Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique

	Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

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.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso

Des communications ultra-sécurisées avec TEOREM | Le Net Expert Informatique

Des communications ultra-sécurisées avec TEOREM

TEOREM est un système de téléphonie mobile et fixe à usage gouvernemental et de Défense. Il permet de protéger les communications vocales ainsi que les SMS sur tous les réseaux opérateurs. TEOREM assure également le rôle de modem chiffrant permettant ainsi l'échange de données entre deux ordinateurs personnels en toute sécurité.

Grâce à sa parfaite interopérabilité avec les différents réseaux de télécommunication fixes (analogiques et numériques) et mobiles (2G / 3G), TEOREM offre une grande polyvalence aux utilisateurs. Enfin, son autonomie, sa miniaturisation et sa grande flexibilité en font une solution unique pour répondre aux besoins des utilisateurs nomades.

Une solution hautement sécurisée et simple d'utilisation :
• Configuration fixe ou mobile (2G / 3G).
• Certifiée jusqu'au niveau Secret Défense pour la France.
• Communications sécurisées de bout en bout.
• Signal lumineux permettant de différencier les appels sécurisés et non sécurisés.

Un système flexible et performant :
• Compatible avec les réseaux d'opérateurs et gouvernementaux.
• Système de gestion centralisé à distance.
• Gestion sans intervention de l'utilisateur final.
• Grande qualité audio : + 15%* comparé aux téléphones standards.

* Selon norme PESQ.

Source : https://www.thalesgroup.com/fr/cybersecurite/teorem

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

---

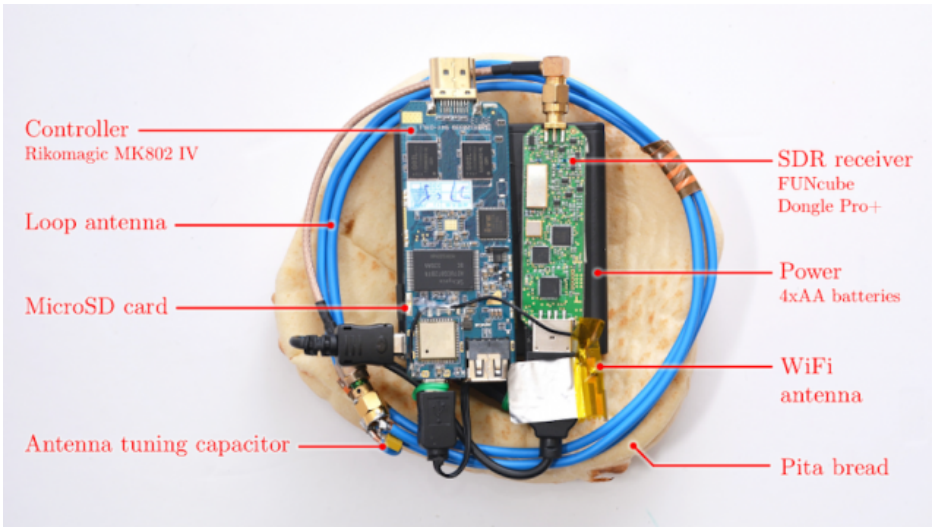
Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations 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

Pour pirater un ordinateur, une pita suffit | Le Net Expert Informatique

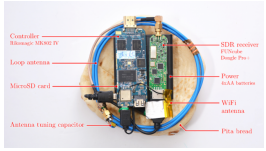


Pour pirater un ordinateur, une pita suffit

Selon une étude de l'université de Tel-Aviv, travailler dans un café pourrait s'avérer risqué pour la sécurité de votre ordinateur

Cette pita, qui donne l'apparence innocente que quelqu'un mange ostensiblement en face de vous dans le café de votre quartier, pourrait contenir un système d'espionnage informatique pouvant infiltrer les protocoles d'encodage les plus sécurisés de votre ordinateur.

