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

1MDB: le scandale financier de la décennie en 5 questions

Révélé par un lanceur d'alerte genevois, le pillage du fonds souverain malaisien 1MDB concerne directement la Suisse. Résumé d'une affaire qui ébranle la finance Mondiale

Pourquoi cette affaire est-elle importante?

L'affaire 1MDB, nom d'un fonds souverain malaisien pillé de plusieurs milliards de dollars par ses dirigeants, est l'un des plus grands scandales financiers du XXIe siècle. Selon la justice américaine, quelque 3,5 milliards de dollars ont été détournés pour enrichir les directeurs du fonds, des hommes d'affaires, des officiels, Tous rejettent ces accusations.

Plus encore que les milliards disparus, la personnalité des acteurs du scandale rend l'affaire exceptionnelle. Autre personnage central, le milliardaire malaisien J.L. Il aurait notamment utilisé les montants détournés pour financer la production du film *Le Loup de Wall Street*, avec L.D.C.

C'est la première fois que l'on assiste au pillage d'un fonds souverain. Le dossier éclaire les failles de la finance internationale face à la corruption.

Quel est le rôle de Genève?

L'affaire a éclaté suite aux révélations d'un Genevois, X.J, directeur administratif de la firme pétrolière P.S jusqu'en 2011. Les transactions de P.S avec 1MDB sont un élément central du scandale.

Début 2015, insatisfait de son dédommagement, X.J remet des centaines de milliers d'e-mails et de documents soustraits à P.S à une journaliste britannique, C. R.B. C'est elle et son blog qui, sur la base de ces documents, révéleront le scandale 1MDB. Arrêté puis condamné en Thaïlande pour vol de données, sur plainte de P.S, X.J se décrit d'abord comme un «traître» qui a commis un acte «répugnant» en livrant des données confidentielles de son employeur pour «faire de l'argent».

Mais tout récemment, lui et ses nouveaux avocats ont changé de ligne de défense. Sa femme affirme qu'il a été manipulé par son employeur P.S, qui l'aurait enfoncé en le poussant à s'auto-accuser. Les nouveaux avocats de X. J tentent actuellement de le faire transférer de Thaïlande en Suisse pour qu'il purge ce qui reste de sa peine.

Quant à P.S, basée à la rue du Rhône, son rôle est mieux connu grâce à la plainte civile déposée par le Ministère de la justice américain le 20 juillet dernier. Selon ce document, la création d'une coentreprise entre P.S et 1MDB en 2009 a permis le détournement de 1 milliard de dollars au profit de J.L.

Le versement du milliard détourné a été présenté comme le remboursement par 1MDB d'un prêt fait par P.S – prêt qui n'aurait en fait jamais existé. De plus, P.S, aurait utilisé les fonds venus de 1MDB pour verser 20 millions de dollars.

La société P.S s'est défendue en affirmant qu'aucun fonds de 1MDB n'a en réalité disparu, ou ne manquerait, et que l'argent versé par 1MDB a été remboursé avec un profit. Selon l'avocat genevois de la famille, «il n'existe aucune procédure pénale dirigée contre les sociétés du groupe P.S, ses employés ou ayants droit économiques».

En Suisse, le Ministère public de la Confédération confirme que l'enquête ouverte en Suisse «n'a jamais concerné les sociétés du groupe P.S, leurs employés ou leurs ayants droit économiques». Elle vise uniquement «des investissements faits en relation avec P.S».

Mais dans un courrier qui a fuité sur Sarawak Report, le MPC juge «particulièrement suspecte» l'une des sommes versées dans le cadre du contrat entre 1MDB et P.S.

Enfin, à Genève toujours, aux Ports francs, se trouveraient plusieurs tableaux achetés par J.L grâce aux fonds détournés. A ce stade de la procédure, l'homme d'affaires n'a pas été inculpé dans les enquêtes ouvertes sur le scandale aux Etats-Unis, à Singapour ou en Suisse.

Quelles banques suisses sont impliquées?

En mai, le gendarme financier suisse, la Finma, a accusé la banque BSI de grossières négligences pour avoir transféré des centaines de millions de francs détournés de 1MDB. Rachetée par sa concurrente EFG, la BSI sera dissoute. Sa filiale à Singapour est l'une des principales entités impliquées dans le scandale. C'est elle qui a reçu le premier milliard de fonds détournés.

Dans sa plainte, la justice américaine a aussi ciblé une petite banque privée active à Genève et Zurich, FBank, dont l'ancien président est l'un des principaux suspects de l'affaire. En mai 2012, F. a transféré presque 600 millions de dollars vers une société offshore qui servait de plaque tournante aux détournements.

La banque privée Edmond de Rothschild et la banque Rothschild AG sont également citées par la justice américaine – la première pour avoir reçu 472 millions sur le compte d'un officiel accusé d'avoir participé aux détournements, la seconde pour avoir accueilli des fonds utilisés pour blanchir les fonds détournés dans l'immobilier américain.

UBS apparaît un peu plus en marge du scandale, dans le transfert de deux milliards de dollars issus de 1MDB.

Enfin, RBS Coutts, à Zurich, abritait les comptes de sociétés de J.L qui ont reçu à peu près 1 milliard de fonds détournés.

Qui enquête contre qui?

En Suisse, le Ministère public de la Confédération enquête contre deux dirigeants de 1MDB et deux officiels impliqués dans les détournements. La procédure est ouverte pour escroquerie, gestion déloyale, gestion déloyale des intérêts publics, faux dans les titres, corruption d'agents publics étrangers et blanchiment d'argent. Le MPC a aussi ouvert une enquête contre la banque BSI pour défaillance d'organisation.

Aux Etats-Unis, le gouvernement a déposé une plainte civile demandant la confiscation de 1 milliard de dollars issus des détournements. Singapour a ouvert sa propre enquête pour blanchiment et a également sanctionné la filiale locale de la banque BSI.

Que va-t-il se passer désormais?

En Suisse, aux Etats-Unis et à Singapour, une extension des enquêtes sur le scandale n'est pas exclue: elles pourraient toucher de nouvelles personnes et aboutir à de nouvelles inculpations.

Le chef de la section anti-blanchiment du Ministère de la justice américain a déjà averti dans le *Financial Times* que mener ces enquêtes à bien serait très difficile – en raison de leur complexité, de leur caractère international.

Lien : https://www.letemps.ch/economie/2016/08/29/1mdb-scandale-financier-decennie-5-questions

Cybercriminalité : La délinquance économique du XXIème

La criminalité économique et financière a pris désormais une connotation « cyber» comme toutes les activités illicites avec le développement d'Internet et des réseaux numériques. Bitcoins, monnaies virtuelles, cloud computing, big data, autant de termes qui surgissent dans cet écosystème numérique dans leurs dimension juridique et stratégique. La dématérialisation des transactions permet aussi un accroissement de l'anonymat des échanges, facilitant ainsi le passage à l'acte des cyberdélinquants. Ainsi, les cyberfraudes, les escroqueries aux faux ordres de virement ciblent les données personnelles échangées et monnayées sur des marchés parallèles, «les Darknets». Ces nouveaux fonctionnements constituent des défis majeurs pour le droit pénal et la procédure pénale qui est désormais un droit en mouvement qui tente de s'adapter à la cyber mondialisation de cette délinquance.

Si le droit pénal classique tant matériel que processuel répond partiellement à ces nouveau défis, le législateur est intervenu pour l'adapter et le moderniser en introduisant de nouvelles techniques d'enquête comme l'infiltration et la captation de données qui sont par ailleurs soumises aux exigences du Conseil constitutionnel et des

cours européennes Complexifiée par cet écosystème numérique, la lutte contre la criminalité économique et financière nécessite aussi la création d'instances spécialisées tant sur le plan national avec par exemple le nouveau procureur de la République financier qu'au niveau international avec Interpol et Europol qui consacrent des moyens supplémentaires à ces cyberinfractions qui ont souvent des ramifications internationales. La police mais aussi la justice sont à un tournant historique sans précédent et s'investissent en urgence dans ce domaine numérique pour préserver à la fois l'ordre public économique et les droits et libertés fondamentaux.

Comment agit cette cyberdélinquance financière, quelles sont ses modes opératoires et comment la combattre? Des réponses à ces questions sont nécessaires et l'Etat2 a mis en place une véritable stratégie de lutte contre ce phénomène qui vise à anticiper de manière efficace les risques numériques. Les initiatives sont nombreuses pour mieux protéger les internautes et lutter contre ces fléaux. On peut citer un rapport publié en juin 2014 aux ministres de l'Intérieur et de l'Economie, à la Garde des Sceaux et à la secrétaire d'Etat chargé du Numérique.

Il est nécessaire de mettre en place une réelle cyberpolitique publique de lutte contre la cybercriminalité. Il convient d'inciter tous les acteurs à se mettre en ordre de marche de façon plus cohérente et constructive pour lutter contre ce fléau avec le souci de répondre au besoin légitime de protection des cybervictimes.

Lien : https://cybercriminalite.wordpress.com/2015/07/03/cybercriminalite-la-delinquance-economique-du-xxi-eme-siecle-le-dernier-ouvrage-de-myriam-quemener/

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.
Lien : http://www.altospam.com/actualite/2009/02/les-nouvelles-formes-de-scam-les-mules-et-le-blanchiment/

TOR, le réseau Internet parallèle infiltré par le crime

30 % des contenus relèvent d'activités illicites et criminelles, financées essentiellement à l'aide du bitcoin.
« Equipe de trois tueurs à gage opérant aux USA, Canada et en Europe. Réponse sous deux jours, "contrat" réalisé sous trois semaines selon la cible. Pas d'enfant de moins de 16 ans ni de politiciens du Top 10 ". C'est une des offres de « services " qui fleurissent sur le réseau Internet TOR. Un Web de l'ombre parallèle, décentralisé, sans règles ni modérateurs et garantissant un grand anonymat à l'aide d'un navigateur Web approprié. Créé par et pour les activistes politiques, il a été dès son origine infesté et infiltré par les activités criminelles, notamment pédophiles. 30 % des contenus relèvent en effet d'activités illicites, confirment des chercheurs (1).
Sur 5.205 sites analysés entre janvier et mars 2015, 1.547, soit 30 %, proposaient des produits et services illégaux, avec une large palette. En tête figurent les sites de ventes

en ligne de drogues, 423 recensés, et qui représentent plus du quart des sites illégaux sur TOR. Ils sont suivis par la finance (21 % des sites illégaux) - blanchiment, cartes de crédit volées, faux billets...- la contrebande-contrefaçon de documents officiels (12 %), les sites extrémistes et violents (9 %) et la pornographie infantile (8 %). Une vingtaine de sites proposaient les services de tueurs à gage, une quarantaine vendait des armes et une centaine mettait en relation avec des pirates informatiques... *« Le bitcoin est la devise la plus couramment utilisée dans ces activités illégales "*, estiment les chercheurs, souvent avec l'aide de services (CleanCoin, Bitcoin Fog...) qui se sont créés et qui ont pour but de brouiller encore davantage les pistes et rendre les transactions 100 % anonymes : en clair rendre le bitcoin « plus blanc que blanc ".

Devise de transaction historique

Le bitcoin est la devise de transaction historique des supermarchés en ligne des drogues, qui ont émergé et qui l'ont adopté dans le sillage de Silk Road, le site précurseur, ainsi que pour toutes les activités financières illégales. L'année dernière, la police allemande a fermé 5 marchés noirs du Web. Cette semaine, ce sont les autorités suédoises qui ont arrêté un vendeur de drogues opérant sur plusieurs plates-formes. Car la demande est soutenue. La proportion d'individus qui ont acheté des drogues sur Internet a été multipliée par 5 depuis 2009 à 25 %. 6,4 % des personnes sont passées par le Web de l'ombre pour acheter ces produits, et dont 4,5 % durant les douze derniers mois. C'est en Suède où cette proportion est la plus élevée (25 %), elle est de 15 % au Royaume-Uni, 12 % aux Etats-Unis et 7 % en France, un pays dans la moyenne mondiale.

Les drogues les plus couramment achetées sur le Web de l'ombre sont la MDMA, une amphétamine connue sous le nom d'ecstasy, puis le LSD, un hallucinogène, le cannabis et la cocaïne. « Il y a peu de sites extrémistes islamiques sur TOR. Ce dernier est moins adapté à leurs opérations de propagande qui nécessitent pour être efficaces d'avoir accès à une large audience. En outre, les terroristes préfèrent communiquer entre eux sur d'autres plates-formes et avec d'autres moyens », estiment les auteurs de l'étude.

