Comment prémunir les visiteurs de votre site internet de cyberattaques ? | Le Net Expert Informatique

Comment prémunir les visiteurs de votre site internet de cyberattaques?

Switch propose un site web visant à aider les propriétaires de noms de domaines internet en Suisse à protéger leur site web contre des cyber-attaques.

Afin d'aider les propriétaires de sites internet à lutter contre les malwares qui pourraient y être installés, Switch met en ligne Safer Internet, un site internet d'information sur les menaces que représentent les criminels sur internet et les mesures préventives à adopter. Michael Hausding, expert en sécurité de Switch, explique les raisons de la mise en place d'un tel site: «Par la plateforme de sécurité Safer Internet, nous nous adressons à tous les détenteurs d'un site web .ch. Nous y donnons des conseils sur la prévention de l'abus de noms de domaine et informons sur les dangers relatifs à des contenus online.»
Les propriétaires de noms de domaines y trouveront notamment cinq conseils pour prévenir des attaques par Drive-by (qui infectent les usagers d'un site contenant un malware) et par Phishing (qui consistent à obtenir des informations personnelles via notamment des sites contrefaits). Parmi ses conseils se trouvent par exemple le fait d'utiliser une système de gestion du contenu (CMS) toujours à jour.
Ce site est disponible en quatre langues: allemand, français, italien et anglais. Il s'adresse en premier lieu aux gestionnaires de sites web qui sont tenus de nettoyer leur site s'il est infecté au risque de les voir bloqué.
La fondation Switch a pour objectif de rendre internet sûr en Suisse.

Le lien vers le site Internet « Safer Internet » de la société « Switch » : http://www.switch.ch/saferinternet

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.ictjournal.ch/fr-CH/News/2015/07/07/Comment-premunir-les-visiteurs-de-votre-site-internet-de-cyberattaques.aspx

Votre identité complète ne coûte que 70 dollars sur le Dark Web | Le Net Expert Informatique

La croissance galopante de la cybercriminalité n'a d'égal que la sophistication de ses techniques. L'objectif de ces attaques: le vol de données personnelles afin de les revendre au plus offrant. Des chercheurs en sécurité informatique ont sondé pendant plusieurs mois le Darkweb afin de dévoiler les dessous des marchés cybercriminels et d'en dévoiler les tarifs en vigueur.

Les bas-fonds du web regorgent de produits illicites: drogues, armes, tueurs à gages, malwares… sont autant de biens et services qu'il est possible de vendre ou d'acheter à des prix variables en toute impunité puisque ces transactions sont intraçables. Car comme nous l'explique Jérôme Granger, chargé de la communication de ce groupe d'experts qui a fouillé ces marchés parallèles (comme Silkroad Reloaded, DeepBay, Pandra ou encore Agora), «les vendeurs accordent beaucoup d'importance à leur réputation et ils vont du coup proposer des prix défiant toute concurrence pour 'un produit de qualité'». À l'heure où des entreprises payent des mille et des cents pour les obtenir afin de nous bombarder de publicités ciblées, nous nous sommes déjà tous demandé ce que valaient nos vies privées sur le marché noir. Des chercheurs du G DATA SecurityLabs ont enquêté et ont passé au crible le fonctionnement de ces lieux d'échanges où moult produits et services illégaux sont disponibles. Et les résultats sont édifiants «puisque nos identités ne valent rien», nous glisse M.Granger.

Grosse quantité à petits prix

Si vous désirez lancer une cyberattaque, vous pouvez trouver un kit du parfait pirate ou tout simplement vous octroyer les services d'un pirate expérimenté. Alors que tous les tutoriels vous sont gracieusement offerts, l'installation d'un programme malware vous coûtera 70 $, tandis qu'une attaque DDoS vous sera facturée 100 $. Mais la denrée la plus convoitée reste l'adresse email parce qu'elle permet de mener des opérations de spam ou d'hameçonnage. Comptez seulement 75 $ pour un million d'adresses valides et 70 $ l'identité complète (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires). Les accès à ces adresses -identifiants et mots de passe- sont eux légèrement plus chères: 20 $ pour un lot de 40.000 comptes. Un prix abordable pour celui qui désire usurper des identités afin de se lancer dans des escroqueries de plus haut vol. Pour les hackers fainéants, des données financières prêtes à l'emploi sont également disponibles, mais elles se payent plus cher à l'image d'une carte bancaire ou un compte Paypal qui sera monnayé à 50 $ pièce. Quant aux produits matériels illicites, ils sont également pléthore sur le Darkweb: le site 01Net nous apprend par exemple «qu'une fausse carte d'identité d'un pays européen se négocie aux alentours de 1.000 €, qu'il faudra verser 4.000 € pour un passeport et qu'au rayon drogues, un gramme de cocaïne de qualité (Amérique du Sud) se vend à partir de 75 € alors qu'un gramme d'ecstasy avec taux de pureté de 84% vaut 19 €».

