Le hacking légal et rémunéré, vous connaissez ?

	Le hacking légal et rémunéré, vous connaissez ?

Le hacking : « accès et maintien frauduleux dans un système de traitement automatisé de données » va changer. Le 21 janvier 2016, l'Assemblée nationale a adopté, en première lecture, un amendement contenu dans le projet de loi pour une République numérique visant à compléter l'article 323-1 du Code pénal, par un nouvel alinéa :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système ».
Cet amendement, nommé « Bluetouff » en référence à l'arrêt de la Cour de cassation du 20 mai 2015 qui avait condamné un internaute pour s'être maintenu frauduleusement dans l'intranet de l'ANSES, prévoit, comme en matière d'association de malfaiteurs, une exemption de peine pour toute personne qui, après avoir constaté, voire exploité, une faille de sécurité en informe immédiatement l'autorité publique ou le maître du système.
Il ne s'agit là que d'une exemption de peine, et non d'une exemption de poursuites, ce qui en d'autres termes signifie que l'auteur du hacking, du piratage pourra être poursuivi et déclaré coupable, mais n'aura pas à exécuter de peines pénales.
Par cet amendement, le Gouvernement entend poursuivre un double objectif. D'abord donner une alternative presque légale au hacker du dimanche qui par défi personnel, et non intention de nuire, est parvenu à s'introduire dans un système d'information. A ce titre, il est regrettable que l'amendement Bluetouff ne prévoit qu'une exemption de peine, l'assurance de ne pas être poursuivi pour hacking aurait, à n'en pas douter, été plus convaincante.
En second lieu, il permettrait de participer à la sécurité du réseau. Garantie en poche de ne pas être pénalisés, nombre d'experts en informatique pourraient collaborer avec les sociétés développant des sites internet, applications ou logiciels pour identifier et corriger les vulnérabilités.
Ce dispositif serait, toutefois, incomplet s'il ne pouvait, par ailleurs, s'appuyer sur des initiatives de plus en plus courantes du secteur privé.
Les grands noms de l'internet et de l'informatique sont de plus en plus nombreux à proposer, souvent contre rémunération, aux hackers bien intentionnés de collaborer avec eux pour détecter les failles de sécurité.
Calqué sur ce qui existe déjà aux Etats-Unis avec la plateforme HackerOne, le site européen Bounty Factory mettant en relation hackers et entreprises du net permet depuis peu, en échange de récompenses pour toute faille décelée et corrigée, de signaler en ligne les vulnérabilités.
Législateur et secteur privé s'acheminent progressivement vers un droit au hacking. En attendant, le Code pénal nous rappelle qu' « accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende ».

Virginie Bensoussan-Brulé
Julien Kahn
Lexing Pénal numérique

Réagissez à cet article

Source : *Le hacking ça peut payer… légalement*

CNIL : les premiers chiffres des blocages des sites terroristes

CNIL : les premiers chiffres des blocages des sites terroristes

---

Depuis fin 2014, la loi sur le terrorisme permet la fermeture administrative des sites faisant l'apologie du terrorisme. La CNIL croule sous les demandes de retraits depuis le 13 novembre.

Depuis les attentats de novembre 2015, la CNIL doit faire face à de nombreuses demandes de retraits de contenus à caractère terroriste sur Internet. Vendredi, lors d'une conférence de presse, la commission présentait le premier bilan de son contrôle sur ces blocages administratifs.

Sites terroristes : plus de demandes que prévu selon la CNIL

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est chargé de surveiller les sites à caractères litigieux sur Internet (contenus pédopornographiques ou incitant au terrorisme). Lorsque ceux-ci font une demande de blocage, de retrait ou bien de déréférencement des moteurs de recherche, c'est la CNIL qui est chargé d'évaluer si une telle sanction est justifiée.
Depuis mars 2015, une « personne qualifiée » au sein de la CNIL a été nommée pour effectuer ses vérifications. C'est Alexandre Linden, conseiller honoraire à la Cour de cassation qui exerce ce rôle. Vendredi, il annonçait que 1439 demandes de retrait de contenus lui étaient parvenues, dont 1286 concernant des sites à caractère terroriste. « C'est beaucoup plus que ce que l'on avait prévu » s'est-il exprimé. Depuis les attentats de novembre 2015, les demandes de retraits ont même explosées.

