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

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

Les 5 tendances en cybercriminalité pour 2016

Bitdefender, leader technologique des solutions antimalware et expert en cyber-sécurité, protégeant plus de 500 millions d'utilisateurs dans le monde entier, publie ses prévisions en matière de sécurité.

Dans son rapport, Bitdefender énonce les cinq évolutions notables qui impacteront notre façon de travailler, de jouer et de se sociabiliser sur Internet, au cours de l'année prochaine.

Malwares et adwares : des frontières de plus en plus floues

L'année 2016 verra un changement majeur dans la façon dont opèrent les cybercriminels. Le domaine probablement le plus impacté par cette refonte sera celui des PUA, dont l'activité s'est déjà accrue sur des plates-formes telles que Mac OS X et Android.

Suite aux nombreuses fermetures de réseaux de machines zombies et arrestations en 2015, les nouveaux cybercriminels transiteront probablement vers des systèmes de monétisation publicitaire spécifiques aux adwares agressifs, plutôt que de développer de nouvelles souches de malwares.

Si pour le moment les botnets constituent toujours une partie importante de l'écosystème de la cybercriminalité, nous assisterons à une augmentation de la sophistication des PUA et des programmes incluant plus de greywares à l'installation.

La publicité sur le Web va également évoluer : étant donné le taux d'adoption ainsi que la popularité des bloqueurs de publicités, les régies publicitaires chercheront à utiliser des mécanismes plus agressifs afin de **contourner ces blocages**.

Les APT abandonneront le facteur de longévité

Les entreprises et les institutions gouvernementales feront toujours face à des attaques de ce type tout au long de 2016.

Cependant, les APT (Advanced Persistent Threats, menaces persistantes avancées) mettront l'accent sur l'obfuscation et la récolte d'informations plutôt que sur la longévité. Les pirates ne s'infiltreront sur le réseau de l'entreprise que quelques jours, voire quelques heures.

Le monde de l'entreprise connaîtra une augmentation des attaques ciblées et des bots fortement obfusqués, avec une courte durée de vie et des mises à jour fréquentes, estime Dragoş Gavriluţ, Chef d'équipe au sein des Laboratoires antimalwares de Bitdefender. La plupart de ces attaques se spécialiseront dans le vol d'informations.

Également, l'évolution latérale de l'infrastructure des fournisseurs de services Cloud ira de pair avec l'avènement d'outils permettant aux pirates de compromettre l'hyperviseur à partir d'une instance virtuelle et de passer d'une machine virtuelle à l'autre. Ce scénario est particulièrement dangereux dans des environnements de «

mauvais voisinage », où un tiers mal intentionné serait amené à partager des ressources sur un système physique avec un fournisseur de services ou une entreprise légitimes.

Des malwares mobiles de plus en plus sophistiqués

Du côté des particuliers, les types de malware sous Android sont désormais globalement les mêmes que sous Windows. Alors que les rootkits sont en perte de vitesse sur Windows, ils vont probablement devenir monnaie courante sur Android et iOS, car les deux plates-formes sont de plus en plus complexes et offrent une large surface d'attaque, affirme Sorin Dudea, Chef de l'équipe de recherche antimalwares.

De nouveaux malwares mobiles**,** aux comportements similaires à ceux des vers, ou un réseau botnet mobile géant, sont deux autres possibilités envisagées pour l'année prochaine, selon Viorel Canja, Responsable des Laboratoires antimalwares et antispam chez Bitdefender. Ces attaques pourraient être la conséquence de techniques d'ingénierie sociale ou de l'exploitation de vulnérabilités majeures (telles que Stagefright) sur des plates-formes non patchées.

L'Internet des Objets (IOT) et la vie privée

La façon dont nous gérons notre vie privée va aussi changer durant l'année 2016. En effet, les récents vols de données ont contribué à mettre une quantité importante d'informations personnelles en libre accès sur Internet, rendant ainsi le **«** doxing **»** (processus de compilation et d'agrégation des informations numériques sur les individus et leurs identités physiques) beaucoup plus facile pour des tiers.

Les objets connectés vont devenir de plus en plus répandus, donc plus attrayants pour les cybercriminels. Compte tenu de leur cycle de développement très court et des limites matérielles et logicielles inhérentes à ce type d'objet, de nombreuses failles de sécurité seront présentes et exploitables par les cybercriminels ; c'est pourquoi la plupart des objets connectés seront compromis en 2016, ajoute Bogdan Dumitru, Directeur des Technologies chez Bitdefender. Également, les réglementations de surveillance de type « Big Brother », que de plus en plus de pays essaient de mettre en place pour contrecarrer le terrorisme, déclencheront des conflits quant à la souveraineté des données et le contrôle de leur mode de chiffrement.

