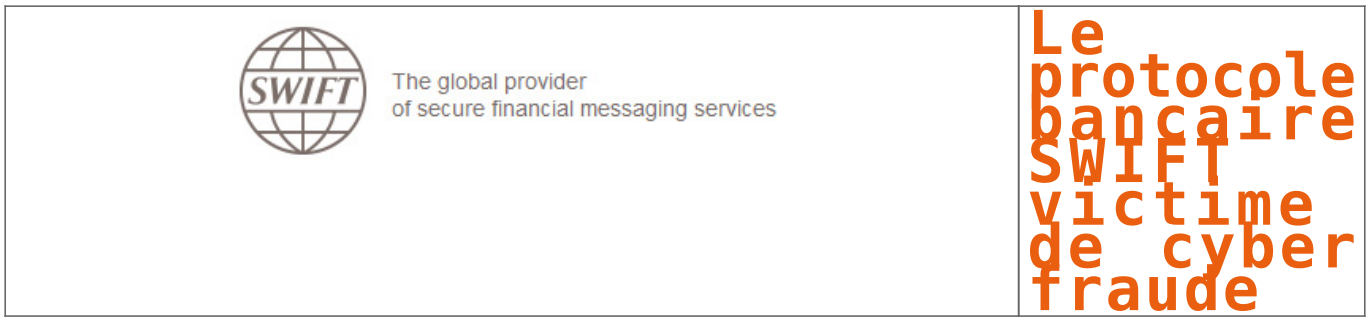
Le protocole bancaire SWIFT victime de cyber fraude



Suite à la récente cyber attaque la Banque du Bangladesh, l'organisme SWIFT vient de reconnaître que son logiciel a été utilisé pour cacher des preuves de transferts frauduleux.Par Aimee Chanthadavong, ZDNet.com | Mardi 26 Avril 2016

SWIFT (Society for Worldwide Interbank Financial Telecommunication), le réseau financier mondial que les banques utilisent pour transférer des milliards de dollars chaque jour, vient d'avertir ses clients « d'un certain nombre de récents incidents de cybersécurité » sur son réseau : les attaquants ont utilisé son système pour envoyer des messages frauduleux.

Cette révélation intervient alors que les autorités du Bangladesh continuent leur enquête sur le vol de 81 millions de dollars en février dernier. Le transfert litigieux a transité d'un compte de la Banque du Bangladesh vers la New York Federal Reserve Bank. Un des enquêteurs, Mohammad Shah Alam, du Forensic Training Institute du Bangladesh, a déclaré à Reuters que la Banque du Bangladesh était une cible facile pour les cybercriminels car il n'y avait pas de pare-feu et que par ailleurs des commutateurs d'entrée de gamme étaient utilisés pour connecter les systèmes informatiques de la banque à SWIFT.

5 paiements frauduleux sur 35 ont été autorisés

Les chercheurs en cyber-sécurité qui travaillent sur ce hold-up ont expliqué le mois dernier qu'un logiciel malveillant avait été installé sur les systèmes informatiques de la Banque du Bangladesh. Ce malware a permis aux attaquants de se dissimuler avant de prendre l'argent. Un rapport interne de la Banque du Bangladesh mentionne que la Réserve Fédérale a été négligente : elle a validé les fausses transactions. Le rapport parle de «faute majeure». Il indique également que 5 paiements frauduleux sur 35 ont été autorisés (pour un total de 951 millions de dollars), et que des entités situées aux Philippines et au Sri Lanka ont reçu une partie des fonds volés. Et c'est une faute d'orthographe commise par les cybercriminels qui a empêché 20 autres millions de dollars de disparaître en plus des comptes de la Banque du Bangladesh.

Ce vol a provoqué la démission du responsable de la Banque du Bangladesh, Atiur Rahman, 64 ans. Il n'avait pas jugé bon d'informer le ministre des finances du Bangladesh, A M A Muhith, de l'incident. Ce dernier avait appris cet évènement dans la presse étrangère.