Des contenus détectés majoritairement sur Twitter

En outre, Alexandre Linden s'est vu soumettre 855 demandes de déréférencement, que ce soit pour du contenu à caractère terroriste ou pédopornographique et 312 demandes de blocages de sites dont 68 à caractère terroriste, par l'OCLCTIC.
La majeure partie des contenus qui ont été retirés avaient été détectés « sur les réseaux sociaux du type Facebook ou Twitter« , explique Alexandre Linden. La CNIL précisant que ce sont la plupart du temps des « scènes de guerre, de scènes de mises à mort (ex : décapitation), des légendes de photographie accompagnant des drapeaux de Daesh et invitant à la haine à l'égard des 'mécréants'« .
Une seule demande de retrait n'a pas été considérée comme justifiée par la Commission, une photo des victimes du Bataclan prise peu de temps après l'attaque des terroristes. « Il faut veiller au contexte. Cette photo était accompagnée d'une légende explicative. Aussi, si elle pouvait faire l'objet d'une atteinte à la dignité des personnes, elle n'était pas constitutive d'une apologie du terrorisme« , justifiait M. Linden … [Lire la suite]

Réagissez à cet article

Source : *CNIL : les premiers chiffres des blocages des sites terroristes*

La Grande Loge de France victime d’une fuite de données massive

	**La Grande Loge de France victime d’une fuite de données massive**

La Grande Loge de France (GLDF) a porté plainte contre X pour #piratage informatique le 12 avril 2016 après la découverte d'un logiciel espion dans son réseau informatique. Fuite de données massive constatée.

C'est dans le blog « *La lumière* » hébergé par l'Express que l'information est sortie. La Grande Loge de France (GLDF) a porté plainte contre X pour piratage informatique le 12 avril 2016 après la découverte d'un logiciel espion dans son réseau informatique.
Toute l'histoire a débuté le 2 avril. Un code malveillant est introduit dans l'informatique de la GLDF. 48 heures plus tard, les informaticiens de La Grande loge tire la sonnette d'alarme. Un malveillant est passé par là. Il aurait réussi à atteindre le cloud de l'administration des Francs-maçons. Il semble qu'un cheval de Troie (ou tout simplement un phishing) a permis de mettre la main sur l'accès à ce « *nuage*« . Un cloud, qui faut-il le rappeler est le diable si le contenu des informations sauvegardées ne sont pas chiffrées, contenait des milliers de documents internes.

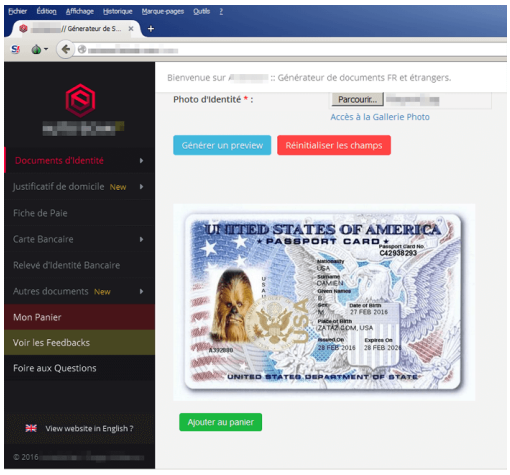
Fuite de données massive

Le pirate a diffusé l'ensemble des documents, sur son blog, le 10 avril, sous le nom de « *Franc Maçons Papers*« . Trouble et étonnante histoire. L'auteur de ce piratage et de sa diffusion ne se cache pas. Il parle même de « ***La plus grosse fuite de documents secrets de l'Histoire de France***« . Il faut dire aussi qu'avec près de 3 Go de données, que j'ai pu constater, la fuite n'est pas légère. A suivre !… [Lire la suite]

