Pour voler vos empreintes digitales, il suffit de prendre vos mains en photo | Le Net Expert Informatique

Pour voler vos empreintes digitales, il suffit de prendre vos mains en photo

Les hackers du Chaos Computer Club ont démontré comment il était possible de pirater des empreintes digitales à l'aide d'un appareil photo standard.

Depuis qu'Apple a lancé son système d'identification par reconnaissance d'empreintes digitales, le Chaos Computer Club n'a de cesse de démontrer que son système peut être piraté. La plus importante association de hackers européenne a présenté lors de son congrès, une nouvelle méthode de vol d'empreintes à partir de photos prises avec un appareil standard.
Le hacker Jan Krissler, alias « Starbug », a démontré comment il avait réussi à photographier les empreintes de la ministre allemande de la Défense Ursula von der Leyen, lors d'une allocution publique, avec un objectif de 200 mm et à moins de 3 mètres de distance. Selon lui, il est ensuite possible de s'en servir pour berner les lecteurs d'empreintes comme celui d'Apple.
Cette technique évite d'avoir à dérober un objet doté d'une surface polie, comme du verre, touché par la cible. Une nouvelle raison de ne pas accorder à la biométrie une totale confiance.

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

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

Source : http://lexpansion.lexpress.fr/high-tech/pour-voler-vos-empreintes-digitales-il-suffit-de-prendre-vos-mains-en-photo_1636132.html

---

Les facilités pour contourner la loi Renseignement | Le Net

Expert Informatique

Les facilités pour contourner la loi Renseignement

Le Projet de loi relatif au Renseignement impose aux hébergeurs et FAI d'installer un dispositif de surveillance de leurs communications, désigné sous le terme générique « boîte noire », pour recueillir les informations et documents « relatifs à des personnes préalablement identifiées comme présentant une menace ». Selon un article du JournalDuNet daté du 30 avril 2015, se référant à l'article 6 de la LCEN, le terme « hébergeur » désigne l'intermédiaire technique qui met à la disposition des tiers les outils permettant de communiquer des informations en ligne. Il peut donc désigner des éditeurs dès lors qu'ils mettent à disposition des espaces de publication « participatifs », édités par les internautes (forums, réseaux sociaux, espaces de commentaires, chronique ou tribune telle que celle-ci, etc.).
Les avis ci-dessous sont rédigés à titre personnel et ne sauraient engager ceux du groupe CCM Benchmark que je dirige (NDLA: société éditrice des sites Journaldunet, CommentCaMarche, Linternaute, etc.).

Jusqu'à ce jour, lorsque des échanges entre individus ont lieu sur un espace de publication hébergé en France, la justice peut à tout moment demander à l'éditeur, sur simple réquisition judiciaire, de lui fournir les données de connexion de l'utilisateur (adresse IP et horodatage) afin de demander l'identification de l'individu auprès de son fournisseur d'accès. Dans la pratique, cela se pratique parfois sans réquisition dans des cas de force majeure, en infraction avec la loi. A partir du moment où il est de notoriété publique que les sites hébergés en France sont équipés d'une boîte noire, il faudrait être un terroriste idiot pour utiliser un espace de discussion hébergé dans un pays ayant installé de tels dispositifs, alors même qu'il existe un grand nombre de services similaires dans des pays n'en ayant pas déployé. Ainsi, l'information qui était jusqu'ici la plupart du temps accessible risque de devenir petit à petit inaccessible aux services de renseignement.
Il restera malgré tout une trace de la connexion chez le FAI me direz-vous ? A partir du moment où des personnes ayant des choses à se reprocher auront besoin de communiquer, pensez-vous qu'ils le feront à découvert ? Evidemment non, il est à la portée de tout le monde d'ouvrir un tunnel crypté vers une connexion située à l'étranger. Toute communication chiffrée (y compris légalement) est dès lors suspecte, ce qui signifie qu'il sera nécessaire de mettre en oeuvre des moyens pour décrypter toutes les communications chiffrées afin d'en vérifier le contenu. Les moyens de cryptologie utilisables en France sont certes soumis à une réglementation spécifique (http://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie), encore faut-il qu'elle soit respectée et on imagine mal des terroristes appliquer à la lettre la réglementation française…
Ainsi, en mettant en place un tel niveau de contrôle des communications, le risque est de faire monter le niveau de sophistication des échanges entre terroristes. Pour peu que la loi soit votée, on peut compter sur le gouvernement pour médiatiser rapidement quelques prises afin d'illustrer la pertinence de la loi. Il est toutefois évident, à terme, que les premières mesures des organisations terroristes consisteront à former leurs membres aux techniques de chiffrement, afin de devenir invisibles sur la toile, alors même que la formation des agents de la force publique prendra des années. L'agilité joue là encore en la faveur des extrémistes.
Il est vrai que l'on ne peut pas rester inactifs face à la menace terroriste, mais une solution clé-en-main basée uniquement sur le numérique et votée en urgence est-elle la meilleure solution ? Certes le projet de Loi permet de mieux encadrer des pratiques qui existaient déjà sans support légal, mais cette Loi risque bien de rendre ces pratiques plus difficiles à mettre en oeuvre, voire caduques. Enfin, sur le fond, la réaction du public suite à l'affaire Charlie Hebdo était sur le thème « Nous n'avons pas peur, nous continuerons à être libre ». Avec ce projet de loi, le message me semble plutôt être « Nous avons peur, mais nous sommes prêts à être moins libres pour y remédier, quitte à ce que cela ne serve à rien ».

