une entreprise participant à une succession de fausses facturations entre des sociétés de plusieurs pays. Ils affectent donc en priorité le montant de la TVA collectée[11]. L'entreprise disparaît après avoir encaissé le montant de la facture taxes comprises. La société qui achète de bonne foi ces droits inexistants, du fait de l'absence d'harmonisation des législations sur ce point, sera amenée soit à devoir les rendre soit à les considérer comme acquis. D'intéressantes analyses juridiques sont en cours afin d'harmoniser le régime de la détention de ces droits.

Les droits attachés aux « quotas-carbone » sont immatériels et les transactions sont réalisées uniquement par Internet, nous l'avons précisé, dès lors, il est aisé de générer un maximum de TVA collectée en multipliant les fausses factures et de l'encaisser sans la reverser. Les paradis fiscaux utilisés facilitent les transferts bancaires en assurant une réelle protection pour les fonds détournés. Les sociétés ont ouvert des comptes dans les places d'Asie ou du bassin méditerranéen toujours peu contrôlées ou mieux encore dans des pays fortement infiltrés par la criminalité. Il faut tout de même préciser que les premiers règlements de comptes entre criminels ont eu lieu et que plusieurs

10 Le système communautaire d'échange de quotas d'émission (SCEQE) (en anglais Emission Trading System, ou European Union Emission Trading System (EU ETS) ou EU ETS) est un mécanisme de l'Union européenne visant à réduire l'émission globale de CO2 et atteindre les objectifs de l'Union européenne dans le cadre du protocole de Kyoto.

11 La Taxe sur la valeur ajoutée fonctionne de la manière suivante : les sommes facturées aux clients (ventes) sont soumises à la TVA (a), les sommes facturées par les fournisseurs (achats) créent de la TVA déductible (b), cette dernière est déduite des montants précédents [(a)- (b)], si le solde généré est positif, il faut payer la TVA par contre si le solde est négatif alors un crédit de TVA est remboursé.

personnes actives dans ce secteur ont été assassinées au cours de l'année dernière.

Les déboursements illégitimes concerneraient des valeurs comprises entre cinq et dix milliards et, si la France a résolu rapidement le problème[12] à partir d'un remarquable travail effectué par TRACFIN, les escroqueries se sont transportées dans d'autres pays moins organisés.

Et pour couronner le tout, une cyber-attaque est montée à l'assaut de ces marchés contraignant les marchés européens à stopper les transactions. Des criminels, on est passé aux cybercriminels, l'attaque, un *phishing* (hameçonnage), a été concertée et a affecté les détenteurs de quotas dans le but d'obtenir les codes d'accès des membres inscrits aux registres[13] nationaux d'émission. Ces codes ont permis aux hackers d'acheter et de vendre des quotas à la place des industriels et des courtiers, mieux, ces données ont été déplacées vers le mécanisme d'échange ITL[14] qui permet de vendre des quotas européens à d'autres pays.

À ce jour, certains registres sont considérés comme de véritables passoires et la réouverture des registres de certains pays n'ayant pas les moyens de les moderniser prendra un peu de temps. La mesure principale exigée est le rajout d'un second mot de passe qui sera demandé lors de chaque connexion, ce qui est tout de même assez simpliste. Cela ne me semble pas de nature à dissuader les criminels patentés[15].

Dans la revue *Intelligence Online*, n° 101, une manipulation relative à une opération d'espionnage industriel a été mise en évidence. L'unité antifraude a déjà arrêté dix dirigeants d'entreprises et onze responsables de sociétés d'investigations privées :

Un informaticien et son épouse ont mis au point un virus de type « cheval de Troie » qui était paramétré pour chaque société cible.

Ce virus était loué 3 800 dollars par ordinateur et par mois à des sociétés d'investigations.

12 La TVA a été suspendue rendant le montage inopérant, il faut toutefois mettre en évidence le fait qu'une bande de criminels, bras cassés, et plus ou moins connus a amené un État à modifier sa législation, c'est remarquable.

13 Ces registres tiennent la comptabilité des quotas, la Caisse des Dépôts en France conserverait environ 130 millions de quotas annuels soit l'équivalent de 1,7 milliards d'euros au cours de janvier 2011.

14 International Transaction Log, une structure de la branche informatique de l'ONU.

15 En l'espèce, un marché a été ouvert sans que les mesures de sécurité les plus évidentes et sans qu'une harmonisation minimale n'ait été prévue. Finalement nous ne sommes pas très éloignés des opérations identifiées lors de la crise des *subprimes*. Le volet « criminalité » se diffuse dans tous les domaines, il est devenu un élément incontournable qui devrait être pris en compte en amont de chacune des évolutions techniques ou commerciales. On constate aussi un réel manque de réactivité comme si la possibilité de frauder sur ce type d'opérations n'avait même pas été envisagée.

Ces dernières disposaient d'un mot de passe pour récupérer sur le serveur des informaticiens les informations piratées.

Ces informations étaient alors revendues à leurs clients.

Les clients étaient tous connus et recherchaient des informations, qui sur les sources des journalistes financiers, qui sur les clients, qui sur les techniques utilisées.

Le « cheval de Troie » était introduit dans les systèmes des cibles par un e-mail ou un cédérom présentant une offre alléchante. Les experts en sécurité informatique utilisent ce stratagème pour procéder à des tests d'intrusion chez leurs clients.

Nous terminerons avec les « casses » récents à la gravité exceptionnelle qui se sont produits au cours des deux dernières années.

