Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html

Près de la moitié des Français confrontés à la cybercriminalité

Près de la moitié des Français confrontés à la cybercriminalité

Ransomware ou vol des données bancaires : près d'un Français sur deux (47%) a déjà été victime de cybercriminalité au cours de sa vie, selon l'étude annuelle Norton/Symantec révélée par Le Parisien / Aujourd'hui en France.

La cybercriminalité touche plus particulièrement les Français, puisque seulement quatre Européens sur dix sont confrontés à ce phénomène.
En détail, plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant qui permet au cybercriminel de demander de l'argent aux utilisateurs en échange de la décontamination de leur ordinateur, alors que 20% des Français confient avoir été victimes du vol de leurs données bancaires.
Ce rapport montre que les Français sont particulièrement méfiants vis-à-vis de la cybercriminalité. Plus de la moitié des sondés (55%) ont aujourd'hui plus peur de se faire voler leurs données bancaires en ligne que de se faire subtiliser leur portefeuille.
Plus de 17.000 consommateurs dans le monde ont été sondé cet automne pour les besoins de cette étude.

Réagissez à cet article
Source : http://www.lejdc.fr/france-monde/actualites/societe/techno/2015/11/30/pres-de-la-moitie-des-francais-confrontes-a-la-cybercriminalite_11685497.html

---

Le ransomware CryptoWall donne la migraine aux forces

de l’ordre

Le #ransomware CryptoWall donne la migraine aux forces de l’ordre

Bâti sur un labyrinthe de serveurs proxy, ce botnet est, pour l'instant, difficile à neutraliser. Pour se protéger, il faut faire des sauvegardes, mais pas n'importe comment.

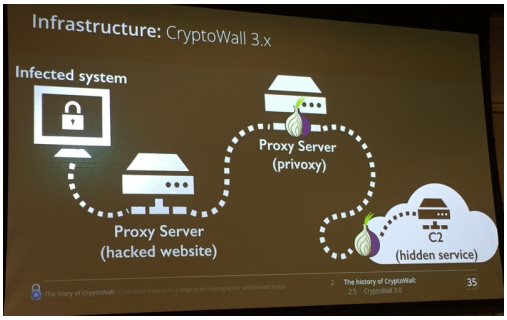
C'est l'un des plus importants « rançongiciels » du moment, et il le sera certainement encore pour un bout de temps. Car les pirates qui se cachent derrière ce néfaste malware ont mis en place un système pour l'instant assez inviolable et diaboliquement efficace. Bienvenue dans l'univers de CryptoWall.

Le chercheur en sécurité Yonathan Klijnsma de la société Fox IT est l'un de ceux qui essayent de pister ses auteurs. Il a profité de la conférence Botconf 2015, qui se déroule actuellement à Paris, pour présenter ses dernières analyses.

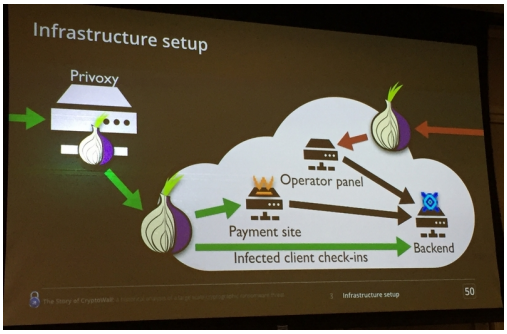
GK — Yonathan Klijnsma

Sur le principe, CryptoWall — qui existe actuellement dans sa version 4.0 — n'a rien d'original. Apparu pour la première fois en novembre 2013, ce code malveillant fonctionne un peu comme son aïeul Cryptolocker. Il infecte les ordinateurs et chiffre les fichiers qui s'y trouvent, ainsi que les noms de ces fichiers. Pour cela, il s'appuie sur les algorithmes AES 256bit et RSA 2048bit. Pour avoir une chance de récupérer ses données, il faut passer à la caisse. Plusieurs moyens de paiement sont acceptés : bitcoin, litecoin, UKash, moneypak, paysafecard, etc.
Ce qui rend ce malware si difficile à terrasser, c'est son infrastructure sous-jacente, composée d'une multitude de serveurs proxy en cascade, des intermédiaires qui servent essentiellement à brouiller les pistes. *« C'est un vrai labyrinthe. On ne sait jamais si la ressource que l'on a détectée est le véritable serveur de commande et contrôle, ou simplement un autre proxy »*, explique Yonathan Klijnsma.