Lien : http://www.lesechos.fr/02/08/2016/LesEchos/22246-100-ECH_tor--le-reseau-internet-parallele-infiltre-par-le-crime.htm

Le Sniffing : Une forme d'attaque sur le réseau couramment utilisée par les pirates

Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisée par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers ont généralement recours à ce procédé pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles. Les pirates informatiques utilisent des sniffers réseau ou renifleurs de réseau pour pouvoir surveiller le réseau et soustraire frauduleusement les différents types de données confidentielles susceptibles de les intéresser.

Mécanisme de fonctionnement d'un sniffer de réseau :

Un Sniffer est généralement utilisé pour intercepter les paquets qui circulent sur un réseau. Il offre, à cet effet, la possibilité pour un hacker d'examiner le contenu d'un certain nombre de paquets qui ne lui ont pas été initialement destinés. En tant que renifleur, cet outil peut donc intercepter tout type d'informations émises à travers le réseau et par conséquent afficher à la fois l'identité des utilisateurs au même titre que leurs mots de passe, surtout lorsque ces informations sont transférées par des

protocoles qui ne sont pas suffisamment sécurisés comme : le FTP (File Transfert Protocol), la DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte). Lorsque les donnés ne sont donc pas cryptées et qu'elles doivent passer à travers une interface réseau de l'ordinateur par l'intermédiaire duquel s'exécute le renifleur réseau ou sniffer, les informations sont immédiatement interceptées par cette machine sans la moindre difficulté.
Afin de vous prémunir contre les risques de Sniffing, vous pouvez consulter l'agence Anti Cybercriminalité pour vous conseiller sur les différentes mesures à prendre en vue d'éviter les pièges tendus par les renifleurs.
Lien : **http://www.anti-cybercriminalite.fr/article/le-sniffing-une-forme-dattaque-sur-le-r%C3%A9seau-couramment-utilis%C3%A9e-par-les-pirates**

Prévention contre le sniffing réseau

Je me suis connecté dernièrement au réseau sans fil de la bibliothèque, et le soir même tous mes comptes avec lesquels je me suis connecté ont été piratés**,** pourtant je n'ai pas donné mon mot de passe à qui que ce soit et personne n'était à côté de moi ! …
C'est une histoire qui n'est pas si rare qu'elle en a l'air, il s'agit d'une attaque par sniffing réseau aussi appelée reniflage réseau en français.

Reniflage réseau ?

Le reniflage réseau consiste à écouter les communications réseau afin de récupérer et d'analyser le contenu transmis. Ce contenu peut-être constitué d'informations très sensibles lorsqu'aucun chiffrement n'est utilisé. Parmi ces informations sensibles, on peut trouver le contenu d'une conversation par mail**,** les cookies ou encore les fameux mots de passe**.**

Alors comment peut-on se faire voler son mot de passe ?

Entrons dans le vif du sujet, comment trouver un mot de passe transitant sur le réseau ? Comment un pirate peut-il nous voler un mot de passe en utilisant un simple renifleur réseau ?

Attention : L'article n'est pas un mode d'emploi pour trouver un mot de passe qui ne vous appartient pas mais une vue générale afin de vous en prémunir sur le mécanisme qu'on pourrait employer contre vous, notamment en vacances. Nous allons un poil plus loin que les recommandations classiques pour voir concrètement ce qu'il se passe.

Exemple avec Wireshark

WireShark est un outil d'analyse de protocoles réseaux destinés aux administrateurs réseau. Il est notamment utilisé pour vous démontrer ce que je veux vous démontrer aujourd'hui. Imaginons que cet exemple me permette de me connecter à mon compte sur un forum, sur un blog ou à n'importe quel autre service demandant un login et un mot de passe :
Si maintenant je commence à capturer le trafic réseau avec Wireshark puis me connecte avec pour login « admin » et pour mot de passe « mdp », je vois aussitôt s'afficher une liste de paquets réseau dont un paquet HTTP**,** plus précisément je vois les informations envoyées par la méthode POST :
Et comme vous le constatez, mon login et mon mot de passe apparaissent tous les deux ici en clair, dans la partie du milieu (*txt=admin&pass=mdp&sub=Envoyer*).
La capture a été faite à partir de ma propre carte réseau, je reçois donc tout ce qui part et arrive vers ma carte uniquement.

Je pourrais très bien configurer Wireshark pour écouter sur mon réseau local complet. Mais bien sûr il lui faudra la clé WEP ou WPA de la box si il s'agit d'un réseau wifi ainsi que l'autorisation bien évidente du propriétaire si ce n'est pas moi même.

Comment se protéger contre le sniffing réseau ?

Vous comprenez maintenant déjà mieux pourquoi on dit souvent qu'il ne faut pas se connecter dans les cybercafés et autres réseaux publics.

Non seulement vous ne savez pas toujours quels programmes sont lancés sur l'ordinateur que vous utilisez, mais en plus vous pouvez être victime de reniflage réseau.

En fait, la meilleure protection contre ce type d'attaque est d'utiliser un protocole de communication sécurisé comme HTTPS.

Voici une capture d'écran d'une interface de connexion semblable à l'écran précédent mais utilisant cette fois HTTPS :

On ne voit plus en clair les données transmises (*Encrypted Application Data*) et on ne peut donc plus trouver un mot de passe sans clé de déchiffrement.

Vous l'avez compris, la meilleure protection contre le sniffing réseau est ici d'utiliser HTTPS.

Que faire si le site n'est pas en HTTPS ?

Me demanderiez-vous, et c'est une excellente question !

Eh bien vous pouvez également utiliser un service VPN qui chiffrera le trafic même pour les sites qui ne sont pas en HTTPS**.**

De quoi surfer sur les réseaux publics en paix.

Lien : http://www.leblogduhacker.fr/prevention-contre-sniffing-reseau/

Bitdefender : L'un des serveurs de l'éditeur piraté, chantage à la clé

L'éditeur roumain de solution de sécurité Bitdefender a **été** victime d'un piratage de l'un de ses serveurs. Le cybercriminel aurait dérobé des données personnelles d'utilisateurs et tente de faire chanter la firme en exigeant de l'argent en échange de son silence.

Il se fait appeler *DetoxRansome* et aurait réussi à s'emparer de données d'identification confidentielles d'utilisateurs présente sur un serveur de la firme. Il est malheureux qu'un piratage puisse toucher une entreprise de sécurité mais ce n'est pas tout… attendez la meilleure !

Des données en clair non chiffrées

Et oui ! Le pirate a pu accéder aux donnée d'identification d'un échantillon représentant 1% de la clientèle PME. Afin de prouver ses dires, le pirate a fourni une liste de noms d'utilisateurs et de mots de passe pour plus de 250 comptes clients dont certains ont été confirmés comme étant actifs. Bitdefender confirme la brèche et ajoute que la base ne contenait que quelques comptes apprenant à des PME, mais que les comptes des grandes entreprises et ceux des particuliers n'ont pas été compromis.

La surprise réside surtout dans le fait que les mots de passe étaient tous en clair et non chiffrés/hashés. Très étonnant (voir décevant) de la part d'une telle firme de sécurité informatique. Espérons que cela va être amélioré prochainement.

Sur le Web underground, le pirate DetoxRansome a mis en vente les données pour 8 Bitcoins et précise que la vulnérabilité provient du service Amazon Elastic Web qui a souvent des problèmes avec le SSL. L'erreur est humaine, et c'est via une technique

de sniffing que ce dernier a pu compromettre les données privées, comme l'explique Hack Film. Bref, aucune vulnérabilité zero-day n'est en cause.

« *Au cours d'une montée de version de l'infrastructure, un seul serveur a été déployé avec un package logiciel plus à jour contenant une faille connue, ce qui a permis d'extraire des informations dessus mais pas de compromettre le système dans son ensemble* », a précisé Catalin Cosoi, responsable de la sécurité chez Bitdefender.

Tous les mots de passe touchés ont été réinitialisés depuis et une enquête approfondissement est en cours.

Du chantage et une rançon à la clé

Comme le montre explicitement ce tweet, le pirate demande une rançon de 15 000 dollars en échange de la non divulgation des données.

"*La question a été immédiatement résolu, et des mesures de sécurité supplémentaires ont été mis en place pour empêcher qu'elle ne se reproduise*," a déclaré le porte-parole de la société dans un communiqué. "*Notre enquête a révélé qu'aucun autre serveur ou services ont été touchés*."

Lien : https://www.undernews.fr/hacking-hacktivisme/bitdefender-lun-des-serveur-de-lediteur-pirate-chantage-a-la-cle.html

L'un des outils préférés des cybercriminels mis à mal par un coup de filet ?

Karspersky publie aujourd'hui sur son blog un compte rendu d'une enquête des autorités russes à laquelle ils ont collaboré. Celle-ci a permis l'arrestation en juin d'un groupe de 50 cybercriminels, baptisés Lurk, qui opéraient notamment l'Angler exploit kit.

L'Angler Exploit Kit connaissait ces dernières années une popularité redoublée. Ce couteau suisse du cybercriminel était une plateforme utilisée pour infecter les machines de victimes : en l'installant sur un serveur et en amenant la cible à se connecter à ce serveur via un navigateur par exemple, le cybercriminel pouvait avoir recours à tout un éventail d'exploits fournis par les créateurs du kit pour tenter d'infecter la machine de la victime.

Simple à utiliser, évolutif et souvent à jour avec les derniers exploits et dernières vulnérabilités découvertes, l'Angler Exploit Kit dominait naturellement le marché. Mais en juin 2016, l'utilisation de cet outil par les cybercriminels a soudainement chuté sans véritable explication.

De nombreux observateurs avaient néanmoins fait le lien entre l'arrestation d'un groupe de 50 cybercriminels par les autorités russes et la soudaine disparition de l'Angler Kit. Dans une longue note de blog, Ruslan Stoyanov, dirigeant de l'unité investigation chez Kaspersky confirme cette théorie et détaille les 5 années passées sur la piste de ce groupe de cybercriminels de haute volée qui avaient été baptisés « Lurk ».

Le nom du groupe Lurk vient du premier malware repéré par Kaspersky en 2011. Celui-ci se présentait sous la forme d'un malware bancaire sophistiqué, qui visait principalement les logiciels bancaires afin de procéder à des virements frauduleux en direction des cybercriminels. Swift a connu plusieurs versions et évolutions, allant parfois jusqu'à fonctionner entièrement in memory pour éviter la détection.

Le malware Lurk se présentait comme un logiciel modulaire, pouvant embarquer plusieurs modules capables de réaliser des actions différentes, mais toujours orientées

vers le vol de données bancaires et l'émission de virements frauduleux depuis les machines infectées.

Une petite PME sans histoire

« Avec le temps, nous avons réalisé que nous étions face à un groupe d'au moins 15 personnes. (…) Cette équipe était en mesure de mettre en place le cycle complet de développement d'un malware : à la fois sa conception, mais aussi la diffusion et la monétisation, à l'instar d'une petite entreprise de développement logiciel » explique Ruslan Stoyanov. Et le groupe Lurk avait également un autre atout de taille dans sa poche : exploitant leur renommée parmi les cybercriminels russophones, ils avaient commencé à louer les services de leur plateforme d'exploit, baptisée Angler Kit.

Cet exploit kit était à l'origine utilisé pour diffuser le malware bancaire Lurk, mais face aux mesures de sécurisation mises en place par de nombreuses banques, les revenus déclinants du groupe les ont forcés à diversifier leur activité. Les premières détections d'Angler Kit remontent à 2013, mais ce kit vendu en Saas par les cybercriminels du groupe Lurk a rapidement gagné en popularité.

Les créateurs du Blackhole kit ont été arrêtés en 2013, ce qui a laissé au nouveau programme du groupe Lurk un boulevard pour devenir le nouvel exploit kit préféré des cybercriminels. Dès le mois de mai 2015, celui-ci dominait largement le marché. Angler Kit pouvait être loué par d'autre groupe de cybercriminels qui s'en servaient pour diffuser différents types de malwares allant du ransomware au traditionnel trojan bancaire.

