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

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

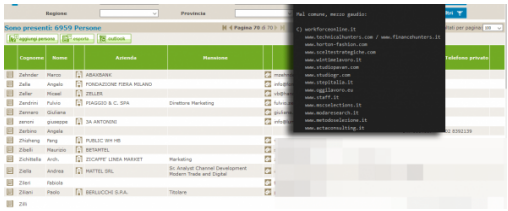
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Le hacking ça peut payer… légalement*

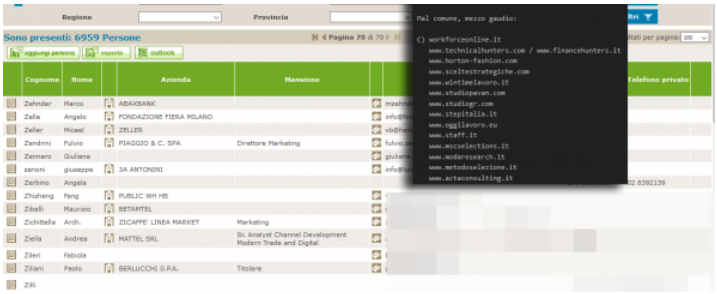
Des milliers de données clients diffusées sur Internet par Anonymous



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]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

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.

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable

	Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable par les anti-virus

Les attaques ransomwares ne baissent pas. Après avoir usurpé des avocats, des comptables, des PME, des mairies, FREE, voici le courriel piégé aux couleurs d'Orange. Ne cliquez surtout pas sur la pièce jointe.

Le courriel s'invite dans votre boites à mails avec comme objet : « ***Votre demande d'assistance*** » ; « ***Votre assistance Orange*** » ; « ***Votre assistance Orance Business***« . La missive pirate indique qu'une anomalie lors d'un prélèvement oblige le lecteur internaute à lire le fichier joint, un PDF piégé baptisé « ***Montant du mois*** » ou encore « ***Montant de la facture***« . Un piège qui, heureusement, est plutôt mal réalisé pour les internautes avertis. Il peut, cependant, piéger les plus curieux. La cible étant clairement les entreprises, une secrétaire, un comptable ou un responsable n'ayant pas vraiment le temps de lire autrement qu'en « Z » sera tenté de cliquer.

Au moment de l'analyse des fichiers, aucun antivirus n'avait la signature de la bestiole en mémoire. **A noter qu'un antivirus, face à ce genre d'attaque ne peut pas grand chose. Chaque mail et fichier joint portent en eux une signature (identification) unique et différente…** [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Attaques ransomwares aux couleurs d'Orange – ZATAZ*

Les établissements scolaires également victimes de ransomwares

Après les hôpitaux, les ransomwares s'attaquent de plus en plus aux établissements scolaires. Retour sur plusieurs cas aux Etats-Unis.

Les ransomwares sont devenus la plaie des responsables sécurité des entreprises ou des administrations. On peut se remémorer le témoignage du RSSI de l'AFP qui en a fait l'expérience. Le secteur hospitalier a été particulièrement touché avec différents exemples. Le plus symptomatique est le Hollywood Presbyterian Medical Center de Los Angeles qui a été obligé de payer 17 000 dollars en bitcoin pour retrouver l'usage de son réseau.

Certains payent la rançon

Après les hôpitaux, les ransomwares s'intéressent à une autre cible : les écoles. Plusieurs cas ont été recensés aux Etats-Unis. En février dernier, plusieurs écoles primaires du Horry County en Caroline du Sud ont été victimes d'un rançongiciel qui a bloqué 25 serveurs. Immédiatement après avoir été alertée par les enseignants, l'équipe IT a débranché les serveurs affectant ainsi les services en lignes des écoles. Après enquête, la porte d'entrée du malware était un vieux serveur non mis à jour. Toujours est-il que les responsables de l'école ont se sont vus réclamer 0,8 bitcoin par ordinateur soit un total de 20 bitcoins (environ 7600 euros). Malgré l'aide du FBI, le conseil d'administration du campus a décidé de payer la rançon demandée.