Autre subtilité : le premier niveau de proxy est constitué de serveurs Web piratés. *« Ce sont de vrais sites totalement légitimes. Les propriétaires, évidemment, ne savent pas que leurs serveurs ont été détournés par des pirates. C'est assez malin de leur part, car cela complique le démantèlement du botnet. On ne peut pas simplement tirer le cordon. Il faut contacter chaque administrateur un par un »*, souligne le chercheur en sécurité.



© DR



© DR

Derrière le serveur Web piraté se trouve un autre proxy qui va faire le lien avec le réseau d'anonymisation Tor, dans lequel les pirates ont planqué toute leur infrastructure d'administration : les clés de chiffrement, le paiement, la diffusion de malware, etc. Tous ces « services » sont créés sous la forme de services Tor cachés (Tor Hidden Service). *« Pour les forces de l'ordre, c'est techniquement très difficile d'identifier les serveurs qui se cachent derrière »*, souligne Yonathan Klijnsma.
Pour avoir une chance de démanteler le réseau, il faut donc utiliser des méthodes d'investigation plus classiques, par exemple en infiltrant des forums de discussion. Mais cette méthode prend du temps et n'est pas forcément couronnée de succès.

Pour l'instant, ce cyberracket constitue donc quasiment le crime parfait. Les auteurs sont tellement insouciants qu'ils n'hésitent pas à se moquer ouvertement de leurs victimes, en les félicitant — sur l'un des écrans d'alerte — d'avoir rejoint *« la grande communauté CryptoWall »*.

Un malware d'origine russe ?

Certains éléments techniques semblent indiquer que les auteurs de CryptoWall — ou une partie d'entre eux — se trouvent en Russie. Un mécanisme dans le code évite, en effet, qu'il ne s'installe sur des ordinateurs qui se trouvent en Russie, en Biélorussie, en Ukraine ou au Kazakhstan. Ce type d'exception est typique pour des cybercriminels qui ne souhaitent pas avoir de problèmes avec les forces de l'ordre locales. *« En même temps, on ne peut jamais être sûr à 100 %. Cela pourrait être un faux indice »*, ajoute le chercheur.
En tant qu'utilisateur, pour se prémunir contre un fléau tel que CryptoWall ou consorts, le mieux c'est de faire des sauvegardes régulières de ses fichiers. Mais attention : pas n'importe comment. Il faut éviter les sauvegardes automatiques sur un disque en réseau sur lequel l'ordinateur est connecté en permanence. *« Dans ce cas, le malware ne va pas seulement chiffrer le contenu de l'ordinateur, mais aussi les sauvegardes »*, explique le chercheur. L'idéal, c'est donc de faire des sauvegardes régulières, mais à la main.

Réagissez à cet article
Source : http://www.01net.com/actualites/cryptowall-le-ransomware-qui-donne-la-migraine-aux-forces-de-l-ordre-934345.html
Gilbert KALLENBORN

Les 7 cyber menaces les plus exploitées chaque jour | Le Net Expert Informatique

Les 7 cyber menaces les plus exploitées chaque jour

Les cyber-attaques qui frappent les États ou les grandes entreprises ont beau être celles qui font le plus régulièrement l'actualité, les cybercriminels usent tout autant de techniques d'escroqueries plus basiques mais tout aussi efficaces, ciblant les individus. La plupart des gens n'étant pas assez informés sur les cyber menaces ou ne suivant pas les mesures de cybersécurité classiques, restent la proie des hackers via des failles pourtant très connues, et exposent leur entreprise à des attaques beaucoup plus importantes.

Il vous qui se reconnaîtraient – ou l'un de leurs collègues ou amis – dans l'un des 7 profils décrit ci-dessous, il est encore temps de perfectionner vos compétences en matière de cybersécurité !

J'ai tendance à cliquer très (trop) rapidement
Un clic peut être suffisant pour être infecté par un virus ou pour être redirigé vers un site web malicieux. Les hackers sont très bons pour créer des contenus destinés à leurrer les utilisateurs et les inciter à cliquer. Ce contenu piégé peut être un message important – paraissant venir d'une personne ou d'une société que vous connaissez bien et en laquelle vous avez confiance – technique que l'on appelle le spear phishing. Il peut aussi simplement s'agir d'un spam, d'une publicité proposant une promotion trop belle pour être vraie ou encore d'une fausse enquête vous demandant de donner certaines informations personnelles.
Aussi, avant de cliquer, une bonne précaution à prendre est de survoler le lien hypertexte avec sa souris pour voir apparaître l'URL de destination et ainsi vérifier sa légitimité. Les liens de phishing contient toujours une petite erreur dans l'écriture du lien qui va donc mener vers un site factice ou infecter votre PC avec un malware. Deuxième précaution : portez plus d'attention aux comportements inhabituels. Une entreprise connue ne demande jamais des mots de passe et autres informations sensibles et n'envoie pas d'emails comportant des fautes d'orthographe ou des images de mauvaise qualité, etc. Ne d'autres termes, au moindre doute, ne cliquez pas !