Représailles compliquées

La lutte contre cette criminalité cachée s'avère aride pour plusieurs raisons. D'abord parce que ces cybercriminels sont difficilement identifiables de par l'utilisation de systèmes qui garantissent leur anonymat (comme Tor, I2P, des VPN ou des Proxy). Ensuite, les opérations menées par les différentes forces policières sont généralement trop lentes et «les sites sont hébergés sur d'autres serveurs en seulement quelques heures», selon Jérôme Granger qui indique qu'«à côté d'une protection redoutable, la seule solution réside dans une sensibilisation constante aux cyberdangers». D'autant plus que la recherche de ces cybercriminels se heurte souvent au droit international car si la coopération européenne est efficace, plusieurs pays comme la Russie et la Chine refusent toujours de céder une partie de leur souveraineté numérique. Un problème qui ne fera que s'amplifier avec le développement fulgurant des objets connectés qui sont déjà les nouvelles victimes de virus et autres logiciels malveillants.

Source : http://fr.metrotime.be/2015/06/11/must-read/votre-identite-complete-ne-coute-que-70-dollars-sur-le-darknet/
Par Gaëtan Gras

Les attaques informatiques s’achètent sur le blackmarket | Le Net Expert Informatique

	Les attaques informatiques s’achètent sur le blackmarket

De 75 dollars le million d'adresses e-mail à plusieurs milliers de dollars pour une faille zero day exploitable… G Data a plongé dans le « blackmarket » pour en ressortir les principaux tarifs du marché de la cybercriminalité.

G Data s'est penché sur le marché de la cybercriminalité pour en étudier fonctionnement et offres de contenus. Baptisé « blackmarket », cet environnement construit autour de sites spécialisés, de forums privés, de structures d'anonymisation (proxy, VPN anonymes, réseau Tor…), de messageries protégées, de serveurs bulletproof (peu regardants sur la nature des fichiers stockés), de moteurs de recherche spécialisés et autres places de marchés de produits illicites, permet d'accéder à des montagnes de données personnelles, des kits de piratages en tout genre et de services d'attaques à la demande.
Au bout de son plongeon dans le blackmarket, les experts du SecurityLabs de l'éditeur allemand spécialisé en solutions de sécurité en a ressorti quelques informations éclairantes sur la vitalité du marché de la cybercriminalité. Un marché dont les tarifs évoluent entre une poignée de dollars et plusieurs centaines. La vente de données personnelles illégalement collectées se situe dans la zone basse des tarifs et, surtout, se commercialisent en volumes. Ainsi les accès aux comptes e-mails (adresse, nom d'utilisateur et mot de passe) se négocient 5 dollars le lot de 10 000. Les seules adresses e-mails, celles que se font notamment dérober les opérateurs et qui seront essentiellement exploitées pour des campagnes de phishing, ne se revendent pas plus de 10 dollars par poignées de 100 000, autour de 75 dollars le million. Les profils numériques qualifiés sont, eux, d'autant plus rentables qu'ils se revendent à l'unité : autour de 50 dollars pour une carte bancaire valide de type Gold ou Premier, un compte bancaire ou Paypal; 70 dollars l'identité complète dite Fullz (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires).

Plusieurs milliers de dollars la faille zero day exploitable
Les cybercriminels financièrement plus ambitieux orienteront leurs activités vers la vente de produits et services. L'installation d'un Bot, bien utile pour prendre le contrôle d'un réseau de PC infectés, se négocie autour de 50 dollars les 1000 machines à la soldes des cyberattaquants. Lesquels pourront également exploiter ces Bots pour organiser des attaques par déni de service distribué (DDoS). Un service proposé entre 10 et 200 dollars l'heure d'attaque. Le tarif pour une campagne de spam, non traçable (via un service de diffusion hébergé sur un serveur bulletproof) tombe en revanche autour de 5 dollars les 20 000 envois.
La création et l'hébergement (sur un serveur piraté) d'une page web infectieuse dans le cadre d'une campagne d'hameçonnage (phishing) se facture entre 10 et 30 dollars. Mais on trouve également des outils d'attaques plus onéreux (car censés être plus efficaces). Par exemple, le kit d'exploitation Nuclear, qui exploite les bannières publicitaires Google Ads pour dérouter l'utilisateur vers un site infectieux, est disponible autour de 1500 dollars. La palme revient aux outils capables d'exploiter les failles zero day de Windows à raison de plusieurs milliers, voire plusieurs dizaines de milliers de dollars, selon G Data.