D'autres non

D'autres ont décidé de ne pas payer la rançon comme dans le cadre du Oxford School District dans le Mississipi. En février dernier aussi, ce réseau de 8 campus a été infecté par un rançongiciel réclamant environ 9000 dollars pour un retour à la normal. Le superintendant de l'établissement, Brian Harvey, a préféré ne pas payer et s'est concentré sur la récupération des données. Dans un entretien accordé à HottyDotty, il précise que « nous avons restauré à partir d'une sauvegarde ». Mais les dégâts étaient importants. « Je ne sais pas combien de données nous avons perdu. Je peux dire que nous avons perdu la plupart des serveurs Windows. La chose la plus importante a été de tout effacer et de tout réinstaller depuis la sauvegarde. » L'attaque a privé les établissements d'Internet pendant plus d'une journée. Les 4 premiers jours après l'attaque ont été focalisés sur la récupération du système des carnets de notes des élèves. D'autres applications ont souffert comme les reporting ou le recrutement des agents. Au final, deux semaines ont été nécessaires pour tout remettre à peu près d'aplomb : les sites web, la gestion de la cafeteria, ainsi que des plateformes pour l'éduction comme PowerSchool et Schoology.

Les parents d'élève s'inquiètent

Autre affaire, le Texas School District qui gère une vingtaine d'établissements. Un ransomware a infecté le réseau, provoquant le blocage de plusieurs fichiers. La direction du district s'est voulue rassurante en expliquant que seule une petite partie des informations est concernée par le blocage. Ce dernier porte néanmoins sur un volume de 2,5 To de données. Les responsables ont choisi de ne pas payer la rançon demandée par les cybercriminels. « Nous avons réussi à effacer les fichiers chiffrés et à réinstaller données à partir d'une sauvegarde », précise un porte-parole du district. Un cas similaire à celui du Mississipi qui inquiète les parents d'élèves. « Ils [NDLR les établissements] détiennent des actes de naissance, des numéros de sécurité sociale ou des données médicales comme les vaccins », souligne une des parents d'élèves.

En France, aucun cas n'a été relevé ou publié sur des expositions à des ransomwares. Les écoles, universités et autres établissements scolaires font partie de cibles privilégiés par les cybercriminels. Obsolescence des parcs informatiques, système IT peu mis à jour, les pirates se ont trouvé un terrain de jeu grandeur nature pour tester et peaufiner leurs attaques. Les sommes demandées restent modestes, un signe selon les spécialistes pour reconnaître le degré de résistance des victimes à payer la rançon. En tout cas, les exemples américains doivent alerter les établissements bancaires européens et français sur les risques des ransomwares… [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

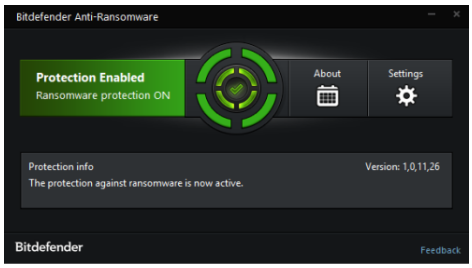
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Les ransomwares prennent le chemin des écoliers*

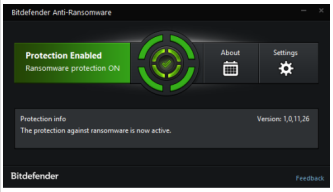
Bitdender met à disposition un outil gratuit de protection contre les Ransomwares



Bitdender met à disposition un outil gratuit de protection contre les Ransomwares

---

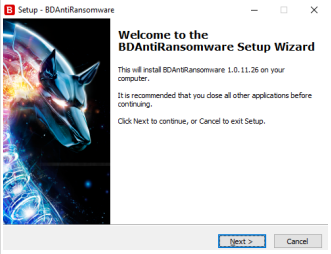
Bitdefender has just released a free tool that can protect against ransomeware viruses. Here is how to install it.



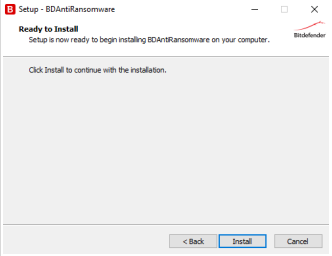
Hackers have been hitting everything from hospitals to police stations with Ransomeware viruses. Bitdefender has released a tool that could help fight it:
“Bitdefender anti-malware researchers have released a new vaccine tool which can protect against known and possible future versions of the CTB-Locker, Locky and TeslaCrypt crypto ransomware families.
“The new tool is an outgrowth of the Cryptowall vaccine program, in a way.” Chief Security Strategist Catalin Cosoi explained. “We had been looking at ways to prevent this ransomware from encrypting files even on computers that were not protected by Bitdefender antivirus and we realized we could extend the idea.”

