CTRF CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER خلية معالجة الإستعلام المالي CTRF

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

Lettre n°96

Bruxelles veut assécher le financement du terrorisme en surveillant bitcoins et cartes prépayées

La Commission européenne a présenté hier un « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* ». Plusieurs volets sont au programme, mais Bruxelles s'attarde particulièrement sur l'utilisation de moyens de paiement anonymes. Crypto-monnaies, cartes de paiement prépayées et espèces sont ainsi visées.

Alors qu'en France, l'état d'urgence est toujours d'actualité, près de trois mois après les attentats de Paris, la Commission européenne cherche des moyens de lutter contre le terrorisme. L'objectif pour les autorités européennes est de couper le robinet du financement des organisations terroristes, grâce à une série de mesures dont la mise en application s'étalerait sur 2016 et 2017.

Surveiller les plateformes d'échange de crypto-monnaies

Pour parvenir à cet objectif, Bruxelles voudrait agir simultanément sur plusieurs leviers. Outre le renforcement de la vigilance concernant « *les flux financiers en provenance de pays tiers à risque* » la Commission aimerait garder un œil sur « *les risques de financement du terrorisme, liés aux monnaies virtuelles* ».

Les crypto-monnaies permettent en effet d'effectuer des transactions financières de manière quasi instantanée d'un bout du monde à l'autre, dans un anonymat relatif. Si la Commission ne peut agir directement sur ces flux, elle peut cependant aller frapper à la porte des plateformes de change proposant de troquer ses bitcoins contre des euros, des dollars ou toute autre monnaie classique.

Bruxelles propose ainsi dans son « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* » d'inclure les plateformes de change de crypto-monnaies dans le champ d'application de la directive anti-blanchiment « *de manière à ce que ces plateformes doivent appliquer des mesures de vigilance à l'égard de la clientèle lors de l'échange de monnaies virtuelles contre des monnaies réelles* ». L'objectif affiché des autorités est de « *mettre fin à l'anonymat associé à ce type d'échange* » d'ici « *la fin du deuxième trimestre* ».

En France, les plateformes d'échange doivent déjà se déclarer auprès de l'ACPR. Le Rapport Tracfin sur les crypto-monnaies publié en juillet 2014 suggérait déjà quant à lui la nécessité d'identifier les clients de ces plateformes, à partir du moment où ils effectuent des échanges entre euros et monnaies virtuelles.

Pas de bannissement des crypto-monnaies

Si Bruxelles souhaite réguler les échanges entre crypto-monnaies et monnaies fiduciaires, il n'est pas prévu de bannir leur utilisation. Si les plateformes d'échange seront soumises à de nouvelles obligations, via la quatrième directive anti-blanchiment, les fournisseurs de portefeuilles numériques pour les monnaies virtuelles (type Electrum, MultiBit) ne devraient quant à eux pas avoir à changer leurs habitudes.

Cependant, la Commission note que les monnaies virtuelles « *sont souvent considérées comme un outil intéressant pour les transferts internationaux d'argent* » et qu'elles « *représentent un marché innovant mais petit* ». Elle rappelle également que la Banque centrale européenne (BCE) avait jugé qu'elles ne représentaient pas une menace du point de vue de la

stabilité financière de la zone euro. Aucune raison donc d'interdire leur utilisation, pour le moment.

Les cartes de paiement prépayées dans le collimateur de l'Europe

Bruxelles veut aussi « *s'attaquer aux risques liés aux instruments prépayés anonymes* », type TransCash ou PCS, qui permettent à n'importe qui de profiter d'une solution de paiement avec un plafond de 2 500 euros par carte, sans vérification d'identité au moment de l'ouverture du service. Ce type de carte ont notamment été utilisées pour la préparation des attentats de Paris, note la Commission Européenne dans une FAQ.

Les mesures autour de ces cartes n'ont pas encore été précisées, mais l'Europe voudrait abaisser le plafond à partir duquel il devient nécessaire de vérifier l'identité du futur détenteur de la carte avant de lui fournir le service. La Commission précise « *qu'il sera veillé à la proportionnalité de ces mesures, eu égard en particulier à l'utilisation de ces cartes par des citoyens vulnérables sur le plan financier* ». Là encore, il est question d'une application d'ici mi-2016.

Les solutions de type Compte Nickel ne devraient quant à elles pas subir de contrecoup particulier, puisqu'elles nécessitent déjà une vérification de l'identité du client avant même l'ouverture du service.

Les espèces posent également problème

Il y a un dernier mode de paiement anonyme qui pose problème à Bruxelles et des centaines de millions de citoyens l'utilisent quotidiennement : les espèces. Intraçables elles sont pourtant omniprésentes dans la vie courante et il est encore impensable de les faire disparaître. L'Europe voudrait néanmoins émettre une « *proposition législative relative aux mouvements illicites d'argent liquide* », dans laquelle la Commission « *étendra le champ d'application du règlement existant afin d'y inclure l'argent liquide envoyé par fret ou par la poste et de permettre aux autorités d'agir à l'égard de montants plus faibles d'argent liquide en cas de soupçons d'activité illicite* ».