Mais le 7 juin, les autorités russes sont parvenues à arrêter les cybercriminels cachés derrière ce système. Kaspersky explique avoir collaboré avec les autorités afin de mener cette investigation, notamment via de l'échange d'informations compilées par la société sur le groupe. Un processus qui semble avoir été long et difficile, mais qui aura finalement porté ses fruits : l'Angler Kit est hors service et peut maintenant laisser la place… au nouvel exploit kit à la mode.

Selon les données récentes compilées par la société Trend Micro, l'exploit kit Neutrino aurait maintenant le vent en poupe et profiterait le plus de la retraite anticipée de son concurrent. Un de coffré, dix de retrouvés ?

31 Août 2016.

Lien : http://www.zdnet.fr/actualites/l-un-des-outils-preferes-des-cybercriminels-mis-a-mal-par-un-coup-de-filet-39841286.htm

Les botnets : acteurs majeurs de l'ombre

L'écosystème d'Internet est d'une complexité insoupçonnée, et en particulier sa part obscure. Au coeur de cet écosystème, les botnets tiennent une place de choix, et sont à l'origine d'un très grand nombre de menaces qui occupent à plein temps les différents acteurs de la sécurité informatique.

Mais tout d'abord, qu'est-ce qu'un botnet? Littéralement, un botnet est la contraction de deux termes: "robot" et "network". Il s'agit donc d'un réseau de robots – robot désignant un agent ou un programme informatique – dont la finalité est malveillante. Les exemples d'activité malveillante sont nombreux, et l'envoi de spam et de virus par email sont des exemples-types de l'activité des botnets. Un botnet est contrôlé par une personne physique: il s'agit du *botmaster (Il peut évidemment y avoir plusieurs botmasters pour un même botnet.)*

Nous allons présenter plus en détail les botnets, en nous intéressant au cycle de vie de ces derniers : ce choix de perspective permettra d'appréhender toute la problématique

relative aux botnets, autant d'un point de vue technique que d'un point de vue économique et juridique.

Naissance d'un botnet

Le support physique d'un agent malveillant – ou *malware* – est une *machine zombie* : il s'agit en général d'un ordinateur contrôlé par le botnet, à l'insu de son utilisateur légitime. Un exemple typique de machine zombie est un ordinateur familial placé derrière une connexion ADSL, dont des éléments essentiels à la sécurité ne sont pas à jour (système d'exploitation, navigateur internet, anti-virus…) et qui a été compromis soit par l'exécution d'une pièce jointe contenant un virus, soit par la visite d'un site web infecté. S'appuyer sur une telle infrastructure a des avantages indéniables d'un point de vue économique : les coûts, que ce soit le hardware, la bande passante ou l'électricité sont intégralement à la charge de son utilisateur légitime.

Donner naissance à un botnet revient à constituer un réseau de machines zombies, par l'intermédiaire d'une phase d'infection virale de grande ampleur. Cette phase d'infection se déroule en plusieurs étapes:

Le développement d'un malware qui permettra à la machine zombie de communiquer avec le botnet, et d'effectuer les activités malveillantes. Ce développement nécessitera en outre l'exploitation d'une faille de sécurité, qui peut être innovante, ou bien déjà connue, pour installer le malware à l'insu de l'utilisateur légitime. A noter que certaines failles de sécurité innovantes – et pouvant potentiellement affecter des systèmes d'exploitation ou des logiciels récents – peuvent être achetées ou vendues sur le marché noir.

La constitution d'un carnet d'adresses, qui est la liste des utilisateurs cibles de la phase d'infection virale. Ces listes peuvent être constituées par des robots qui collectent des adresses emails trouvées sur Internet (En parcourant des forums de discussion par exemple.) ou bien être achetées directement sur le marché noir.

L'envoi d'une campagne d'emails qui, soit contient le malware sous forme de pièce attachée, soit fait référence à ce malware par l'intermédiaire d'un lien vers un site web infecté. L'envoi de cette campagne peut d'ailleurs être sous-traité en sollicitant les services d'un autre botnet.

La réception d'un email contenant le malware sous une des formes précisées précédemment et l'installation de ce dernier par certains utilisateurs cibles de la phase d'infection virale. Le taux d'infection est très variable et dépend d'une part du niveau de protection de chaque utilisateur, et d'autre part de la qualité de la faille de sécurité exploitée.

Suite à cette phase d'infection initiale qui permet au botnet de prendre vie, d'autres phases d'infection peuvent avoir lieu pour agrandir le botnet (De la même manière, des phases d'infection peuvent avoir lieu pour reconstituer un botnet qui a été partiellement démantelé.). Un botnet peut atteindre une taille considérable : on estime par exemple que le botnet Bredolab était constitué à son paroxysme de près de 30.000.000 de machines zombies.

Vie d'un botnet

Suite à l'installation du malware sur la machine cible, ce dernier va contacter un des nombreux serveurs de contrôle et de commande du botnet (Les serveurs de contrôle et de commande sont généralement installés chez des hébergeurs, car ils doivent avoir une capacité – en terme de bande passante, de stockage et de traitement – importante. Le pilotage et la supervision de millions de machines zombies nécessite des ressources importantes et un niveau de compétence technique élevé). Ces serveurs servent à piloter (La communication entre les machines zombies et les serveurs de contrôle et de commande est effectuée selon un protocole propre au botnet, qui peut

être éventuellement crypté.) les activités des machines zombies, à collecter des informations, et également à mettre à jour le malware : ils constituent la clé de voûte de l'infrastructure de communication du botnet.
Le malware va espionner la machine cible, et remonter toute information utile : numéro de cartes bancaires, mots de passe, données personnelles (nom, prénom, numéro de sécurité sociale… utilisés à des fins d'usurpation d'identité), carnet d'adresses…. Ces données seront ensuite agrégées, et utilisées directement ou bien revendues sur le marché noir par le botmaster. A noter que les adresses email collectées sont d'une grande importance pour le botnet, car elles permettent d'effectuer de nouvelles phases d'infection virale permettant d'agrandir ce dernier.
En outre, le malware va effectuer les différentes tâches qui lui seront affectées, parmi lesquelles :
L'envoi d'une campagne de spam ou de virus, en utilisant un modèle d'email et une liste de destinataires : à ce modèle seront ajoutés des éléments variables et aléatoires, de manière à échapper aux systèmes de filtrage par signature.
Effectuer une attaque par déni de service distribué (Une attaque par déni de service consiste à rendre indisponible un service internet en le saturant de demandes de connexion. On parle d'une attaque par déni de service distribué si un grand nombre de machines participe à cette opération, ce qui est toujours le cas pour un botnet. On pourra citer par exemple l'attaque menée en décembre 2010 par le groupe Anonymous contre les sites de Paypal, Visa et Mastercard, lors de l'affaire Wikileaks, et qui a été largement médiatisée)
Effectuer de la fraude au clic (Le fraude au clic consiste à effectuer de manière automatisée des clics sur des liens publicitaires, ce qui remet en cause le modèle économique des liens sponsorisés, qui est très populaire sur Internet. On estime que plus de 20% des clics sur les liens publicitaires sont d'origine frauduleuse) pour générer des revenus publicitaires frauduleux.
Effectuer du calcul intensif, en particulier pour casser certaines clés de cryptage.
Ces activités peuvent être exercées pour le compte du botmaster, mais dans la plupart des cas elles sont vendues comme une prestation à d'autres acteurs : industriels de la contrefaçon (La contrefaçon concerne principalement les montres de prestige, les produits de luxe, les médicaments – dont le fameux Viagra – et l'édition logicielle), organisations criminelles…
Prenons l'exemple classique du spam :
Une organisation souhaite proposer à la vente des contrefaçons (montres de prestige, produits de luxe…).
Elle contacte le botmaster, et lui demande d'envoyer une campagne publicitaire à grande échelle. Le botmaster joue donc le rôle de prestataire de service pour le routage des emails : il fournit - contre rémunération (Les prix sont variables, et dépendent surtout de la qualité du carnet d'adresses. On estime que l'envoi d'un million de spams coûte en moyenne moins de 100$ pour le client) – les moyens techniques d'envoi ainsi que les carnets d'adresses des destinataires.
La campagne de spam est envoyée, avec une volumétrie souvent considérable (On a estimé par exemple la capacité d'envoi quotidienne du botnet Rustock à environ 30.000.000.000 d'emails. C'est un volume considérable, et cela donne la mesure de la dangerosité des botnets). Du fait des moyens techniques mis en œuvre pour limiter le spam, un pourcentage assez faible atteindra le destinataire final, et le taux de transformation sur le site de contrefaçon sera d'autant réduit. Toutefois, la volumétrie considérable en amont – souvent plusieurs millions voire milliards d'emails – lié au

coût quasi-nul en terme d'infrastructure – le coût financier étant à la charge des propriétaires des machines zombies – font que ce modèle reste très rentable.
L'organisation qui vend les contrefaçons reçoit par la suite un grand nombre de commandes, qu'elle pourra choisir d'honorer ou pas : si elle honore la commande, elle enverra donc la contrefaçon au client et crée ainsi une relation commerciale classique ; si elle ne l'honore pas, elle utilise les données bancaires capturées pour un autre usage.
L'argent gagné par l'organisation vendant des contrefaçons restant dans un cadre illégal, elle devra le blanchir. A ce titre, elle pourra encore une fois utiliser les services proposés par le botmaster en envoyant une campagne d'emails pour recruter des *money mules (A noter que le terme de mule désigne dans le langage courant une personne transportant de la drogue d'un pays à l'autre, et parfois à son insu.)*. Une money mule est une personne physique acceptant – contre forte rémunération – d'effectuer des opérations bancaires pour le compte d'une entreprise : ces opérations bancaires permettent à l'entreprise de blanchir des sommes d'argent, et la money mule prend à son insu toutes les responsabilités légales relatives à cette opération.

Mort d'un botnet

Étant donné le rôle essentiel donné aux serveurs de contrôle et de commande, le démantèlement d'un botnet passe par la mise hors service de ces derniers, et cette opération nécessite une intervention des autorités auprès des sociétés hébergeant les serveurs de contrôle et de commande.
On pourra ainsi citer le cas du botnet Bredolab, qui le 25 octobre 2010, a été fortement affaibli suite à la saisie par les autorités hollandaises de 143 serveurs auprès de l'hébergeur hollandais LeaseWeb. Toutefois, le botnet est toujours en vie, grâce à la présence d'autres serveurs de contrôle et de commande en Russie et au Kazakhstan.
Autre exemple: le botnet Grum, qui a été complètement démantelé en juillet 2012, avec des opérations menées conjointement par les autorités en Hollande, au Panama et en Ukraine.
La capacité à mettre hors service un botnet est par conséquent principalement conditionnée par la bonne volonté des autorités des pays où sont hébergés les serveurs de contrôle et de commande : la problématique n'est plus d'ordre technique, mais d'ordre juridique et politique.