Installation could not be easier

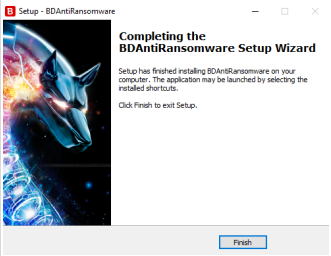
1. Download the file:
https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
2. Run it:



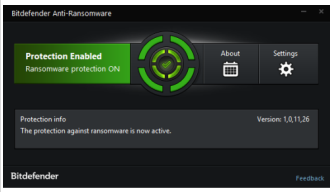
3. Click Next, and then install:



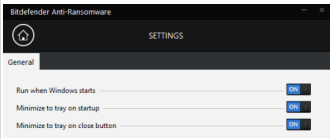
4. And then Finish



And that is it!



How easy was that?
If you want you can change the settings for the program. You may want to set it to “minimize on startup” and “minimize to tray on close”:



But it is pretty much an install and forget about it type app, no fuss, no muss.
Bitdefender has always been one of my favorite anti-virus programs, and this is a handy tool to have.
Check it out!

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Source : *How to install Bitdender’s free Ransomware Protection Tool | CYBER ARMS – Computer Security*

Apple a essayé d’aider le père de l’enfant mort à récupérer des données

Apple a essayé d’aider le père de l’enfant mort à récupérer des données

---

Contrairement à ce que disent officiellement ses conditions d'utilisation, Apple accepte bien, au cas par cas, de donner à des vivants l'accès aux données iCloud d'un utilisateur mort.
Il y a ce qu'Apple écrit dans ses conditions d'utilisation, et il y a la pratique, plus humaine. À la suite de la lettre envoyée à Tim Cook par ce père endeuillé, qui souhaitait avoir accès aux données de l'iPhone de son enfant de 13 ans mort d'un cancer des os, CNN rapporte qu'Apple a bien essayé de venir en aide à l'architecte italien Leonardo Fabbretti.

Fidèle à sa position de principe, Apple n'a pas accepté de tenter de casser la protection de l'iPhone 6 de l'enfant, qui aurait permis d'accéder aux données chiffrées contenues sur le téléphone, y compris aux photos et vidéos prises par l'enfant peu avant sa mort.
En revanche, au terme de quelques conversations, les équipes d'Apple ont bien accepté de regarder si des données n'avaient pas été synchronisées avec un cloud iCloud, ce qui aurait permis de les divulguer au père – il n'y avait toutefois aucune sauvegarde.

CE N'EST PAS LE PREMIER ÉCART QU'APPLE ACCEPTE DE RÉALISER, SANS JAMAIS ACCEPTER D'EN FAIRE UNE POLITIQUE GÉNÉRALE
Officiellement, Apple (qui a refusé de commenter) ne réalise pourtant pas ce type d'opération, y compris au bénéfice des parents ou des héritiers d'un défunt. « Dès réception d'une copie d'un certificat de décès, votre Compte pourra être résilié et l'intégralité du Contenu de votre Compte pourra être supprimée », dit simplement le contrat des conditions d'utilisation d'iCloud.
Il indique que le compte iCloud est « incessible et que tous les droits liés à votre identifiant Apple ou Contenu dans le cadre de votre Compte seront résiliés au moment de votre décès ».

Ce n'est pas le premier écart qu'Apple accepte de réaliser, sans jamais accepter d'en faire une politique générale, ni même de reconnaître officiellement des critères d'exceptions. Début 2016, au Canada, une veuve avait déjà obtenu d'Apple qu'il lui transmette les données de son défunt mari. Mais le transfert n'avait pu être obtenu qu'après médiatisation de l'affaire, et intervention d'une association.
L'article de CNN rapporte par ailleurs que Leonardo Fabbretti a pu rencontrer les équipes de l'entreprise israélienne Cellebrite qui propose de l'aider gratuitement à accéder aux données de l'iPhone 6.
Pour le moment, les hackers employés par le FBI pour débloquer l'iPhone 5C du tueur de San Bernardino auraient réussi à extraire le listing des données stockées, mais pas encore les données elles-mêmes. Ils se diraient toutefois « optimistes » sur leurs chances de succès. S'ils parvenaient à débloquer ainsi un iPhone 6, réputé plus sûr, l'annonce viendrait porter un nouveau coup à l'image de forteresse imprenable qu'Apple essaye de donner à l'iPhone… [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

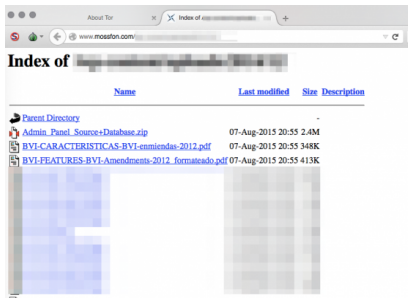
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *iCloud : Apple a essayé d'aider le père de l'enfant mort à récupérer des données – Politique – Numerama*