On rappellera que le plafond pour les achats en espèces est passé de 3 000 à 1 000 euros en France le 1er septembre dernier, et que depuis le 1er janvier, les français doivent présenter une pièce d'identité pour toute opération de change d'une valeur de plus de 1 000 euros. Depuis le 1er janvier, les banques doivent également signaler à Tracfin tout dépôt ou retrait d'espèces d'un montant supérieur à 10 000 euros par mois.

Le cas épineux du billet de 500 euros

La Commission, la Banque centrale européenne et Europol vont également travailler de concert pour évaluer la nécessité d'un retrait de la circulation des billets de 500 euros. Ceux-ci représentent un tiers de la valeur de l'ensemble des billets en circulation, alors même qu'ils ne sont que très peu utilisés lors de paiements.

« *Ces billets sont très demandés au sein des groupes criminels qui s'en servent pour transporter leur argent, en raison de leur grande valeur et de leur faible volume* ». Il est en effet plus facile de transporter clandestinement un seul billet de 500 euros qu'une liasse de 50 billets de 10 euros. Il reste encore à voir si cette mesure sera vraiment efficace, les billets de 100 et 200 euros n'étant pas beaucoup plus difficiles à camoufler.

https://www.nextinpact.com/news/98359-bruxelles-veut-assecher-financement-terrorisme-en-surveillant-bitcoins-et-cartes-prepayees.htm

Cyberattaque : la rançon en bitcoins, garantie d'anonymat

Les auteurs de la cyberattaque mondiale lancée vendredi exigent le versement des rançons en bitcoins car cette monnaie immatérielle permet l'anonymat mais, face à la mobilisation internationale, cela ne suffira peut-être pas pour couvrir leurs traces, assurent des experts.

Le bitcoin, qui tire son origine d'un logiciel mis en ligne en février 2009 par un ou plusieurs informaticiens se cachant sous le pseudonyme de Satoshi Nakamoto, est une monnaie virtuelle autorégulée, qui préserve l'anonymat de ses propriétaires.
Sur l'écran qui apparait sur les centaines de milliers d'ordinateurs infectés par le virus "WannaCry" au cours des derniers jours, dans 150 pays, figure un lien pour permettre aux victimes d'acheter des bitcoins, puis une adresse où envoyer la rançon, en échange de laquelle les pirates promettent de décrypter les fichiers que leur virus a crypté.
"Le bitcoin, c'est le cash du numérique", explique à l'AFP Nicolas Debock, investisseur chez Balderton Capital, spécialiste des monnaies virtuelles. "Les transactions sont totalement anonymes, non répudiables. En revanche, elles sont totalement traçables".
"Toutes les transactions sont inscrites dans les chaînes de stockage, appelées blockchains. C'est anonyme, mais tout le monde peut surveiller une adresse bitcoin et voir comment l'argent bouge", ajoute-t-il. "Personne ne pourra leur prendre cet argent, mais il sera possible de suivre à la trace l'activité de ce compte".
Pour Pierre-Antoine Gailly, rapporteur en 2015 d'une étude sur le bitcoin et les monnaies virtuelles pour le Conseil économique, social et environnemental français (Cese), cela pose "un problème majeur".
"Le bitcoin n'a besoin d'aucune banque, donc cette circulation +monétaire+ échappe à toute supervision, à tout contrôle", dit-il à l'AFP. "Les comptes n'ont pas d'adresse physique, pas d'adresse bancaire, il n'y a pas d'hébergeur central: l'anonymat est mis en tête de gondole".

'Un coup très fort'

L'ampleur des dégâts infligés aux ordinateurs du monde entier, le nombre de victimes et de pays concernés par ce piratage d'une gravité inédite va certainement pousser les services internationaux d'enquête et de renseignements à surveiller de près l'adresse bitcoin sur laquelle les rançons ont été ou vont être versées, estiment les experts.
Des services existent, appelés "tumblers", qui promettent aux détenteurs de bitcoins d'anonymiser entièrement leurs comptes en monnaie virtuelle.
"Le tumbler va diviser les sommes en bitcoins en milliers de petits morceaux, les répartir sur des milliers d'adresses différentes et faire plein de transactions", explique Manuel Valente, directeur à Paris de la maison du Bitcoin. "Au bout d'une semaine, on remet tous ces bitcoins sur une nouvelle adresse, en espérant avoir couvert ses traces. Ce sont des systèmes de blanchiment de bitcoins. Sur le darkweb, il y a des gens qui proposent ce genre de service".
Mais si, face à l'importance du préjudice, les polices et services de renseignement du monde entier, avec leurs formidables puissances de calcul, s'allient pour surveiller le compte bitcoin des pirates, cet argent virtuel sera intouchable sans se faire repérer.
Pour Clément Francomme, directeur général de Utocat, entreprise de logiciels spécialisée dans la technologie blockchain, les pirates le savent si bien que la collecte d'argent via les rançons n'est peut-être pas le véritable but de cette cyberattaque.
"L'idée était peut-être de montrer au reste du monde qu'ils ont fait un coup très très fort. Avec une attaque pareille, ils vont être très connus dans le milieu des pirates internationaux. Cette équipe a fait une démonstration de force et je suppose que, dans pas très longtemps, il va y en avoir une autre", dit-il.
"C'est une démonstration de puissance, pour construire un CV. Ils pourraient ne pas avoir envie de dépenser ces bitcoins, sachant qu'ils vont être très surveillés, mais plutôt de se servir de leur renommée mondiale pour vendre des services à côté".
http://www.lepoint.fr/economie/cyberattaque-la-rancon-en-bitcoins-garantie-d-anonymat-15-05-2017-2127569_28.php