Les ransomwares deviennent multiplateformes

Les ransomwares sont probablement la menace la plus importante pour les internautes depuis 2014 et resteront l'un des plus importants vecteurs de cybercriminalité en 2016. Alors que certains pirates préfèrent l'approche du chiffrement de fichiers, certaines versions plus novatrices se concentreront sur le développement de « l'extortionware **»** (malware qui bloque les comptes de services en ligne ou expose les données personnelles aux yeux de tous sur Internet).

Les ransomwares visant Linux vont se complexifier et pourraient tirer parti des vulnérabilités connues dans le noyau du système d'exploitation pour pénétrer plus profondément dans le système de fichiers. Les botnets qui forcent les identifiants de connexion pour les systèmes de gestion de contenu pourraient aussi se développer. Ces identifiants pourraient être ensuite utilisés par les opérateurs de ransomwares visant Linux pour automatiser le chiffrement d'une partie importante d'Internet.

Enfin, les ransomwares chiffrant les fichiers s'étendront probablement aux systèmes sous Mac OS X, corrélant ainsi avec les travaux de Rafael Salema Marques et sa mise en garde illustrée autour de son 'proof of concept' malware nommé Mabouia. En effet, si le principe de conception de Mabouia reste pour le moment privé, il pourrait être créé par des cybercriminels enrichissant alors leurs offres orientées MaaS (Malware-As-A-Service).

Lien : **http://www.bitdefender.fr/actualite/les-5-tendances-en-cybercriminalite-pour-2016-3096.html**

Le palmarès des arnaques sur internet
Délinquance numérique

Voici quelques exemples d'arnaques sur le web :

L'hameçonnage ou phishing

Il s'agit de mails personnalisés envoyés en nombre, contenant des sollicitations apparemment légitimes provenant de personnes ou d'institutions connues. Votre banque vous envoie un courriel vous demandant de changer votre code de carte bleue à la suite d'une fraude au Moyen-Orient ?

Ne mordez pas, il s'agit d'un hameçonnage ou "phishing" ! La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, afin de récupérer des données telles que vos coordonnées de compte bancaire, mots de passe...

Quelques mesures simples peuvent vous prémunir :

- Vérifiez toujours le nom et l'adresse de l'expéditeur et l'objet du mail, et ne l'ouvrez pas en cas de doute.
- Protégez votre ordinateur et évitez de télécharger ou d'exécuter des pièces jointes de source inconnue ou suspecte.
- Soyez également attentif à la qualité de la rédaction du mail ou du site, souvent approximatifs et remplis de fautes.
- Enfin, signalez-les arnaques aux plateformes : signal-spam.fr et phishing-initiative.com.

L'escroquerie à la loterie

Qui n'a jamais reçu un mail promettant un gain mirifique à un jeu-concours, la demande urgente d'un mandat par Western Union pour un soi-disant collègue en voyage, ou l'alléchante annonce dont veut vous faire profiter un « ami », au sujet d'une voiture flambant neuve à un prix ridicule ? On vous exhorte, en général, à effectuer un premier versement pour couvrir de prétendus frais et débloquer la somme ou le lot. Evidemment, les fraudeurs ne reprennent jamais contact et s'évanouissent dans la nature avec votre argent.

L'arnaque "à la nigériane"

C'est l'un des spams les plus courant, lui aussi basé sur les frais anticipé : un inconnu requiert votre aide pour transférer des fonds prétendument déposés sur un compte étranger (en général, l'héritage d'un parent ou d'un ami) et vous promet un confortable pourcentage, à condition que vous lui fassiez d'abord parvenir rapidement une avance d'argent. La victime ne se verra jamais verser un seul centime.

Le kidnapping de disque dur

Après avoir ouvert une page web infectée, ou cliqué sur un lien malveillant qui déclenche un téléchargement automatique, l'écran de votre ordinateur se grise. Vous avez beau cliquer, rien ne se produit. Puis apparaît, en haut à gauche, votre image filmée en direct par votre propre webcam. Quelqu'un a pris le contrôle de votre machine ! Cet angoissant scénario se nomme "virus-rançon", ou "ransomware".