#PanamaPapers : Les failles informatiques de Mossack Fonseca…

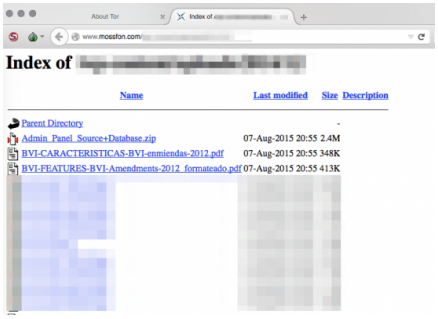


#PanamaPapers : Les failles informatiques de Mossack Fonseca…

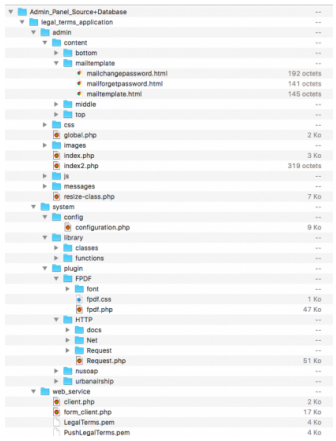
Un internaute vient de nous mettre sous le nez quelques éléments très, très … dur de trouver un qualificatif adapté. On se doutait bien en jetant un bref coup d'œil que le cabinet d'avocats panaméens avait une fâcheuse tendance à faire n'importe quoi, n'importe comment.
On peut également toujours spéculer sur l'origine de la fuite mais là n'est pas le problème, pour tout vous dire, l'origine de la fuite, on s'en fout, c'est la masse de données qui parle, et ce sont ces données qui sont importantes. Nous ne sommes évidemment toujours pas en mesure d'affirmer d'où vient la cette énorme fuite, mais comme nous le sentions, en collectionnant de si mauvaises pratiques, Mossack Fonseca s'assurait à plus ou moins long terme un drame.

Le WTF du jour

Aujourd'hui… la sauvegarde d'une application interne et d'un jeu de données, probablement sensibles, sauvegardés dans un répertoire public du site web vitrine de la société :

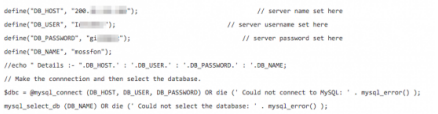


Et l'adresse IP internet du serveur de stockage des documents



La structure de l'application et son fichier de configuration
Et maintenant, admirez la complexité du password :

Rien de tel que de choisir le même mot de passe que le nom d'utilisateur et de base de données… et SURTOUT ne rien chiffrer, des fois qu'on oublierait un mot de passe si complexe.
… et évidemment



La base de données SQL est probablement un jeu de données tests qui est aussi sauvegardée au même endroit :

… oui tout ça accessible depuis un WordPress qui n'est pas à jour, installé sur un Apache mal configuré. …
… [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Source : *PanamaPapers : Mossack Fonseca une incroyable bourde ? : Reflets*

Chrome et Safari perdent face aux hackeurs

Chrome et Safari perdent face aux hackeurs

Comme tous les ans, lors de la conférence CanSecWest, les éditeurs de navigateurs soumettent leurs applications à une série de hackeurs tentant d'y orchestrer leurs attaques.

La communauté des *white hackeurs* joue un rôle fondamentale dans la sécurité des applications. Ces experts tentent effectivement de déceler des failles avant qu'elles ne soient exploitées par des personnes malveillantes. Pour inciter ces travaux, les éditeurs de navigateurs offrent des récompenses tout au long de l'année mais prennent également part à des concours. Le plus connu reste certainement Pwn2Own organisé chaque année.

Après une première journée Chrome, Safari et le lecteur Flash n'ont pas résisté aux *exploits* des hackeurs. Par la même occasion ces vulnérabilités ont permis de mettre à mal les dernières versions de Windows et OS X.

L'équipe 360Vulcan, de la société chinoise Qihoo 360, a réussi à exploiter une faille de Flash Player lui permettant d'exécuter du code à distance avec une autre affectant le kernel de Windows pour obtenir une élévation des droits du système. Ils ont obtenu 80 000 dollars (60 000 pour Flash Player et 20 000 pour Windows).

Cette même équipe a réussi à malmener le navigateur de Google sur le système Windows. Ils ont cette fois combiné 4 vulnérabilités : une au sein de Chrome, deux dans Flash Player et une dans le kernel de Windows. Cet exploit n'a en revanche été récompensé qu'à moitié puisque la faille de Chrome avait précédemment été partagée avec Google… quand bien même 360Vulcan n'était pas au courant. Ils ont toutefois obtenu 52 000 dollars.