Réagissez à cet article

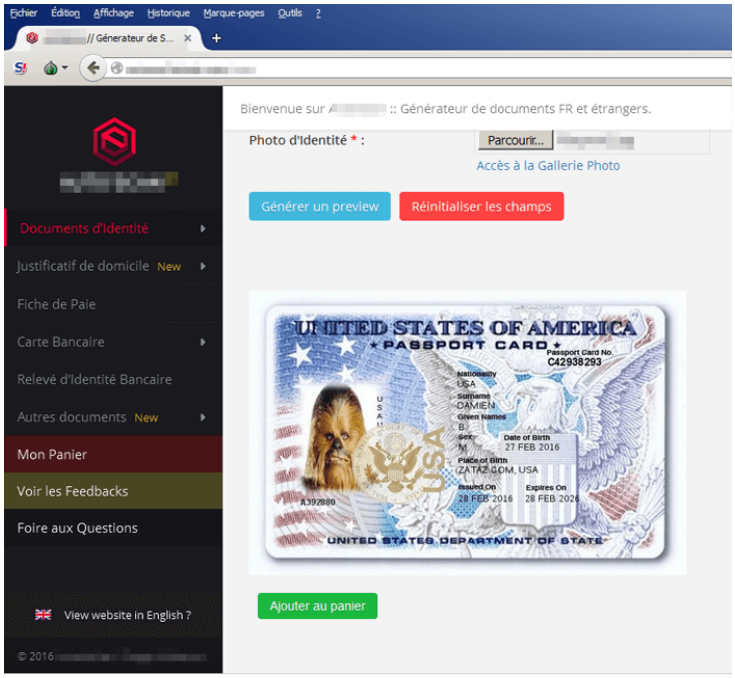
Source : *ZATAZ Fuite de données massive après un piratage chez les Francs-Maçons – ZATAZ*

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



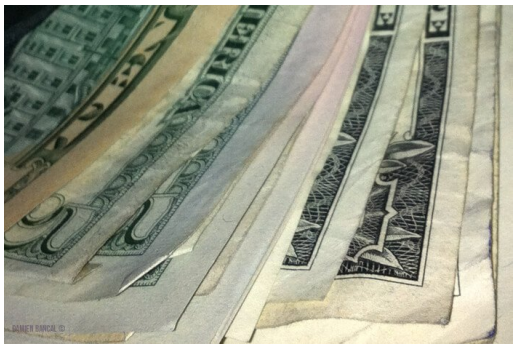
Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.
Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

Arnaque : Fausse collecte de dons via une opération de financement participatif



Arnaque : Fausse collecte de dons via une opération de financement participatif

---

Fausse collecte de dons : Participer à une collecte d'argent via un Financement participatif sur Internet ? Prudence ! Informez vous correctement des organisateurs pour ne pas finir dans les mains d'une arnaque !

Les parents de la petite Marlie, 1 an, n'en reviennent toujours pas. Cette famille canadienne a eu l'idée, il y a quelques semaines, de lancer un appel au don, sur Internet, pour permettre à leur fille atteinte de leucémie de recevoir un traitement médical coûteux.
Ils n'auraient jamais douté qu'un escroc du web profiterait de l'occasion pour mettre en place, sur un site de crowdfunding, le même appel aux dons. Une fausse collecte de dons qui aurait pu mal finir.
Cette campagne de sociofinancement reprenait toutes les données concernant l'enfant, dont la photo. Le malveillant n'a pas eu de mal à trouver les informations. Il les a recopié directement sur la page créée par les parents. La campagne avait été lancée sur le portail Gofundme.
250 dollars canadiens (300 euros) avaient déjà été promis avant que les autorités ne fassent fermer l'appel malveillant. La famille a déposé plainte.
Bref, prudence aux appels aux dons sur les sites de financement participatif. Prenez le temps de vous renseigner… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Fausse collecte de dons via une opération de*

La Lutte Contre la Cybercriminalité en Côte d’Ivoire. Plus qu’un enjeu économique, une réputation à la clé

	La Lutte Contre la Cybercriminalité en Côte d’Ivoire. Plus qu’un enjeu économique, une réputation à la clé

La Côte d'Ivoire a très longtemps souffert d'une image que l'on associait régulièrement aux diverses arnaques sur Internet. Le pays doit avant tout rassurer.

Il suffit d'analyser les principales arnaques sévissant sur les réseaux sociaux, sites de loisirs ou petites annonces en France pour qu'on constate que l'interlocuteur à l'identité fausse mais attrayante soit accessible à partir d'un numéro +225, l'indicatif de la cote d'ivoire.
Certes, Maliens et Nigérians font aussi partie de la fête, mais que ça soit Monsieur Loulou ROBERT, Monsieur Jean OVIDIE, Monsieur Alain BRULIN, se faisant passer tout à tour pour une personne intéressée par un véhicule, une poupée barbie ayant reçu un coup de foudre, votre meilleur ami à qui on a volé son télépone et ses papiers ou bien une riche personne désirant partager son héritage, ces brouteurs sont Ivoiriens.
Devant l'ampleur du phénomène et l'enjeu majeur que représente la sécurité des systèmes d'information à l'échelle de la Côte d'Ivoire, de l'Afrique et du monde entier, les autorités et les acteurs économiques du pays on commencé il y a quelques années à réagir en multipliant des actions de formations, de sensibilisation et de perfectionnements technologiques.