J'ignore toujours les demandes de mises à jour
Les fournisseurs de solutions de sécurité investissent en permanence pour renforcer la sécurité de leurs produits face aux cyber-attaques et publient des patchs et mises à jour pour résoudre chaque problème rencontré. Toutefois, si ces mises à jours ne sont pas installées par les utilisateurs eux-mêmes, ceux-ci restèrent vulnérables aux attaques. Les navigateurs web sont le meilleur exemple d'outils utilisés au quotidien et pouvant facilement être exploités par les hackers. Lorsque l'on sait que seulement 18% des utilisateurs d'Internet Explorer utilisent la dernière version du navigateur, il est évident que les failles à exploiter pour les hackers sont nombreuses.

Je suis friand de Free Wi-Fi
Les espaces de Free Wi-Fi sous unit permis d'être plus connectés ou encore d'éviter les frais de connexion exorbitants lorsque vous sommes à l'étranger. Ces connexions étant ouvertes à tout le monde et ne contrôlé, il est très facile pour les hackers d'intercepter les données qui transitent via le Wi-Fi. Utiliser le Wi-Fi gratuit, c'est bien, mais il est clairement recommandé de ne pas consulter son compte en banque ou encore réaliser des achats en ligne avec sa carte d'identité lorsque l'on est connecté via un réseau Wi-Fi public. Dès lors que vous utilisez régulièrement un réseau de Wi-Fi public pour travailler, vous devez être en amure de vous connecter à un VPN pour renforcer la sécurité de votre connexion.

J'utilise des applications gratuites
Si vous êtes fan des dernières applications, jeux ou gadgets, vous devez savoir que certaines applications gratuites peuvent être infectées par des malwares. Celles-ci permettent aux hackers de collecter vos données à des fins malveillantes, sans que cela ne vous soit jamais notifié. Aussi, il est recommandé de télécharger des apps issues de sources connues.

J'utilise le même mot de passe pour tous mes comptes en ligne
Les hackers savent pertinemment que la plupart des gens réutilisent les mêmes mots de passe pour plusieurs sites. Ils vont ainsi dérober un mot de passe sur un site peu sécurisé et essayer d'utiliser ce même mot de passe sur des sites de vente très connus ou des réseaux sociaux sur lesquels vous pourriez avoir un compte, jusqu'à ce qu'ils trouvent des informations personnelles, financières ou même liées à votre entreprise. Le meilleur moyen de se prémunir de ce type de risques est d'utiliser des mots de passe compliqués et personnalisés pour chaque site web. Il existe de nombreux conseils en ligne pour savoir comment créer des mots de passe fort et facilement mémorisables.

Je ne verrouille jamais ma session
Le moyen le plus facile de dérober des données de valeur ou de pénétrer dans la vie privée d'une personne est d'accéder physiquement à son ordinateur non verrouillé puis de copier ses données ou de se connecter aux sites sur lesquels le mot de passe est enregistré et dont l'accès se fait automatiquement. Cela ne nécessite aucune compétence technique et, même si la personne est intentionnée est repérée par une caméra, cela ne permet absolument pas de la tenir pour responsable, en portant de la faille. Le conseil ici est évident, ne jamais laisser sa session ouverte sur son PC lorsque l'on s'absente.

Je partage énormément (trop) en ligne
Sont-ont la rue de leur fête de votre mère ? Le nom de votre première école ? Ce sont autant de questions de sécurité qui vous permettent de récupérer votre mot de passe oublié, et il serait bien dommage que quelqu'un puisse retrouver ces informations sur votre profil Facebook. Si vous êtes accro aux réseaux sociaux, mais que vous souhaitez vous protéger ainsi que votre entreprise des nombreuses menaces en ligne, vous pourriez commencer par restreindre l'accès à vos publications, à vos amis uniquement. Faites un nouveau tour sur votre profil et reconsidérez à quel point cette ou cette information pourrait être utile si elle tombait entre de mauvaises mains.

De la même manière, informez-vous sur les termes et conditions des sites que vous fréquentez régulièrement dans la mesure ou certains d'entre eux pourraient déclarer collecter vos données et les utiliser pour de la publicité voire même les partager avec des sociétés tierces.

