La fraude au Président n’arrive pas qu’aux autres

La fraude au Président n’arrive pas qu’aux autres

Des millions d'euros envolés dans une escroquerie aux faux virements bancaires. Une entreprise Dunkerquoise découvre qu'elle vient de perdre plus de neuf millions d'euros dans la manipulation de ses informations bancaires.

Qu'ils sont fatigants ces gens qui savent toujours tout. Il y a quelques semaines, lors d'une conférence que m'avait demandé une collectivité locale, un responsable d'un bailleur social m'expliquait qu'il ne fallait pas trop exagérer sur les risques de piratage informatique, de fuites de données… J'expliquais alors comment des malveillants s'attaquaient aussi aux locataires de logements sociaux. Le monsieur expliquait alors, pour conforter ses dires « ***depuis que j'ai un antivirus et le firewall incorporé*** […] ***je n'ai plus jamais eu d'ennui avec mon ordinateur portable***« . Le monsieur travaillait pour un bailleur social de la région de Dunkerque (Nord de la France – 59). Et c'est justement à Dunkerque, chez un bailleur social, *Le Cottage social des Flandres*, qu'une nouvelle affaire de fraude au président vient de toucher la banlieue de la cité de Jean-Bart. Une manipulation des informations bancaires qui coûte 25% du chiffre d'affaires de la victime.

23 versements de 400.000 euros

Alors, cela n'arrive qu'aux autres ? L'entreprise Dunkerquoise n'est pas une structure à la Nestlé, Michelin, Total, Le Printemps. 140 employés, 6.000 locataires et un quelques 40 millions d'euros de chiffre d'affaires. Bref, une petite entreprise comme il en existe des dizaines de milliers en France. Le genre d'entité économique qui pense que les pirates informatiques, les escrocs ne s'intéresseront pas à elles. Erreur grave ! Pour *Le Cottage social des Flandres*, les professionnels de la Fraude au Président, la fraude au FoVI, se repartis avec 23 virements de plus de 400.000 euros. Bilan, 9,8 millions d'euros envolés dans les caisses d'une banque basée en Slovaquie. Autant dire que revoir l'argent revenir à la maison est peine perdue. D'autant plus que la fraude a couru du 7 avril au 23 mai. Piratage qui n'aura été découvert qu'un mois plus tard, au départ en vacances d'un dès comptable. Bref, en manquement évident de sérieux, et cela dans toutes les strates stratégiques de l'entreprise. Surtout à la lecture de la Voix du Nord : un responsable explique que l'arnaque était tellement bien montée que la société n'y a vu que du feu, et plus grave encore « ***On a les reins solides, on va pouvoir faire face***. » Après tout, 9,8 millions d'euros « ne » représente que 25% du CA de cette société (Sic !).

Méthode rodée mais simple à contrer

Un exploit que cette fraude ? Les adeptes du social engineering (l'étude de l'environnement d'une cible avant de s'attaquer à son univers informatique) savent très bien que non. Dans l'affaire Dunkerquoise, un compte mail piraté aurait permis le début de cette fraude au président. Détail troublant, les courriels arrivaient ailleurs que sur une adresse type adresse@Cottages.fr ? Car si piratage il y a eu, c'est l'ensemble des services couplés au domaine qui ont pu être corrompu. A moins que le responsable usurpé utilisait un gMail, Yahoo! ou tout autre compte webmail. Toujours est-il que le pirate a mis la main sur une adresse officielle et a pu ainsi manipuler les employés.