Cependant, dans le but de faciliter le développement économique en Côte d'Ivoire et en Afrique des principales entreprises en les rassurant, créer et organiser des forums en 2016 (Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone à Grand-Bassam en février dernier et le 8ème édition de l'IT Forum à Abidjan en juin prochain) est un bon début mais ne suffit pas.
En effet, enfin d'enrayer le phénomène de la cybercriminalité, il est important, essentiel et urgent que la Côte d'Ivoire et ses voisins de l'Afrique de l'ouest s'engage à adhérer pour une coopération internationale comme a commencé à le faire à ce jour (15/04/2016), un seul pays d'Afrique, l'Afrique du Sud, en signant la Convention de Budapest.

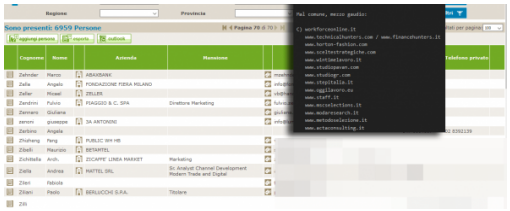
Source : Denis JACOPINI
Illustration : http://abidjantv.net

Etat des signatures et ratifications de la Convention de Budapest

---

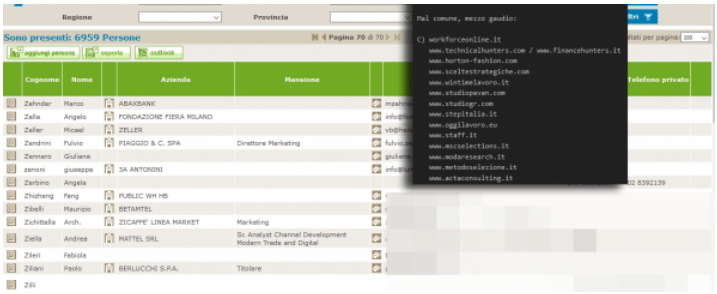
Réagissez à cet article

Des milliers de données clients diffusées sur Internet par Anonymous



Des milliers de données clients diffusées sur Internet par Anonymous

Données clients diffusées sur Internet – Des internautes ont lancé, sous la signature Anonymous, une opération contre le business des laboratoires pharmaceutiques. Ils veulent dénoncer « les porcs et les connivences entre les gouvernements et les sociétés« . En Italie, c'est un hébergeur qui fait les frais d'une cyber action.



Étonnante revendication que celle lancée par les Anonymous. Lundi 11 avril, des internautes ont lancé un appel pour cibler « ***les porcs et les connivences entre les gouvernements et les sociétés pharmaceutiques***« . Pour les organisateurs, la mission est de collecter des informations, des données, pour les diffuser ensuite. « ***Nous voulons dire la vérité sur le cancer, la nutrition, les médicaments…*** » indique les personnes cachées derrière la signature et le masque Anonymous. « ***Notre santé est plus importante que leur profit !*** […] ***Beaucoup d'entre vous ont déjà pris conscience de ce système axé sur les profits, il est temps de prendre des mesures, il est temps d'exposer la corruption et demande justice pour les victimes*** ».

En Italie, des données clients diffusées sur Internet

En Italie, l'agence web Engitel, basée à Milan, se faisait pirater et voler plusieurs milliers de données par Anonymous Italia et un second groupe du nom de LulzSecITA. 40 sites impactés, plus de 2 800 fichiers sensibles ont d'abord été diffusés. Ici pas d'attaque SQL, mais ce qui semble être une copie conforme des données clients, et leur site web, via l'espace d'administration de l'entreprise Milanaise.

Anonymous Italie, la source initiale de la fuite, a affirmé qu'il y avait plus de 1,8 millions de données d'utilisateurs. Ils vont le prouver en diffusant plusieurs autres dossiers, via MEGA. Dans l'un des dossier que j'ai pu consulter, des fichiers qui permettent de contacter les responsables des sites Internet (J'ai pu en dénombre 6 959) de sociétés italiennes telles que MTV Italie, La Repubblica, Facebook Italie, Gucci, FastWeb, Microsoft, Wind, Ducati… « ***Voici notre premier chapitre de notre opération Nessun Dorma,*** indique les hacktivistes. ***Nous sommes fatigués des mensonges habituels diffusés dans tous les médias au sujet du monde du travail*** ».