Pire encore, ont déclaré les chercheurs de l'Université de Tel-Aviv, les utilisateurs de cet ordinateur ne peuvent pas faire grand chose pour se protéger.
« Des techniques d'atténuation… pourraient inclure des cages Faraday », des écrans en métal spécialement posés au sol qui bloquent les radiations… « Pourtant, la protection peu chère de PC de niveau commercial semble difficile », explique l'équipe.
Dans un article publié mardi, les chercheurs décrivent le très faible coût de l'équipement de type Radio Shack, que l'on peut facilement cacher dans un pain pita standard et qui peut être utilisé pour « lire » des impulsions électromagnétiques provenant du clavier d'un ordinateur standard, y compris les frappes sur le clavier afin de décrypter les documents sécurisés.
De manière amusante, l'Université de Tel-Aviv a appelé l'attaque PITA, Instrument portable pour l'acquisition de signaux.



L'étude, menée par les chercheurs Daniel Genkin, Itamar Pipman, Lev Pachmanov et Eran Tromer a été publiée pour coïncider avec une conférence majeure de sécurité informatique qui va avoir lieu à l'Université de Tel-Aviv (UTA) cette semaine.
« Nous avons pris avec succès des codes d'ordinateurs de divers modèles fonctionnant avec GnuPG (une source populaire d'encodage, en utilisant le standard d'encodage OpenPGP) en quelques secondes », a écrit l'équipe de l'UTA dans l'article, intitulé « Voler des codes de PC en utilisant une radio : des attaques électromagnétiques à moindre coût sur une exponentiation de fenêtres ».
En plus d'OpenPGP, l'équipe a été capable de dupliquer avec réussite les attaques sur d'autres systèmes d'encodages, très sécurisés, y compris RSA et ElGamal.
« L'attaque envoie quelques textes informatiques bien conçus et lorsque ces textes sont décryptés par la cible, ils entraînent l'occurrence de valeurs spécialement structurées dans le logiciel d'encodage », ont déclaré les chercheurs.
En utilisant un appareil qui peut recevoir des signaux radio, une simple radio ou une clé USB pouvant recevoir des émissions et les lire sur l'ordinateur, les chercheurs ont été capables d'observer les fluctuations dans le champ électromagnétique entourant l'ordinateur et de traduire ces fluctuations en frappes de clavier en utilisant un programme d'analyse.
L'article fournit des détails complets sur l'équipement nécessaire (tout est disponible et peu cher dans un magasin local d'électronique ou sur Internet), et sur la façon d'assembler et de connecter les parties, et même de les plier dans un pain pita.

L'équipement détecte les fluctuations dans le champ électromagnétique émis par le matériel informatique (clavier et processeur) lorsque l'ordinateur essaie de décrypter les signaux (les modules d'encodage contiennent des composants qui peuvent être exploités pour fonctionner automatiquement lorsque le texte encodé est rencontré).

En envoyant ces textes pièges, les pirates peuvent voler les codes d'authentification sur l'ordinateur de l'utilisateur, leur autorisant un accès libre aux documents et aux données encodés.

Une attaque PITA pourrait probablement être utilisée par des pirates en cas d'une attaque qui « balaie » des données et les documents d'un ordinateur.

Si ces données sont encodées, il est peu probable que les pirates pourront les lire (en fonction de niveau de complexité du codage), mais avec des clés d'encodage, les pirates pourraient trouver des informations encodées comme des numéros de cartes de crédit ou des mots de passe.

La seule mise en garde est que la pita « espion » a besoin de se trouver à 50 centimètres de la cible.

Mais d'après l'équipe, la totalité de l'opération peut être réalisée en quelques secondes, rendant l'attaque parfaite pour les pirates dans les cafés où de nombreux utilisateurs d'ordinateurs profitent des installations électroniques, du wifi et de boissons pour travailler.

Un pirate pourrait obtenir les codes dans une attaque « en marchant », attaque menée en transportant une « pita empoisonnée » sur un plateau avec de la vraie nourriture. L'étude notait pourtant que la « qualité du signal variait fortement en fonction du modèle de l'ordinateur cible et de la position de logiciel espion ».

L'équipe de UTA n'est pas la première à penser à utiliser des impulsions électromagnétiques pour pirater des systèmes.

En 2014, des chercheurs de l'Université Ben Gourion (UBG) ont pu utiliser un programme pirate sur un téléphone portable pour collecter des radiations électromagnétiques provenant de claviers, de moniteurs et d'autres équipements pour lire des informations importantes.