Parce que pour éviter un FoVI, c'est aussi simple que de protéger son argent personnel, normal. C'est d'ailleurs très certainement là où le bât blesse. Ce n'est pas mon argent, donc j'en prends soin, mais pas trop. Penser que cela n'arrive qu'aux autres est une grande erreur. Éduquer vos personnels, éduquez-vous, patrons, dirigeants…

Pour éviter un FoVI, contrôler ses informations bancaires

N'autoriser le transfert d'argent qu'après applications de mesures décidées en interne, et quelle que soit l'urgence de la demande de manipulation des informations bancaires. D'abord, la somme d'argent. Plafonner le montant. Si ce montant dépasse le chiffre convenu, obligation d'en référer à la hiérarchie. Un élément qui doit obligatoirement faire « tiquer » dans les bureaux : la demande d'un second transfert, d'une nouvelle modification des Le mot-clé principal « informations bancaires » n'apparait pas dans le titre SEO de la page par la même personne, même entité, doit également être indiquée à la hiérarchie. « ***Paulo, c'est normal de faire 23 versements de 400.000 euros en 2 mois ?*** » – « ***Oui ! Le boss achète des chouquettes en Slovénie. Il me l'a dit par mail !***« . La validation de transfert doit se faire par, au moins, deux personnes différentes, dont un supérieur hiérarchique.

Article original de Damien Bancal

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

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

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

Contactez-nous

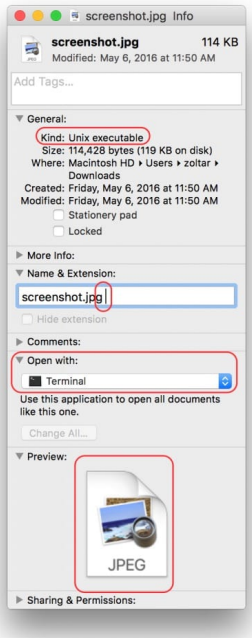
Réagissez à cet article

Original de l'article mis en page : ZATAZ Informations bancaires : la fraude au Président n'arrive pas qu'aux autres – ZATAZ

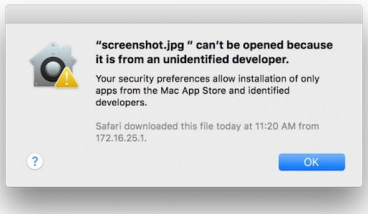
Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

	Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

Faut-il y voir la rançon du succès des Mac ? Toujours est-il qu'OSX/Keydnap est le deuxième malware de la semaine sur OS X, après Backdoor.MAC.Eleanor. Découvert par ESET, ce nouveau logiciel malveillant est pour le moment d'origine inconnue, mais on connait son mode de fonctionnement.
Téléchargé en pièce jointe ou depuis un site interlope, Keydnap se présente sous une forme bien innocente : une archive ZIP qui contient ce qui ressemble à une image (.jpg) ou un document texte (.txt). Sauf que le suffixe du document contient une espace, ce qui lance un Terminal, et non Aperçu ou TextEdit comme on peut s'y attendre.



En cliquant sur le document, un mécanisme se met en place qui fait prendre des vessies pour des lanternes. L'application attendue s'ouvre et présente le document qui va bien… sauf que dans l'intervalle, le fichier aura ouvert un Terminal (l'icône du Terminal apparait brièvement dans le dock avant d'être remplacée par celle de l'application standard). Une fois l'exécutable lancé, Gatekeeper prévient que le fichier provient d'un développeur non enregistré et qu'il ne peut pas ouvrir le document :



Ce message d'alerte intervient si et seulement si Gatekeeper n'autorise que les applications provenant du Mac App Store et des développeurs identifiés. Sur OS X El Capitan, on peut choisir de lancer une app téléchargée depuis « n'importe où », mais plus sous macOS Sierra.
Une fois lancé, le malware crée une porte dérobée et remplace le contenu de l'exécutable par un leurre téléchargé sur internet ou intégré dans le code du logiciel malveillant – il peut s'agir du document effectivement attendu, comme une image :