Un nouveau virus crée de la monnaie virtuelle

Après WannaCry, une autre attaque informatique massive a été découverte en début de semaine : Adylkuzz exploite les mêmes failles de sécurité que WannaCry. Il enrichit les pirates en créant de la monnaie virtuelle.

«On ne connaît pas encore l'ampleur (des dégâts) mais des centaines de milliers d'ordinateurs» pourraient avoir été infectés, a indiqué Robert Holmes, vice-président Produit chez Proofpoint. Il assure que l'attaque est «de bien plus grande envergure» que WannaCry et a débuté avant cette dernière, le 2 mai voire le 24 avril.

Proofpoint affirme avoir d'ailleurs détecté Adylkuzz en enquêtant sur WannaCry. Ce virus qui a frappé de très nombreux ordinateurs en fin de semaine dernière a notamment paralysé les services de santé britanniques et des usines du constructeur automobile français Renault.

Faille de Windows

Concrètement, Adylkuzz s'introduit dans des PC vulnérables grâce à la même faille de Windows utilisée par WannaCry, un problème détecté par la NSA (l'agence de sécurité nationale américaine) mais qui a fuité sur le net en avril. La divulgation des données avait été revendiquée par le groupe de pirates «Shadow brokers».

Le «malware» exploite alors l'ordinateur contaminé pour créer de façon invisible, des unités d'une monnaie virtuelle appelée Monero, comparable au Bitcoin.

Même si le Bitcoin, la plus connue des monnaies virtuelles, garantit un fort anonymat à ses utilisateurs, ses transactions restent traçables. Monero va elle encore plus loin dans l'opacité puisque la chaîne de transactions est complètement cryptée, ce qui en fait un outil prisé des pirates.

Attaque quasi-invisible

Avec Adylkuzz, les ordinateurs créent de la monnaie, «ce n'est pas de l'argent qui est volé» à qui que ce soit, résume Gérôme Billois, expert au cabinet Wavestone. L'attaque est quasi-invisible pour l'utilisateur, expliquent aussi les différents experts interrogés.

«Les symptômes de l'attaque sont un accès plus difficile aux contenus partagés Windows et un ralentissement des performances de l'ordinateur», précise Proofpoint dans une note de blog, selon laquelle l'attaque est toujours en cours.

Paradoxalement, cette attaque «est moins impactante que WannaCry pour les entreprises puisqu'elle n'entraîne pas d'interruption des services», poursuit Gérôme Billois. «Elle ne met pas les entreprises à genoux comme WannaCry» qui crypte les documents en exigeant une rançon pour les dévérouiller, ajoute-t-il.

https://www.lecourrier.ch/149509/un_nouveau_virus_cree_de_la_monnaie_virtuelle

Nouvelle cyberattaque, 200 000 ordinateurs infectés produisent de la monnaie virtuelle via la blockchain

Une nouvelle attaque informatique, basée sur la même faille que Wannacry a déjà infecté plus de 200 000 ordinateurs mercredi 17 mai. Contrairement à la précédente vague survenue vendredi 12 mai, les postes infectés ne sont pas blockés mais produisent de la monnaie virtuelle via la blockchain. Il ne s'agit pas de bitcoin, mais de Monero, une devise électronique plus récente. Selon les experts, la Corée du Nord pourrait être à l'origine de cette initiative.

Un virus informatique exploitant les mêmes failles que le logiciel de rançon WannaCry apparu vendredi 12 mai, s'est introduit, mercredi 17 mai, dans plus de 200.000 ordinateurs et

a commencé à fabriquer de la monnaie virtuelle, a-t-on appris mardi auprès d'experts en cybersécurité.
Ce virus, qui appuie la thèse d'une implication de la Corée du Nord dans cette vague de cyberattaques, a commencé à infecter des machines fin avril ou début mai mais n'avait pas encore été découvert car il ne bloque pas les ordinateurs, tout en continuant à créer de la monnaie virtuelle, déclarent des spécialistes de la société Proofpoint