Il vous interdit l'accès à votre ordinateur dans le but de vous faire chanter, en vous accusant d'avoir téléchargé illégalement des fichiers et d'être en violation de pseudo lois sur le copyright, ou même de posséder des photos pédophiles. La seule façon de retrouver le contrôle de son ordinateur : s'acquitter d'une "amende" dans les 48

heures via un site de paiement (dont évidemment, les transactions sont impossibles à suivre).
Que faire quand on est victime d'un virus-rançon ? Ne pas tenir compte des menaces et contacter tout de suite un expert en sécurité informatique, voire porter plainte. En mesures préventives, s'équiper d'un antivirus, procéder aux mises à jour de son système d'exploitation et faire une sauvegarde de ses données.

L'escroquerie à l'offre d'emploi

Les escrocs commencent par identifier un demandeur d'emploi, et lui proposent un job, extraordinairement bien payé. En fait, c'est un subterfuge ayant pour seul objectif de recruter un intermédiaire pour une opération de blanchiment d'argent. En échange d'une commission, la victime est priée d'utiliser son propre compte en banque pour recevoir des fonds, puis les transférer sur le compte de l'arnaqueur. Il s'agit, en fait, d'argent sale issu d'activités criminelles.

Lien : https://www.axaprevention.fr/conseils-internet/delinquance-numerique/palmares-des-arnaques-sur-internet

Le "directeur des données", nouveau métier star dans les banques

Sous la double pression des enjeux liés à la réglementation et au big data, 16% des banques ont déjà nommé un "chief data officer", contre 14% seulement des sociétés de télécoms et 9% des groupes de médias.
A nouvelle époque, nouveau métier star dans la finance. Les traders ont eu leur heure de gloire dans les années 1980. Dans la foulée de la crise financière de 2008 et de l'arsenal réglementaire qui s'en est suivi, ce sont les profils de gestionnaires des risques et de la conformité qui sont devenus très recherchés par les établissements bancaires.
Aujourd'hui, à l'heure de la révolution des données, les sociétés de services financiers font les yeux doux aux "chief data officers" (CDO, en français "directeurs des données"). Quelle fonction se cache derrière ce énième acronyme barbare ? "Le poste de chief data officer est nouveau, compliqué à définir. Il existe différents profils de CDO, en fonction, notamment, du degré de maturité des banques en matière de transformation digitale", prévient Stanislas de Roys, responsable du secteur banque chez Capgemini Consulting, qui a récemment réalisé une étude sur le sujet avec l'Efma, une association chargée de la promotion des innovations dans la banque et l'assurance.
Dans les grandes lignes, "le chief data officer est au cœur de la transformation digitale, c'est lui qui gère la mine d'or des données avant que celle-ci ne soit transformée en "extraits" utilisables", résume Stanislas de Roys. A. Charles Thomas, le premier chief data officer recruté par la banque américaine Wells Fargo - pas plus tard que l'an dernier - se définit, lui, comme "un chef d'orchestre, chargé de s'assurer que l'ensemble des services jouent en harmonie." Concrètement, le chief data officer, qui cumule compétences en systèmes d'informations, marketing et mathématique, est responsable de la gouvernance des données, éparpillées en divers endroits de l'entreprise. C'est lui qui, par son rôle de coordinateur, va définir et mettre en œuvre une stratégie assurant la richesse, la fiabilité et la cohérence des données internes et externes à l'entreprise.

50% des banques auront nommé un CDO d'ici à 2017, selon Gartner

Certes, ces nouvelles stars que sont les chief data officers sont courtisées par des industries de tous bords, aucun secteur d'activité ne pouvant faire l'économie de la transformation numérique. Mais les banques ont une longueur d'avance en la matière : à l'échelle mondiale, "*16% d'entre elles emploient un CDO, contre 9% des groupes de médias seulement*", indique Stanislas de Roys. Voire plusieurs chief data officers, un pour chaque métier de la banque (banque de détail, banque de financement et d'investissement, etc.). Le secteur bancaire devance même celui des télécoms, que l'on penserait pourtant plus en pointe dans ce domaine, 14% des groupes de "telcos" comptant un chief data officer dans leurs effectifs.

Dans la même veine, le cabinet Gartner estime que la moitié des grandes banques et compagnies d'assurance dans le monde auront nommé un CDO d'ici à 2017, contre une proportion de 25% seulement pour l'ensemble des grands groupes, tous secteurs confondus. De fait, en novembre dernier, Deutsche Bank a recruté son tout premier chief data officer, en la personne de JP Rangaswami, et l'assureur italien Generali s'apprête à faire de même. Quant à Cathy Doss, la chief data officer de la banque américaine Capital One, n'est-elle pas considérée comme la pionnière mondiale des CDO ? Comme souvent, les Anglo-Saxons ont flairé avant l'Europe Continentale le potentiel de ce métier mais "*les banques françaises sont aujourd'hui très conscientes de l'importance de la fonction de chief data officer*", insiste Stanislas de Roys.