Lien : http://www.sih-solutions.fr/les-botnets-acteurs-majeurs-de-lombre/

Le blanchiment d'argent par Bitcoin sera plus facile grâce à Dark Wallet

Un collectif de codeurs est sur le point de lancer Dark Wallet, un logiciel de portefeuille Bitcoin qui vise à protéger l'identité de son utilisateur dans le cadre de ses transactions financières.
Si Dark Wallet fonctionne tel que promis, ce logiciel pourrait s'avérer être un véritable cauchemar pour les organismes de surveillance financière qui tentent par tous les moyens d'empêcher que le Bitcoin ne devienne la monnaie d'échange des blanchisseurs d'argent et du marché noir.
Car contrairement à ce que l'on pourrait croire, les transactions de Bitcoins sont loin d'être anonymes. Chaque paiement effectué à l'aide de la populaire cryptomonnaie est enregistré dans une base de données – le registre public, également surnommé Block Chain – qui stocke la totalité des transactions financières passées. Avec cette information, il est donc possible de connaître à quelle adresse (ou dans quel portefeuille) un Bitcoin spécifique a été logé à n'importe quel moment de son histoire,

et par conséquent retracer les dépenses de ses anciens propriétaires. À moins que ceux-ci n'aient pris des dispositions afin de masquer leurs activités.
Et c'est justement l'objectif de Cody Wilson et Amir Taaki, les créateurs de Dark Wallet. Le plus aberrant dans toute cette histoire, c'est que ces derniers ne tentent pas de minimiser le risque que leur outil puisse servir aux transactions douteuses – ils en font plutôt la promotion. «C'est carrément un logiciel de blanchiment d'argent», a affirmé Wilson dans le cadre d'un débat sur le sujet en mars dernier.
En dépit de ces provocations, les organismes de surveillance financière sont généralement restés muets au sujet de l'initiative. Par contre, l'agence américaine luttant contre le blanchiment d'argent et le financement du terrorisme, le Financial Crimes Enforcement Network, a déclaré au magazine *Wired* qu'elle est «bien consciente des nombreux efforts technologiques émergents visant à renverser la transparence financière» et qu'elle restera «vigilante à l'égard de toute activité pouvant faciliter au blanchiment d'argent et à d'autres délits financiers».
Dark Wallet est le fruit d'une campagne de sociofinancement sur Indiegogo qui s'est déroulée en octobre dernier. Le logiciel parvient à tromper le Block Chain grâce à une technique nommée CoinJoin : chaque fois qu'un utilisateur dépense des Bitcoins, sa transaction est combinée avec celle d'un autre utilisateur de Dark Wallet choisi au hasard. Les deux transactions sont ainsi enregistrées comme une seule dans le registre public, et puisque la négociation de cette transaction bipartie est cryptée, il est pratiquement impossible de déterminer combien de Bitcoins ont été transigés et par quel portefeuille.
Bien que l'application puisse être politiquement incorrecte, elle n'est pas illégale pour autant. Wilson et Taaki défendent leur démarche en implorant le Premier amendement de la Constitution américaine qui garantit la liberté d'expression. Mais Wilson ne peut s'empêcher d'être honnête. «Je veux [que ce soit un] moyen pour permettre des transactions privées sur le marché noir, que ce soit pour des inhalateurs de médicaments sans prescription, du MDMA pour les amateurs de drogues, ou des armes.»
Il ne nie pas non plus que Dark Wallet pourrait provoquer des crimes beaucoup plus odieux, comme la pornographie juvénile, les tueurs à gages et le terrorisme. «Eh bien, oui, de mauvaises choses vont inévitablement se produire sur ces marchés», raconte Wilson. «La liberté est une chose dangereuse.»
Lien : http://branchez-vous.com/2014/04/30/le-blanchiment-dargent-par-bitcoin-sera-plus-facile-grace-dark-wallet/

Comment le Bitcoin a permis l'explosion des ransomwares

Les systèmes de paiement via Bitcoin ont de nombreux usages légitimes. Mais comme beaucoup d'autres technologies, ils ont également été exploités par les cybercriminels pour extorquer de l'argent.
Le ransomware est en plein boom. CryptXXX, Locky ou les centaines d'autres variantes de malware chiffrant les données permettent aux cybercriminels de récupérer des centaines de milliers de dollars en extorquant les utilisateurs infectés par ce type de malware et qui souhaitent récupérer l'accès à leurs données.
Les experts en cybersécurité considèrent que les ransomware représentent aujourd'hui la cybermenace la plus problématique. L'attaque la plus tristement célèbre est celle ayant visé le Hollywood Presbyterian Center, lorsque le service de l'hôpital de Los

Angeles a été contraint de déclarer une « urgence interne » après que son système d'information a été bloqué par une attaque de cybercriminels exigeant une rançon.
La plupart des demandes de rançons sont exigées en bitcoins, la cryptomonnaie basée sur les technologies de blockchains. Celle-ci offre un système de paiement sécurisé, souvent difficile à pister. La monnaie parfaite pour ceux qui souhaitent procéder à des transferts d'argent dissimulés.

Les moyens de paiement anonymes jouent en faveur des cybercriminels

La popularité du Bitcoin est en pleine croissance ces dernières années et le ransomware a connu une véritable explosion en 2016. Ces deux phénomènes peuvent-ils être liés ?
« Cela aide, je pense qu'on ne peut pas le nier. L'existence de moyens de paiement anonymes joue définitivement en faveur des cybercriminels » explique David Emm, chercheur en cybersécurité au sein de Kaspersky Lab.
Néanmoins, les extorsions en ligne n'ont pas attendu l'arrivée du Bitcoin pour se développer. Emm rappelle ainsi que certains cybercriminels ont notamment eu recours au système postal pour recevoir des paiements liés à des escroqueries s'appuyant sur des virus.
« Ça ne fonctionnait pas vraiment, car la police pouvait assez simplement surveiller les boîtes postales et arrêter les personnes venant récupérer leurs contenus », poursuit Emm.
Ces échecs ont poussé les cybercriminels à se tourner vers les outils de paiement en ligne, en utilisant des services tels que Western Union ou Paypal pour récupérer les sommes versées par les victimes de certains programmes malveillants. Mais ces différents systèmes sont systématiquement liés à un compte bancaire, ce qui permet aux autorités de retrouver leur trace.
La campagne du ransomware Cerber est un des exemples ou les paiements en Bitcoin étaient transférés via plusieurs portefeuilles bitcoins différents. Une technique de blanchiment d'argent qui permet aux cybercriminels de couvrir leurs traces.
« Nous avons vu des dizaines de milliers de bitcoins transférés vers une seule même adresse. À partir de là, les sommes sont à nouveau transférées vers des milliers d'adresses bitcoins différentes. Cela s'appelle un « mixing service » et c'est assez courant avec le bitcoin » précise Maya Horowitz, group manager des opérations renseignement chez Checkpoint.
« Si vous souhaitez récupérer de l'argent dans un seul portefeuille, mais que vous ne souhaitez pas que l'on puisse tracer l'argent, vous aurez recours à ce type de service. L'argent est reparti, puis revient par la suite vers vous, mêlé à d'autres paiements » ajoute-t-elle.
La capacité à rester sous le radar est la principale raison poussant les cybercriminels à avoir recours au Bitcoin. « Cela permet d'échapper bien plus facilement aux services de police » explique Maya Horowitz. Elle explique que lorsque les cybercriminels convertissent les bitcoins vers une autre monnaie, les autorités sont parfois capables d'établir un lien entre le portefeuille et un compte en banque et de retrouver les cybercriminels. « Cela arrive de temps en temps, surtout si les cybercriminels n'ont pas recours aux « mixing services » : les autorités sont alors capables de remonter jusqu'à la personne et de procéder à son arrestation » ajoute-t-elle.

Le Bitcoin "permet d'échapper bien plus facilement aux services de police"

Les Bitcoins permettent de rester anonymes, mais permettent également de transférer directement l'argent extorqué dans les mains des criminels. Un avantage que d'autres formes de cybercrime financier, tel que les trojans bancaires, n'offrent pas. Dans le

cas d'un trojan bancaire, il y aura toujours une trace de la transaction frauduleuse, qui peut offrir suffisamment de détails pour remonter jusqu'au coupable.
« C'est une des raisons qui pousse les cybercriminels à se tourner vers le ransomware. C'est tout simplement plus simple pour eux de fonctionner uniquement avec des bitcoins » explique Maya Horowitz.
L'utilisation de bitcoins offre également d'autres avantages. Cette méthode est bien plus flexible que les systèmes de paiement en ligne traditionnels, qui nécessitent généralement des détails financiers ou des informations de connexion pour être utilisés. Si les cybercriminels estiment que leur campagne a été un succès ou que les autorités pourraient tenter de les arrêter, ils peuvent simplement récupérer l'argent et passer à autre chose.
« Dans le monde d'aujourd'hui, particulièrement avec les facilités de paiement en ligne, n'importe qui peut facilement devenir l'équivalent de Del boy. Vous vous déplacez avec votre mallette, vous vous installez, puis lorsque vous apercevez la police à l'horizon, vous décampez » résume David Emm. « Vous développez une méthode d'attaque en particulier, puis lorsque vous estimez que celle-ci a rapporté suffisamment d'argent, vous disparaissez et vous pouvez réapparaître avec une nouvelle adresse de paiement. Cette fluidité et la rapidité de l'opération leur permet de se dissimuler bien plus facilement » ajoute-t-il.
Mais si le bitcoin a effectivement permis dans une certaine mesure le développement du ransomware, il n'est pas l'unique raison de cette croissance. La nature spécifique du Bitcoin a néanmoins incité les cybercriminels à s'en emparer, tout comme ils ont pu le faire avec d'autres technologies d'anonymisation telles que Tor.
« La réalité, c'est que les cybercriminels utiliseront toujours ce qui est disponible. Dans une certaine mesure, ils sont incroyablement paresseux : si le Bitcoin n'existait pas, ils trouveraient un autre moyen de réceptionner les paiements. Mais l'existence de ce système est l'outil parfait pour qu'ils puissent mettre la main sur ces flux financiers » explique Greg Day, directeur et RSSI chez Palo Alto Network.
On pourrait au final considérer qu'Internet a été un énorme cadeau fait aux criminels. Ceux-ci ont pu profiter du développement des malwares, des trojans bancaires, et développer de nombreuses activités illégales sur le dark web. Le Bitcoin n'est que le dernier venu d'une longue série de technologies qui ont profité au monde dans son ensemble tout en donnant dans le même temps aux réseaux criminels. 23 Août 2016
Lien : **http://www.zdnet.fr/actualites/comment-le-bitcoin-a-permis-l-explosion-des-ransomwares-39840980.htm**

Japon:
Le bitcoin n'est pas une monnaie
et les gains liés doivent être imposables

Le bitcoin "n'est pas une monnaie" et les gains afférents sont imposables, estime le gouvernement japonais.
Selon un document approuvé vendredi en conseil des ministres et commenté par le porte-parole Yoshihide Suga, le Japon ne reconnait pas le bitcoin comme une monnaie et les gains qui y sont liés seront désormais imposables**.** Selon ce texte, les autorités n'accordent au bitcoin que le statut de "chose" qui ne peut en outre être prise en charge par les banques commerciales, précise aussi cette déclaration préparée en réponse à une question d'un parlementaire de l'opposition.

Cette évolution dans la position des autorités japonaises face au bitcoin, qui existe depuis 2009, découle de la faillite récente d'une des plates-formes d'échange**,** MtGox, installée au Japon.

Taxer les bénéfices des investissements en Bitcoins

"Il est naturel" que le ministère des Finances s'interroge sur la possibilité d'imposer les transactions en bitcoins, a commenté Suga. Selon les médias, l'Agence des impôts tend en effet à considérer que la taxe sur la consommation (équivalent de la TVA française) doit être payée pour des achats réglés en bitcoins**.**

Ainsi, les impôts sur les sociétés doivent être acquittés pour les firmes qui en profitent, de même que devraient être taxés les bénéfices que des particuliers tirent d'investissements en Bitcoins.

Lien : http://www.rtl.fr/actu/conso/japon-le-bitcoin-n-est-pas-une-monnaie-et-les-gains-lies-doivent-etre-imposables-7770221805

Le fisc américain ne reconnaît pas le bitcoin comme monnaie

Tout en estimant que le bitcoin n'est pas une monnaie réelle, l'administration fiscale américaine considère qu'il doit être imposable.

Pour la première fois, les autorités fiscales américaines se sont penchées sur le statut du bitcoin. Le fisc américain ne reconnaît pas le bitcoin comme monnaie mais comme un actif susceptible d'être soumis à l'impôt, selon une note consultée par *l'AFP*. "Les monnaies virtuelles peuvent être utilisées pour acheter des biens et des services ou être stockées comme investissement (...) mais elles n'ont pas de valeur légale", a assuré le fisc américain (IRS). La plus connue d'entre elles, le bitcoin, sera donc traitée comme un "bien" et les plus-values qui en sont tirées seront imposées comme les gains sur le capital**.**

Le bitcoin soumis à l'impôt

D'éventuels salaires versés en bitcoin seront par ailleurs soumis à l'impôt sur le revenu en calculant sa valeur au moment où la transaction a été accomplie, a précisé l'IRS. Les paiements effectués avec cette monnaie virtuelle seront eux aussi concernés. Créé en 2009 et échangé de gré à gré, le bitcoin traverse une profonde crise de confiance liée à la fermeture de l'une de ses principales plateformes d'échanges, victime d'une attaque informatique.