Plus d'un million de dollars de monnaie virtuelle produits

D'après Ryan Kalember, un dirigeant de cette société de cybersécurité américaine, les auteurs de l'attaque pourraient avoir gagné plus d'un million de dollars, bien plus que l'argent généré par l'attaque WannaCry.
De la même façon que WannaCry, le virus profite d'une faille de Windows, qui n'apparaît plus dans les dernières versions du système d'exploitation de Microsoft, mais tous les particuliers et entreprises n'ont pas forcément installé les mises à jour.
Les monnaies virtuelles basées sur une technologie de blockchain opèrent en permettant la création d'une nouvelle monnaie en échange de la résolution de problèmes mathématiques complexes.
Les "mineurs" numériques travaillent sur des ordinateurs spécialement configurés pour résoudre ces problèmes et produire de la monnaie virtuelle, dont la valeur fluctue en fonction de la demande du marché.
Le bitcoin est la monnaie virtuelle la plus répandue mais le nouveau programme viserait une monnaie virtuelle plus récente, appelée Monero. Selon les experts interrogés par Reuters, cette monnaie a récemment été convoitée par des hackers liés à la Corée du Nord.
La Corée du Nord a attiré l'attention dans le cas WannaCry pour un certain nombre de raisons, par exemple le fait que certaines lignes de code utilisées dans le développement d'anciennes versions du rançongiciel apparaissent également dans des programmes développés par le groupe Lazarus, soupçonné par de nombreux chercheurs d'être géré par Pyongyang.
Il est toutefois trop tôt pour en être certain et l'enquête n'en est qu'à ses prémices.
Début avril, la société de cybersécurité Kaspersky Lab avait déclaré qu'une branche de Lazarus spécialisée dans les gains financiers avait installé un logiciel pour produire de la monnaie virtuelle Monero sur un serveur en Europe.
L'apparition de cette nouvelle campagne d'"extraction" de monnaie s'appuyant sur la même faille de Windows que WannaCry pourrait n'être qu'une coïncidence, ou suggérer que la Corée du Nord pourrait être responsable dans les deux affaires.
Les similitudes entre le cas évoqué par Kaspersky Lab, WannaCry et Monero sont aux yeux de Ryan Kalember "plus qu'une coïncidence".
"Il y a de véritables recoupements. Ce n'est pas comme si on voyait des mineurs Monero partout dans le monde", dit le responsable de Proofpoint.
http://www.usinenouvelle.com/article/nouvelle-cyberattaque-200-000-ordinateurs-infectes-produisent-de-la-monnaie-virtuelle-via-la-blockchain.N541349

TripAdvisor : Des mots de passe visités et réinitialisés

Le site de voyage a réinitialisé un certain nombre de mots de passe après la compromission d'un nombre non précisé de comptes d'utilisateurs de TripAdvisor.
TripAdvisor a réinitialisé un nombre inconnu de comptes après que le service en ligne ait averti que certains comptes pourraient avoir été compromis.

Le site de réservation de voyage a déclaré que, s'il n'avait pas été piraté, les fraudeurs avaient "tenté de vérifier les combinaisons de courriels et de mots de passe" à partir de données volées à d'autres entreprises.
Un porte-parole de l'entreprise ne précise pas la source des données volées ni combien de comptes ont été compromis. Il a également refusé de faire de plus amples commentaires.

Facebook achète des mots de passe sur le dark web

Cependant, le nombre de comptes était suffisamment important pour alerter le procureur général de la Californie, qui exige que les entreprises avisent les clients d'une violation de données ou d'une exposition touchant plus de 500 résidents de l'Etat.
TripAdvisor a envoyé des courriels à des clients dont les comptes sont soupçonnés d'avoir été visités par un tiers. La société a déclaré qu'elle avait "invalidé" les anciens mots de passe et demandé aux utilisateurs de réinitialiser leurs mots de passe via un formulaire en ligne.
C'est le dernier exemple d'une entreprise qui répond à une violation d'une autre entreprise en forçant la réinitialisation des mots de passe.
Amazon, par exemple, réinitialise régulièrement les mots de passe des utilisateurs qu'il estime faibles ou lorsque les mots de passe ont été compromis auprès d'autres sites. Les clients qui réutilisent le même mot de passe sur différents sites risquent davantage de compromettre les comptes sur d'autres sites et services.
C'est pourquoi des entreprises comme Facebook se procurent activement des données piratées sur le Dark Web afin de vérifier si celles-ci correspondent aux comptes de ses propres utilisateurs et pouvoir ainsi prévenir des attaques.
Au cours des deux dernières années, nous avons constaté des failles massives sur MySpace, LinkedIn, Tumblr et AdultFriendFinder, représentant collectivement plus d'un milliard de comptes d'utilisateurs.
http://www.zdnet.fr/actualites/tripadvisor-des-mots-de-passe-visites-et-reinitialises-39852560.htm

Identifiants volés, carburant du cyber crime

Le responsable du site Haveibeenpwned, qui permet aux utilisateurs de vérifier que leurs identifiants n'ont pas été compromis dans un piratage, annonce l'ajout d'un milliard de nouveaux mots de passe à leur base de données. Une matière première qui vaut de l'or pour les cybercriminels.
Le site Haveibeenpwned (est-ce que j'ai été piégé ?) est bien connu des amateurs de sécurité. Administré par Troy Hunt, ce site a pour objectif de rassembler dans une base de données l'ensemble des identifiants de connexions volés circulant sur le web, dès lors que ceux-ci sont mis en vente ou révélés publiquement par les cybercriminels.
Le site permet aux internautes de vérifier que leurs identifiants ne font pas partie de ces stocks de mots de passe volés. Il suffit pour cela d'entrer un identifiant (et jamais votre mot de passe), et le site se charge de vérifier si celui-ci est présent dans les bases de données collectées par le site.
HaveIbeenPwned a mis la main sur de nombreuses bases de données volées ayant ressurgies au fil des jours sur différents forums et autres places de marché illégales. Mais Troy Hunt a annoncé hier l'arrivée d'un milliard de nouveaux identifiants au sein de la base de données. Dans un long post de blog, il explique que les cybercriminels ont développé des outils utilisés pour des scénarios de « credential stuffing », une pratique qui consiste à tester des milliers de couples identifiants/mots de passe sur un site. Ces outils s'appuient sur des listes de « combos », vendues aux utilisateurs : pour vingt dollars, on peut ainsi s'offrir une liste de 50.000 identifiants à tester sur un site visé par Anti-Public.

