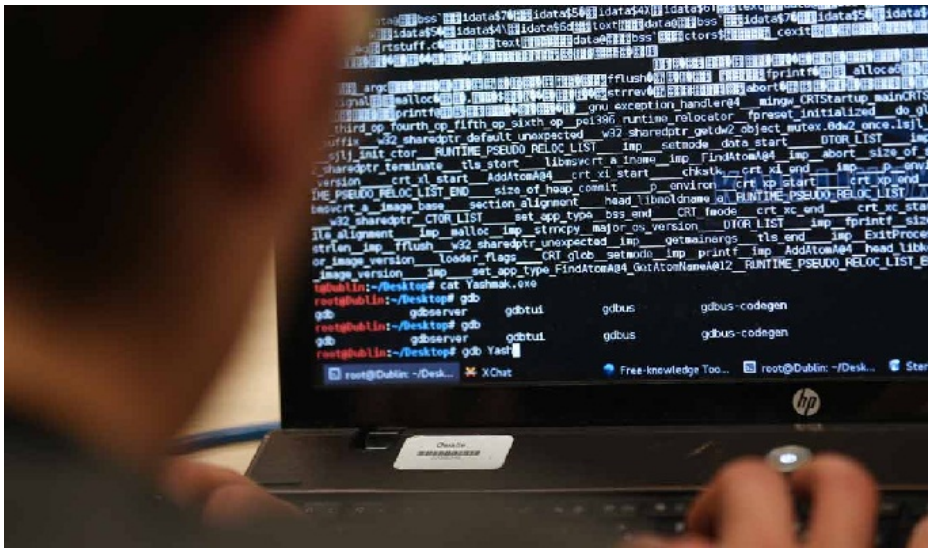
Cyberattaques terroristes déjouées au Maroc



Cyberattaques terroristes déjouées au Maroc

Des cyberattaques de sites étatiques planifiées par des individus soupçonnés d'avoir des penchants extrémistes et des relations avec Daech ont été déjouées dans le Royaume du Maroc grâce à une vaste opération antiterroriste qui a abouti à l'arrestation et la garde à vue de 52 personnes.

Selon un communiqué du ministère de l'Intérieur cité par des médias locaux, dont le Matin.ma, ainsi que le quotidien ivoirien Fraternité Matin, cette opération antiterroriste a été menée sous la houlette du parquet général et visait 343 individus.

Outre des projets terroristes ciblant des centres de loisir, des festivals, des établissements sécuritaires du Royaume, des cyberattaques à un niveau de préparation bien avancée devaient être dirigées contre les institutions marocaines. Objectif? Bloquer le fonctionnement des structures étatiques et paralyser l'économie.

D'autres personnes arrêtées par les forces de police marocaine sont soupçonnées de recruter des combattants mineurs via les réseaux sociaux.

Article original de Alselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Terrorisme : des cyberattaques déjouées au Maroc | CIO MAG

Ma vie disséquée à travers mes données personnelles

Ma vie disséquée à travers mes données personnelles

Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

Le site Internet des avocats de Mossack Fonseca, encore piraté !

Le site Internet des avocats de Mossack Fonseca, encore piraté !

Nous aurions pu penser que l'affaire des fuites de données du Panama Papers et du cabinet d'avocats Mossack Fonseca aurait permis à ces derniers de comprendre ce qu'était la sécurité informatique ! Raté !

Mossack Fonseca, pour rappel, un cabinet d'avocats basé au Panama qui a connu des fuites de données, voilà quelques mois. Des juristes qui cherchent des opportunités économiques aux entreprises, banques, artistes, politiques et sportifs ayant de l'argent à placer… hors de leur juridiction fiscale nationale.

Plusieurs fuites de données avaient été révélées en mars 2016, visant les clients de cette entreprise d'Amérique Centrale. Je vous expliquais comment, en quelques clics de souris et l'ami Google, j'avais pu accéder à plusieurs dizaines de milliers de CV, sauvegardés dans le portail web de « Monseca », comme du vulgaire papier. La presse Internationale, via les Panama Papers avaient diffusé des centaines d'informations sur des « VIP » ayant tenté de cacher à l'administration fiscale l'argent qu'ils possédaient.