La double pression de la réglementation et du big data

Il faut dire que s'il existe un secteur d'activité qui regorge de données sur ses clients, c'est bien celui de la banque. Paiements par cartes, retraits d'argent aux distributeurs, et maintenant consultations frénétiques de son compte bancaire via son smartphone... Il ne se passe pas un jour sans qu'un client ne fournisse des informations sur lui-même à sa banque, sans même s'en rendre compte. C'est dire si le big data revêt un caractère particulièrement crucial pour le secteur bancaire. Grâce à l'analyse et au croisement d'énormes masses de données structurées et non structurées (publications sur les réseaux sociaux, emails, etc.), le big data permet en effet aux banques de disposer d'une connaissance très pointue de leurs clients et, partant, de leur proposer le bon produit ou service, au bon moment, et via le bon canal de distribution.

Mais les données ne représentent pas seulement un enjeu commercial, pour les banques. Depuis la crise de 2008 et le tsunami réglementaire qui s'est abattu sur l'industrie financière, les banques doivent fournir aux régulateurs des données encore plus précises, plus fines et plus sûres que par le passé, que ce soit pour évaluer leur santé financière, ou pour lutter contre le blanchiment d'argent, le financement du terrorisme ou l'évasion fiscale. Faute de quoi les banques risquent de lourdes amendes, à l'image du total de 100 milliards de dollars dont les banques américaines ont écopé entre 2008 et 2013. La fonction de chief data officer semble donc bien promise à un bel avenir.

Lien : **http://www.latribune.fr/entreprises-finance/le-directeur-des-donnees-nouveau-metier-star-dans-les-banques-483363.html**

Fraude et blanchiment d'argent
La face cachée du financement des échanges internationaux

Le financement du commerce est vital pour l'économie internationale. D'ailleurs, l'Organisation mondiale du commerce (OMC) estime que 80 à 90 % des transactions de commerce international en dépendent. Son fonctionnement doit donc être efficace

et résister aux manœuvres des fraudeurs et blanchisseurs d'argent. Les administrations adoptent aujourd'hui les solutions d'analyse et de gestion des données les plus pointues pour contrer ce fléau, mais il est tel qu'elles doivent accélérer considérablement le déploiement de ces solutions si elles veulent contrôler la situation.

Dans le domaine du financement des échanges commerciaux, les fraudes peuvent engendrer des pertes de plusieurs millions d'euros. Les fraudeurs sont motivés par les sommes en jeu, ceux qui pratiquent le blanchiment d'argent y voient un moyen de dissimuler des activités illicites ou criminelles, avec peu de risques d'être démasqués.

Tous misent sur la faiblesse des contrôles humains et la dépendance toujours actuelle aux documents papier. Ceci, couplé aux complexités du commerce, à la diversité linguistique et à la multitude d'organisations impliquées, constitue un terreau idéal pour la fraude et le blanchiment.

Malgré une meilleure prise en compte des enjeux, personne ne sait vraiment comment s'attaquer au problème, ce qui n'est guère surprenant compte tenu de la diversité des types de fraudes liées aux échanges commerciaux. L'une des typologies les plus courantes est le double financement : importateurs et exportateurs se mettent d'accord pour produire un chiffre d'affaires factice en vue d'obtenir des crédits, ou pour simuler une opportunité commerciale leur permettant de récupérer chacun de leur côté des financements puis disparaître dans la nature.

Au nombre des autres techniques couramment employées figurent la falsification de comptes, la couverture de directeurs révoqués et la constitution de structures opaques dissimulant des répartitions de capitaux douteuses ou risquées.

En matière de blanchiment d'argent, l'approche classique consiste à surfacturer ou sous-facturer des prestations, à livrer des quantités supérieures ou inférieures, voire à expédier des conteneurs vides, dans le seul but de transférer des fonds.

Pour s'attaquer à ces problèmes, les autorités doivent traiter de grandes quantités de données, la plupart étant non structurées et mal intégrées avec les autres informations.

Le défi est d'autant plus difficile à relever qu'il est nécessaire d'effectuer une analyse avec un niveau de granularité allant jusqu'à la quantité de marchandises dans chaque conteneur, aux parcours empruntés et à la durée des trajets.