Source : http://www.silicon.fr/besoin-dune-attaque-ddos-comptez-entre-10-200-dollars-de-lheure-118545.html
Par Christophe Lagane

L’analyse comportementale, la nouvelle cyber-arme ? | Le Net Expert Informatique

IdentityGRC 2015 est la dernière offre de détection comportementale de la fraude et de la fuite de données de Brainwave, co-fondée par Sébastien Faivre. (crédit : D.R.)

L’analyse comportementale, la nouvelle cyber-arme ?

C’est bien connu, en matière de sécurité les risques ne proviennent pas seulement de l’extérieur du périmètre de l’entreprise mais bien de l’intérieur. Téléchargement de fichiers non autorisés, vol de données confidentielles ou encore accès à des informations par un collaborateur ayant quitté depuis des mois l’entreprise sont, malheureusement, une réalité qui dépasse – parfois – de loin la fiction. Et bien souvent, à la base de cette problématique, on trouve une gestion et/ou une politique de gestion des droits d’accès défaillante ou en tout cas plus en mesure de répondre à une évolution malsaine des comportements.
« Le constat que l’on fait aujourd’hui est que d’une façon générale la sécurité des accès et la configuration des droits d’accès pour accéder à des applications ou données sont souvent les parents pauvres de la sécurité informatique », explique Sébastien Faivre, co-fondateur de Brainwave. « En général, le département informatique et les métiers se renvoient la balle en termes de responsabilités dans les cas où on se rend compte que des personnes qui ont quitté l’entreprise ou changé de département ont toujours accès à des informations sensibles ou que d’autres encore ont des droits d’accès excessifs à des données critiques ».

Des jeux d’API couplés à des algorithmes d’analyse
Pour faire face à ce type de menace, le jeune éditeur francilien Brainwave (créé en 2010) a développé IdentityGRC qui permet de récupérer toutes les informations de configurations de l’ensemble des systèmes de l’entreprise afin de proposer une cartographie de l’ensemble des droits d’accès aux applications. Et ce, des systèmes CRM, ERP, gestion financière (SAP, Salesforce.com, Microsoft Dynamics CRM…) que des solutions cloud de sauvegarde et de partages documentaires (Google Drive, Dropbox…) ou encore des grands systèmes (AS400, RACF, CA Top Secret…). Pour y parvenir, plusieurs jeux d’API ont été développés, couplés à des algorithmes d’analyse, brevetés depuis fin 2010, afin de pouvoir poser des questions en langage naturel de type « Quelles sont les personnes ne faisant pas partie des ressources humaines qui ont accès aux fiches de paye des salariés ? ».
Aujourd’hui, Brainwave va plus loin en matière de détection mais surtout de prévention de la fraude et de fuite des données. « La version 2015 d’IdentityGRC propose de l’analyse comportementale permettant de mettre sous surveillance des comportements anormaux comme par exemple identifier une personne qui récupère bien plus de fichiers que ses collègues, mais également d’automatiser le diagnostic et la résolution des comportements suspects », fait savoir Sébastien Faivre. Une approche différente selon Brainwave des traditionnelles offres de sécurité centrées davantage sur les flux de comportements au niveau des postes de travail que sur le comportement du point de vue des applications, indépendamment du reste de tout terminal.