Six mois plus tard, nous aurions pu penser que ces « professionnels » avaient pris quelques cours, du moins d'éducation numérique, pour protéger leurs sites Internet. Raté ! D'abord le noyau Linux qui fait tourner leur serveur. Un pirate Russe leur a stipulé, sur Twitter, qu'il datait toujours de 2013. Autant dire qu'il s'est empressé de lancer une petite attaque, histoire de réveiller ses interlocuteurs. Une autre fuite, cette fois avec le fichier phpinfo.php, accessible d'un clic de souris, offrant a qui sait le lire, des données pouvant être exploitées à des fins malveillantes.

A noter que de nouvelles révélations sont annoncées dans cette affaire du Panama Papers. Du blanchiment d'argent et du détournement concernant des hommes d'affaires, en Afrique !

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : ZATAZ Fuites de données : le site des avocats de Mossack Fonseca, encore ! – ZATAZ

---

150 Go de données médicales volées seraient dans la nature !

150 Go de données médicales volées seraient dans la nature !

Un pirate (ou un groupe) aurait mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie américain, contenant des données précises sur le suivi de patients. Une tendance de plus en plus répandue outre-Atlantique.

Les données médicales semblent prisées des pirates. Un (groupe de) pirate(s), nommé Pravvy Sector, aurait ainsi mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie de l'Ohio, rapportait hier Motherboard. Le contenu trouvé concernerait à la fois les cliniques elles-mêmes (avec des données sur ses ressources humaines) et les patients, avec des indications précises sur leur suivi médical, leur traitement ou encore leurs informations d'assurance.

Motherboard a contacté trois patients présents dans le fichier identifié, dont deux ont pu confirmer que les informations publiées étaient exactes pour eux. L'origine des données, qui semblent bien venir du réseau de cliniques lui-même, n'a pas pu être confirmée. Contactée par le site américain, l'organisation n'a pas encore répondu à ses demandes de commentaires.

Bien avant cette publication, Pravvy Sector aurait été en quête de reconnaissance, contactant directement certains médias avec les contenus de « fuites » précédentes. Mais le plus important est la tendance que deviennent les incidents liés aux données médicales. Comme le relève The Verge, 49 intrusions affectant plus de 500 personnes ont été signalées dans le secteur médical, depuis le début de l'année.

En juin, une autre fuite présumée concernait 655 000 enregistements médicaux, via plusieurs organismes. Si l'ensemble des données n'a pas pu être authentifié, un échantillon l'avait été à l'époque par Motherboard. Contrairement à la publication de Pravvy Sector, les informations étaient cette fois vendues sur un site spécialisé.

Article original de Guénaël Pépin

Réagissez à cet article

Original de l'article mis en page : États-Unis : 150 Go de données médicales seraient dans la nature

Attention à l’application « Rio Olympics 2016 «

	Attention à l’application « Rio Olympics 2016 «

Avec l'approche des jeux Olympiques de Rio, le téléchargement d'applications thématiques va battre son plein. Gare aux applications dangereuses !
Rio Olympics 2016 Keyboard, un clavier publicitaire dangereux !

La société Lookout Mobile Security vient d'alerter ZATAZ de certains problèmes de confidentialité et des enjeux rencontrés par les utilisateurs et les entreprises avec l'application Rio Olympics 2016 Keyboard. Une APP disponible en version iOS et Android.
L'application officielle de l'entreprise américaine NBC Universal Media, Rio 2016 Olympics keyboard est en apparence une simple extension de clavier pour les personnes qui suivent les jeux Olympics. Cependant, il a identifié que cette application était capable de compiler plus d'information qu'initialement prévu par son développeur, exposant ainsi la confidentialité des données des amateurs des JO de RIO et possiblement des entreprises pour lesquelles ils travaillent.
Finalement, l'équipe de recherche a informé NBCUniversal des enjeux de confidentialité identifiés dans les versions Android et iOS de l'application officielle Rio 2016 Keyboard. NBCUniversal a réagi rapidement pour résoudre les problèmes identifiés et s'assurer que les versions disponibles seraient sécurisées avant l'ouverture des Jeux Olympiques d'été de Rio. Si vous avez téléchargé l'application, effacez là. A vous de décider, ensuite, si vous installez la nouvelle version.