Par ailleurs, la qualité des données dans les transactions internationales est généralement médiocre. De ce fait, les administrations ont du mal à se faire une idée précise des opérations réalisées dans un même pays, et encore plus à cerner leur exposition aux fraudes et au blanchiment d'argent.

La lutte contre ces activités n'a jamais été aisée, et rares sont les organisations qui ont fait véritablement preuve d'efficacité en la matière.

Comment doivent-elles s'y prendre pour rectifier le tir ?

La première étape consiste à appliquer aux données existantes les dernières solutions de gestion et de nettoyage des données pour créer une vue d'ensemble des informations pertinentes. Il s'agit d'une première phase d'exploration et de découverte, mais une fois les données pertinentes collectées, elle doit être complété des méthodes de qualité des données. Les fournisseurs de solutions disposent d'outils pour cela, mais cela ne suffit pas. Les banques doivent également prendre leurs responsabilités et résoudre les problèmes que posent encore aujourd'hui leurs données, et déployer des programmes pour collecter des données de meilleure qualité.

Il faut néanmoins rester pragmatique et ne pas viser la perfection. Les entreprises doivent faire avec ce qu'elles ont et utiliser diverses techniques pour améliorer leurs contrôles, en utilisant plus de données et de contexte dès lors que de nouvelles sources peuvent être analysées. Elles doivent miser sur la technologie pour améliorer leurs

programmes de conformité et de lutte anti-fraude, et utiliser notamment des techniques de visualisation pour identifier les scénarios, anomalies et valeurs aberrantes.

Les fraudes et le blanchiment d'argent relèvent ni plus ni moins de la tromperie. Pour lutter efficacement contre ces activités, les entreprises doivent exploiter des sources de données tierces qui les aideront à avoir une vision complète de la situation, à lancer une analyse multidimensionnelle de leurs données et à identifier les domaines d'intérêt. Dans ce contexte, l'ancrage des données dans ce qui constitue la réalité : navires, ports, marchandises, compagnies, directeurs, propriétaires, etc… contribue à éclaircir les questions et à fournir des informations pertinentes et réutilisables.

Une fois qu'elles savent « à quoi ressemblent leurs données », les entreprises peuvent commencer à les contrôler et à les analyser, et à instaurer un système de surveillance complet, qui relie efficacement les données internes et celles de sources tierces, tout en offrant une couverture des risques à la fois solide et homogène. L'idéal est de se concentrer sur plusieurs étapes du cycle de vie de la surveillance et du contrôle, tout en ayant la possibilité d'ajouter des informations plus contextuelles au sein d'une plate-forme capable de les traiter efficacement.

Dans ce genre de scénario, il est profitable d'exploiter des technologies d'analyse des big data, comme Hadoop couplé à des outils d'analyse haute performance. De nouvelles fonctionnalités comme l'exploration dynamique des données aident les enquêteurs à analyser et identifier les problèmes.

En parallèle, les data scientists ou spécialistes des données peuvent améliorer la détection en adoptant une approche analytique hybride qui consiste à incorporer des règles métier et à interroger des bases de données pour repérer des actes criminels déjà commis. Ils peuvent par la suite utiliser des techniques de détection des anomalies, de text mining et d'analyse des réseaux sociaux pour identifier les infractions jusqu'alors inconnues ou complexes, et établir les relations entre fraudeurs et blanchisseurs d'argent.

En permettant des analyses plus contextuelles, ces technologies facilitent le contrôle des volumes d'alertes. Elles offrent un système d'alerte à plusieurs niveaux et des techniques plus sophistiquées pour les clients à haut risque et/ou les scénarios de faux positifs. Il est ainsi plus facile pour les entreprises de gérer les volumes d'alertes et de déployer une stratégie efficace basée sur les risques.

Grâce à toutes ces fonctionnalités, les équipes en charge de la conformité peuvent repérer les comportements suspects ou inhabituels, prévenir les actes frauduleux et de blanchiment d'argent dans le secteur du financement du commerce. Avec pour finalité de traduire les coupables en justice.

Lien : **https://business-analytics-info.fr/7816/fraude-et-blanchiment-dargent-la-face-cachee-du-financement-des-echanges-internationaux/**

Les pertes liées à la cybercriminalité évaluées à 400 Md$

La cybercriminalité causerait un préjudice de 400 milliards de dollars par an dans le monde, selon étude réalisée par McAfee et le Center for Strategic and International Studies. Les entreprises américaines seraient les plus touchées par des actes de malveillance et de piratage.