Bref, comme l'indiquent les pirates dans leur – communiqué de presse – : Si vous voulez la paix, préparez la guerre. A noter que plusieurs sites Suisses (aiti.ch, e-lavoro.ch, aitiservizi.ch, e-impresa.ch, jobopportunity.ch, BFKconsulting.ch, helvia.ch et workandwork.ch) ont été piratés lors de cette opération… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Anonymous : des milliers de données clients diffusées sur Internet – ZATAZ*

Jigsaw, un rançongiciel avec compte à rebours destructeur

Jigsaw, un rançongiciel avec compte à rebours destructeur

Une heure… C'est le délai que laisse à sa victime le rançongiciel Jigsaw pour verser sa rançon. Passé ce délai, il commence à détruire les fichiers de l'ordinateur en accélérant son rythme toutes les heures. Des experts en sécurité ont trouvé le moyen de s'en débarrasser. Pour l'instant.

Apparemment, le versement d'une rançon en bitcoins ne suffit plus à certaines cyber-fripouilles, auteurs de ransomwares, pour fournir à leurs victimes la clé qui leur permettra de déchiffrer les fichiers de leur ordinateur. Il s'en trouve maintenant pour exiger des utilisateurs attaqués qu'ils s'en acquittent en moins d'une heure. Un nouveau programme dénommé Jigsaw chiffre les fichiers et commence à les détruire petit à petit jusqu'à ce que le malheureux utilisateur verse l'équivalent de 150 dollars en monnaie virtuelle Bitcoin. Après une heure, le ransomware détruit l'un après l'autre les fichiers, puis, après chaque cycle de 60 minutes, augmente le nombre de fichiers supprimés. Si aucun paiement n'est effectué dans un délai de 72 heures, tous les fichiers restants disparaissent. « Essayez de tenter quelque chose d'amusant et l'ordinateur appliquera certaines mesures de sécurité pour détruire vos fichiers », prévient un message du pirate accompagnée du masque du personnage de tueur Jigsaw, de la série de films d'horreur Saw.

Et ce n'est pas une menace en l'air.

Le malware est tout sauf inactif. Selon certains experts du forum de support technique BleepingComputer.com, ce rançongiciel détruit un millier de programmes à chaque fois que l'ordinateur redémarre ou que son processus est relancé. Dans un billet, Lawrence Abrams, fondateur du site, constate que c'est la première fois que l'on voit ce type de menaces propagées par le biais d'une infection par ransomware. La bonne nouvelle, pour l'instant, c'est que les experts ont élaboré une méthode pour déchiffrer les fichiers affectés par Jigsaw sans avoir à payer la rançon.

Inactiver Jigsaw puis déchiffrer les fichiers à l'aide d'un utilitaire

La première chose à faire, c'est d'ouvrir le gestionnaire de tâches de Windows et de terminer tous les processus appelés firefox.exe ou drpbx.exe qui ont été créés par le ransomware, indique Lawrence Abrams. Puis, il faut lancer l'utilitaire Windows MSConfig et supprimer l'entrée de démarrage pointant vers %UserProfile%AppDataRoamingFrfxfirefox.exe. Cela arrêtera le processus de destruction des fichiers et empêchera le malware de se relancer au redémarrage du système. Les utilisateurs pourront alors télécharger l'utilitaire Jigsaw Decrypter hébergé par BleepingComputer.com afin de déchiffrer leurs fichiers. Lorsque ce sera fait, il est hautement recommandé de télécharger un logiciel anti-malware à jour et de lancer un scan complet de son ordinateur pour désinstaller entièrement le ransomware.
En novembre, un précédent programme d'attaque dénommé Chimera menaçait de diffuser les fichiers des utilisateurs sur Internet. Toutefois, rien n'a prouvé qu'il était en mesure de le faire. Par comparaison, Jigsaw met ses menaces à exécution et révèle une évolution inquiétante sur ce terrain. Si les experts en sécurité ont trouvé un moyen de déchiffrer les fichiers cette fois, rien ne garantit qu'ils pourront le faire avec les prochaines versions. Les pourvoyeurs de ransomware sont généralement prompts à corriger leurs erreurs… [Lire la suite]

Pour info, en plus des technologies indispensables comme l'**anti-phishing** (pour **se protéger des e-mails de phishing**) et l'**anti-malware** (pour **se protéger des malwares cachés dans des e-mails ou des sites internet infectés**) qui protègent les clients contre les menaces d'Internet, ESET Smart Security 9 contient une toute nouvelle protection des transactions bancaires. Cette fonction met à disposition l'ouverture d'un navigateur sécurisé pour veiller à ce que toutes les transactions financières en ligne soient effectuées en toute sécurité. L'utilisateur peut également paramétrer lui-même tous les sites bancaires de paiement en ligne qu'il consulte le plus fréquemment.