Lien : http://www.rtl.fr/actu/international/le-fisc-americain-ne-reconnait-pas-le-bitcoin-comme-monnaie-7770748393

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 : installation d'un programme malveillant
– Produits Logiciels malveillants (Ransomware/Crypter,Exploits).
Faux papiers, armes, drogues, carding et skimming (pour escroquerie et piratage de CB)
Données personnelles : emails, CB française volée ou le compte Paypal, 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.
Lien : http://www.journaldugeek.com/2015/06/09/prix-donnees-black-market/

Un nouveau système de paiement électronique a été dévoilé à des banquiers lors d'une réunion secrète à New York

Le mois dernier, une « réunion secrète » qui avait impliqué plus de 100 cadres supérieurs de certaines des plus grandes institutions financières aux États-Unis a eu lieu à New York. Au cours de cette « réunion secrète », une société connue sous le nom « Chain » a dévoilé une technologie qui transforme les dollars américains en véritables «actifs numériques». Selon les témoignages, il y avait des représentants du Nasdaq, de Citigroup, Visa, Fidelity, Fiserv et Pfizer dans la salle, et « Chain » revendique aussi d'être en partenariat avec Capital One, State Street et First Data. Cette technologie «révolutionnaire» est destinée à changer complètement la façon dont nous utilisons l'argent, et cela représenterait une étape importante vers une société sans numéraire et donc sans argent liquide. Mais si ce nouveau système de paiement électronique est un tel progrès et est si bénéfique pour la société, pourquoi a t-il été dévoilé au cours d'une réunion secrète pour les banquiers de Wall Street ? Y a t-il plus d'enjeux qu'on veut bien nous le dire ?
Aucun d'entre nous n'aurait probablement jamais entendu parler de cette réunion secrète, s'il n'y avait pas eu cette publication de Bloomberg. Ce qui suit provient de leur article intitulé « Au sein de la réunion secrète Où Wall Street a testé une monnaie numérique »…
Un Lundi, récemment au mois d'Avril, plus de 100 cadres supérieurs de certaines des plus grandes institutions financières au monde se sont réunies à une réunion privée dans un bureau du NASDAQ sur Times Squares. Ils n'étaient pas venus là pour simplement parler de la technologie blockchain (chaîne de blocs), cette nouvelle technologie dont certains prédisent qu'elle va transformer la finance, mais pour développer et tester cette technologie par le biais d'un logiciel.

A la fin de la journée, ils avaient tous vu quelque chose de révolutionnaire: des dollars américains transformés en véritables actifs numériques, capables d'être utilisés instantanément dès l'ouverture d'un commerce. Voilà la promesse d'un blockchain, où le système actuel complexe, lourd, susceptible d'entraîner des erreurs, qui prend des jours pour transférer de l'argent à travers la ville ou dans le monde entier est remplacé instantanément par un nouveau système quasi sûr et qui répond en temps réel.

Ce n'est donc pas seulement Michael Snyder rédacteur en chef du Blog de l'effondrement économique qui fait référence à cette «réunion secrète». C'est dorénavant expliqué par Bloomberg. Et je pense qu'il y a une bonne raison pour laquelle cette réunion se soit tenue en secret, parce que le grand public serait certainement alarmé par ce pas de géant vers une société sans argent liquide.

Bien que l'argent déposé sur un compte bancaire se déplace déjà électroniquement et constamment aujourd'hui, il y a une différence entre ce système actuel et la monnaie numérique (monnaie virtuelle). Les paiements électroniques actuels sont en réalité des messages avertissant que l'argent a besoin de passer d'un compte à un autre, et ce mode de fonctionnement est lent puisqu'il prend du temps durant le processus de paiement. Pour les clients, transférer de l'argent entre les comptes peut prendre des jours puisque les banques attendent des confirmations. En revanche, les dollars numériques sont pré-chargés dans un système tel qu'un blockchain (chaîne de blocs). Ainsi, ils peuvent être échangés quasiment instantanément contre n'importe quel actif.

« Au lieu d'attendre à chaque réception et à chaque confirmation de paiement, ce qui correspond au dispositif actuel», a déclaré Ludwin. « Le paiement et le règlement et donc les échanges s'effectueraient quasiment en temps réels. »

Pourquoi serait-ce si alarmant d'assister à un basculement majeur vers une société sans cash. En Suède, 95 % de toutes les transactions se font déjà sans argent liquide, et les distributeurs automatiques de billets sont retirés par centaines. Au Danemark, les représentants du gouvernement ont en fait un objectif déclaré de « supprimer l'argent liquide » d'ici 2030. Et en Norvège, la plus grande banque du pays a publiquement appelé à supprimer totalement l'argent liquide.

D'autres pays en Europe ont déjà interdit les transactions en liquide dépassant un certain montant….

Comme je l'avais écrit précédemment, les transactions en espèces de plus de 2.500 euros ont déjà été interdites en Espagne, et récemment la France comme l'Italie ont interdit toutes les transactions liquide de plus de 1.000 euros.

Peu à peu, l'argent liquide disparaît, et ce que nous avons vu jusqu'à présent n'est que le début. 417 milliards de transactions électroniques ont été réalisées en 2014, et le nombre total pour 2015 devrait être beaucoup plus élevé.

Cette pression mondiale vers une société sans argent liquide va s'intensifier, parce que les banques et les gouvernements ont vraiment envie de voir l'idée d'un tel système s'installer.

es banques aiment vraiment ce concept d'une société sans argent liquide qui forcerait tout le monde à devenir leurs clients de façon contrainte. Ainsi, personne ne pourrait plus cacher son argent sous le matelas à la maison ou essayer de payer toutes ses factures avec de l'argent liquide. Cela éviterait par la même occasion d'assister à des ruées devant les banques en cas de faillite bancaire car plus personne ne pourrait ainsi retirer d'argent liquide puisqu'il n'en n'existerait plus. Avec ce système d'une société sans cash, nous serions tous dépendants des banques, et elles gagneraient beaucoup d'argent en raison des frais qu'elles collecteraient au travers des transactions liées à l'utilisation des cartes de crédit et de débit.

Les gouvernements voient beaucoup d'avantages dans une société sans argent liquide. Du coup, ils nous expliquent qu'ils seraient en mesure d'agir contre les trafiquants de drogue, les fraudeurs fiscaux, les terroristes et contre le blanchiment d'argent, mais la vérité est que cela leur permettrait d'observer, suivre, surveiller et contrôler la quasi-totalité de nos transactions financières. Nos vies deviendraient des livres ouverts pour les dirigeants et gouvernements, et la vie privée financière serait quelque chose qui appartiendrait définitivement au passé.

En outre, des formes variées de contraintes et de tyrannies dans un tel scénario sont évidentes.

Imaginez un monde où votre gouvernement pourrait jouer le rôle de juge et d'arbitre sur ceux qui seraient autorisés ou non à utiliser le système sans cash. Il pourrait exiger que nous nous soumettions à une forme d'identification qu'elle aurait elle-même crée avant que vous ne soyez autorisé à utiliser ce système imposé, et il est même concevable qu'une sorte de serment de fidélité (des règles) serait nécessaire.

Bien sûr, si vous ne soumettez pas à leurs demandes, vous ne pourrez pas acheter, vendre, ouvrir un compte bancaire ou obtenir un emploi sans accès à leur système sans cash.

Espérons que les gens puissent comprendre vers où le monde se dirige. L'argent liquide est un droit fondamental de notre liberté, et si ce droit nous est retiré alors cela ouvrira la porte à toutes sortes d'abus.

Même maintenant, l'utilisation de l'argent liquide devient petit à petit un acte criminel aux Etats-Unis. Par exemple, si l'argent liquide est utilisé pour payer une chambre d'hôtel, c'est alors considéré par les autorités fédérales comme étant une « activité suspecte » qui devrait être signalée au gouvernement. Bien sûr, il n'est pas encore illégal de payer sa facture d'hôtel en liquide pour l'instant, mais selon le gouvernement, c'est la méthode utilisée par les «terroristes» et cela doit donc être surveillé de près.

Il ne faut pas beaucoup d'imagination pour voir vers où nous nous dirigeons. Et pour ceux d'entre nous qui comprennent où en est la situation actuelle, tout ceci explique clairement qu'il est déjà trop tard.

Lien : http://www.businessbourse.com/2016/05/03/un-nouveau-systeme-de-paiement-electronique-a-ete-devoile-a-des-banquiers-lors-dune-reunion-secrete-a-new-york/

Les pirates capables de voler des données même si votre ordinateur est éteint et pas connecté

1) **Lorsque des institutions gouvernementales ou des entreprises souhaitent stocker des informations confidentielles, ils utilisent le plus souvent un réseau en « air-wall », déconnecté d'internet, et isolé de toute connexion extérieure.**

Récemment pourtant, plusieurs chercheurs ont démontré qu'il était possible, une fois ce réseau contaminé par un virus spécifique, d'en récolter les données.

Bien que les particuliers soient sans doute moins la cible de ce type d'attaque informatique, sont-ils tout aussi vulnérables ?

En tant que particulier, nous sommes encore plus vulnérables à ce type d'attaque ou d'infiltration qui, une fois installé sur une machine permet d'y revenir et de se servir. Nous avons en effet moins penser la sécurité de nos données par rapport à une entreprise par exemple mais le risque demeure le même voire même plus grand. Le ver installé sur un PC, il est en effet possible de faire ce que l'on veut, de s'installer

confortablement et d'y revenir à sa guise. Une des seule façon de pirater un PC éteint serait d'être en rapport avec la C-MOS et nécessiterait donc un accès physique à la machine. Ce n'est donc à la portée du premier venu.
Comme pour votre Webcam éteinte il est tout aussi possible d'en prendre la main à distance et certains vont même jusqu'à utiliser un cache ou collant qu'ils posent sur le Webcam pour s'en protéger. Un ordinateur quand il est éteint c'est juste la boite d'alimentation qui est éteinte mais la carte mère continue à recevoir de l'énergie. (Un voyant lumineux au niveau de la carte mère est toujours présent). Il est donc toujours plus prudent de débrancher totalement son ordinateur et surtout de ne pas le laisser en mode veille ou veille prolongée. Il est également possible si l'on veut se protéger totalement de fermer son boîtier Wifi mais attention aux mises à jour qui se font parfois la nuit sur ces matériels.

2) Qu'est ce qui peut-être récupéré ? Qu'est ce que ces pirates informatiques sont dans la mesure de faire par ce type de procédé ?

Une fois dans la machine, on peut tout faire avec quelques manipulations que connaissent bien ces hackers. A la base il y a quelques années, le but était simplement d'avoir pu infiltrer ou craquer une machine.
Aujourd'hui, ce sont tous vos contacts de messagerie, les fichiers stockées, les mots de passe qui peuvent être récupérés par exemple au même titre que tous les documents personnels. Il n'y a donc pas de limites.
Tous ces éléments pourraient se retrouver un jour sur la toile et servir par exemple dans le cas d'adresses de messagerie servir à des banques de données réutilisées par la suite pour faire des envois en masse comme cela se pratique dans le cas des mails nigérian.
Prendre la main sur votre machine revient à avoir la clé de votre domicile, le code de votre alarme et tout peut alors être envisagé en vue de vous voler des informations et des accès à des sites que vous utilisez et sur lesquels vous passez des actes d'achat par exemple. Aujourd'hui on parle même de vol de données qui pourraient vous faire chanter.

3) Quel est le niveau d'informatique nécessaire pour mettre en oeuvre correctement cette pratique ? Des solutions simples sont-elles mise à la disposition des amateurs ?

Dés que ces cybercriminels ont réussi à installer un virus ou un cheval de Troie (souvent aussi nommé malware ou logiciel malveillant) votre ordinateur devient une source potentielle de revenus. ils auront accès à toutes vos données personnelles (messages, mails, documents bancaires, mots de passe, photos, vidéos, …) stockées sur votre disque dur et pourront surveiller votre activité sur Internet et sur votre machine
Aujourd'hui pas besoin d'être un grand expert sur le sujet en dehors de quelques types d'infiltrations spécifiques sur des sites dits plus sécurisés. En effet, malheureusement beaucoup d'aide est apportée aux cyberdélinquants par Internet.. Des solutions contenues dans certains forums permettent à des petites mains de se lancer tout d'abord dans le cadre d'arrêt d'une machine en réseau dans une entreprise. Petit à petit, pirates, hackers ou encore crackers découvrent les modes opératoires des plus grands pour se les approprier et pour aller plus loin comme s'il y avait un concours entre eux.

4) Comment s'en prémunir ? Doit-on se résigner à avoir un ordinateur vierge de toute connexion à internet, avec des protocoles de sécurité stricts -comme par exemple ne pas utiliser de clé usb étrangère et ne pas prêter les siennes- ?