L'équipe de l'UBG a démontré comment les données collectées par le programme espion, auparavant placé sur un ordinateur (à travers une attaque de phising ou une autre méthode), pouvaient être captées par un téléphone portable qui créait un réseau local en utilisant des impulsions émanant de matériel informatique.

Les informations du système cible pouvaient être captées, même s'il n'est pas connecté à internet ou à un réseau local (Ethernet).

Le pire, a déclaré l'équipe, est qu'il n'y a pas grand chose que les utilisateurs d'ordinateur puissent faire pour éviter ces attaques, si ce n'est éviter les cafés et garder leur ordinateurs loin des pitot.

Malheureusement, l'équipe a déclaré « qu'empêcher la fuite à un bas niveau de prévention est presque impossible » parce que mettre en place des mesures efficaces (comme des cages Faraday) serait très gênant à cause du matériel informatique excessif ou ralentirait la capacité au point que les utilisateurs seraient incapables d'accomplir le moindre travail.

« Même lorsqu'un programme cryptographique est sûr mathématiquement, ses mises en place peuvent être vulnérables à des attaques de réseaux secondaires qui exploitent des émanations physiques », a déclaré l'équipe. Le pirate « peut facilement viser les ordinateurs ».

« Nous avons testé de nombreux ordinateurs de modèles variés », et lorsqu'il s'agit d'une attaque PITA, chaque utilisateur d'ordinateur devrait se sentir concerné.

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

Source : http://fr.timesofisrael.com/pour-pirater-un-ordinateur-une-pita-suffit/
Par David Shamah

L'Afrique a besoin de cybersécurité| Le Net Expert Informatique

L'Afrique a besoin de cybersécurité

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.
Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.
Le Security Day, qui se tiendra les 15 et 16 mars 2016 à Dakar, sera l'occasion d'aborder l'ensemble de ces sujets.

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 : Newsletter n°3 FIC
https://www.forum-fic.com/site/FR/Newsletter/S_inscrire_a_la_newsletter,C58881,I58949.htm

Exclusif : 47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle | Le Net Expert Informatique

	47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immochan, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin »…

Source : http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html

Grosse menace sur les mots de passe contenus dans le trousseau d’Apple | Le Net Expert Informatique

Grosse menace sur les mots de passe contenus dans le trousseau d’Apple

Peu importe que vous utilisiez iOS ou OS X, vos mots de passe sont en danger s'ils sont stockés dans le trousseau d'Apple.

Des chercheurs universitaires ont découvert une énorme faille de sécurité chez Apple, une faille suffisamment importante pour que la marque à la pomme n'ait pas encore réussi à la corrigé alors qu'elle a été signalée au mois d'octobre dernier. Pour causse, elle touche le mécanisme censé protéger les mots de passe : le trousseau.
L'idée du trousseau est simple : centraliser les identifiants et mots de passe pour que l'utilisateur n'ait pas à les ressaisir. Le problème, c'est que des chercheurs universitaires ont découvert toute une série de failles de sécurité.
Alors que le bac à sable est censé isoler les données pour qu'elles soient protégées, les chercheurs sont parvenus à percer le mécanisme.
Ils ont aussi créé un malware capable d'afficher tous les mots de passe de l'Apple's Keychain, c'est-à-dire ceux stocker dans le trousseau, ce qui expose tous les identifiants utilisés par les applications tierces : Facebook, Twitter, iCloud, Gmail, etc.
« Nous sommes parvenus à pirater tout le service Keychain, où Apple stocke les mots de passe et les autres paramètres de ses applis ainsi que les sandbox containers' dans OS X », explique Luyi Xing, responsable de cette recherche. « Nous avons découvert de nouvelles faiblesses dans les mécanismes de communication entre applis au sein d'OS X et d'iOS, qui pourraient être exploitées pour dérober des données confidentielles d'Evernote, Facebook et d'autres applis largement utilisées. »
Pour l'heure, le problème est énoncé, mais aucune solution n'est pour le moment encore disponible, le problème subsiste dans les versions actuelles d'iOS et d'OS X.