De son côté le chercheur coréen JungHoon Lee a obtenir une élévation de droits sur OS X via un hack sur Safari. Il a obtenu 60 000 dollars. L'année dernière, l'homme s'était fait remarquer en obtenant au total 225 000 dollars. Il montrera la semaine prochaine deux autres attaques contre Chrome et Microsoft Edge sur Windows.

Le magazine Computerworld, qui rapporte l'information, ajoute que l'équipe de sécurité de Tencent a obtenu 40 000 dollars en faisant tomber Safari, et 50 000 dollars en présentant une attaque contre Flash Player…. [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Source : *Pwn2Own : Chrome et Safari tombent face aux hackeurs*

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

C'est peut-être l'absence de prise en compte de patchs de sécurité pour un plug-in WordPress et pour le CMS Drupal qui aurait permis de récupérer chez Mossack Fonseca les fameux Panama Papers qui font trembler le monde de la finance.

La fuite massive des documents de Mossack Fonseca, le cabinet panaméen qui gère des compagnies offshores, n'a pas fini de faire parler d'elle. Les 11,5 millions de documents contenus dans les 2,6 To de données – les fameux Panama Papers – ont déjà ébranlé de nombreuses sociétés et les sphères politiques, poussant par exemple le Premier ministre de l'Islande à démissionner. Mais comment ces données ont-elles été obtenues ?

NÉGLIGENCE INFORMATIQUE

De nombreuses questions demeurent concernant l'origine de la fuite qui provient d'une source anonyme. Mais beaucoup s'accordent sur le fait que la sécurité informatique a été négligée par Mossack Fonseca, ce que le cabinet avoue à demi mots en portant plainte pour piratage informatique.

Dans un mail qu'il ne fallait pas prendre pour un poisson d'avril, le cabinet avait expliqué à ses clients dès le 1er avril qu'il avait été victime d'une « brèche non autorisée de [son] serveur mail », comme le montre une copie publiée par Wikileaks le 3 avril. Bien sûr, les réactions sur Twitter ne se font pas fait attendre, amusées par la date d'envoi du mail et par l'absence de chiffrement des courriers électroniques de la part d'une entreprise qui met en avant « ses prestigieux services en ligne », comprenant « un compte sécurisé qui vous permet d'accéder n'importe où aux informations de votre société ».

DE L'IMPORTANCE DE METTRE À JOUR DRUPAL ET WORDPRESS

De récentes informations corroborent la thèse du piratage, qui aurait pu être facilitée par des vulnérabilités au sein des CMS utilisés par Mossack Fonseca, à savoir les gestionnaires de contenus Drupal et WordPress.

Comme le rapporte Forbes, le portail client du cabinet fait tourner une vieille version de Drupal (7.23). Or cette version est antérieure à un patch de sécurité qui corrigeait une énorme faille à partir de la version 7.32. Dans une notice de sécurité, Drupal allait jusqu'à recommander une nouvelle installation aux utilisateurs n'ayant pas mis à jour immédiatement après la sortie du correctif.

Il se peut donc qu'un attaquant ait exploité cette faille durant les deux années pendant lesquelles le cabinet n'a pas mis à jour sa version du CMS. Mais d'autres experts en informatiques ont découvert une autre porte qui aurait pu permettre à un hacker d'entrer dans le système.

Si le portail client du cabinet est sous Drupal, le site principal est lui sous WordPress. L'entreprise Wordfence, spécialisée dans la sécurité de l'omniprésent gestionnaire de contenus, a remarqué que l'installation WordPress utilisait une ancienne version du plugin Revolution Slider, connue pour présenter une faille sérieuse.

La version 3.0.95 de Revolution Slider (et les versions antérieures) contiennent en effet une vulnérabilité qui permet à un assaillant d'envoyer un fichier sur le serveur web sans avoir à s'identifier. L'entreprise note qu'un attaquant aurait donc pu prendre le contrôle du serveur sur lequel se trouvait l'installation WordPress… Le même serveur qui hébergeait les très précieux e-mails du cabinet.

En l'occurrence, rien ne prouve que les failles au sein des installations WordPress et Drupal du cabinet aient facilité la fuite des données. Dans la mesure où les journalistes n'ont pas rendu publics les documents, il sera d'ailleurs difficile de déterminer d'où ils proviennent. De son côté, le cabinet affirme qu'il s'agirait d'une attaque effectuée depuis l'étranger, écartant par la même toutes idées de fuites internes.

… [Lire la suite]

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Source : *Panama Papers : des WordPress et Drupal mal gérés à l'origine d'un piratage ? – Tech – Numerama*