A partir de 75 000 euros la licence perpétuelle
Distingué par le Gartner dans la catégorie des « cool vendors » dans son rapport Magic Quadrant 2013 en Identity Analytics and Intelligence, Brainwave n’a pas attendu pareille reconnaissance pour se tailler une place dans les entreprises. Surtout les grandes, avec des clients comme PSA Peugeot-Citroën, Natixis, Crédit Agricole, BNP Paribas, ou encore Aéroports de Paris et Eutelsat qui utilisent ses solutions. En tout, l’éditeur revendique une cinquantaine de références en France mais également au Bénélux, en Suisse, au Royaume-Uni, au Magrehb ou encore au Canada où il a ouvert récemment un bureau commercial. Autofinancée jusqu’en 2014, la société a levé 2,5 millions d’euros fin 2014 afin de donner un nouvel élan à sa croissance internationale mais également renforcer ses équipes R&D (une dizaine de personnes sur 30 collaborateurs au total). Brainwave a réalisé l’année dernière un chiffre d’affaires de 2 millions d’euros et indique être rentable.
IdentityGRC 2015 est proposée à partir de 75 000 euros en licence perpétuelle, auquel vient s’ajouter près de 20 000 euros de maintenance annuelle. Deux modes de tarification sont proposées : nombre de personnes sur lequel un audit sécurité est réalisé ou bien en fonction du nombre d’applications. Quant à la disponibilité de l’offre, elle est pour le moment uniquement en on-premise. « Nous ne proposons pas d’offre en mode cloud public. Nos clients considèrent que ce type de données est sensible et préfèrent donc un déploiement sur site. Cependant, certains clients ont choisi un déploiement dans un cloud privé chez un infogéreur », explique Sébastien Faivre.

Source : http://www.lemondeinformatique.fr/actualites/lire-avec-identitygrc-2015-brainwave-s-ouvre-a-l-analyse-comportementale-61157.html
Par Dominique Filippone

L’employé, la première faille de sécurité | Le Net Expert Informatique

	L’employé, la première faille de sécurité

Si les entreprises se concentrent toujours sur leur protection informatique vis-à-vis des intrusions externes, se méfient-elles assez de leurs propres employés ? Pas toujours à en croire certaines histoires de ces dernières années.

L'ennemi a beau souvent être à l'extérieur de l'entreprise, il n'en reste pas moins que les employés eux-mêmes peuvent devenir de véritables problèmes, à plus ou moins grande échelle. Bien entendu, les plus grands risques internes sont faits à l'insu du collaborateur, du fait de son manque de technique et/ou d'attention, mais parfois, l'acte malveillant est réellement sciemment.

L'affaire Coca Cola

Fin 2013, le géant Coca Cola, qui compte tout de même près de 130 000 employés, s'est par exemple rendu compte qu'elle avait été victime durant de longues années d'un voleur d'ordinateurs portables. L'employé en question a ainsi dérobé 55 ordinateurs sur plusieurs années, volant ainsi des données sur environ 74 000 personnes, la plupart étant des employés du géant américain ou des collaborateurs reliés à la firme.

Réalisé par un employé (au nom inconnu) ayant en charge les équipements informatiques, non seulement l'acte en lui-même a sonné comme une véritable claque pour la firme US, mais surtout, parmi toutes les données concernées, 18 000 concernaient les numéros de sécurité sociale, données particulièrement sensibles outre-Atlantique.

Pire encore, selon un mémo de Coca Cola envoyé aux employés et révélé par le Wall Street Journal, aucune des données volées n'était chiffrée. Nous apprenons aussi qu'afin d'éviter la panique, le spécialiste de la boisson gazeuse a tenté de résoudre le problème en secret durant plusieurs semaines. Les vols ont ainsi été remarqués en décembre 2013, mais la firme a attendu le 24 janvier pour en informer ses employés.

Plus que le côté technique, cette histoire nous montre donc que la sécurité est aussi (surtout ?) une question de processus. La « faille » de Coca Cola ainsi été humaine et organisationnelle plus qu'autre chose.

Boeing aussi

Coca n'est toutefois pas la seule très grande compagnie concernée par ce genre de problématique. En 2006, un employé de Boeing a par exemple été licencié non pas pour avoir dérobé du matériel et des données, mais du fait de sa responsabilité dans un vol d'ordinateur. Le collaborateur a ainsi enfreint les règles de l'entreprise en téléchargeant des informations confidentielles sur son PC portable sans même les chiffrer.

Problème, l'employé avait téléchargé des données personnelles de 380 000 employés actuels et passés de la compagnie, comme des numéros de sécurité sociale, des noms, des adresses, etc. Le tout fut ensuite volé en décembre 2006, entraînant le licenciement du collaborateur.

Cette faute grave n'était pas une première, puisque selon le porte-parole de Boeing, deux autres vols d'ordinateurs portables contenant des données sur les employés ont été dérobés entre 2005 et 2006. « Nous encourageons les gens à travailler hors du serveur, ce qui permettrait de garder l'information derrière le pare-feu. Si vous téléchargez des informations sur votre ordinateur portable, cela est censé être temporaire et l'information est censée être cryptée » a bien insisté Boeing à l'époque. Du simple bon sens a priori peu respecté par certains de ses employés.