Réagissez à cet article

Original de l'article mis en page : ZATAZ L'appli Rio Olympics 2016 Keyboard dangereuse – ZATAZ

Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Les deux experts qui avaient piraté une Jeep Cherokee récidivent dans le cadre de la Black Hat en démontrant une attaque sur le même véhicule.

En 2015, la Black Hat avait vu deux spécialistes en sécurité, Charlie Miller et Chris Valasek, prendre le contrôle à distance d'une Jeep Cherokee de 2014. Un exploit qui a obligé Chrysler, propriétaire de Jeep, à procéder à un rappel de près de 1,4 million de véhicules. Une opération de mise à jour coûteuse pour le constructeur automobile. Il en a profité aussi pour lancer un Bug Bounty, avec des primes allant de 150 à 1500 dollars.

Un programme auquel les deux experts ne pourront pas concourir. Car ils démontrent à la Black Hat 2016 que la sécurité des voitures connectées n'est toujours pas optimale, malgré les récentes mises à jour. Dans une présentation, ils présentent une attaque contre la même Jeep Cherokee de 2014. A la différence de l'année dernière, cette attaque n'est pas menée à distance, mais avec un accès physique à la voiture. Néanmoins, le duo précise qu'avec du temps elle pourrait être réalisée via un terminal embarqué ou à distance via une liaison sans fil.

Blocage des freins et coup de volant intempestif

Une fois dans la voiture, Charlie Miller a branché son ordinateur sur le réseau du véhicule, nommé bus CAN, via un port situé sous le tableau de bord. Ce réseau envoie des instructions aux différents capteurs (consommation, confort, détection de panne, etc). L'accès à ce réseau est normalement sécurisé avec le patch de sécurité élaboré l'année dernière à la suite du premier piratage de la Jeep. Il semble que des failles subsistent et les deux spécialistes ont pu contourner certains garde-fous.

Parmi les actions réalisées, ils ont bloqué les freins. Charlie Miller s'est servi du mode maintenance pour rendre inopérant le freinage. D'habitude ce blocage des freins ne peut s'opérer qu'à une faible vitesse soit 5 miles par heure. Dans une vidéo, le duo roule sur une route de campagne et d'un coup (après un compte à rebours) le volant se met à tourner à 90 degrés plantant la Jeep dans le fossé. Pour se faire, Charlie Miller s'est servi de la fonction tourner le volant dans la fonction parking automatique (qui se fait habituellement en marche arrière et à faible vitesse). Concrètement pour réaliser leur piratage, les deux experts se sont attaqués à la fois aux bus CAN, mais surtout en ciblant directement les ECU (electronic control units) dont un a été placé en mode maintenance et un autre utilisé pour envoyer des commandes malveillantes.

Interrogé par nos confrères de Wired, Chrysler ne considère pas cette attaque comme un danger pour la sécurité des véhicules. En premier lieu, elle nécessite un accès physique à la voiture. De plus, les experts ont utilisé une Jeep Cherokee ne disposant pas de la dernière version du logiciel embarqué d'infotainment (vecteur de leur première attaque en 2015). Les experts précisent que même avec la dernière version, cette attaque est toujours possible.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Direction, frein : les hackers de Jeep récidivent à la Black Hat

Si le E-commerce était retranscrit dans la réalité

Si le E-commerce était retranscrit dans la réalité

Une Vidéo qui retranscrit ce que nous vivons sur la toile dans le processus de vente des sites en ligne.

Je pense qu'énormément de personnes vont se reconnaitre dans cette vidéo si vous achetez régulièrement sur la toile. Vous le savez quand vous souhaitez acheter un produit, le « tunnel d'achat » est souvent long et fastidieux. Entre la première visite et la réception de l'email de confirmation de commande, il se peux que vous passiez un certain nombre de minutes. Surement trop long j'en suis sûr. Trop d'informations à donner, création de compte, j'en passe et des meilleurs. Je suis sur que vous avez déjà été confronté aux « Kapcha » indécodable ou encore à l'expiration de la session…

Voila ce que résume cette vidéo. Une caricature de ce qu'il nous arrive en ligne. J'ai trouvé cela très drôle et très bien monté.