Le « Stuxnet » est d'abord apparu en janvier 2010 dans les ordinateurs d'un prestataire de service de sécurité Biélorusse, dont le site avait été bloqué pendant un certain temps. L'analyse a démontré que ce ver était conçu d'abord pour rechercher des paramètres précis afin d'intégrer un code manipulateur dans le système. Il semble qu'il ait été créé dans le but de causer des problèmes dans la gestion des réacteurs nucléaires iraniens. Les spécialistes prétendent que ce ver relevait de la génération précédente, on attend avec impatience les vers qui vont suivre... L'infection a été faite à partir de clefs USB subrepticement abandonnées sur des postes de travail.

Ensuite un grand nombre de détournements effectués à l'encontre de SONY ont secoué la communauté internet mais nombreux étaient ceux qui s'attendaient à de tels problèmes. Cette fraude récente est exemplaire des risques qui peuvent être rencontrés sur l'internet. Les attaques des pirates sur les serveurs du *play station network* reliant la console PS 3 à internet pour les achats et les jeux en ligne et « Qriocity », le système vidéo et musique ont finalement touché le service « online entertainment » gestionnaire de jeux de rôle en ligne. Les informations concernant 24,6 millions de comptes utilisateurs ont été dérobées, elles concernaient les noms, l'adresse, la date de naissance, les numéros de téléphone, les mails ainsi que les identifiants des mots de passe. Les données bancaires (numéros de carte ou comptes) plus anciennes de 23 000 utilisateurs ont été aussi volées. Ce qui a causé le 3 mai une interruption de tous les services. L'intégralité des comptes du *play station network,* soit plus de 77 millions de comptes, ont été volés. Il est fort possible que 10 millions de données relatives à des cartes bancaires ont été dérobées à cette occasion. Le problème a été rendu possible du fait qu'une faille connue n'a pas été corrigée ou pas suffisamment et par un manque de sécurité.

À la même période les clients d'Amazon web n'ont pu accéder à la fin du mois d'avril à leurs données pendant un certain laps de temps considéré comme insupportable. Une défaillance interne était la cause de ce *bug*.

Enfin, des informations collectées par la société habilitée à procéder à des repérages d'adresses IP (*Internet Protocol*) sur les réseaux de téléchargement P2P pour le compte d'ayants droit à la suite de la loi Hadopi, auraient été librement accessibles[16] sur l'un des serveurs de l'entreprise pendant plusieurs jours. Révélée par un blogueur spécialiste en sécurité, cette faille permettait notamment d'accéder aux fichiers des relevés effectués par la société. Ces derniers contenaient les informations faisant le lien entre l'adresse IP et le téléchargement.

Ces dérapages auxquels se sont rajoutés Lockheed Martin, Google, Nintendo et City group ont mis en évidence la problématique du risque qui jusque-là n'intéressait que les spécialistes, et cela peut mettre en cause, indirectement certes, le développement du *cloud computing* ou de l'informatique en nuage, dont le marché global devrait passer de 40 milliards en 2011 à 250 milliards en 2020, car les risques de piratage sont présents mais aussi ceux relevant de l'indisponibilité du réseau. Ce type d'informatique à distance permet de limiter les coûts en utilisant les capacités de stockage ouvertes sur internet.

Deux problèmes sont donc clairement posés : les prestataires ont-ils suffisamment consolidé leur système de sécurité pour rassurer les clients ? Le risque d'indisponibilité des données est-il suffisamment pris en compte ?

Pour terminer, on comprend aisément que la lutte contre la cybercriminalité implique une mobilisation sans faille de l'ensemble des acteurs et un renforcement de la coopération internationale. Les données circulent à la vitesse de la lumière et sont difficiles à pister. La cybercriminalité pose de nombreux défis et dans le cybermonde qui évolue sans cesse, les services de police et de justice luttant contre celle-ci doivent mettre en place des stratégies d'anticipation des menaces et de répression au risque de mettre en péril les internautes et de freiner le développement de la société du numérique. La criminalité est depuis longtemps présente dans ce domaine en particulier sur les sites de paris sportifs. Il s'agit d'une délinquance intelligente, qui regroupe les techniciens et les spécialistes du secteur ainsi que les professionnels des montages de blanchiment.

Internet n'a inventé que peu de fraudes réellement nouvelles, il permet, facilite, amplifie la propagation des fraudes existantes. L'internet est criminogène du fait de sa dématérialisation et de l'impunité de l'acte qu'il procure. Avec l'internet s'est créé un nouvel espace social, complètement irréel et dématérialisé. Le seul lien avec la réalité est constitué par les fonds détournés. On distingue généralement deux types d'infractions, celles commises au moyen de l'internet ou de l'informatique qui ne sont qu'une variante ou l'application d'un montage connu, et celles qui sont propres à la

16 *L'Expansion* du 20 mai 2011.

manipulation des outils informatisés. Les premières existaient déjà depuis longtemps mais elles connaissent un nouveau développement sur internet. Les gains détournés sont toujours encaissés dans un paradis fiscal dans son acception la plus large, c'est-à-dire dans n'importe quel pays à condition qu'il ne collabore pas à un échange d'informations. L'utilisation de sociétés écrans pour monter les systèmes de détournements est aussi très largement pratiquée. De plus la grande criminalité agit de façon plus mobile que jamais...

Notre conclusion sera toute entière présente dans une citation des années 90 émise par Ignacio Ramonet dans *Le Monde* : « Avec internet vous naviguerez constamment entre l'extase et l'effroi », l'extase lorsque les juristes sont amenés à créer un statut juridique nouveau, celui de l'avatar par exemple, et l'effroi lorsqu'on tente de faire l'inventaire des fraudes possibles.

noelpons@hotmail.fr*

* Dernier ouvrage commun : *L'investigation informatisée des fraudes- Recherche informatisée et prévention,* Paris, octobre 2010, éditions Emerit publishing.