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

Source : http://www.journaldunet.com/ebusiness/expert/60824/la-loi-renseignement-sera-contournee.shtml
Par Jean- François Pillou – CCM Benchmark

Des pirates informatiques volent 5 millions de dollars à Ryanair | Le Net Expert Informatique

Des pirates informatiques volent 5 millions de dollars à Ryanair

Un peu moins de 5 millions de dollars (4,5 millions d'euros) ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert électronique frauduleux passé via une banque chinoise ».

La compagnie travaille actuellement avec ses établissements bancaires et les autorités compétentes afin de récupérer ces fonds. Elle annonce dans un communiqué, publié mercredi 29 avril, que ceux-ci ont été « bloqués » et que des mesures ont été prises pour sécuriser les comptes de Ryanair. L'identité des pirates est encore inconnue.

Facture de kérosène

La société, dont le siège est à Dublin, assure des liaisons principalement en Europe. La plupart de ses transactions sont effectuées en euros, mais elle dispose aussi de comptes en dollars. D'après The Irish Times, les fonds en dollars ciblés par les pirates informatiques étaient destinés à payer ses factures de kérosène.

Le quotidien ajoute que l'agence judiciaire chargée du dossier en Irlande, le Criminal Assets Bureau (« bureau des biens d'origine criminelle ») de Dublin, avait pu identifier où la somme subtilisée avait été transférée grâce à un système de coopération internationale avec des agences jumelles en Asie.

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

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

Source : http://www.lemonde.fr/pixels/article/2015/04/29/des-pirates-informatiques-volent-5-millions-de-dollars-a-ryanair_4625234_4408996.html#Zc4r8duqZpt2kWJo.99

Une cyberarnaque aux ramifications africaines mise au jour après un an d'enquête

| Le Net Expert Informatique

Une cyberarnaque aux ramifications africaines mise au jour après un an d'enquête

Un an d'enquête a été nécessaire aux enquêteurs du commissariat de Decazeville pour boucler une affaire de cybercriminalité aux ramifications africaines.

Au terme d'un an de difficiles investigations, les enquêteurs du commissariat de Decazeville viennent de boucler un dossier complexe de cybercriminalité aux ramifications internationales, mettant en cause une quadragénaire decazevilloise.
L'affaire a commencé lorsqu'une plainte a été déposée en France, à propos d'un objet vendu sur des sites bien connus de vente entre particuliers (Le Bon Coin, E-Bay). L'objet a été envoyé à Decazeville mais le vendeur n'a jamais été payé. Le temps passant, les dossiers affluent de toute la France, une vingtaine de victimes recensées auprès de 11 parquets en France (Bretagne, Loire, Guadeloupe, mais aussi en Midi-Pyrénées). Les colis sont livrés soit dans un point relais, soit directement à une adresse voire à une adresse tierce mais au nom de la même personne.
Cette dernière, quadragénaire decazevilloise, a été entendue à plusieurs reprises par la police decazevilloise saisie en enquête préliminaire.
Au départ de l'arnaque se trouve un acquéreur pour un objet quelconque (bibelots, téléphone etc). Il contacte le vendeur par mail. Au bout de quelques mails, il indique être à l'étranger et propose que le colis, pour des raisons logistiques soit envoyé en France dans un point relais ou chez quelqu'un de sa connaissance.