Je pense que pour ceux qui réalise des sites web, c'est souvent la problématique principale. Comment ne pas perdre de clients potentiels dans un processus de vente fastidieux et trop complexe.

Article original de David Gaborit

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Si le E-commerce était retranscrit dans la réalité. – Olybop

---

Les conséquences inatendues des changements trop fréquents de mots de passe

Les conséquences inatendues des changements trop fréquents de mots de passe

---

Il est préférable d'opter pour des mots de passe robustes, plutôt que d'imposer des changements fréquents, réaffirme la responsable des technologies de la FTC.

Fraîchement nommée chef des technologies de la Federal Trade Commission (FTC), Lorrie Cranor (également professeur à l'université Carnegie Mellon), avait été surprise par un tweet officiel mis en ligne en janvier. Le régulateur américain du commerce préconisait alors un changement fréquent de mots de passe. La spécialiste s'y est opposée. Depuis, elle fait évoluer la politique interne sur le sujet.

« Je suis allée voir les personnes en charge des médias sociaux et leur ai demandé pourquoi [la FTC dit à tout le monde de changer de mots de passe] », a commenté Cranor lors de la conférence *Passwords* de BSidesLV 2016, dont *Ars Technica* s'est fait l'écho. *« Elles m'ont répondu ceci : 'C'est probablement un bon conseil, car à la FTC nous changeons nos mots de passe tous les 60 jours' »*.

Lorrie Cranor s'est alors entretenue avec le #DSI et le RSSI de la FTC. Elle a souligné, rapport d'experts à l'appui, que les changements fréquents n'améliorent pas la sécurité, mais encouragent au contraire l'utilisation de mots de passe plus susceptibles d'être découverts et détournés.

Un modèle, des mots de passe

Lorsque des utilisateurs doivent changer de mots de passe tous les 90 jours, par exemple, ils ont tendance à utiliser un même modèle. C'est ce qui ressort d'une étude publiée en 2010 par des chercheurs de l'université de Caroline du Nord (UNC) à Chapel Hill.

« Les utilisateurs prennent leurs anciens mots de passe, puis ils les changent légèrement [d'une lettre, d'un chiffre ou d'un symbole] pour obtenir un nouveau mot de passe », a expliqué Cranor. Or la capacité de ces mots de passe à résister aux attaques par force brute est faible. 17 % des mots de passe testés par les chercheurs de l'UNC auraient ainsi été découverts en moins de cinq tentatives.

Il est donc préférable, selon eux, d'utiliser des mots de passe forts, plutôt que d'en changer souvent. La double authentification est également recommandée, notamment pour les applications sensibles.

Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Les changements fréquents

de mots de passe nuisent à la sécurité

Le bitcoin victime d’une faille dans le système ?

Le bitcoin victime d’une faille dans le système ?

Bitfinex, plus grande place d'échange de bitcoins en dollars, suspend son activité après le vol de près de 120 000 bitcoins dans son système. La cryptomonnaie a perdu 5,5 % de sa valeur dans la journée.

La plateforme de change hongkongaise Bitfinex a annoncé mardi dans un communiqué avoir « *découvert une faille de sécurité qui l'oblige à geler toute transaction* […] *ainsi que tout dépôt et retrait de fonds* ». « *Je peux confirmer que la perte à la suite du hack est de 119 756 BTC* », a déclaré Zane Tackett, CTO du groupe, sur Reddit. Au cours actuel de 540 dollars pour un bitcoin, la valeur des bitcoins qui se sont volatilisés s'élève à environ 65 millions de dollars.

En noir, la valeur d'échange du bitcoin au dollar (échelle de droite). En vert et en rouge, les volumes des transactions (échelle de gauche en milliers de bitcoins).