La porte dérobée créée par Keydnap est persistante, même si on multiplie les redémarrages du Mac. Il demandera aussi le mot de passe de la session, déguisé sous la forme d'icloudsyncd. Une fois en possession de cette information, il transforme le Mac en open-bar : l'objectif du malware est de récupérer les informations du Trousseau d'accès, qui contient les identifiants et mots de passe de vos logiciels et services en ligne.
À la lumière de cette nouvelle affaire, on comprend mieux pourquoi Apple exige maintenant des logiciels signés sur macOS Sierra.
Merci à Mickaël Bazoge pour son enquête et son article

Réagissez à cet article

Original de l’article mis en page : Nouveau malware sur OS X : OSX/Keydnap détrousse le Trousseau d’accès | MacGeneration

---

Conséquences innatendues des cyberattaques

	**Conséquences innatendues des cyberattaques**

Les dégâts informatiques de premier jour ne constituent pas la seule conséquence d'une cyberattaque pour une entreprise. Il y a aussi la réduction en nombre des clients, déçus notamment du vol ou de la perte de leurs données. Certains peuvent même penser à poursuivre l'entreprise en justice. L'après est ainsi encore plus dure à gérer pour les dirigeants et les responsables informatiques.

Impact sur la confiance des consommateurs

La préparation d'une cyberattaque peut prendre plusieurs semaines, voire des mois. Par conséquent, leurs effets vont bien au-delà des « simples » dégâts informatiques. Une étude internationale réalisée par VansonBourne et publiée le 12 mai dernier le confirme, en insistant sur des atteintes sur la performance commerciale de la société victime. Elle révèle en effet que la confiance des consommateurs vis-à-vis de cette dernière s'amenuise après les attaques. Logique quand on sait que bon nombre de clients de TV5 Monde et Orange ont encore du mal à oublier les attaques respectives d'avril 2015 et de 2014 ayant entraîné une fuite de données. Cette étude avance même que 34% des Français voient leur loyauté envers une marque ayant laissé fuiter leurs données, diminuée. Les efforts de cybersécurité devront ainsi se trouver dans le plan de toute entreprise qui se veut être compétitive.
Les consommateurs sont également nombreux à perdre le désir d'acheter auprès d'une entreprise victime d'une attaque informatique. Plus de trois sur quatre ont même affirmé qu'ils iraient jusqu'à arrêter l'achat de produits ou services chez cette dernière, notamment si la vulnérabilité exploitée provient de l'erreur de l'équipe dirigeante. Pour une erreur humaine d'un subordonné, les clients sont plus compréhensifs. La publication de cette étude confirme par ailleurs que la sécurité des données figure depuis quelques années parmi les critères les plus considérés par les Français avant une décision d'acheter. Ce paramètre a été pris en compte par 61% des Français en 2015, contre 53% en 2014.

Risques de poursuite en justice

La perte de chiffre d'affaires est donc quasiment incontournable pour toute entreprise qui vient de faire l'objet d'une attaque informatique d'ampleur. Elle est toutefois moins grave par rapport à un autre risque, celui de la poursuite en justice. Cette étude a en effet permis de connaître que 50% des Français sont prêts à poursuivre en justice les entreprises attaquées pour négligence ou inattention apportée à la protection de leurs données personnelles. Target et Sony Picture en ont déjà payé le prix, trouvant même, parmi les auteurs de ces poursuites, leurs propres salariés. Face à ce risque, certaines entreprises envisagent de garder secrètes toutes les attaques atteignant leur système d'information. Serait-ce une bonne initiative de leur part ? La réponse est non. A l'heure d'Internet, la moindre information peut se trouver à la portée de tout le monde. Une éventuelle fuite pourrait ainsi écorner définitivement l'image d'une société choisissant une telle démarche. Au contraire, cette société devrait plutôt informer le plus rapidement ses clients, pour faire preuve de transparence. Cette démarche sera par ailleurs rendue obligatoire par le règlement européen sur la protection des données, un texte dont la mise en vigueur est prévue en mai 2018.