Faux site de paiement
Pour le paiement, il propose l'ouverture d'un compte E-Bay via un mail avec un lien. Sauf que le lien débouche sur un faux site, facturant l'ouverture d'un compte (alors que c'est usuellement gratuit), via un paiement en ligne soit via l'achat de coupons PCS (150 €) dans des tabacs-presse.
C'est en se rendant compte qu'il y avait anguille sous roche que la Decazevilloise, en besoin d'argent, aurait été recrutée par les cerveaux Ivoiriens et Béninois de l'affaire, pour servir de destinataire aux colis. Charge à elle ensuite de revendre les colis (livrés mais non payés aux vendeurs) puis de reverser 60 % du prix en guise de commission aux arnaqueurs africains ; lesquels avaient en outre capté ses coordonnées bancaires.
Le préjudice total avoisine actuellement environ 10 500 € mais d'autres plaintes pourraient abonder l'enquête.
Le dossier a été transmis au parquet de Rodez qui doit décider, au regard des éléments qui lui sont apportés, notamment sur e l'état psychologique et psychique de la Decazevilloise mise en cause, des mesures de poursuites à l'encontre de cette dernière. Mais aussi éventuellement demander une enquête complémentaire voire l'ouverture d'une information judiciaire. Ou bien encore la saisine d'un office central spécialisé dans la lutte contre la cybercriminalité internationale.
Le commissariat de Decazeville appelle à la plus grande vigilance les acheteurs ou vendeurs via le web, en s'assurant du paiement d'un objet avant son envoi.

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

Source : http://www.ladepeche.fr/article/2015/04/10/2084456-une-cyberarnaque-mise-au-jour.html
Par Bernard-Hugues Saint-Paul

La Maison Blanche victime d’une cyberattaque « préoccupante » | Le Net Expert Informatique

La Maison Blanche victime d’une cyberattaque « préoccupante »

Des e-mails non classés secrets adressés au président des Etats-Unis, Barack Obama, et envoyés par lui ont été lus l'année dernière par des hackeurs russes qui ont pénétré une partie du système informatique de la Maison Blanche, a affirmé samedi 25 avril le New York Times.

Au début du mois d'avril des responsables américains avaient reconnu qu'il y avait eu un « événement » relatif à la sécurité à la fin de l'année dernière, mais avaient refusé de confirmer les informations selon lesquelles des Russes seraient derrière ces cyberattaques. Selon le quotidien américain, qui cite des responsables ayant été informés de l'enquête sur ces faits, l'attaque a été « beaucoup plus intrusive et préoccupante » que cela n'a été officiellement reconnu. Les personnes cités laissent entendre que les hackeurs étaient liés au pouvoir russe.

« Aucun réseau classé secret atteint »

Les pirates ont réussi à accéder aux archives des e-mails de personnes employées à la Maison Blanche et avec lesquelles M. Obama communiquait régulièrement, écrit le New York Times. C'est dans ces archives que les hackeurs ont pu voir des e-mails que le président avait envoyés et reçus, selon les sources citées par le quotidien. Son compte mail lui-même ne semble pas avoir été piraté. Les hackeurs auraient par ailleurs également pénétré le système non secret du département d'Etat américain.

Les pirates ne semblent en revanche pas avoir pénétré les serveurs qui contrôlent le trafic de messages du BlackBerry de Barack Obama, et la Maison Blanche a assuré qu'aucun réseau classé secret n'avait vu sa sécurité compromise. « Mais des responsables ont reconnu que le système non classé secret contient régulièrement beaucoup d'informations considérées comme hautement sensibles : horaires, échanges d'e-mails avec des ambassadeurs et des diplomates (…) et, inévitablement, débats politiques », écrit le quotidien.

On ignore combien de courriels du président ont été lus par les pirates. « Néanmoins, le fait que les communications de M. Obama étaient parmi celles qui ont été ciblées par les hackeurs – qui sont suspectés d'être liés au pouvoir politique russe, voire de travailler pour lui – a été l'une des conclusions de l'enquête les plus étroitement protégées », selon le New York Times.