De plus en plus, il faudra apprendre à se protéger et à avoir une culture sécuritaire en

ce qui concerne les matériels que nous utilisons et que nous connectons à notre PC car ils seront autant de sources et de moyens d'attaque pour ces délinquants.
Tout ce qui est installé, introduit et (télé)chargé sur nos machines doit faire l'objet d'une sorte de scan ou contrôle si l'on veut rester dans une protection plus sereine. Nous en sommes loin aujourd'hui quand nous validons la mise à jour d'un logiciel sans être sûr qu l'envoi émane de la société en question. Certains internautes ont découvert tardivement que des exécutables s'étaient installés sur leur PC mais n'ont pu en mesurer l'impact sur leurs données, logiciels, etc.
L'objectif premier du hacker va être d'installer un virus ou un cheval de Troie sur votre ordinateur. Il se présente simplement sous la forme d'un exécutable (par exemple .exe), soit installé suite à l'attaque d'un de vos logiciels mal configurés ou obsolètes (la version installée n'est pas la dernière et contient donc des failles de sécurité). Ces failles sont en général la conséquence d'un bug de programmation dans l'application qu'un hacker saura mettre à profit pour prendre le contrôle de votre ordinateur.
Ces logiciels sont très nombreux en voici quelques uns à titre d'exemple :

- Microsoft Windows, bien sûr ;
- Les suites bureautiques (Microsoft Office, OpenOffice) ;
- Les navigateurs (Internet Explorer, Firefox, Chrome, Opera, Safari, …) ;
- Les logiciels multimedia (Acrobat Reader, Flash, Shockwave, Windows Media Player, Quicktime, RealPlayer, WinAmp, iTunes, VLC,);
- Les messageries instantanées (Windows Messenger, Pidgin, …) ;
- Java ;

On a pu ainsi découvrir des cas de figure où les PC des internautes sont devenus des serveurs à leur insu se voyant alors stocker à des jours et des heures des données de personnes malveillantes qu'ils ne pouvaient alors contrôler sur leur propre machine.
De même d'autres ont accepté avec trop de simplicité et de naïveté une clé USB offerte avant l'entrée dans un salon ou symposium. Le but étant de garder la clé mais pas son contenu, ils ont ouvert cette dernière sans penser à l'exécutable qui allait s'installer sur la machine et qui allait devenir un moyen d'infiltration sans limite pour l'offreur.
Certaines applications sur ces clés vont même pendant qu'un tiers tente de recopier un fichier à partir de votre machine scruter votre PC pour lui sous-tirer tous vos contacts et ce que vous pouvez imaginer avec sans vous garantir qu'il n'aura pas pris la main sur votre PC pour y revenir ultérieurement.

5) Comment savoir si notre ordinateur est infecté par ce type de virus ? Comment s'en apercevoir ?

Assurez vous tout d'abord d'avoir la bonne dernière version officielle de vos logiciels et pensez à utiliser des solutions comme Anti Hacks qui détectera les problèmes de configuration et les logiciels obsolètes sur votre machine et qui, surtout, se chargera de configurer automatiquement les logiciels et vous aidera à les mettre à jour.
Ensuite un anti-virus que vous mettrez à jour tous les jours et pas à la petite semaine comme le font la plupart d'entre nous (Beaucoup utilisent celui offert pour une période donnée par le fournisseur du PC mais oublient de le changer ou de l'actualiser dans le temps se retrouvant alors sans protection)
En attendant :

- surveillez vos barres d'outils et les liens que vous n'auriez pas ajouter personnellement
- contrôlez votre pointeur de souris qui à certains moments se déplacerait de façon inattendue

- regardez l'adresse URL du site que vous consultez car il pourrait changer lors d'une transaction financière par exemple
- Veillez aux fenêtres intempestives qui s'affichent sur votre PC sans que vous n'interveniez et aux pages qui s'installent en arrière plan et que vous ne découvrez qu'une fois que vous fermez votre session Internet ou machine. Elles pourraient bien être la source d'un début d'installation d'une cyber-surveillance
- Enfin si tout va plus lentement sur votre ordinateur pensez à contrôler les fichiers qui se lancent au démarrage et surtout n'oubliez pas que le meilleur anti-virus est parfois de remettre à plat tous les six mois votre PC !!!

Lien : https://cybercriminalite.wordpress.com/2014/12/08/les-pirates-capables-de-voler-des-donnees-meme-si-votre-ordinateur-est-eteint-et-pas-connecte/

Comment lutter contre la fraude documentaire ?

Dans l'Hexagone, 3 à 6% des 10 millions de documents d'identité émis tous les ans par l'état (passeport ou Cartes Nationales d'Identité) seraient frauduleux et établis sur la base de faux documents. Selon l'ONU, la fraude identitaire au niveau mondial coûterait 7 600 milliards de dollars ! Dans ce contexte, il s'avère de plus en plus stratégique pour les entreprises et les institutions de maîtriser tous les moyens de prévention et de détection de la fraude documentaire.

La fraude documentaire en quelques chiffres

50% de ces fraudes sont liées à l'utilisation d'identités fictives, 30% sont des usurpations d'identité, 20% des substitutions (on "loue" sa carte vitale ou sa carte d'identité).

Si en France, les forces de l'ordre confisquent environ 10 000 fausses pièces d'identité par an, ces chiffres fluctuent à la hausse ou à la baisse. Il est actuellement difficile de déterminer si une baisse des saisies correspond à une baisse réelle du nombre de faux documents en circulation ou à une meilleure qualité de production de ces faux documents, ce qui les rendraient plus difficiles à détecter.

Selon le Reso-Club, le préjudice de la fraude documentaire en France est aujourd'hui estimé à 20 milliards d'euros dont 17 milliards au seul détriment de l'Unedic. Ces chiffres confirment que nous sommes confrontés à un phénomène de masse, qui a des répercussions sur l'ensemble de notre écosystème : l'entreprise, le citoyen et l'Etat.

Il existe des solutions efficaces mais elles ont un coût…

Des experts du contrôle documentaire sont aujourd'hui capables de détecter tous les faux documents existants. Ils s'appuient sur une solide connaissance des sécurités documentaires, une maîtrise des techniques utilisées par les faussaires ainsi que sur des outils reconnus (compte fil, loupe binoculaire, éclairage spécifique). Chacun de ces experts peut traiter en moyenne 200 documents par an, ce qui correspond à un coût de revient de l'ordre de 1000 € par contrôle. Au vu de cet impact financier, on imagine aisément que ces moyens ne peuvent être mis en œuvre que pour des usages ciblés : enjeux financiers importants, procédures judiciaires, etc.

Comment lutter contre la fraude documentaire quand le niveau de risque ne justifie pas un contrôle aussi onéreux ?

Si des solutions techniques existent, elles sont rarement déployées. La cryptographie apporte par exemple des solutions simples et quasiment infalsifiables. Ainsi, un simple code à barres 2D peut suffire pour certifier la validité d'un document et des informations qu'il contient.

Cette solution peut régler toutes les questions d'usurpation d'adresse. Si plusieurs grands "producteurs" de justificatifs de domicile ont annoncé qu'ils intègreraient cette technologie dans leurs factures, seul un opérateur de téléphonie l'a déployée à ce jour.
La France est également l'un des rares pays à ne pas proposer de référentiel des cartes d'identités. Dans la plupart des pays d'Europe, vous pouvez saisir sur un site dédié le numéro d'une carte d'identité. Grâce aux informations qui figurent sur le document, le système en ligne vous indique s'il s'agit d'un document authentique.
En 2013, la délégation nationale à la lutte contre la fraude prévoyait également la généralisation de cette solution pour 2014 et la mise en place d'un dispositif Checkdoc de contrôle en ligne de la validité des pièces d'identité pour le début de l'année 2015. Nous en sommes encore loin…
Même si le certificat numérique personnel est un dispositif de cryptographie très performant qui permettrait à son détenteur de prouver son identité, de signer électroniquement des documents ou encore de crypter des échanges de données, son utilité en termes de lutte contre la fraude documentaire dépend directement de la sécurité de sa procédure de délivrance.
En attendant que des solutions performantes soient déployées à grande échelle, il existe néanmoins des solutions pragmatiques pour répondre aux enjeux de la fraude documentaire :

- l'utilisation des sécurités existantes telles que les sécurités visuelles : zones MRZ valides par exemple (bande d'information codée que l'on trouve au bas de nos CNI, permis de conduire, passeports, titres de séjour et autres cartes grises et qui comporte des clés de contrôle). Si le contrôle de validité des zones MRZ n'assure pas un niveau de sécurité très élevé, c'est déjà un début.
- la détection des doublons. Dans certaines fraudes documentaires, une même facture EDF peut être utilisée plusieurs dizaines de fois avec des « habillages » différents. Un réseau d'alerte est aujourd'hui capable de détecter ces doublons et de les signaler aux préfectures. Cette détection pourrait être systématisée et mise à disposition de toutes les personnes concernées.
- le contrôle de cohérence. S'assurer que l'ensemble des pièces qui composent un dossier sont bien cohérentes entre elles permet de renforcer le niveau de sécurité d'un dossier.

Les contrôles de cohérence permettent aujourd'hui d'accélérer les processus d'acceptation des dossiers, d'optimiser les taux de transformation et d'augmenter la productivité des entreprises.
Ainsi, si la simple détection des zones MRZ permet de réduire les risques de fraude documentaire de 70%, le contrôle de cohérence de l'ensemble d'un dossier va contribuer à augmenter considérablement ce pourcentage.
Les contrôles de cohérence effectués par la solution Jouve Mobile Capture par exemple assurent la conformité d'un dossier que ce soit pour un document qui le constitue ou l'ensemble de celui-ci. L'ensemble des données (Etat civil, Adresse) des documents du dossier sont vérifiées et comparées, un pourcentage de similitude du dossier est alors fourni.
S'il n'existe pas de solution en ligne pour vérifier la validité d'une pièce d'identité Française, cette base existe néanmoins pour les comptes en banque. On peut ainsi vérifier si les coordonnées bancaires fournies par un utilisateur correspondent à la bonne identité.
Enfin, d'autres sécurités plus difficiles à contrefaire mais aussi à contrôler seront prochainement opérationnelles. Nous ne les détaillerons pas dans cet article afin d'éviter que les faussaires puissent anticiper leur arrivée mais elles sont prometteuses.

En conclusion, les services de l'Etat et les entreprises sont confrontés au problème de la fraude documentaire qui est en croissance continue et leur coûte cher. Tous ces acteurs devraient y faire face et mutualiser leurs investissements pour garantir rapidement des contrôles fiables et cohérents

Lien : http://www.jouve.com/fr/comment-lutter-contre-la-fraude-documentaire

Fraude documentaire: Comment les clandestins passent au travers des contrôles de police

La plus courte distance entre deux points est la ligne droite. Cet enseignement de géométrie élémentaire n'est pas l'axiome préféré des clandestins. Bien au contraire, les filières d'immigration illégales redoublent de créativité pour contourner les routes classiques encombrées de policiers. Certains Syriens, par exemple, n'hésitent plus à traverser l'Atlantique pour se rendre en Amérique latine avant de rejoindre l'Allemagne ou la France, via des vols internationaux moins suspects. Et donc moins contrôlés.

C'est pour connaître les nouvelles tendances de l'immigration clandestine et établir l'état des lieux de la fraude documentaire que la police aux frontières (PAF) organise un séminaire ce jeudi au siège de l'Organisation de coopération et de développement économiques (OCDE). Parmi les 180 invités figurent des représentants de polices voisines, d'organisations européennes comme Frontex ou Europol ainsi que des industriels spécialisés dans le contrôle et la sécurité des identités.

Plusieurs techniques

La fraude documentaire est au cœur de la problématique. Dans un cas sur deux, les filières clandestines ont recours à des faux papiers. Les techniques pour s'en procurer sont multiples :

- Faire appel à un faussaire qui reproduit plus ou moins bien un passeport ou une carte d'identité.
- Fabriquer de faux justificatifs qui permettent ensuite de se procurer, auprès des préfectures ou des mairies, un vrai titre d'identité.
- Voler l'identité d'une personne et tenter de se faire passer pour elle en imitant physiquement la personne.