Ce sont ces listes d'identifiants agrégés que Troy Hunt est parvenu à récupérer et s'emploie à ajouter à la base de données du site HaveIbeenpwned. Un milliard d'identifiants, mais comme le précise l'administrateur, une large partie d'entre eux avaient déjà été incorporés à la base via les précédents ajouts. « 75,78% des adresses étaient déjà présentes sur HIBP. Cela représente beaucoup, mais chaque fois que je charge les données d'une nouvelle brèche dans la base de données, environ 60% des adresses sont déjà présentes dans le système » explique Troy Hunt, qui confie avoir hésité à ajouter à sa base de données des informations dont il ne connaît pas la provenance exacte.

En effet, ces couples identifiants/mot de passe ne proviennent pas d'un seul service, mais du cumul de nombreuses bases de données ayant circulé sur le web et au sein des réseaux cybercriminels. Impossible de le relier à une attaque spécifique, mais la taille de l'archive reste impressionnante.

Un lourd passif

Et pourtant, rien de bien surprenant quand on se penche sur les brèches de sécurité nombreuses de 2016. LinkedIn, Myspace, Tumblr, et évidemment Yahoo : 2016 a été une année chargée en terme de cybercrime et chaque fois, des centaines de millions se retrouvaient dans la nature. Et malheureusement, les mauvaises habitudes rendent ces données d'autant plus précieuses. Comme l'explique à ZDNet.fr Aeris, administrateur système chez Cozy Cloud et expert en sécurité « Ça a surtout beaucoup de valeur, car les gens ont une fâcheuse tendance à utiliser le même mot de passe partout. Une compromission d'un mot de passe LinkedIn est la quasi-certitude d'obtenir des accès à des comptes Paypal ou à des boîtes mail. »

On pourra objecter que les données volées sont fréquemment chiffrées par les entreprises et que les données brutes ne donnent donc pas exploitables directement par les cybercriminels. C'est d'ailleurs la ligne de défense de beaucoup d'entreprises victimes d'un vol de données de ce type : « Ne vous inquiétez pas, les données sont chiffrées et donc inaccessible aux attaquants. Mais changez votre mot de passe quand même. » Oui, la communication de crise ne s'offusque pas forcément d'injonctions contradictoires : si les données sont chiffrées, après tout pourquoi changer ? Mais difficile de les blâmer :dans ce genre de situation, mieux vaut prévenir que guérir.

Si le chiffrement des mots de passe est une bonne pratique, elle ne suffit pas à elle seule à assurer la sécurité des informations. Selon les outils utilisés pour générer ces condensats (le nom que l'on donne aux données une fois qu'elles sont passées par une fonction de hachage. Hash est aussi un anglicisme fréquemment utilisé) la protection est en effet plus ou moins forte : MD5 et SHA1 présentent ainsi des faiblesses mathématiques qui permettent de décrypter les condensats générés par ceux-ci. Outre cet aspect, l'implémentation faite par l'entreprise joue également dans l'équation : présence ou non de sel, utilisation des bons algorithmes…

D'autant que si un algorithme est considéré comme solide aujourd'hui, difficile de dire ce qu'il en sera dans 5 ou 10 ans. « La robustesse d'une base de données volée, c'est compliqué à déterminer. J'aurais tendance à dire qu'une base volée est une base décryptée, au moins sur le moyen ou le long terme » résume Aeris.

Et c'est ce qui nous ramène aux bases de données massives récupérées par Troy Hunt sur son service. Les multiples piratages et vol de données qui s'accumulent peu à peu posent un problème bien plus inquiétant sur le long terme, puisqu'ils viennent nourrir un « pool » de données volées réutilisées par les cybercriminels. « C'est un peu le principe actuel : chaque base de données volée alimente une grosse base de données mondiale qui sera testée en intégralité sur les fuites suivantes » résume Aeris. Cette « base de données mondiale » évoquée par Aeris est celle que l'on retrouve dans les services tels du type Anti-public et qui proposent ces listes de « combos » issus de différents piratages.