SWIFT a reconnu que l'attaque incluait la modification des logiciels SWIFT sur les ordinateurs de la banque pour dissimuler les preuves de transferts frauduleux. « SWIFT est au courant d'un certain nombre d'incidents de cyber récents dans lesquels des personnes malveillantes dans l'entreprise, ou des pirates externes, ont réussi à envoyer des messages SWIFT depuis les back-offices, PC ou postes de travail des institutions financières connectées au réseau SWIFT » avertit l'organisme dans une message d'avertissement à ses clients.

L'avertissement, émit par SWIFT via une alerte confidentielle envoyée sur son réseau lundi, ne donne ni le nom des victimes ou le montant des sommes dérobées. SWIFT a également publié une mise à jour de sécurité pour le logiciel que les banques utilisent pour accéder à son réseau.

SWIFT : 3 000 institutions financières, 11 000 banques

Cette mise à jour doit sécuriser son système vis à vis du malware que les chercheurs de BAE Systems soupçonnent avoir été utilisé dans le hold-up de la Banque du Bangladesh. Les preuves collectées par BAE suggèrent que les pirates ont manipulé le logiciel Alliance Access de SWIFT, que les banques utilisent pour s'interfacer avec la plate-forme de messagerie de SWIFT, afin de brouiller les pistes. BAE a cependant mentionné ne pas pouvoir expliquer comment les commandes frauduleuses ont été créés et poussés à travers le système. SWIFT a cependant fourni des éléments sur la façon dont tout cela est arrivé. L'organisme explique que le modus operandi était similaire dans toutes les opérations frauduleuses. Les agresseurs ont obtenu des informations d'identification valides et ont pu créer et approuver des messages SWIFT.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une coopérative détenue par 3 000 institutions financières. Sa plate-forme de messagerie est utilisé par 11 000 banques et autres institutions à travers le monde et est considéré comme un pilier du système financier mondial. SWIFT a dit aux clients que la mise à jour de sécurité doit être installée avant le 12 mai… [Lire la suite]

Réagissez à cet article

Source : *Le protocole bancaire SWIFT victime de cyber fraude – ZDNet*

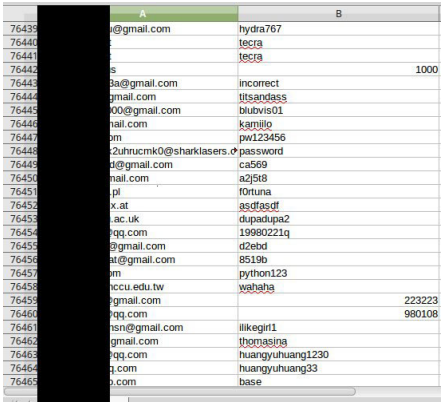
Un site Internet pour adultes piraté. Les comptes d’accès bradés sur le BlackMarket

Un site Internet pour adultes piraté. Les comptes d’accès bradés sur le BlackMarket

---

Un internaute a tenté de revendre les données de 270 000 amateurs de sites pornographiques dans le blackmarket. Le business du Porn Account pour les nuls !

Vous avez peut-être entendu à la radio et lu dans la presse généraliste ce piratage de données ayant visé 270 000 amateurs de sites pornographiques. Un piratage qui a débuté via l'attaque par injection SQL de plusieurs sites pour adultes appartenant au groupe Paper Street Media.
Le pirate a expliqué avoir contacté l'entreprise pour « discuter ». Soyons clair, il a tenté de leur soutirer de l'argent en proposant la faille qui lui a permis d'extraire les informations des clients (IP, mail, mots de passe…).
Paper Street Media n'a pas répondu dans le sens de l'internaute. Bilan, l'adolescent a mis en vente, dans le blackmarket, la base de données volée pour 360 euros. Pourquoi revendre les données dans le BM ? Toutsimplement pour que les professionnels du porn account puissent sauter sur l'occasion.
Dans cette même boutique qui aurait servi au pirate à revendre cette base de données [je n'ai pas retrouvé le vendeur], d'autres « commerçants » proposent des accès « piratés » aux sites interdit au – de 18 ans de Paper StreetMedia pour 9 $. Je vous laisse faire l'addition. Nous sommes très très loin des 360 euros réclamés ! « **Je peux me faire entre 300 et 500 dollars par semaine** » m'indique un de ces vendeurs de Porn Account croisé dans une boutique spécialisée.