Moralité de ces deux histoires : la sécurité est avant tout une affaire d'organisation, de processus et de règles. S'il est évident qu'il faut se prémunir des actions malintentionnées extérieures, « l'ennemi » peut aussi être à l'intérieur, que ce soit du fait d'actes réalisés délibérément ou non. BYOD ou non, les comportements des employés peuvent être cruciaux pour la sécurité de l'entreprise. Rédiger une politique stricte et mettre en place des systèmes de surveillances (ou au moins de vérification), notamment pour ceux manipulant des données sensibles, est ainsi indispensable si l'on veut éviter de lourdes déconvenues…

Source : http://www.zdnet.fr/actualites/l-employe-la-premiere-faille-de-securite-39819662.htm

« Vol » de documents via Google, la condamnation de Bluetouff confirmée | Le Net Expert Informatique

	« Vol » de documents via Google, la condamnation de Bluetouff confirmée

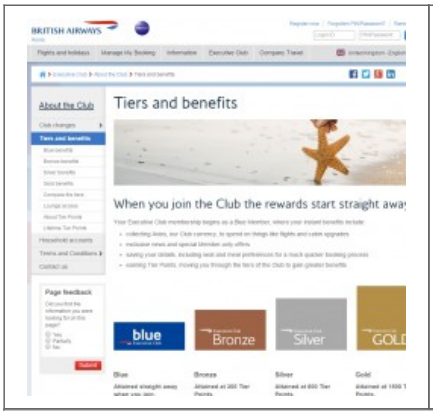
Olivier Laurelli, relaxé en première instance, avait accédé sans piratage à un extranet accessible par le moteur de recherche. Condamné en appel, son pourvoi en cassation a été rejeté.

Trop fouiller dans Google peut être cause de sanction judiciaire. Olivier Lorelli, alias Bluetouff, blogueur reconnu dans le domaine de la sécurité informatique, cofondateur du site Reflets.info, en fait l'amère expérience. Le spécialiste voit en effet sa condamnation pour « maintien frauduleux » dans le système et « vol » de documents confirmée par la Cour de cassation, révèle Le Parisien.
Rappel des faits. En 2012 Bluetouff avait trouvé par hasard « le serveur extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses), utilisé par les chercheurs pour stocker et échanger leurs documents de travail. Au lieu d'être protégées par un identifiant et un mot de passe, comme elles auraient dû l'être, ces données, indexées sur Google, étaient accessibles sans le moindre piratage. »
Le blogueur télécharge alors 8.000 de ces documents internes, sur des données de santé publique. Il publie plus tard un article sur les nanoparticules qui utilise une infime partie de ces documents, ce qui alerte l'Anses, laquelle lance la police sur l'affaire. La DCRI identifie le blogueur, et s'ensuivent une perquisition à son domicile, la saisie de son matériel informatique et une garde à vue de 30 heures. Rien que ça.

« Gogleu ? Lojin ? »
Olivier Laurelli est presque logiquement relaxé en première instance. En avril 2013, les juges considèrent qu'il n'y a pas eu de piratage pour accéder aux documents (récit par l'intéressé) : « Il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier Laurelli a pu récupérer l'ensemble des documents sans aucun procédé de type « hacking » », écrivaient-ils.
L'Anses ne fait d'ailleurs pas appel, contrairement au Parquet qui ne digère pas cette relaxe. Mauvaise pioche pour Bluetouff, le second procès, en décembre dernier, a opposé le pseudo-pirate à des juges visiblement très loin de maîtriser le sujet.
Un journaliste de Médiapart rapporte que « la magistrate chargée de rappeler les faits semblait même ne pas connaître Google, prononcé à la française « gogleu », ni savoir ce que signifie un « login », prononcé « lojin ». Difficile, dans ces conditions, d'expliquer qu'il est effectivement possible de tomber sur des documents de travail par une simple recherche… […] « Vous ne vous souciez pas de savoir si vous alliez tuer toute la planète? » s'indigne ainsi une magistrate alors que l'accusé vient de lui expliquer que ces documents n'étaient, visiblement, pas confidentiels. »
Si les juges relaxent le blogueur du chef d'« accès frauduleux », il le condamne néanmoins à une amende de 3.000 euros pour « maintien frauduleux dans un système de traitement automatisé de données » et « vol » de documents. De plus, cette peine sera inscrite à son casier judiciaire.
Olivier Laurelli et son avocat, Olivier Iteanu, décident alors de se pourvoir en cassation, pourvoi donc rejeté : la condamnation est donc confirmée. Dénonçant un « vrai scandale », l'avocat du blogueur, a annoncé à nos confrères son intention de saisir la Cour européenne des droits de l'Homme. Selon lui, on « fait payer » à son client des écrits « mettant en cause des entreprises et des services français ».
Le fait qu'aucun piratage n'ait été effectué n'a pas ému la cour qui rappelons-le ne juge que la forme, pas le fond de la procédure. Reste que cette condamnation confirmée constitue une très mauvaise nouvelle pour les lanceurs d'alerte.