Si vous ne chiffrez pas pour vous, par pitié faites-le pour les autres

Et la sécurité défaillante d'un service devient en prime un risque pour ceux qui se croyaient protégés par un chiffrement fort : « Un seul service A pourri (pas salé, en clair, etc.) qui fuite, c'est potentiellement un autre service B, fuité précédemment, mais qui lui était correctement protégé, qui va sauter. Parce qu'un mot de passe, qui résistait aux attaques sur B, va être trouvé sur le service A, et donc sera immédiatement testé et trouvé sur B. » Les vols d'identifiants représentent donc évidemment un risque pour la sécurité de l'entreprise et de ses clients, mais par effet de rebond, ils amoindrissent également la sécurité du reste de l'écosystème et d'autres entreprises.

Au vu de ces différents phénomènes conjugués, il vaut mieux être réaliste et partir du principe que les mots de passe que l'on utilise sur différents forums seront un jour ou l'autre cassés. C'est d'ailleurs ce qui est arrivé à Troy Hunt lui-même : il explique ainsi avoir eu la joie de retrouver une adresse et un mot de passe au sein de l'archive qu'il ajoutait à sa base de données. Pour bénéficier d'une protection supplémentaire, la meilleure initiative reste d'utiliser un générateur de mots de passe, qui sera capable de générer des mots de passe longs et complexes qui seront bien plus complexes à décrypter pour les cybercriminels.

http://www.zdnet.fr/actualites/identifiants-voles-carburant-du-cybercrime-39852112.htm

Namibie : vers une législation sur les transactions électroniques

Une législation sur les transactions électroniques et la cybercriminalité est en gestation en Namibie. Selon un communiqué du ministère namibien de l'Information et des Communications, publié mardi 23 mai, le gouvernement a entrepris de mettre en place une législation concernant les transactions électroniques et les questions de cyber sécurité associées.

Pour le secrétaire permanent dudit ministère, Mbeuta Ua-Ndjarakana, ce projet de loi vise à promouvoir les services publics par voie électronique, le commerce électronique et les communications électroniques entre les institutions publiques, les organismes privés et les citoyens.

Et de poursuivre : « ce projet de loi visera également à développer un environnement sûr, sécurisé et efficace pour permettre aux consommateurs, aux entreprises et aux agences ou organismes publics d'effectuer et d'utiliser des virements électroniques ».

Les transactions électroniques revêtent une importance croissante pour les pouvoirs publics, les entreprises et les consommateurs dans la plupart des pays. Le commerce électronique se développe, créant de nombreuses possibilités, mais se heurte encore à l'obstacle majeur qu'est le manque de sécurité et de confiance. La fraude en ligne et les atteintes à la sécurité des données suscitent des inquiétudes grandissantes et appellent des réponses législatives et réglementaires adéquates, qui permettent de faire croître le commerce intérieur et extérieur.

Il n'est cependant pas facile d'adopter un cadre juridique et réglementaire satisfaisant, étant donné la variété et la complexité des législations et réglementations et l'évolution rapide des technologies et des marchés.

Ainsi, la Namibie ambitionne de relever le défi de toute la complexité notée dans le monde des transactions électroniques.

http://www.financialafrik.com/2017/05/23/namibie-vers-une-legislation-sur-les-transactions-electroniques/#.WSa8c7jSMxg

Un hacker russe reconnaît avoir encaissé des millions via un botnet

Un pirate russe de 41 ans a plaidé coupable devant la justice américaine. Il reconnaît avoir, grâce à un malware, infecté des milliers de serveurs informatiques dans le monde et généré ainsi des millions de dollars en paiements frauduleux.

Un hacker russe a plaidé coupable pour l'installation d'un malware sur des dizaines de milliers de serveurs informatiques dans le but de générer des millions de dollars en paiements frauduleux, selon le Département US de la Justice.

Maxim Senakh, 41 ans, a admis avoir installé le programme malveillant Ebury sur des serveurs partout dans le monde, dont des milliers hébergés aux Etats-Unis. Senakh, au sein de l'organisation criminelle pour laquelle il travaillait, a utilisé le malware pour créer et opérer un botnet.

Ce réseau d'ordinateurs compromis avait pour objet de générer et rediriger le trafic Internet à des fins de fraude au clic et d'envoi de spam. Ce botnet a ainsi permis aux cybercriminels de dégager des millions de dollars de revenus, d'après la justice américaine.

Maxim Senakh a reconnu avoir personnellement tiré des bénéfices du botnet Ebury. Pour rappel, Ebury combine rootkit et backdoor, et cible principalement les serveurs Linux. Selon le CERT allemand, grâce ce malware, les pirates sont à même de voler mots de passe et identifiants et d'utiliser les systèmes piratés pour expédier d'importants volumes de spam.

Le plaider coupable d'un pirate russe est un fait rare pour le ministère de la Justice, à qui des hackers russes de premier plan ont échappé pendant des années. Plus tôt en mars, le DOJ a inculpé quatre hackers, dont deux espions russes, responsables des cyberattaques massives contre Yahoo.

Des pirates russes sont également soupçonnés d'être impliqués dans des attaques lors des élections présidentielles américaines. L'ancien président Barack Obama avait appelé à des sanctions radicales contre la Russie pour ses cyberattaques.

Senakh avait été interpellé par la police finlandaise en 2015 et extradé aux US. Après l'arrestation, les autorités russes avaient qualifié celle-ci d'illégale, estimant qu'il s'agissait d'un "abus de la loi en violation des normes procédurales internationales" rapportait Reuters.