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

Source : http://www.linformatique.org/grosse-menace-sur-les-mots-de-passe-contenus-dans-le-trousseau-dapple/

Alerte partage ! Les

antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse | Le Net Expert Informatique

Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse

Un chercheur du Project Zero de Google a dévoilé une vulnérabilité critique affectant plusieurs produits et logiciels proposés par l'éditeur de sécurité ESET. La vulnerabilité est exploitable à distance et permet l'exécution de code malveillant sur la machine visée.

Les solutions de sécurité, comme n'importe quel autre logiciel, sont également exposées à des failles de sécurité qui peuvent permettre à un attaquant d'exécuter du code sur la machine. C'est d'ailleurs probablement l'une des raisons ayant poussé la NSA et le GCHQ à orienter leurs efforts de reverse engineering sur les produits de Kaspersky et d'autres éditeurs antivirus, afin de transformer ces obstacles en porte d'entrée au système de la cible.
La faille décrite par le chercheur Tavis Ormandy, qui avait déjà décelé une vulnérabilité affectant les logiciels de Sophos en 2012, porte plus précisément sur le moteur d'émulation utilisé par les produits de la société ESET. Cet outil est utilisé par l'antivirus pour faire tourner les instructions exécutées par la machine dans un environnement isolé, afin de détecter du code potentiellement malveillant pour l'utilisateur.

Même la version Linux est touchée
Malheureusement, celui-ci présente une vulnérabilité permettant à l'attaquant d'exécuter du code en disposant d'un haut niveau de privilège. Outre cet aspect, l'attaque est envisageable via un certain nombre de vecteurs : web, messagerie, ou périphérique de stockage, tous étant susceptibles d'être scannés par les programmes d'ESET à la recherche de code malveillant. La faille affecte les logiciels même dans leur configuration par défaut.
La vulnérabilité affecte de nombreux logiciels proposés par ESET : NOD32 Antivirus pour Windows, Cyber Security Pro pour OS X, NOD32 pour Linux Desktop, Endpoint Security et NOD32 Business Edition.
Un correctif est également proposé par ESET depuis le 22 juin, afin de corriger la faille de sécurité repérée par le chercheur. Le blog post détaille notamment divers moyen d'exploiter la faille, ainsi que des mesures d'atténuations : ainsi, couper l'analyse temps réel des outils d'ESET pourrait réduire le risque, en désactivant l'analyse automatique dans les outils proposés par la société slovaque. Mais la meilleure solution reste évidemment de patcher. Et vite.

Source : http://www.zdnet.fr/actualites/les-antivirus-eset-victimes-d-une-faille-de-securite-39821472.htm
Par Louis Adam

Les nouvelles cibles de la Cybercriminalité | Le Net Expert Informatique

	Les nouvelles cibles de la Cybercriminalité

Le piratage de TV5 Monde il y a quelques semaines est symptomatique du futur qui se prépare en matière de cybercriminalité. A mesure que les attaques deviennent plus sophistiquées, les pirates se rapprochent des infrastructures critiques. Ainsi, l'an passé, 43 % des entreprises œuvrant dans l'énergie (mines, compagnies du gaz, pétrolière) ont été la cible des cybercriminels au moins une fois dans l'année, rapporte une étude Symantec. Même constat chez Trend Micro, qui pointe que 47 % de l'industrie a fait l'objet d'une attaque, soit plus que les sites gouvernementaux. « Les attaques contre les infrastructures critiques deviennent une préoccupation grandissante de tous les gouvernements. En raison des conséquences potentielles des attaques, ces sites sont devenus très attractifs pour les pirates », dit l'étude de Trend Micro.