« Certains rivalisent d'ingéniosité pour ressembler aux photos sur les passeports : teintures, effets de mode, cosmétique… », détaille auprès de *20 Minutes* Jean-Michel Brevet, chef du bureau de la fraude documentaire et à l'identité au sein de la direction centrale de la PAF. Cette technique du « look alike » (apparence similaire) est utilisée dans près d'un quart des fraudes mises à jour par les policiers. Du coup, ces derniers ont développé des techniques pour repérer les usurpateurs. Notamment aux frontières grâce à la méthode finlandaise de reconnaissance faciale qui consiste à sonder le visage en six parties (yeux, menton, front, cheveux…) afin d'obtenir une « vision globale plus précise », poursuit le commissaire.

Les filières les plus sophistiquées s'essayent frontalement aux nouvelles technologies. « Aujourd'hui, même les documents modernes en polycarbonate, avec des puces, sont attaqués », reconnaît Jean-Michel Brevet. Si les Thaïlandais ou les Pakistanais parviennent à imiter parfaitement des faux passeports, même biométriques, tous n'en sont pas capables.

Lien : http://www.20minutes.fr/societe/1627255-20150610-fraude-documentaire-comment-clandestins-passent-travers-controles-police

Factures, justificatifs, actes d'état civil : Les nouvelles cibles des faussaires

Les faussaires abandonnent les pâles copies de carte d'identité et privilégient désormais l'obtention indue de vrais documents grâce au vol de pièces justificatives… Ils sont 8% à déclarer avoir été victimes d'usurpation d'identité au cours des dix dernières années. Mais ils ne peuvent s'en prendre qu'à eux-mêmes. Car les Français laissent traîner trop d'informations derrière eux. Dans les poubelles, sur Internet, au travail… Ou ne déclarent pas assez systématiquement la perte de leurs papiers d'identité.

Sur les 30 millions de cartes nationales d'identité (CNI) en circulation, environ 3 millions d'entre elles seraient d'origine frauduleuse, soit 10%, soufflent les spécialistes de la question. Ce chiffre qui n'est pas officiel traduit l'ampleur du phénomène. Chaque année, le bureau de la fraude documentaire de la Police aux frontières (PAF) publie entre 60 et 80 fiches d'alerte pour avertir les services de l'administration et consulats sur des malfaçons.

Immigration clandestine

En raison de l'amélioration des techniques de protection sur les documents officiels (puces, hologrammes, biométrie…), les faussaires ont tendance à abandonner l'idée de les copier à l'identique. En revanche, la production de pièces justificatives, pour se faire délivrer une vraie-fausse carte d'identité, explose. Les fraudeurs vont tenter d'obtenir un vrai titre d'identité par les voies légales.

Actes d'état civil, justification de domicile, factures d'électricité… Tout papier officiel est bon à voler pour les fraudeurs qui s'en servent ensuite pour monter des dossiers et obtenir des papiers d'identité indus ou ouvrir des comptes en banque puis souscrire des crédits. Si bien que les enquêteurs de l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (Ocriest) saisissent régulièrement des dossiers prêts à être déposés en préfecture, en mairie ou dans les consulats. Un tel dossier complet peut être revendu environ 5.000 euros.

Le vol d'identité est certes le plus souvent en lien avec l'activité clandestine. Mais il peut aussi servir à récupérer un faux permis de conduire, ou éviter de le perdre en se procurant de fausses plaques d'immatriculation. Depuis 2008, les policiers ont constaté une augmentation de 50% de ces types de délit.

Lien : **http://www.20minutes.fr/societe/1234249-20131009-20131009-factures-justificatifs-actes-detat-civil-nouvelles-cibles-faussaires**

Société sans argent liquide,

Saviez-vous que 95 % de toutes les transactions en Suède se font sans argent liquide ? Et saviez-vous que le gouvernement du Danemark a pour objectif déclaré de « supprimer l'argent liquide » d'ici 2030 ?

Partout dans le monde, nous assistons à une marche inexorable vers une société sans numéraire, et c'est nulle part ailleurs plus vrai qu'en Europe du Nord. En Suède, des centaines de succursales bancaires n'acceptent plus de recevoir ou de distribuer de l'argent liquide, et des milliers de distributeurs automatiques de billets ont été définitivement retirés. Actuellement, les billets et les pièces ne représentent que 2 %

de l'économie suédoise, et de nombreux magasins ne prennent absolument plus l'argent liquide. L'idée d'une « société sans numéraire » était autrefois considérée comme de la science-fiction, mais maintenant, on nous raconte que c'est « inévitable », et les autorités insistent même en nous expliquant que cela leur permettra de combattre les criminels, les terroristes, les trafiquants de drogue, le blanchiment d'argent et autres fraudeurs fiscaux. Pourquoi abandonnerions-nous ce processus ?

En Suède, la transition vers une société sans argent liquide est accueillie avec enthousiasme. Ce qui suit est l'extrait d'un article du New York Times, qui a été publié le samedi 26 décembre 2015…

Les paroissiens peuvent transmettent des dons électroniques par le biais d'une application à leurs églises. Les vendeurs à la sauvette portent des lecteurs de cartes de crédit. Même le Musée dédié au groupe Abba, en dépit d'être un sanctuaire pour le groupe de pop des années 1970 qui avait écrit le tube « Money, Money, Money », considère que les liquidités font partie du siècle dernier et n'accepte pas les billets et les pièces de monnaie.

Peu d'endroits dans le monde ne basculent aussi rapidement vers un avenir sans numéraire que la Suède. Ce pays est devenu accro aux paiements par cartes de crédit ou par le biais d'applications électroniques.

Pour moi, donner de l'argent par voie électronique à l'église me semble si bizarre. Mais c'est aussi en train d'arriver ici aux États-Unis. En Suède, certaines églises recueillent la plupart de leurs dons et offrandes de cette manière…

Récemment, un dimanche, lors d'un office religieux, le numéro de compte bancaire de l'église a été projeté sur un grand écran. les fidèles ont sorti leurs téléphones portables et ont effectué un don par le biais d'une application appelée Swish, un système de paiement mis en place par les plus grandes banques suédoises qui est en passe de devenir un système de paiement rival aux autres.

D'autres fidèles faisaient la queue devant un terminal bancaire spécial nommé « Kollektomat » , où ils peuvent transférer des fonds à diverses oeuvres de l'église.

L'an dernier, sur 20 millions de couronnes qui ont été recueillies au travers de dons, plus de 85 % provenaient de cartes bancaires et autres systèmes de paiement électroniques.

Et bien sûr, ce n'est pas juste la Suède qui bascule rapidement vers une société sans argent liquide. Au Danemark, les responsables gouvernementaux ont pour but « de supprimer complètement l'argent liquide » d'ici 2030…

La Suède n'est pas le seul pays à vouloir se débarrasser de la monnaie sonnante et trébuchante. Son voisin, le Danemark, avance également à grands pas vers une réduction de la circulation des billets dans le pays.

Il y a 20 ans, environ 80 % des citoyens danois utilisaient l'argent liquide lors de leurs achats. Alors qu'aujourd'hui, à l'aube de l'année 2016, ce pourcentage a considérablement chuté et atteint dorénavant 25 %.

« Nous souhaitons nous débarrasser des espèces », a déclaré Thomas Grane, directeur de Matas IT. « La gestion des espèces, les dispositifs de sécurité autour des billets et tout le reste coûte cher. Oui, nous voulons promouvoir le paiement numérique, et c'est bien sûr pourquoi nous venons d'introduire le paiement par téléphone mobile afin d'accélérer ce processus«.

Finalement, les établissements pourraient bientôt avoir le droit de refuser toute opération en numéraire ce qui est encore une pratique courante en Suède. Les représentants du gouvernement ont déjà fixé une date limite à l'année 2030 pour supprimer complètement d'ici là, la monnaie papier.

Pouvez-vous imaginer un monde sans argent liquide ?
Telle est pourtant la tournure que prennent les événements et en particulier en Europe. Comme je l'avais écrit précédemment, les transactions en espèces de plus de 2.500 euros ont déjà été interdites en Espagne, et récemment la France comme l'Italie ont interdit toutes les transactions en espèces de plus de 1.000 euros.
Peu à peu, l'argent liquide disparaît, et ce que nous avons vu jusqu'à présent n'est que le début. 417 milliards de transactions électroniques ont été réalisées en 2014, et le nombre total pour 2015 devrait être beaucoup plus élevé.
Les banques jubilent, car ce processus leur permet de faire toujours plus d'argent en raison des frais qu'elles collectent au travers des transactions liées à l'utilisation des cartes de crédit et de débit. Et les gouvernements apprécient aussi ce changement parce que les paiements électroniques leur permettent d'avoir la main et donc de suivre et de surveiller ce que nous faisons tous beaucoup plus facilement.
Actuellement, personne ne s'élève contre ce qu'il se passe. Au lieu de cela, la plupart d'entre nous semblent tout simplement accepter que ce changement soit « inévitable », et nous sommes sûrs que ce sera pour le meilleur évidemment… Et peu importe où que vous alliez dans le monde, la propagande semble être la même. Par exemple, ce qui suit provient d'une source d'informations australienne …
Et ainsi nous nous préparons à tourner la page de l'année 2015 et ouvrir celle de 2016, une année charnière dans laquelle l'Australie va accélérer le processus en vue de devenir véritablement une société sans numéraire.
La société sans numéraire sera un nouveau monde exempt de pièces de 1 et de 2 dollars ou de billets de 5 ou 10 dollars. Un nouveau monde dans lequel toutes les transactions commerciales, allant de l'achat d'un i-pad ou d'un hamburger en passant par les machines à sous, l'achat d'un journal, le paiement des factures ou les frais de pressing, seront payés par voie électronique.
Et dans ce même article, les lecteurs sont informés que l'Australie sera probablement « une société totalement sans argent liquide » en 2022 …
La banque Westpac prévoit que l'Australie sera une société complètement sans numéraire en 2022 – soit dans seulement 6 ans. Déjà la moitié de toutes les transactions commerciales s'effectuent actuellement par voie électronique.
Même dans certains des quartiers les plus pauvres au monde, nous assistons à une évolution vers une société sans numéraire. En 2015, les banques en Inde ont fait de grands progrès sur ce front, et des exonérations d'impôts sont envisagées par le gouvernement comme une incitation à « encourager les gens à éviter les transactions en espèces ».
Pensez-vous qu'une société sans numéraire puisse réduire la criminalité et faciliter notre vie de tous les jours ?
Peut être.
Mais alors pourquoi abandonnerions-nous ce projet ?
Pour moi, l'Amérique est censée être un pays de liberté où nous pouvons aller là où nous le souhaitons et faire ce que l'on veut sans pour autant être surveillé constamment par le gouvernement. Si les gens choisissent d'utiliser des formes de paiement électronique, c'est une chose, mais si nous sommes tous contraints d'aller vers un tel système, je crains que cela n'entraîne une réduction énorme de nos libertés fondamentales.
Et il est trop facile d'imaginer les conséquences d'un monde où un gouvernement obligerait à utiliser un moyen de paiement électronique. Cela donnerait à ce gouvernement un contrôle total sur nos vies, de ceux qui pourraient utiliser ce

«système» de ceux qui ne le pourraient pas. Les formes variées de contraintes et de tyrannies dans un tel scénario sont évidentes.
Que feriez-vous si vous ne pouviez pas acheter, vendre, trouver un emploi ou ouvrir un compte bancaire sans « données d'identification » ? Les informations que vous demande le gouvernement pourraient à terme se retourner contre vous.
C'est certainement une chose à laquelle il faut dorénavant penser.
Beaucoup de gens se réjouiront sans doute de voir notre monde basculer rapidement vers une société sans numéraire, mais je ne le ferai pas. Je crois qu'un véritable système sans argent liquide engendrera de nombreux problèmes, et je n'en veux pas.
Lien : **http://www.businessbourse.com/2015/12/29/la-societe-sans-argent-liquide-cest-maintenant/**

L'expert Nader Hadded propose le paiement par chèque ou par carte pour les paiements supérieurs à 1000 dinars

Après la proposition faite par Achraf Ayadi, de changer la monnaie tunisienne par une autre monnaie afin de lutter contre la corruption et le terrorisme, Nader Hadded, expert international en économie a proposé, sur les ondes d'Express Fm, la mise en place d'une loi obligeant les Tunisiens à payer par chèques ou cartes bancaires, les achats ou prestations de plus de 1000 dinars.
Contacté par le *Huffpost Tunisie*, le spécialiste explique que " le projet va frapper toutes les transactions frauduleuses en liquide et réduire les crimes tels que le blanchiment d'argent "
Interrogé sur la faisabilité du projet, il répond : "Le projet est tout à fait faisable , on parle aujourd'hui de Cashless society , en Suède surtout que les transactions en liquide ne représentent que 2%. Certes, il y a des étapes à suivre si on veut vraiment éradiquer le terrorisme qui s'auto finance de l'économie parallèle mais c'est faisable"
Quant aux risques du projet, l'expert considère que les risques générés par la monnaie virtuelle sont moins graves que ceux de l'argent liquide dans un monde menacé par le terrorisme, selon ses dires. "Les gens pourront utiliser les cartes bancaires dans n'importe quelle transaction peu importe le montant , avec 'carte contact' , l'idée c'est la démocratisation des transactions électroniques qui n'autorisent pas à un client de dépasser sa limite de fond disponible" précise-t-il.
Qu'est ce que la Carte contact ?
C'est une carte bancaire ordinaire avec une puce NFC, et une technologie contact pour réduire le temps d'insertion de la carte dans la machine et taper le code. Elle a pour objectif d'accélérer les transactions et de limiter le temps d'attente, en facilitant les étapes.
Le spécialiste a appelé à une série de mesures à adopter pour garantir la stabilité socio-économique en Tunisie, il appelle avant tout à la lutte contre la corruption, à la capitalisation des banques et des caisses sociales, à l'élaboration d'une stratégie claire du remboursement des dettes, de trouver le meilleur moyen de réinvestir les recettes, hors salaires.
Il appelle également les Tunisiens à payer leurs impôts comme une partie de leur citoyenneté et exhorte le gouvernement à construire une relation de confiance avec les Tunisiens d'une part, et à travailler sur l'axe de la planification d'autre part, puisque le gouvernement d'union nationale n'est pas un gouvernement de gestion des affaires courantes.