	A	B
76439	[redacted]@gmail.com	hydra767
76440	[redacted]	tecra
76441	[redacted]	tecra
76442	[redacted]s	1000
76443	[redacted]3a@gmail.com	incorrect
76444	[redacted]gmail.com	titsandass
76445	[redacted]00@gmail.com	blubvis01
76446	[redacted]ail.com	kamiilo
76447	[redacted]m	pw123456
76448	[redacted]2uhrucmk0@sharklasers.c	password
76449	[redacted]d@gmail.com	ca569
76450	[redacted]ail.com	a2j5t8
76451	[redacted].pl	f0rtuna
76452	[redacted]x.at	asdfasdf
76453	[redacted].ac.uk	dupadupa2
76454	[redacted]qq.com	19980221q
76455	[redacted]@gmail.com	d2ebd
76456	[redacted]at@gmail.com	8519b
76457	[redacted]m	python123
76458	[redacted]ccu.edu.tw	wahaha
76459	[redacted]gmail.com	223223
76460	[redacted]qq.com	980108
76461	[redacted]isn@gmail.com	ilikegirl1
76462	[redacted]gmail.com	thomasina
76463	[redacted]qq.com	huangyuhuang1230
76464	[redacted]q.com	huangyuhuang33
76465	[redacted]o.com	base

Un pirate russe revend des milliers de comptes du site Naughty America.
A noter que j'ai pu consulter [ci-dessus] un document diffusé par un autre pirate informatique. Ce dernier, il est russe, a mis la main sur 150 000 comptes clients du site pornographique Naughty America. Un injection SQL, une backdoor (shell) dans le serveur et les comptes clients ont fini dans les mains du pirate.

Pendant ce temps…
… le groupe hôtelier Trump est de nouveau piraté. Des logiciels d'espionnage ont été retrouvés dans les ordinateurs des hôtels Trump situés à New York, Toronto et Honolulu. Même type d'attaque vécue en juillet 2015. Cela donne une idée de la gestion de la sécurité informatique de ce groupe. Les pirates visaient les identités et les données bancaires.
En ce qui concerne les numéros de CB, pas besoin d'être intelligent pour comprendre l'intérêt. Achats de produits dématérialisés qui seront revendus moitié prix [blanchir l'argent détourné]… En ce qui concerne les informations dédiées aux identités : fraude bancaire [ouverture de compte], usurpation d'identité, … [Lire la suite]

Réagissez à cet article

Source : *Porn Account : 270000 amateurs de pornos piratés – Data Security BreachData Security Breach*

Un piratage sur Tor par le

FBI prive les victimes d’une justice

Un piratage sur Tor par le FBI prive les victimes d’une justice

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

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*

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.