Maxim Senakh connaîtra sa peine le 3 août. Il risque une condamnation à 10 ans de prison.

http://www.zdnet.fr/actualites/un-hacker-russe-reconna-t-avoir-encaisse-des-millions-via-un-botnet-39850478.htm

Les crypto-monnaies, le nouvel or?

Aujourd'hui, l'engouement pour les monnaies virtuelles ne connaît plus de limites. Les experts en matière de bitcoins mettent cependant en garde contre une possible correction.

Les détenteurs d'argent numérique – c'est-à-dire sous forme de code informatique – se frottent les mains. On dénombre aujourd'hui dans le monde plus de 700 de ces crypto-monnaies, et la plupart d'entre elles ont vu leur valeur s'envoler au cours des dernières semaines. Le bitcoin, l'ancêtre de l'argent numérique, a atteint ces derniers jours le chiffre astronomique de 2.800 dollars, soit trois fois plus qu'il y a trois mois, et 400% de plus qu'il y a un an. Lors de ses débuts il y a sept ans, il valait à peine 0,06 dollar. Ceux qui y ont cru à l'époque sont devenus riches comme Cresus.

Ses créateurs en sont convaincus: les devises virtuelles devraient révolutionner le monde financier, en particulier à cause de la technologie qui se cache derrière l'argent virtuel: le

"blockchain", dont le potentiel est infini. Il permet de réaliser des transactions financières en toute sécurité, sans l'intervention d'un tiers. Pour résumer: moins cher et plus rapide.
"Avec le blockchain, on n'a plus besoin d'une banque pour contrôler si l'échange d'argent s'est déroulé correctement, explique Sander Van de Moortel, journaliste et investisseur en bitcoins. Les transactions ont intégralement lieu sous le contrôle des parties concernées et la technologie permet de garantir que les bitcoins ne sont pas émis deux fois."
Dans la foulée de la crise de l'euro, les avantages concrets d'un système financier aussi décentralisé sont douloureusement limpides. En 2013, les épargnants d'une banque chypriote en déroute ont quasiment vu partir en fumée une partie de leur argent. Suite à la crise, on a assisté à une ruée sur les banques. Le bitcoin en a profité.
En outre, la crypto-monnaie détenue dans un portefeuille numérique ne peut être confisquée, car seul le propriétaire y a accès. Les incertitudes politiques se trouvent d'ailleurs à la base de la récente hausse des monnaies virtuelles. Ce n'est pas un hasard si celles-ci sont populaires dans les pays financièrement instables comme le Venezuela et l'Argentine. En Chine, certains essaient de contourner les contrôles des capitaux en recourant au bitcoin.
Depuis la naissance du bitcoin en 2009, les devises virtuelles prolifèrent. La technologie blockchain est d'ailleurs accessible à tous: il suffit d'une petite modification de code, et vous disposez d'une nouvelle monnaie.

Ether et ripple

L'ether fait partie des monnaies qui occupent le devant de la scène. En trois mois, sa valeur a augmenté de 1.450%. Elle est surtout célèbre à cause de son potentiel en matière de "contrats intelligents" (smart contracts). La technologie qui se trouve derrière l'ether contrôle si les conditions du contrat sont remplies et effectue ensuite le paiement automatiquement. Une fois de plus, les intermédiaires ne sont pas de la partie. Le ripple est une autre monnaie populaire: en trois mois, sa valeur a été multipliée par 45.
Mais l'argent virtuel réussira-t-il à s'imposer en tant que moyen de paiement? Le Japon a récemment reconnu le bitcoin comme moyen de paiement légal, ce qui a dopé son cours.
"Les investissements en bitcoins ne tombent pas sous la garantie des 100.000 euros, qui s'applique aux comptes bancaires électroniques."
FSMA
"Il existe encore de nombreux obstacles au niveau fiscal, explique l'avocat d'affaires Thomas Spaas, également président de la Belgian Bitcoin Association. Il y a peu, la Cour de Justice européenne a reconnu le bitcoin comme moyen de paiement légal. Aucune TVA n'est due lors de l'achat et de la vente de bitcoins. Cela donne de l'espoir sur le plan de la protection juridique des investisseurs en bitcoins en cas de vol ou de fraude. Mais il en faudra beaucoup plus pour faire vaciller la solide position de l'argent traditionnel."
Le bitcoin a peut-être un avenir plus radieux en tant qu'"or numérique". Le nombre maximum de bitcoins en circulation est fixé à environ 21 millions. De ce fait, on ne peut en créer indéfiniment, comme c'est le cas des banques nationales qui peuvent faire tourner la planche à billets traditionnels. Le bitcoin est donc protégé contre l'inflation, et conserve en principe sa valeur, tout comme l'or.
Malgré tout, il vaut mieux y réfléchir à deux fois avant d'investir en bitcoins. L'autorité de contrôle belge, la FSMA, met en garde contre les limites de la protection des investisseurs. "Les investissements en bitcoins ne tombent pas sous la garantie des 100.000 euros, qui s'applique aux comptes bancaires électroniques", nous explique-t-on. Les plateformes de négociation en bitcoins ont déjà été piratées à plusieurs reprises, provoquant de lourdes pertes chez les investisseurs. Par ailleurs, les obstacles pratiques sont légion. Par exemple, il faut du temps pour obtenir la confirmation d'une transaction.
La plupart sont cependant d'accord pour dire que la valorisation actuelle du bitcoin n'est pas tenable à terme. Tuur Demeester, investisseur de la première heure, met en garde contre des