Les cyberattaques pourraient entraîner jusqu'à 400 milliards de dollars de pertes par an tout autour du globe, révèle la seconde étude réalisée par l'éditeur de solutions de sécurité McAfee, filiale du groupe Intel. avec l'aide du Center for Strategic and

International Studies (CSIS). Le rapport souligne qu'il est toutefois difficile d'estimer les dommages des actes de malveillance et de piratage sur Internet, dont la plupart ne sont pas signalés. Il s'est appuyé sur des données publiques recueillies par les organisations gouvernementales et les universités du monde entier, y compris en Allemagne, aux Pays-Bas, en Chine, en Australie et en Malaisie, ainsi que sur des entretiens passés avec des experts.

Le rapport évalue les pertes liées aux cyberattaques à 375 milliards de dollars en fourchette basse et à 575 milliards de dollars en fourchette haute. «Même le chiffre le plus bas est plus élevé que le revenu national de la plupart des pays et des gouvernements du globe», analyse le rapport. En 2009, une autre étude réalisée par McAfee avait estimé le coût global de la cybercriminalité à 1 milliard de dollars, chiffre qui avait été critiqué et qui, selon l'entreprise, présentait des défauts. Selon les conclusions du spécialiste de la sécurité et du CSIS publiées en mai 2013, la cybercriminalité n'aurait probablement pas coûté plus de 600 milliards de dollars sur le plan mondial, ce qui correspond au coût estimé du commerce mondial de la drogue.

Des données à considérer avec précaution

Ces chiffres sont toutefois à prendre avec recul, car le rapport indique que la plupart des actes de cybercriminalité ne sont pas signalés, que peu d'entreprises communiquent sur les attaques et que la collecte de données cohérentes est difficile à effectuer car les pays ne sont pas d'accord sur une définition standard de ce qui constitue la cybercriminalité. « Quelques pays ont fait de sérieux efforts pour calculer leurs pertes causées par les cybercriminels, mais la plupart ne s'y sont pas mis », souligne l'étude. Ses auteurs ont constaté que les données agrégées de 51 pays dans toutes les régions du monde représentaient 80% du revenu mondial. En utilisant ces données pour estimer un coût global ajusté par région, l'étude « suppose que le coût de la cybercriminalité constitue une part constante du revenu national, ajusté au niveau de développement. »

Augmentation des attaques suite au développement du online

Le document a examiné les coûts directs et indirects des cyberattaques, comme la perte de la propriété intellectuelle et des données de l'entreprise, le coût des réseaux sécurisés, l'atteinte à la réputation et les frais de recouvrement. La croissance d''Internet et son utilisation pour le développement de l'activité économique signifie que «le coût de la cybercriminalité va continuer à augmenter suite à l'accroissement des services en ligne », a déclaré le rapport. Selon ce dernier, ce sont les entreprises américaines qui ont subi les pertes les plus élevées. « L'explication de ces variations dépasse la portée de cette étude, mais il est possible que les cybercriminels décident de l'endroit où ils commettront leurs actes en évaluant la valeur de leur cible et la facilité d'entrée », conclut le rapport.

Lien : **http://www.lemondeinformatique.fr/actualites/lire-les-pertes-liees-a-la-cybercriminalite-evaluees-a-400-md$-57730.html**

Immobilier : Les big data au secours de la lutte contre le blanchiment d'argent

En Australie, l'immobilier est le nouveau refuge du blanchiment d'argent. L'institut local de criminologie estime que 4,5 milliards de dollars australiens (2,8 milliards d'euros) s'évaporent ainsi chaque année, en grande partie en raison d'acquisitions immobilières illégales de la part de ressortissants étrangers. Les big data représentent

une piste prometteuse dans la lutte anti-blanchiment puisque leur usage améliore de 30 % la détection des transactions frauduleuses.

La guerre au blanchiment d'argent est déclarée. Les autorités australiennes multiplient les saisies et les reventes de biens immobiliers acquis illégalement par des acheteurs étrangers. Pour lutter contre cette fraude entraînant une bulle spéculative défavorable à la population locale, le gouvernement emprunte la voie de la dissuasion. Les fraudeurs — essentiellement basés en Asie du sud-est — ont jusqu'au 30 novembre pour se faire connaître et bénéficier d'une amnistie, après quoi ils encourront au mieux une amende salée de 127 500 dollars australiens (80 000 euros), au pire une peine de 3 ans de prison. Les intermédiaires impliqués dans la transaction — agents immobiliers et conseillers financiers — seront aussi sanctionnés.