Article original de sekurigi.com complété par Denis JACOPINI

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les traces laissées par les cyberattaques – @Sekurigi

Privacy Shield : un « bouclier » troué à refuser !

	#Privacy Shield : un « bouclier » troué à refuser !

Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette décision, adoptée dans la plus grande précipitation, ne répond pas aux inquiétudes exprimées ces dernières semaines à tour de rôle par le groupe des CNILs européennes, le Parlement européen et différents gouvernements européens, ainsi que par les associations de défense des droits.

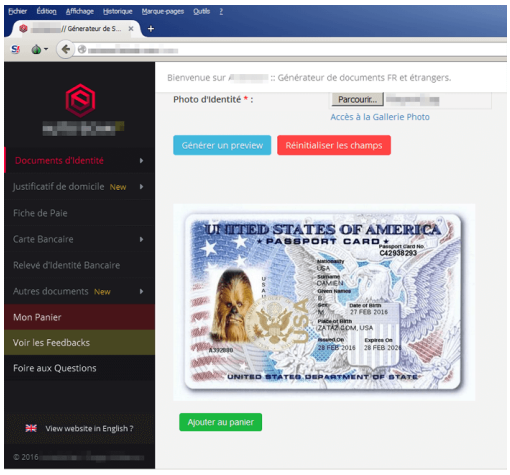
Le 6 octobre 2015 la Cour de justice de l'Union européenne avait annulé l'accord du « Safe Harbor » couvrant les transferts de données depuis 2000, estimant que celui-ci permettait une collecte massive des données et une surveillance généralisée sans offrir de voies de recours effectives aux États-Unis pour les individus concernés en Europe. Aujourd'hui, force est de constater que le Privacy Shield ne répond pas non plus aux exigences de la Cour de justice.
Sur les principes de respect de la vie privée qui incombent aux entreprises couvertes par le Privacy Shield, on peut se demander l'utilité même d'une telle décision dans la mesure où celle-ci ne se substituera pas aux clauses contractuelles types ni aux règles internes d'entreprises, moins contraignantes et actuellement en vigueur, mais qu'elle s'y ajoutera. Cela signifie que si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations qui lui incombent en matière de vie privée, elle pourra continuer à traiter des données avec les deux mécanismes internes cités plus hauts.
Mais le cœur de la décision se retrouve plutôt dans le chapitre sur l'accès aux données par les autorités publiques des États-Unis. Dans le texte, il n'est pas question de « surveillance de masse » mais plutôt de « collecte massive ». Or, si les États-Unis ne considèrent pas la collecte de masse comme de la surveillance, l'Union européenne, elle, par l'intermédiaire de sa Cour de justice, a tranché sur cette question en considérant, dans l'affaire C-362/14 Schrems c. Data Protection Commissioner, que la collecte massive effectuée par l'administration des États-Unis était de la surveillance de masse, contraire à la Charte des droits fondamentaux de l'Union européenne. Cette décision avait mené à l'invalidation du « Safe Harbor », et tout porte à croire que les voeux pieux et les faibles garanties d'amélioration exprimées par le gouvernement américain ne suffiront pas à rendre la décision du Privacy Shield adéquate avec la jurisprudence européenne.
Il en va de même sur la question des possibilités de recours. L'une des exigences de la CJUE, des CNIL européennes, du contrôleur des données personnelles et de la société civile était que toute personne concernée par un traitement de données avec cet État tiers puisse avoir la possibilité de déposer une plainte et de contester un traitement ou une surveillance illégale. Pour pallier cette sérieuse lacune du Safe Harbor, un mécanisme de médiateur (« #Ombudsperson ») a été instauré. L'initiative aurait été bonne si ce médiateur était réellement indépendant. Mais d'une part il est nommé par le Secrétaire d'État, d'autre part les requérants ne peuvent s'adresser directement à lui et devront passer par deux strates d'autorités, nationale puis européenne. L'Ombudsperson pourra simplement répondre à la personne plaignante qu'il a procédé aux vérifications, et pourra veiller à ce qu'une surveillance injustifiée cesse, mais le plaignant n'aura pas de regard sur la réalité de la surveillance. Cette procédure ressemble à celle mise en place en France par la loi Renseignement avec la #CNCTR et, pour les mêmes raisons, ne présente pas suffisamment de garanties de recours pour les citoyens.
Le projet de Privacy Shield, préparé et imposé dans la précipitation par la Commission européenne et le département du Commerce américain, ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. Les gouvernements européens et les autorités de protection des données doivent donc absolument refuser cet accord, et travailler à une réglementation qui protège réellement les droits fondamentaux. Les nécessités d'accord juridique pour les entreprises ayant fait de l'exploitation des données personnelles leur modèle économique ne peuvent servir de justification à une braderie sordide de la vie privée de dizaines de millions d'internautes européens.
Article original de La Quadrature du Net