investissements irrationnels. "Je vois aujourd'hui beaucoup d'investisseurs se jeter sur le bitcoin alors qu'ils ne maîtrisent pas suffisamment ses rouages, estime-t-il. On ne pourra pas éviter une correction."
http://www.lecho.be/les-marches/actu-general/Les-crypto-monnaies-le-nouvel-or/9903919?ckc=1&ts=1497528453

Un commerce illégal de la faune découvert sur le Darknet par Interpol

Selon une nouvelle recherche réalisée par Interpol, les trafiquants illicites de la faune ont commencé à se tourner vers le Darknet, a indiqué ce mercredi l'organisation internationale de la police basée à Lyon, France.
Les experts du Complexe mondial pour l'innovation d'Interpol ont trouvé des éléments limités mais probants, concernant l'usage du Darknet par des criminels pour vendre des produits illégaux de la faune provenant d'espèces en danger, tels que le corne de rhinocéros, l'ivoire d'éléphant ou encore des parties de tigres.
Financé par le Fonds international pour le bien-être des animaux (IFAW), le département d'Etat américain et l'African Wildlife Foundation (AWF), le rapport de recherche intitulé "La faune illégale dans le Darknet" a souligné que la majorité des transactions était réalisée en monnaie cryptée telle que le Bitcoin.
Entre décembre 2016 et avril 2017, 21 publicités concernant des produits faits de corne de rhinocéros, d'ivoire et de parties de tigres dont certaines datant de 2015, ont été identifiées par les experts d'Interpol.
Pour David Higgins, directeur du programme de sécurité environnementale de l'organisation, l'utilisation émergente du Darknet faisait partie d'une augmentation globale de l'utilisation des plates-formes en ligne pour le commerce illicite de la faune.
"Les criminels chercheront toujours à identifier de nouveaux domaines pour tirer profit de leurs activités illicites et le Darknet ne fait pas exception", a-t-il déclaré.
"Nous devons veiller à ce que l'application de la loi dans les pays membres bénéficie du soutien et des ressources dont ils ont besoin pour s'attaquer à la criminalité de la faune sur les marchés physiques et virtuels afin de protéger notre vie sauvage et notre biodiversité mondiale partagée", a-t-il ajouté.
"La bonne nouvelle est que les chercheurs ont trouvé des quantités très limitées de produits disponibles à la vente sur le Darknet", a fait savoir Tania McCrea-Steele, responsable du projet IFAW Global Wildlife Cybercrime.
"La mauvaise nouvelle est que les chercheurs d'Interpol ont trouvé des publicités vendant des parties de certaines des espèces les plus en danger sur terre sur l'une des plates-formes Internet les plus difficiles à contrôler", a-t-elle précisé.
Selon le rapport, l'usage de l'anonymat et le cryptage financier que permet le Darknet sont des atouts pour les commerçants illégaux de la faune.
"Plus de 96% du contenu d'Internet ne sont pas indexés par les moteurs de recherche standard, ce qui fait que le Deepweb dont fait partie le Darknet, représente environ 500 fois la taille du World Wide Web", indique le rapport, rappelant que le Darknet est généralement utilisé pour promouvoir les services illégaux ou les activités criminelles telles que le trafic de drogue, la criminalité financière, la cybercriminalité et en ligne et l'exploitation sexuelle des enfants.
En Afrique du Sud - qui compte la plus grande population de rhinocéros blancs et noirs du monde - le nombre de rhinocéros dont les cornes ont été coupées a augmenté "de plus de 90 fois entre 2007 et 2015, avec 1 054 animaux tués en 2016 seulement", souligne le rapport.

En 2016, plus de 20 tonnes d'ivoire d'éléphant, apprécié comme "l'or blanc" dans certaines régions d'Asie, en Chine, ainsi qu'aux Etats-Unis, ont été saisies par les forces de l'ordre à l'échelle mondiale a fait savoir Interpol.

"Les gros chats asiatiques sont tués pour leurs parties comme leur peau, leurs griffes, leurs dents, leurs os et leur sang, qui sont utilisés dans la médecine traditionnelle ainsi que le vin d'os de tigre, entre autres utilisations", explique le rapport.

Interpol a un partenariat de longue date avec IFAW dans la lutte contre la criminalité mondiale concernant la faune à la fois sur et hors ligne. En 2013, un projet d'Interpol soutenu par IFAW, concernant le commerce illégal d'ivoire en ligne, a mis au jour des centaines d'articles d'une valeur d'environ 1,45 million d'euros à vendre sur des sites d'enchères dans neuf pays européens sur une seule période de deux semaines.

http://french.china.org.cn/foreign/txt/2017-06/15/content_41029207.htm