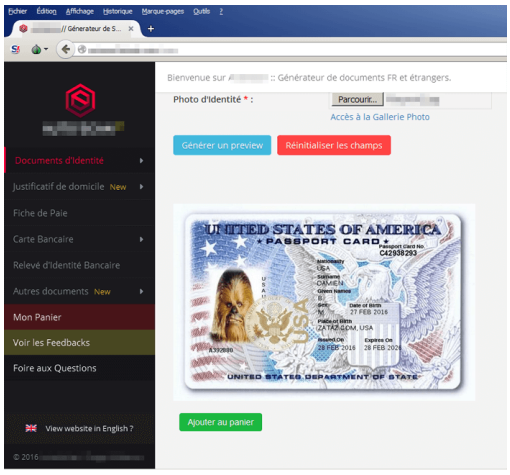
Fuite de données massive

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

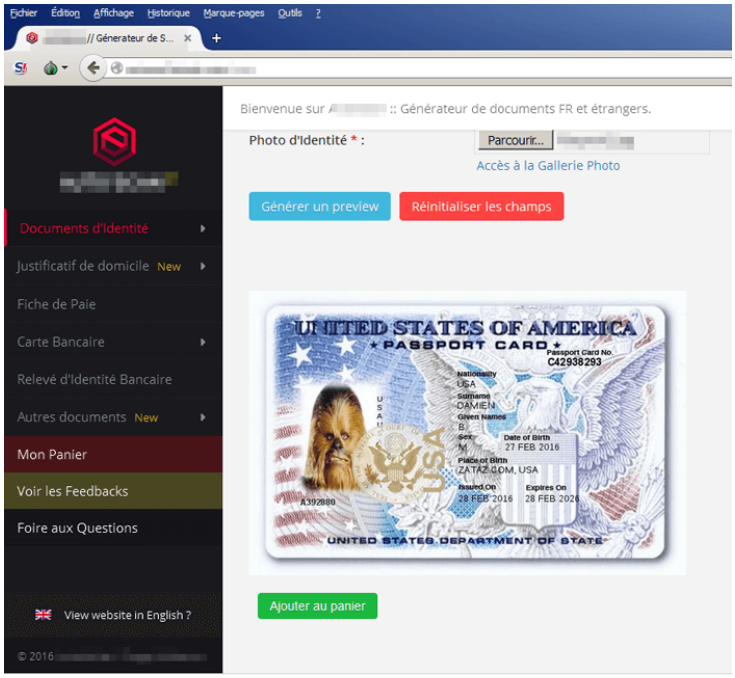
Source : *ZATAZ Fuite de données massive après un piratage chez les Francs-Maçons – ZATAZ*

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.



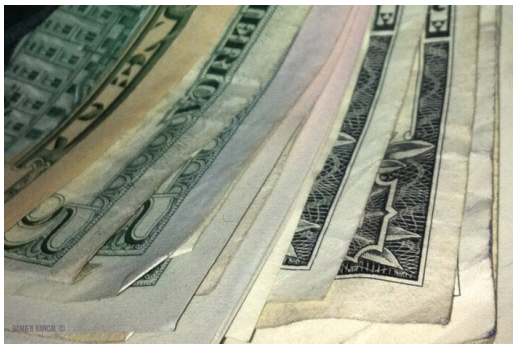
Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. 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.

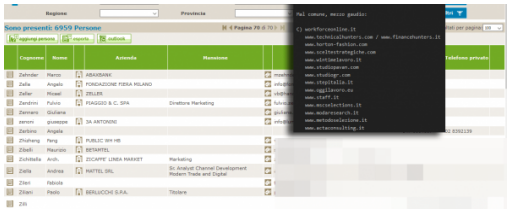
Source : Denis JACOPINI
Illustration : http://abidjantv.net

Etat des signatures et ratifications de la Convention de Budapest

---

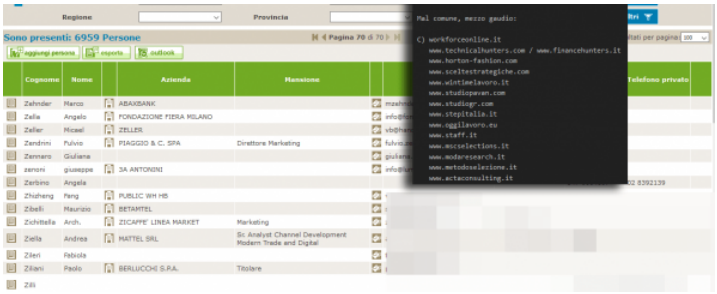
Réagissez à cet article

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