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : un « bouclier » troué à refuser ! – Global Security Mag Online

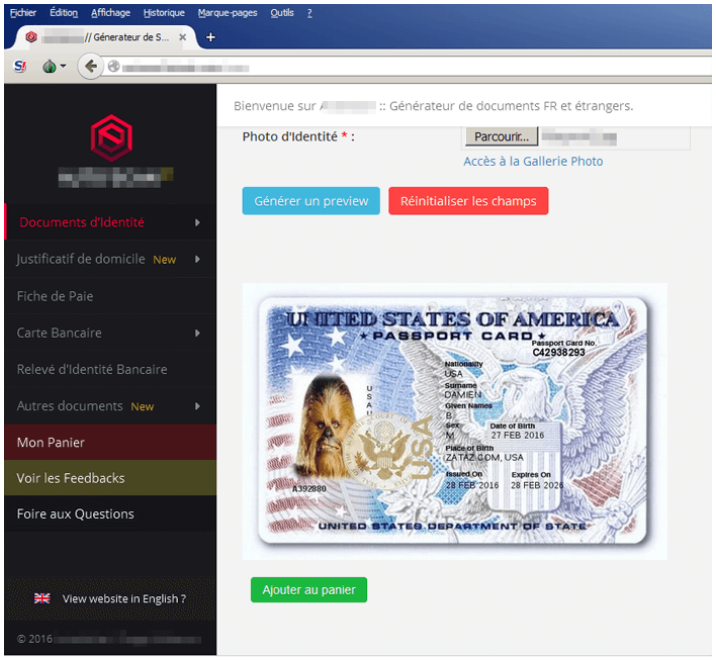
---

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.

Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

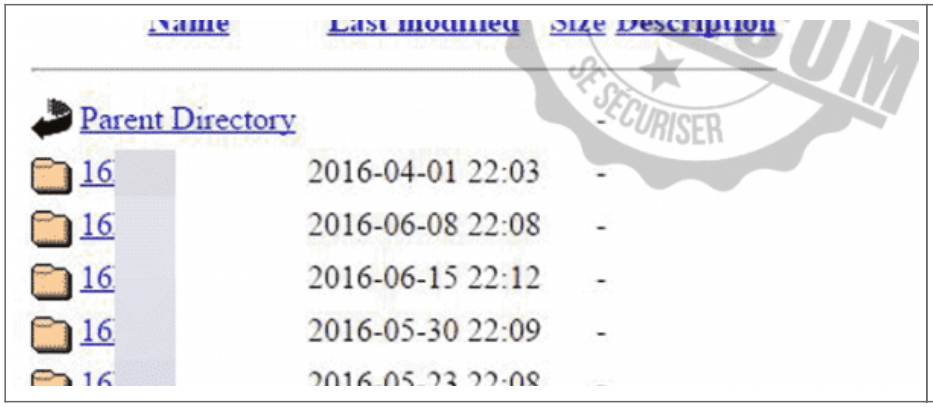
Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Fuite de données colmatée pour l'Université de Bordeaux



Fuite de données colmatée pour l'Université de Bordeaux

Un problème informatique à l'université de Bordeaux donnait accès à plus de 15 000 dossiers d'étudiants. La CNIL est intervenue à la suite du protocole d'alerte de ZATAZ pour faire colmater une fuite de données que personne n'avait vue.