Le cours du bitcoin a perdu 5,5 % contre le dollar dans la journée de mardi, soit une chute de 13 % en deux jours. La valeur de la cryptomonnaie avait cela dit perdu 6,2 % lundi, sans que le lien avec le hack soit avéré. C'est au total l'équivalent de 1,5 milliard de dollars qui s'est évaporé de la capitalisation marchande du bitcoin cette semaine.

Avant l'incident, Bitfinex était la plus grosse plateforme de change avec le dollar, totalisant 8,5 % de tous les échanges de bitcoins. Elle était néanmoins derrière le chinois OKCoin, dont 90 % du trading s'effectue en yuans.

LES ATTAQUANTS DOIVENT COMPROMETTRE LES DEUX ORGANISATIONS AVANT D'OBTENIR LES FONDS

La plateforme hongkongaise assure sa sécurité avec BitGo, une firme basée à Palo Alto (Californie), via un système de multi-signature. Lors du partenariat, Bitfinex avait déclaré que grâce à un tel procédé, « les attaquants doivent compromettre les deux organisations avant d'obtenir les fonds ». Aujourd'hui, BitGo affirme ***ne pas avoir découvert de brèches*** *de son côté.*

En février 2014 s'était déjà produit ***un événement similaire*** *d'une ampleur bien plus grave. La plateforme tokyoïte Mt.Gox, où s'échangeaient à l'époque 70 % des bitcoins du monde, avait également affirmé avoir été victime de pirates : 744 408 bitcoins, soit 450 millions de dollars selon la valeur du cours au moment de l'incident, avaient été dérobés au système.*

Depuis, MtGox a mis la clé sous la porte après de forts soupçons sur son honnêteté, et qui perdurent encore aujourd'hui. En l'espace d'un mois, la cryptomonnaie avait plongé 30 % mais, habituée à une volatilité extrême, elle s'en était vite remise.

Article original de Victoria Castro

Réagissez à cet article

Original de l’article mis en page : Le bitcoin dévisse après un piratage à 65 millions de dollars – Business – Numerama

---

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Avant même la sortie sous Android de Prisma, une application populaire de retouche photos, Google Play Store s'était retrouvé inondé de fausses applications.

Les chercheurs d'ESET ont découvert de fausses applications imitant Prisma, dont plusieurs Chevaux de Troie dangereux. Dès l'avertissement d'ESET, le service sécurité de Google Play a retiré toutes les fausses applications du store officiel d'Android. Ces dernières auront tout de même atteint plus d'1,5 millions de téléchargements.
Prisma est un éditeur de photos unique publié par les laboratoires de Prisma. D'abord développé pour iOS, cette application a remporté d'excellents résultats de la part des utilisateurs d'iTunes et de l'App Store d'Apple. Les utilisateurs d'Android étaient à leurs tours impatients de la découvrir sur le Google Play (disponible depuis le 24 juillet 2016).
« La plupart des fausses applications de Prisma disponibles sur Google Play ne disposent pas d'une fonction retouche photo. A l'inverse, elles affichent uniquement des annonces, avertissements ou de faux sondages pour tromper l'utilisateur qui fournit des informations personnelles le concernant ; ou encore pour le faire souscrire à de faux services type SMS onéreux », commente Lukáš Štefanko, Malware Researcher chez ESET.
La plus dangereuse des fausses applications imitant Prisma et trouvée dans le Google Play est un Cheval de Troie téléchargeur détecté par ESET comme Android/TrojanDownloader.Agent.GY. Des informations sur les périphériques sont envoyées au serveur C&C, ce qui lui permet de télécharger sur demande des modules supplémentaires et de les exécuter afin de voler des données sensibles telles que le numéro de téléphone, l'opérateur, le pays, la langue etc.
A cause de ses capacités de téléchargement, la famille des malwares type Android/TrojanDownloader.-Agent.GY pose de sérieux risques pour les plus de 10.000 utilisateurs Android qui ont installé cette application dangereuse avant d'être retiré du Google Play Store.

Pour se protéger, Denis JACOPINI recommande l'application suivante :

Article original de Eset

Réagissez à cet article