Le diplômé de l'Université d'Oxford a recommandé également la création d'un e-gouvernement pour lutter contre la bureaucratie qui fait fuir les investisseurs "En Angleterre, on peut créer son entreprise en ligne, en un temps très court. En Tunisie, ça peut durer longtemps avec la lenteur de l'administration" souligne-t-il.
Haddad, appelle aussi à faire de l'anglais, la deuxième langue officielle en Tunisie
Par ailleurs, l'expert est revenu sur la proposition d'Achraf Ayadi quant au changement de la monnaie en circulation afin de contrôler l'argent cash et à lutter contre la fuite de capitaux et au blanchiment d'argent, selon lui, bien qu'intéressant, ce projet n'est pas faisable en Tunisie " Il est coûteux et lent de réaliser ce projet en Tunisie, il faudra l'appliquer par étapes et par zones géographiques comme l'euro" précise-t-il. Publication 25/08/2016.
Lien : **http://www.huffpostmaghreb.com/2016/08/24/nader-haddad-paiement-_n_11676110.html**

Le flot montant de la cybercriminalité polonaise

Quand on songe à une carte de la cybercriminalité, la Pologne n'est pas nécessairement le premier pays qui vient à l'esprit.
Pourtant, ce serait faire preuve de négligence que de ne pas regarder ce qu'il s'y passe actuellement. Les nombreux incidents rapportés au cours de l'année 2015 par la presse nationale polonaise et internationale – du piratage du serveur principal de la banque polonaise Plus Bank en juin 2015 par l'un des administrateurs du forum underground Torepublic, aux attaques de plusieurs grands cabinets d'avocats en août 2015 – indiquent que la Pologne n'est pas étrangère aux cyber attaques et qu'une économie souterraine autonome, composée d'activités illicites très variées, est en plein essor dans le pays.
L'augmentation de ces attaques s'explique par l'état du cyber-environnement polonais qui ces dernières années est devenu intéressant à exploiter pour les fraudeurs :
• D'une part, il est légitime de penser que la lutte contre la cybercriminalité étant plus efficace dans les pays les plus développés, les attaques utilisant des techniques simplistes tel que le phishing mais aussi des techniques plus complexes telles que les attaques par malware bancaire, ont tendance à se déplacer progressivement vers les pays à croissance plus rapide où le taux de foyers disposant d'une connexion internet est encore relativement bas et augmente de manière constante. Le pourcentage de la population disposant d'une connexion internet en Pologne ne représente que 70 % aujourd'hui (soit une augmentation de 10 % entre octobre 2014 et octobre 2015), il reste donc encore une marge de progression importante à ce niveau-là. Cette masse potentielle de futurs nouveaux internautes non-initiés aux dangers du Web, forme une cible de qualité pour les fraudeurs.
• D'autre part, bien que des progrès notables aient été accomplis ces dernières années dans le domaine de la sécurité informatique privée, le système judiciaire en Pologne reste encore relativement inadapté pour répondre aux enjeux de la cybercriminalité. Il existe bel et bien un large éventail de prescriptions censées régir les comportements indésirables observés dans le cyberespace. Par exemple, les attaques contre le système informatique de la compagnie aérienne polonaise LOT, le 21 Juin 2015, peuvent constituer une violation de plusieurs règlementations dont : le droit à la protection des bases de données, les droits d'auteur concernant les programmes informatiques ou encore les droits relatifs à la protection des données personnelles. La classification juridique d'une attaque peut varier en fonction du préjudice qui a été causé, et en

fonction de la façon dont l'attaque a été menée. Toutefois, dans la pratique, l'application de ces règles se révèle souvent compliquée pour les autorités, en particulier les délits impliquant des éléments techniques complexes de type « hacking », « sniffing », attaques par malware et attaques DDOS. Dans ces cas-là, l'évaluation de la preuve et l'identification des responsabilités deviennent longues et ardues et nécessitent de manière quasi-systématique la nomination d'experts dans le domaine informatique afin de comprendre ne serait-ce que le mode opératoire de la fraude. De manière illustrative, même dans le cas où la police parviendrait à identifier les personnes à l'origine de l'attaque du système informatique de la compagnie LOT, si ces dernières se sont connectées à plusieurs serveurs situés dans différents pays, il sera difficile, voire impossible, de les tenir pour responsables.

Un intérêt particulier pour les malwares bancaires

Les activités « underground » en Pologne restent encore globalement furtives à ce stade mais semblent déjà vouloir s'autonomiser petit à petit pour devenir un lieu central où s'opèrent tous types d'activités illégales.

Parmi ces activités, les cybercriminels expriment depuis quelques années un intérêt tout particulier pour les malwares bancaires qui représentent la menace la plus sévère pour le cyberespace polonais actuellement

L'achat de parties de codes malveillants s'effectue majoritairement sur les marchés noirs étrangers (dont une grande partie sur les marchés russes).

Toutefois, il y a une tendance depuis l'an dernier à l'augmentation de malwares écrits en langue polonaise visant la population polonaise uniquement. Ces nouvelles catégories de malware se révèlent souvent simplistes mais restent innovants dans leur fonctionnement.

En 2015, le malware bancaire de création polonaise le plus utilisé a sans doute été Banatrix. Apparu pour la première fois en 2013, il se plaçait déjà en quatrième position des malwares bancaires les plus utilisés en 2014

Une de ses variantes a, sans doute, été utilisée à nouveau au début du mois d'octobre 2015 dans une série d'attaques ciblant un office municipal à Jaworzno.

Profitant de l'absence de procédures de vérification de l'exactitude des transferts externes, plus de 500 000 euros au total ont été volés et transférés vers des comptes bancaires appartenant à des personnes sans-abris (recrutées spécialement par les fraudeurs et utilisées comme mules), puis converties en BTC sur des plateformes d'échange bitcoin.

Comme le décrivent nos homologues du CERT Pologne, le fonctionnement de ce malware repose sur des principes très basiques. Le malware va parcourir, à l'aide de CreateToolhelp32Snapshot et Process32Next, tous les processus actifs en vue de trouver un des processus suivants : chrome.exe, iexplore.exe, IEXPLORE.EXE, firefox.exe, opera.exe.

Dès lors que ces éléments sont identifiés, le malware va parcourir la mémoire du processus afin de détecter éventuellement une chaîne de 26 chiffres (qui correspond au format spécifique des numéros de comptes bancaires polonais).

Cette chaîne sera ensuite remplacée par une séquence de chiffres, appartenant au fraudeur, reçue depuis un serveur C&C[1].

Le champ d'action de Banatrix est donc relativement large car il importe peu que la victime fasse un copié-collé du numéro de compte d'un destinataire ou qu'elle rentre le numéro manuellement, le remplacement du numéro s'effectuera malgré tout dans la mémoire du processus actif – avec en bonus une animation graphique à l'effet Matrix (d'où la dénomination choisie de « Banatrix », qui est l'association de « BAN[2] » et « Matrix »)

L'utilisation de ces nouveaux types de malwares, dont font partie VBKlip, Slave et Backspacetrix notamment, montrent non seulement, que les cybercriminels polonais ne manquent pas d'inventivité, mais surtout qu'il y a une réelle volonté de rendre le marché underground du pays plus autonome.

Les autres opérations cybercriminelles locales observées incluent :

- Les attaques de phishing, le spam, le blanchiment d'argent, les attaques DdoS, l'espionnage industriel, la diffusion de contenus pédophiles et de contenus violents
- Le commerce C2C (cybercrime to cybercrime), dont l'achat et la vente régulière : de botnets, d'outils injection, de vulnérabilités, de faux passeports, de faux billets, de bases de données volées, de comptes bancaires vierges, de données bancaires volées, de drogue, d'armes…

Les sites ou forums sur lesquels s'effectuent ces échanges utilisent des systèmes d'escrow[3] sécurisés, acceptent principalement les paiements en Bitcoin et chiffrent les communications via le chiffrement PGP

Le marché en Pologne étant encore relativement jeune, il n'existe pas d'étude aujourd'hui mesurant précisément les profits générés par les cybercriminels polonais, ou encore le niveau du préjudice économique subi par les utilisateurs finaux.

Plusieurs tendances spécifiques ressortent de ce schéma.

La fraude bancaire en ligne est une des catégories de fraude qui intéresse le plus les cybercriminels polonais.

Ces derniers appliquent des méthodes connues ou précédemment inconnues (par exemple en utilisant des outils innovants créés localement) afin de voler de l'argent, et les montants transférés frauduleusement se révèlent souvent être des montants à six chiffres. Plus globalement, cette croissance est due à l'amélioration des malwares bancaires importés de l'étranger et à la formation de groupes criminels plus stables dont le professionnalisme et l'expérience ont grandi au fil des dernières années.

Il est, ainsi, probable que les malwares bancaires de création polonaise, évoqués précédemment, se complexifient aussi à leur tour dans un futur proche. Cela soulève plusieurs questions : les cibles de ces nouveaux malwares deviendront-elles plus diversifiées et globales dans les années à venir ? Si oui, quels pays seront visés en premier ?

Le spam est également une des tendances fortes qui ressortent de ce schéma. La manière la plus courante et la plus simple de monétiser le spam est l'utilisation de programmes d'affiliation qui permettent notamment de vendre des imitations de produits de grandes marques, des produits pharmaceutiques contrefaits, ou encore de faire de la publicité mensongère pour des sites de rencontre en ligne.

Nous avons observé, enfin, un fort développement du marché cybercriminel interne (C2C) qui cherche à se consolider et à s'autonomiser afin de garantir une croissance pérenne des activités qui y sont présentes. Cela se reflète par un renforcement de l'interconnexion entre les groupes cybercriminels, basé notamment sur le partage mutuel de données compromises, de « bonnes pratiques » ou encore de botnets.

Ainsi, de plus en plus d'incidents n'impliquent plus seulement un mais plusieurs groupes cybercriminels.

En conséquence, il semble y avoir en Pologne un abandon progressif du modèle traditionnel désorganisé au profit d'un modèle plus organisé impliquant d'avantages de groupes et utilisant un système de gestion centralisé.

22/03/16

[1] Un serveur de Command and Control est une machine utilisée pour coordonner les actions d'ordinateurs infectés par un programme malveillant

[2] Norme internationale pour désigner les numéros de comptes bancaires

[3] Un système d'escrow est un système de paiement dans lequel un intermédiaire neutre assure à l'acheteur, comme au vendeur, une exécution sûre de la transaction
Lien : https://www.lexsi.com/securityhub/le-flot-montant-de-la-cybercriminalite-polonaise/