Pour accroître son efficacité, cette méthode forte pourrait être complétée par une détection en amont des acquisitions frauduleuses grâce à des outils analytiques. Selon Alexon Bell, expert anti-blanchiment chez SAS, une approche hybride incluant modélisation prédictive et analyse des réseaux sociaux permet en effet de détecter 30 % d'incidents de fraude supplémentaires. Juguler le blanchiment d'argent dans le secteur immobilier devient d'autant plus urgent que les territoires du crime financier organisé s'étendent. Avec un montant de 25 milliards de dollars australiens (15,5 milliards d'euros), par exemple, le marché des jeux d'argent représente un eldorado…

Lien : **https://business-analytics-info.fr/7738/immobilier-les-big-data-au-secours-de-la-lutte-contre-le-blanchiment-dargent/**

« Le Big Data permet de traquer la fraude et l'addiction»

Le Big Data sert à détecter le blanchiment d'argent, les tables de poker fictives ou à prévenir le risque d'addiction au jeu à la Française des jeux. C'est ce que décrit Axel Bolotgittler, Data Scientist à la Française des jeux, lors de la journée nationale des études de l'Adetem.

On voit souvent le Big Data comme Big Brother, il peut aussi être employé pour la bonne cause. C'est ce qu'annonce La Française des jeux qui indique employer le Big Data à la fois pour détecter les risques de fraude, notamment de blanchiment d'argent, et détecter les addictions potentielles au jeu.

Un usage éthique du Big Data

C'est ce qu'a décrit Axel Bolotgittler, Data Scientist à la Française des jeux, lors de la journée nationale des études organisée par l'Adetem, l'association des professionnels du marketing, le 23 janvier. « Nous observons les données d'un point de vue éthique » indique-t-il. « Pour la lutte contre la fraude et le blanchiment d'argent, et pour le jeu responsable, afin de lutter contre l'addiction, un phénomène à risques » précise-t-il.

Il détaille la situation à la Française des jeux. Les données sont issues des points de vente, avec des données forcément anonymes car les clients ne s'identifient pas lorsqu'ils jouent, et sont enregistrées depuis 34 000 points de vente. « Nous avons 26 millions de clients pour 10 milliards d'euros de chiffre d'affaire » rappelle-t-il.

Travail à partir de l'horodatage et du lieu de vente

De quelles informations dispose la Française des jeux ? Elle connaît l'horodatage, l'heure, le lieu, le type de jeu. « On pense aller plus loin afin d'identifier le blanchiment d'argent. Les points de vente sont interconnectés, et on observe si on mise dans un point de vente, et on se fait payer dans un autre » déclare-t-il.

En ce qui concerne l'addiction, « On observe si une même grille est jouée avec des montants qui augmentent, c'est un signe possible d'addiction » indique-t-il. Il ajoute : « nous voulons aller dans la prévention et la prédiction, pour dire s'il y a possibilité d'addiction ou de blanchiment. »

Les tables fictives détectées en temps réel

Encore mieux, il s'agit de détecter si des tables de Poker fictives, s'organisent avec un phénomène de collusion où plusieurs joueurs s'allient contre un seul. « Pour tous les sites de Poker, les tables fictives sont très compliquées à trouver. Un site le détectait en 10 jours, après le phénomène de collusion. Grâce au Big Data, ils arrivent à trouver en temps réel quand il y a collusion. C'est l'intérêt du Big Data pour la prévention » pense-t-il.

Il reconnaît que le Big Data n'en est qu'à ses débuts à la Française des jeux. *"On commence tout juste à croiser les données entre makerting, commercial et finances. Les données du service sécurité sont délivrés sous forme de rapports word pour l'audit. Ils permettent de détecter les points de vente à risque" conclut-il.*

Lien : http://www.larevuedudigital.com/2014/01/23/le-big-data-nous-permet-de-traquer-la-fraude-et-laddiction-pour-la-francaise-des-jeux/

Le Big Data, acteur incontournable dans la lutte anti-fraude

Une récente étude de L'IDC, prévoit qu'en 2019, le marché mondial des technologies Big Data atteindra 48,6 milliards de dollars. Cette étude met en lumière les deux secteurs d'activité qui y investissent le plus : il s'agit de l'industrie et du secteur bancaire. Il n'est pas surprenant de retrouver le secteur financier en tête du classement.

Depuis 2008, on voit en effet apparaître une montée de la « Criminalité économique ».

Trois types de fraudes sont principalement concernés : les fraudes externes au secteur, les fraudes internes et les fraudes managériales.