13,2 millions d'euros par an

Les dommages commis par les cybercriminels coûtent 13,2 millions d'euros par an à chaque entreprise de l'énergie, soit plus que dans n'importe quelle industrie, selon une étude réalisée par Poneman pour HP, relayée par Bloomberg. Pour se protéger, le secteur énergétique devrait porter son investissement en cybersécurité à 1,9 milliard de dollars d'ici à 2018, note ABI Research. Depuis quelques années, les exemples d'attaques contre des sites sensibles se multiplient. En France, le spécialiste du nucléaire Areva a avoué en 2011 que des pirates s'étaient introduits dans son réseau informatique pendant deux ans. En 2012, la compagnie pétrolière Aramco a vu 30.000 de ses ordinateurs infectés par un virus. Après avoir subi l'assaut des Anonymous, sorte de Robin des bois autoproclamés du Net, la compagnie nationale du pétrole koweïtien a déconnecté ses trois raffineries d'Internet. Sans être certaines d'être immunisées contre le fléau. Stuxnet, le virus conçu pour attaquer les sites nucléaires iraniens, s'est propagé sur des sites qui n'étaient pas connectés à Internet.

Afin de garder un temps d'avance sur des grands groupes qui se protègent mieux qu'hier, les cybercriminels font évoluer leurs méthodes. Pour atteindre leur cible, ils passent de plus en plus par des sous-traitants ou des fournisseurs. Pour preuve, les entreprises de B to B (commerce interentreprise) ont été ciblées par 15 % des 6 milliards d'attaques répertoriées en 2014 par NTT Com Security.

En attendant, si la crainte d'un virus qui ferait dérailler un train ou plongerait une ville dans le noir est dans tous les esprits, l'essentiel de la cybercriminalité a encore des motifs financiers. L'an passé, 18 % des attaques ont visé des institutions financières, devançant tous les secteurs d'activité.

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

Source : http://www.lesechos.fr/tech-medias/hightech/021137768977-cybercriminalite-les-nouvelles-cibles-1128488.php
Par Sandrine Cassini

La contradiction est manifeste entre la perception des salariés et la réalité en matière de cybersécurité | Le Net Expert Informatique

	La contradiction est manifeste entre la perception des salariés et la réalité en matière de cybersécurité

Les salariés français ont une connaissance relativement précise des notions liées à la cybersécurité des entreprises. Même si les cyberattaques semblent relativement fréquentes, ils jugent leur entreprise relativement bien protégée sur ces enjeux même si tous ne connaissent pas en détail sa politique en matière de sécurité. Dans ce cadre, ils identifient comme principales menaces : les virus informatiques, le vol de données et la perte de données liée à une erreur humaine. Tels sont les principaux constats que l'on peut tirer de la première étude* portant sur la cybersécurité vue par les collaborateurs, dévoilée ce 17 juin au Bourget par Capgemini et Sogeti.

Selon l'étude « Cybersécurité, Objets connectés et Systèmes industriels », les salariés français ont dans leur ensemble une connaissance assez précise des différentes notions liées à la cybersécurité : plus des trois quart estiment savoir précisément ce qu'est un virus informatique (88%), un hackeur (80%), un pare-feu (75%) ou une cyberattaque (75%). Seuls les salariés « seniors » sont plus hésitants, même si une majorité d'entre eux reste familier avec ces termes.
Dans ce cadre, 85% des salariés estiment que leur entreprise est bien protégée contre les attaques informatiques et les hackeurs. C'est plus particulièrement le cas des salariés des grandes entreprises pour lesquels ce score monte à 90% (contre 75% pour les PME). Ils jugent ainsi dans leur grande majorité la politique de sécurité informatique de leur entreprise adaptée à leur secteur (85%), efficace (85%) et claire (72%). Elle mériterait toutefois d'être davantage connue (61%).
36% des salariés déclarent que leur entreprise a déjà fait l'objet d'une cyberattaque. Ce score monte à 47% pour les salariés des grandes entreprise. Or, selon Kaspersky, plus de 90% des entreprises ont déjà subi une attaque informatique. Plus spécifiquement, 19% des salariés ont connu une attaque informatique de leur ordinateur professionnel. Pour 5% cela est même régulier. On remarquera que les salariés des PME sont plus nombreux a avoir subi ce type d'attaque que ceux des grandes entreprises. En revanche seule une minorité s'est déjà fait voler du matériel informatique professionnel : 8% un ordinateur, 6% leur téléphone portable. « Ces chiffres contradictoires montrent la complexité de la cybersécurité : celle-ci représente un risque asymétrique pour l'entreprise. Tous les chiffres indiquent que le nombre d'attaques croît considérablement d'année en année (120% de 2013 à 2014) ; attaques dont les salariés de l'entreprise n'ont pas nécessairement connaissance », commente Bernard Barbier, Responsable de la Sécurité des Systèmes d'Information du groupe Capgemini.
Cette contradiction entre la perception des salariés et la réalité de la menace est également illustrée dans le sondage par un fort sentiment de sécurité parmi les salariés. 65% d'entre eux estiment en effet que leur entreprise est plutôt bien protégée, et 20% très bien protégée contre les attaques informatiques et les hackeurs. Ce sentiment est surtout partagé au sein des ETI4 (93%) et des grandes entreprises (90%). « Ce sentiment de sécurité des salariés (65%) est une fois encore en totale contradiction avec les résultats de récentes études démontrant que les campagnes de phishing sont d'une très grande efficacité et qu'elles représentent plus de 80% des attaques réussies. En réalité, il suffit d'un seul PC infecté pour entraîner de lourdes conséquences financières et de réputation pour l'entreprise. On peut par ailleurs se demander si ce sentiment de sécurité n'entraîne pas un manque de vigilance des salariés dans le traitement des messages électroniques venant de l'extérieur de l'entreprise », explique Bernard Barbier.