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

Source : http://www.lemonde.fr/ameriques/article/2015/04/26/la-maison-blanche-victime-d-une-cyberattaque-preocucupante_4622869_3222.html

---

Revivez 70 ans de menaces informatiques | Le Net Expert Informatique

Revivez 70 ans de menaces informatiques

Depuis les premiers « phreakers », qui pirataient les lignes téléphoniques, jusqu'à Heartbleed, qui a semé la panique sur le web, la menace informatique a évolué au fil des années. À mesure que la sécurité progresse, les pirates innovent.

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

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

Source : http://www.zdnet.fr/actualites/70-ans-de-menaces-informatiques-39818348.htm

Lufthansa victime d'une cyberattaque | Le Net Expert Informatique

Lufthansa victime d'une cyberattaque

Le site de la compagnie aérienne allemande Lufthansa a été victime d'une attaque informatique, a indiqué vendredi 10 avril l'hebdomadaire Der Spiegel. Des individus ont réussi à se procurer les données personnelles d'utilisateurs du site LH.com.

L'attaque a été menée via un « botnet » (machine zombie), une série de noms d'utilisateurs et de mots de passe ont été automatiquement testés jusqu'à l'aboutissement du méfait, selon Der Spiegel.
Lufthansa a indiqué avoir immédiatement pris les mesures nécessaires, « mais celles-ci n'ont pas pu empêcher l'accès illicite aux données personnelles de certains utilisateurs ».

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

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

Source : http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2282639/2015/04/10/Lufthansa-victime-d-une-cyberattaque.dhtml

---

Bientôt finis tous les mots de passe ! | Le Net Expert Informatique

Bientôt finis tous les mots de passe !

Pour en finir avec les mots de passe, PayPal propose d'implanter une puce dans votre cerveau, ou de vous faire ingérer un dispositif "d'identification embarquée" (dans une micropuce).

Il ne s'agit encore que d'une idée, mais pour Jonathan LeBlanc, chef du développement de PayPal, l'avenir est en marche et bientôt nous pourrons oublier les mots de passe, et même les dispositifs biométriques (scanner de l'iris, empreintes digitales), qui « sont déjà obsolètes ».
« Tant que les mots de passe demeureront un standard pour identifier les internautes, les gens continueront à utiliser 'password123' pour se connecter… », indique-t-il au Wall Street Journal.
Dans une présentation destinée à être utilisée dans plusieurs conférences sur le sujet, intitulée « Tuez tous les mots de passe », Jonathan LeBlanc prône le développement de nouveaux systèmes, adaptés à la « technologie actuelle », qui tendrait vers une « véritable intégration avec le corps humain ».
Pour Jonathan Leblanc, les systèmes d'analyse du rythme cardiaque via des systèmes embarqués et ingérables sont l'avenir. Ils devraient permettre « d'identifier naturellement un corps » – et donc de barrer la route, définitivement, aux cyberpirates. D'autres « périphériques internes » pourraient être utilisés, comme des implants cérébraux. Les dispositifs ingérables seraient de leur côté alimentés par l'acide de l'estomac, qui ferait office de « batterie ».
Des banques, comme Halifax, testent des systèmes d'identification reposant sur l'analyse du rythme cardiaque des individus – mais pour l'heure, il s'agit de bracelets intelligents, et non de micropuces à avaler. Selon Jonathan Leblanc, les ingénieurs de PayPal planchent d'ores et déjà sur un système similaire.

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

Source : http://www.zdnet.fr/actualites/paypal-tuez-tous-les-mots-de-passe-39818340.htm
Par Fabien Soyez

En 2015 les cybercriminels préfèrent la propagation de

virus aux spams | Le Net Expert Informatique

En 2015 les cybercriminels préfèrent la propagation de virus aux spams

Ceci d'après l'analyse des boîtes emails de professionnels utilisant la technologie de filtrage de Vade Retro (soit plus de 150 millions de boîtes emails analysées) sur février et mars 2015. Cette analyse montre une nouvelle tendance forte en matière de cybercriminalité. Les attaques de spam de masse et classiques sont délaissées par les hackers au profit d'attaques de virus ciblées et plus élaborées.