Le Big data constitue une aide précieuse dans la lutte contre les fraudes et l'amélioration de la sécurité, que les banques doivent impérativement mettre en place pour respecter leurs obligations réglementaires et réduire leurs coûts liés à ces fraudes.

Une lutte anti-fraude dépassée qui n'évolue pas assez vite

Aujourd'hui et malgré l'utilisation de plus en plus avérée du Big Data, nous faisons le constat suivant :

- Les outils traditionnels utilisés encore en grande majorité dans le secteur financier n'accordent que trop peu d'attention aux fraudes non avérées, alors qu'elles sont aussi importantes.
- Bien que l'analyse humaine soit très performante, la détection de la fraude est encore trop lente, alors que les techniques des hackers sont de plus en plus pointues.
- Le processus de modélisation dans le datawarehouse est lourd et rigide.

Si les avancées sont considérables en matière de détection, elles ne sont pas encore suffisantes pour contrer les attaques qui ont toujours un temps d'avance. La mise en place d'un système de Big Data est une aide considérable en matière de lutte anti-fraude, qui permet également de respecter les obligations réglementaires.

Le Big Data, une aide précieuse pour respecter les obligations réglementaires

Les obligations réglementaires auxquelles les banques doivent rendre compte sont drastiques. Pour répondre à ces impératifs, le Big Data est la meilleure solution.

En effet, la BCE (banque centrale européenne) leur impose d'être très réactives aux audits qu'elles doivent effectuer.
Les reportings qu'ils ont pour obligation de rendre régulièrement ont pour impératif d'être sans faille. Les risques internes et externes doivent être éliminés sans prérogative. Pour connaître le détail de ces obligations réglementaires suivez ce lien.

Le Big Data améliore considérablement l'expérience de lutte anti-fraude

En matière de sécurité, les améliorations apportées par le big data sont considérables.

Que permet l'utilisation du Big Data dans le secteur financier ?

- Le traitement en temps réel des données et donc une réactivité inégalée.
- La réduction des délais de traitement des opérations de détection de 3 semaines à 5 minutes. Ce qui est une avancée considérable.
- L'augmentation des taux de détection positifs

Tout ceci réduit leurs couts liés à la fraude bancaire.

De quelle manière ?

- Les solutions existantes ont été améliorées grâce à des algorithmes.
- Les comportements anormaux détectés sont affinés.
- On peut désormais détecter les fraudes non avérées en temps réel. (Grâce à un large volume de données analysées).
- Il est désormais possible de faire des focus sur les comportements à risques grâce au machine learning.

La création de score de suspicion notamment permet une meilleure prévision des fraudes (ces scores qui vont de 0 à plus de 3, note la probabilité qu'un client ou une personne a de frauder ou non en fonction de l'analyse d'un certains nombres de données)

- L'utilisation des données de **l'**open data (des données publiques), comme celles de twitter et de facebook, permettent de traquer les entités frauduleuses. Ces données peuvent fournir beaucoup d'informations telle que la localisation géographique. Elles sont notamment très utiles en ce qui concerne la fraude à la carte bancaire. Les banques peuvent ainsi vérifier si la localisation géographique d'une personne correspond au lieu d'utilisation de sa carte bancaire et détecter si une fraude est en cours en temps réel.
- En termes statistiques, il existe plusieurs approches tel que des régressions statistiques, des lois statistiques (loi de Benford,…), des approches basées sur des réseaux de neuronaux, du clustering ou encore des arbres de décisions, utilisées dans la lutte anti-fraude.

Collaborer ensemble pour rendre le processus efficace

Mais pour que la mise en place d'un système de Big Data soit efficace, les services doivent collaborer ensemble.
Dans un autre article, nous avions ainsi évoqué quelles étaient les limites de la technologie face aux négligences humaines. Vous pouvez vous y reporter afin de découvrir quelles sont les règles à bien respecter pour garantir un bon niveau de sécurité.
Les organismes financiers n'ont plus d'autres choix pour lutter contre les fraudes que d'investir massivement dans le Big Data pour améliorer considérablement la détection des fraudes non avérées en temps réel. Outre la réduction considérable des coûts liés aux fraudes, il permet aux organismes financiers de pouvoir respecter leurs obligations réglementaires imposées par la BCE. Nous verrons dans un prochain article que les big data ont encore d'autres utilités pour le secteur financier.

Lien : http://jems-datafactory.fr/2015/12/11/le-big-data-acteur-incontournable-dans-la-lutte-anti-fraude/