Tout a débuté voilà quelques semaines. Benjamin postule sur la plateforme APOFLUX de l'Université de Bordeaux. Rapidement, APOFLUX permet de déposer ses vœux pour rejoindre un cursus, une formation. Comme l'indique le site, APOFLUX est un outil de dépôt de vœux « ***Il ne s'agit en aucun cas de votre inscription administrative définitive à l'Université de Bordeaux***« . Bref, un espace ou les étudiants déposent des dizaines d'informations allant du simple au très sensible. « ***En cherchant une information sur mon dossier,*** m'expliquait alors Benjamin, ***je me suis rendu compte d'un – truc – plutôt moche***« . Et je trouve que le terme moche est très poli. Via un espace web non protégé baptisé « Dépôt », n'importe quel internaute avait accès à l'ensemble des dossiers des étudiants postulants. Chaque espace de stockage offrait à la lecture des curieux, de maladroits de la souris ou de violeurs d'intimité numérique, les relevés de notes, lettres de motivations, CV… ainsi qu'à l'ensemble des candidatures passées par APOFLUX. Le lien avait beau être en HTTPS, le S voulant dire que les connexions entre l'internaute et le serveur était chiffré, cela ne protégeait pas pour autant les informations sauvegardées.

Fuite de données colmatée, étudiant dans le silence

J'ai saisi la CNIL, qui au passage est d'une efficacité redoutable dès que je leur communique une alerte. Le problème a été colmaté en quelques heures. Pour le moment, l'université n'a pas contacté les étudiants concernés par cette fuite d'information. Espérons qu'aucun malveillant ne soit passé par là avant l'alerte de ZATAZ. Impossible de savoir depuis quand ces « portes ouvertes » étaient accessibles sur la toile.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Fuite de données colmatée pour l'Université de Bordeaux – ZATAZ

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l’article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

Quelques chiffres sur les risques du WiFi public

Quelques chiffres sur les risques du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi *« un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec »*.

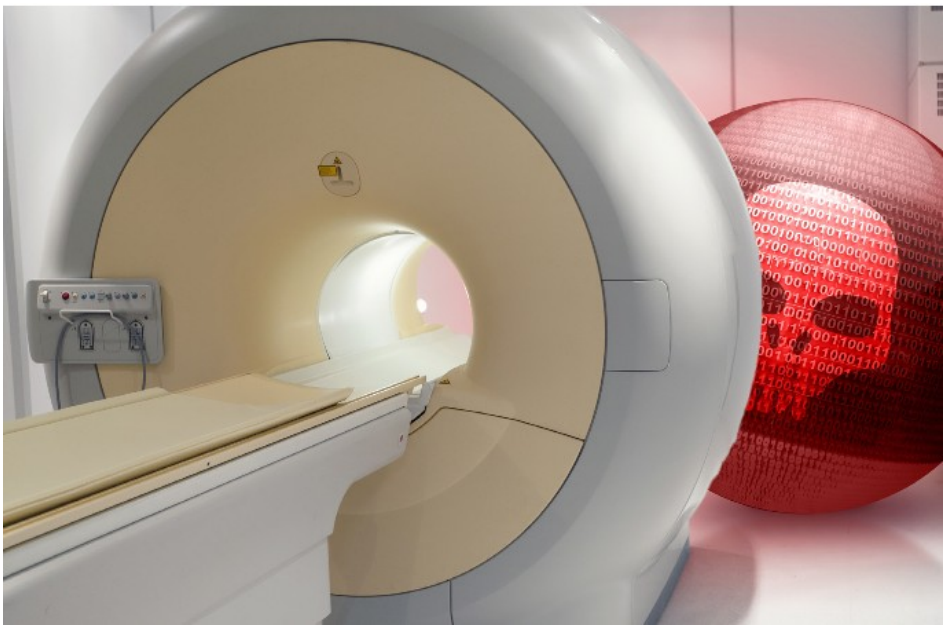
Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers *« intermédiaires »*, il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky,

Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires ignorent les risques du WiFi public

Risques d’infection dans le médical des Objets Connectés



Risques d’infection dans le médical des Objets Connectés

La faible sécurité des équipements de santé connectés entraîne la résurgence des vieux virus comme Conficker.

Un des problèmes de la montée en puissance de l'Internet des objets ? La sécurité.
Spécialistes, constructeurs, éditeurs répètent à longueur de conférences qu'il faut absolument que l'IoT soit « secure by design ». Entendez par là que les capteurs, le protocole de communication, la plateforme de traitement de l'information, l'architecture soient sécurisés dès leur conception.
Oui mais voilà, c'est sans compter sur le fameux héritage technique. Le monde de la santé rentre typiquement dans ce cadre et tout particulièrement les outils médicaux connectés. On pense ici aux IRM, scanners, radios, ou pompes à insuline. Ces équipements sont de plus en plus ciblés par les cyberattaquants, car ils sont moins bien protégés que des PC ou des serveurs.
Conséquence de cette faible sécurité, les vieux virus se rappellent aux bons souvenirs des administrateurs et des RSSI. Un rapport de la société de sécurité TrapX Labs, disséquant une attaque baptisée MEDJACK.2, montre que les attaques utilisent des malwares comme networm32.kido.ib ou le ver Conficker en complément de menaces plus sophistiquées. Moshe Ben Simon, co-fondateur de TrapX, résume bien ce paradoxe : « *un loup intelligent déguisé avec des vieux habits de mouton* ».

Mise en place de backdoors

Premier constat, les équipements médicaux connectés à Internet fonctionnent avec des versions de Windows non corrigées allant de XP (qui n'est plus supporté par Microsoft) aux versions 7 et 8. Des cibles de choix pour les anciens virus. « *Ces vieux virus sont utilisés avec des malwares (en l'occurrence MEDJACK.2) plus élaborés pour installer des backdoors dans l'établissement de santé et ensuite mener une campagne par exfiltration de données, voire se transformer en #ransomware* », souligne le rapport.
Les échantillons de Conficker que les experts de la société de sécurité ont analysé, montrent que le ver a été modifié pour avoir une meilleure capacité à se déplacer dans un réseau. Pire, son évolution fait qu'il est devenu indétectable pour les équipements médicaux. Dans son enquête auprès de 3 hôpitaux, TrapX relève qu'aucune alerte n'a été remontée par les établissements sur la présence de Conficker. A son apogée en 2009, Conficker avait infecté entre 9 et 15 millions d'ordinateurs. Il avait, comme capacité, de casser les mots de passe, d'enrôler les PC dans des botnets, etc. La version actuelle est diffusée par phishing envoyé aux personnels de l'hôpital.

Les données patients : la ruée vers l'or

L'objectif de ces attaques : obtenir les dossiers patients. Des informations très demandées sur le Dark Web et affichant une forte valeur marchande au marché noir. « *Les cybercriminels peuvent voler l'identité d'un patient pour se faire rembourser par les assurances des traitements coûteux et, en plus, revendre ces traitements au marché noir* ». TrapX estime qu'un dossier médical se monnaye entre 10 et 20 dollars sur le marché, contre 5 dollars pour une information financière. En début de semaine, on apprenait le vol de 9,3 millions de données de santé de citoyens américains. Le calcul est vite fait…
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : Conficker revient infecter l’IoT médical