Sur les mois de février et mars 2015, le niveau de spam a connu une baisse – même s'il représente toujours 72% du flux d'emails adressés aux utilisateurs dans le cadre professionnel (contre 77% en décembre et 79% en janvier), alors que le niveau de virus est stable à un niveau très haut depuis le mois de janvier 2015 soit 0,3% du flux total d'emails.

En 2015, les virus sont en croissance de près de 300 % par rapport à 2014

Dimitri Perret, Responsable Marketing Vade Retro Technology insiste sur l'importance de cette tendance : « Depuis le début de l'année 2015, le niveau de virus que nous observons est très élevé – même si le chiffre de 0,3 % paraît peu significatif, le virus a tout de même connu une hausse de 300 % entre la fin de l'année 2014 et les premiers mois de 2015. Cela démontre une nouvelle tendance : la qualité plutôt que la quantité. Pour des raisons de rentabilité, les hackers préfèrent envoyer moins de spam de type viagra et autres, pour s'orienter vers des emails plus ciblés et plus dangereux. Ces virus sont de natures ransomware, où une somme d'argent est demandée pour débloquer le poste infecté. On y retrouve aussi (et toujours) les virus pour infiltrer les réseaux et développer ou renouveler leurs parcs de botnets (postes zombies, utilisés pour envoyer les spams et virus). Le retour sur investissement est donc plus élevé. »

Les virus utilisés ont généralement une finalité financière. Très agressifs, ils sont par exemple cachés dans des fichiers .zip contenant un fichier screensaver qui est en fait un cryptolocker. Les virus de ce type peuvent être utilisés par les hackers pour crypter les données du disque dur de l'entreprise et pratiquer du ransomware. Le phishing est également toujours très utilisé pour pénétrer les réseaux en invitant les utilisateurs à cliquer sur des liens frauduleux via des faux emails ressemblants de plus en plus à de vrais emails d'entreprise.

Le spam évolue

Comme dit plus haut, le spam reste malgré tout très utilisé. De plus il évolue. Les envois massifs de spam sont aujourd'hui trop vite détectés par les technologies anti-spam, les cybercriminels font donc évoluer leurs méthodes pour tenter de franchir les outils de détection et voler « sous les radars ». Concrètement cela consiste à envoyer des vagues de spam plus petites et plus courtes mais vers des utilisateurs plus ciblés (technique du Snowshoe par exemple). Derrière cela, la finalité est de développer ou renouveler un réseau de botnet afin de propager du malware de manière plus discrète et efficace.

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

Source : http://www.programmez.com/actualites/en-2015-les-cybercriminels-preferent-la-propagation-de-virus-aux-spams-22509

Thales aurait été la cible d’une cyberattaque | Le Net Expert Informatique

Thales aurait été la cible d’une cyberattaque

Le groupe aurait été victime d’une intrusion dans son système d’informations. Ce mercredi, Thales confirme l’attaque mais indique avoir renforcé sa sécurité depuis.

Selon des informations du Canard Enchainé, le groupe français Thales a été victime d’une attaque informatique. L’offensive a duré plusieurs jours avant de s’interrompre vers la mi-février. Plusieurs pirates seraient parvenus à s’introduire dans des systèmes d’informations du groupe basés aux Etats-Unis, au Canada, en Australie, en Grande-Bretagne puis en France.
Pour l’hebdomadaire, Thales a bien confirmé l’attaque dont le but était de prendre le contrôle de l’ensemble du système d’informations du groupe. L’idée était également de se maintenir dans ce dernier pour récupérer des informations de la société ou d’infecter des postes.
Depuis cette attaque, que Thalès ne commente pas davantage quant à ses motifs ou ses moyens, le groupe précise avoir renforcé ses mesures de sécurité. Une note aurait également circulé auprès de certains collaborateurs du groupe en vue de revoir les process internes de sécurité.

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 protection juridique du chef d’entreprise.
Contactez-nous

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

S o u r c e ;
http://www.clubic.com/reseau-informatique/securite-reseaux/actualite-763182-thales.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_16/04/2015&partner=-&svc_position=939819221&svc_misc=-&crmID=639453874_939819221&estat_url=http%3A%2F%2Fwww.clubic.com%2Freseau-informatique%2Fsecurite-reseaux%2Factualite-763182-thales.html