Au final, les salariés ont trois grandes craintes quand à la cybersécurité de leur entreprise : les virus informatique (pour 48%), le vol de données (43%) et la perte de données suite à une erreur humaine (38%). On notera que les craintes sont fortement liées au secteur d'activité de l'entreprise. Ainsi les salariés de l'industrie craignent davantage le vol de données tandis que ceux du commerce ou du BTP pointent davantage les virus informatiques.

Le vol des données informatiques constitue le premier motif de crainte des salariés. Pour 23% d'entre eux, cela constitue même la plus grosse menace informatique qui pèse sur leur entreprise. De plus, 10% des salariés déclarent avoir subi un vol de leur ordinateur professionnel. « Ces chiffres démontrent la nécessité de protéger les données qui sont au cœur de l'activité de l'entreprise. La priorité est par conséquent de mettre en place des politiques de chiffrement des données : chiffrement des emails et des PC portables », poursuit Bernard Barbier.

Et de préciser que « ce sondage souligne que les salariés de l'entreprise ont un sentiment positif quant à la sécurité de leur système d'information classique. En revanche, la perception du niveau de sécurité des systèmes industriels (contrôle commande des usines) semble avoir plusieurs années de retard car la cyber menace est plus récente. Pourtant, le danger est plus dramatique encore, avec des conséquences matérielles et humaines, comme dans l'hypothèse d'une explosion d'usine. Le cyber terrorisme pourrait d'ailleurs viser en priorité ce domaine dans un avenir proche ».

Didier Appell, responsable, au sein de l'entité sectorielle mondiale « Cybersecurité » du Groupe, de l'offre Cybersécurité industrielle de Sogeti High Tech, le pôle d'expertise en Ingénierie et conseil en technologies du groupe Capgemini, précise : « Les entreprises ont fourni de gros efforts pour sensibiliser leurs salariés aux risques que représentent les attaques cybernétiques. Par extension, cette sensibilisation doit être également portée sur les systèmes industriels de supervision, de commande et contrôle ainsi que des systèmes embarqués car là aussi nous relevons une contradiction entre la perception des salariés et la réalité des menaces. Nous sommes effectivement de plus en plus sollicités par nos clients pour les aider à renforcer leur sécurité sur tous ces aspects ».

* L'étude a été réalisée auprès d'un échantillon de 1010 salariés français de bureau d'entreprises privées. La représentativité de l'échantillon est assurée selon la méthode des quotas sur les critères de sexe, d'âge, de catégorie socioprofessionnelle, de taille d'entreprise, de secteur d'activité de l'entreprise, de statut de l'employeur (public/privé) et de région de résidence. L'échantillon a été interrogé en ligne sur système CAWI (Computer Assistance for Web Interview) du 13 au 26 mai 2015.

Source : http://www.infodsi.com/articles/156643/contradiction-est-manifeste-entre-perception-salaries-realite-matiere-cybersecurite.html