Réagissez à cet article

Le Sénégal lutte toujours plus contre la cybercriminalité

	Le Sénégal lutte toujours plus contre la cybercriminalité

Le Sénégal veut se doter de moyens efficaces pour lutter contre la cybercriminalité. C'est ce qu'a déclaré ce matin, le ministre des Postes et des Télécommunications, lors de la cérémonie d'ouverture d'un panel dédié à ce fléau.

Cette rencontre contre intervient un an après que le Sénégal et le royaume des Pays-Bas ont lancé à la Haye, une initiative internationale sur la sensibilisation des Etats et des différents acteurs sur la question de la cybersécurité », a déclaré Yaya Abdoul Kane.

Selon lui, cette plateforme est venue à son heure puisqu'elle peut permettre de doter les pays africains et les experts, d'espace «pour échanger sur les expériences réussies et les bonnes pratiques en matière de cybersécurité. Nous pensons, après cette réflexion, pouvoir avoir des éléments sur lesquelles nous allons pouvoir nous baser pour affiner notre stratégie nationale sur la cybersécurité», révèle-t-il.

Pour avoir de bons résultats dans cette lutte, le Sénégal compte prendre les devants. Et c'est dans ce sens, informe le ministre des Postes et des Télécommunications, que « la formation des magistrats, mais également la création au niveau de la Police d'une brigade spécialisée en cybersécurité», a commencé.

Mais notre pays ne compte pas en rester là puisque : «qu'il est aujourd'hui opportun de renforcer ce dispositif et d'arriver à avoir une stratégie nationale sur la cybersécurité, mais aussi d'arriver à l'harmonisation d'un cadre juridique et règlementaire au niveau sous régional, voir international, pour une meilleure prise en charge de la question», conclut-il… [Lire la suite]

Source : *Lutte contre la cybercriminalité: Le Sénégal au premier rang*

San Bernardino : c’est une faille zero day qui a permis au FBI de craquer l’iPhone 5c

	San Bernardino : c’est une faille zero day qui a permis au FBI de craquer l’iPhone 5c

Le FBI est parvenu à récupérer les données stockées dans l'iPhone 5c du tueur de San Bernardino grâce à une faille zero day. Cette vulnérabilité, qui ne toucherait pas les modèles plus récents d'iPhone, aurait ensuite permis aux enquêteurs d'utiliser un appareil pour rentrer le code de déverrouillage à quatre chiffres, sans activer les mesures de protection de l'appareil.

La première d'entre elles est un délai qui s'accroit : après trois tentatives, il faut attendre une minute ; après la tentative suivante, le délai est de cinq minutes. La deuxième mesure est l'effacement des données au bout de dix tentatives infructueuses. Sans le délai, craquer un iPhone protégé par un code à 4 chiffres ne prend que 26 minutes d'après le décompte du FBI, le temps de tester les 10 000 combinaisons possibles.

Trouver cette faille a été le travail de chercheurs en sécurité qui ont été rémunérés pour ce travail, explique le *Washington Post*, et malgré le battage médiatique autour de Cellebrite, l'entreprise ne serait pour rien dans cette découverte…
Alors que les « white hats » rapportent les vulnérabilités aux constructeurs et éditeurs pour qu'ils les corrigent, les « black hats » exploitent ces failles pour voler des données ; le hacker qui a donné un coup de main au FBI fait partie d'une autre catégorie, les « grey hats ». Après la découverte d'une vulnérabilité, ils tentent de la vendre à des gouvernements ou à des entreprises spécialisées dans la surveillance, sans prévenir les constructeurs.
Le gouvernement américain s'interroge maintenant pour divulguer la faille en question à Apple, qui a par ailleurs indiqué son intention de ne pas poursuivre les autorités pour connaitre la vulnérabilité… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : c'est une faille zero day qui a permis au FBI de craquer l'iPhone 5c | MacGeneration*