Source : http://www.zdnet.fr/actualites/vol-de-documents-via-google-la-condamnation-de-bluetouff-confirmee-39819710.htm

Alerte : Comptes clients piratés chez British Airways | Le Net Expert Informatique



Alerte : Comptes clients piratés chez British Airways

Une action de piratage a visé de nombreux comptes de clients de la compagnie aérienne British Airways. Les points fidélité amassés tout au long des différents trajets ont été effacés.

Depuis quelques jours, un grand nombre de clients de la compagnie aérienne British Airways ont eu la désagréable surprise de trouver que le solde de points fidélités accumulés grâce à leurs précédents trajets en avion avaient disparu. D'autres n'ont tout simplement plus accès à leur compte fidélité, appelé Executive Club. Une situation qui serait loin d'être le fruit du hasard ou d'un bug informatique, mais qui a plutôt à voir avec une opération de piratage sur un grand nombre de comptes.

Interrogée sur un forum dédié par un utilisateur, British Airways a admis avoir été mis au courant d'une activité non autorisée sur son compte. « Il semble que cela soit le résultat d'un tiers utilisant de l'information obtenue quelque part sur Internet, via un processus automatisé, pour tenter d'accéder aux comptes Executive Club », a indiqué British Airways dans un mail. Bien que les pirates sont parvenus à accéder à des comptes, British Airways n'est pour l'instant pas au courant d'accès à des pages d'information de comptes, historiques de vols ou détails de cartes de paiement.

Selon un message posté par la compagnie, les mots de passe des comptes affectés par ce piratage ont été changés et l'utilisation des points fidélité « Avios » suspendue pour quelques jours. La société a par ailleurs également répondu aux utilisateurs affectés par le problème sur Twitter.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-aux-comptes-clients-pirates-chez-british-airways-60700.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Laboratoire d'analyses

médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés

Aujourd'hui, rebelotte avec le même groupe Rex Mundi et, là encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.

Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »

Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates

Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

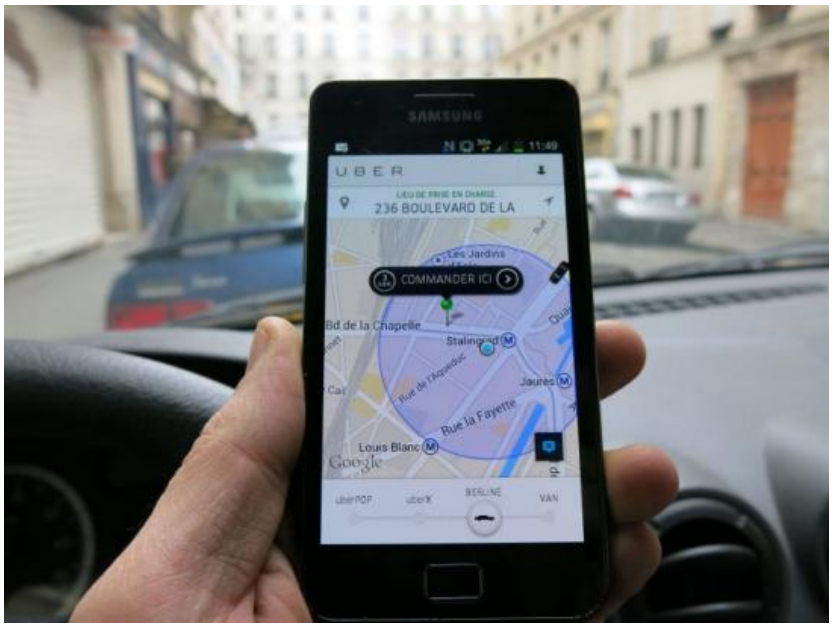
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINE et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Reste – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Puricard
Laboratoire de Saint Rémy de Provence

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm

50 000 chauffeurs d'Uber victimes d'une attaque informatique | Le Net Expert Informatique



50 000 chauffeurs d'Uber victimes d'une attaque informatique