La cybersécurité commence avec vous !
Sans aucune que soit la technologie, ce que l'utilisateur fait reste la plus grande partie de l'équation à résoudre. Les sites web que vous utilisez et l'entreprise pour laquelle vous travaillez peuvent faire le maximum pour assurer la protection de vos données, ils restent toutefois dépendants de vos actes. L'humain est le maillon faible de la sécurité, et pour changer cela nous devons tous prendre nos responsabilités et jouer notre rôle. Les bonnes pratiques de cybersécurité qui commencent à la maison, avec nos données et terminaux personnels, peuvent être facilement étendues à nos vies professionnelles.

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
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.globalsecuritymag.fr/Christophe-Dolly-Cisco-France-Les,20160728,64749.html
Par Christophe Dolly, Cisco France

La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

La société Vtech, spécialisée dans les jeux ludo-éducatifs, a indiqué que la base de données de ses clients inscrits à son espace de téléchargement d'application, dont Explora Park en France, a été piratée.

Une technique d'injection de code SQL a été utilisée
On ne peut pas dire que Vtech ait été gâté pour Noël. Alors que les fêtes de fin d'année approchent à grands pas, la société spécialisée dans la vente de jouets et de jeux vidéo ludo-éducatifs a subi la plus grande cyberattaque de son histoire. Et le moins que l'on puisse dire, c'est que l'addition pourrait être salée avec près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants, tous inscrits à son service de téléchargement et de vente en ligne.

Près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants…
Connu en France sous le nom d'Explora Park, cet espace permet de télécharger jeux, applications et autres e-books pour différentes consoles et tablettes de la marque dont notamment Storio et Mobigo. «
Un accès non autorisé à la base de données clients de notre espace d'apprentissage a eu lieu le 14 novembre. Dès que nous en avons eu connaissance, nous avons lancé une enquête et pris des mesures pour nous défendre contre de futures attaques », a indiqué Vtech dans un communiqué. « Notre base de données clients contient des informations de profils incluant des noms, mails, adresses, mots de passes chiffrés, réponses aux questions secrètes, adresses IP, adresses mails et historique de téléchargement. » En revanche, la société a précisé que la base de données piratée ne contenait aucune donnée et information bancaire.

Une attaque par injection de code SQL. Les conséquences de ce piratage pourraient être lourdes.
Si Vtech n'a pas officiellement indiqué le nombre de clients impacté par ce vol de données, il pourrait s'élever à plus de 4,8 millions, selon nos confrères de Motherboard qui avaient prévenu la société après avoir été contacté à ce sujet par des pirates la semaine dernière.
D'après eux, le piratage a été perpétré par le biais d'une attaque par injection de codes SQL. Une technique classique permettant d'insérer des commandes malveillantes dans les formulaires d'un site web dans le but de collecter de façon détournée des informations sensibles et/ou confidentielles pour ensuite obtenir un accès root aux bases de données serveurs et permettre un accès complet à ces dernières.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-piratage-vtech-5-millions-de-donnees-clients-exposees-63117.html
Par Dominique Filippone

La menace du phishing plane sur les PME : trois étapes

pour éviter le pire

La menace du phishing plane sur les PME : trois étapes pour éviter le pire

Les attaques informatiques ciblant de grands groupes, comme TV5monde, font régulièrement la une des journaux. Selon le rapport 2014 PwC sur la sécurité de l'information, 117 339 attaques se produisent chaque jour au niveau mondial.

Depuis 2009, les incidents détectés ont progressé de 66%.
Cependant, ce type d'attaques, très répandue, cible en grande partie les PME. Selon un rapport de l'ANSSI, 77% des cyber-attaques ciblent des petites entreprises.
Les conséquences peuvent être désastreuses pour ces structures à taille humaine, n'ayant pas forcément la trésorerie suffisante pour assurer leur activité en attendant le remboursement de leur assurance. Le coût d'une attaque peut s'avérer très élevé et la crédibilité de l'entreprise visée peut également en pâtir.
Suite à une attaque informatique du type « fraude au président », la PME française BRM Mobilier a ainsi perdu cet été 1,6 M€ et se trouve aujourd'hui en redressement judiciaire.
En mai dernier, le PMU a effectué un test grandeur nature en envoyant un faux email, proposant de gagner un cadeau, avec une pièce jointe piégée. Résultat : 22% des salariés ont téléchargé la pièce jointe et 6% ont cliqué sur le lien contenu dans l'email et renseigné leurs données personnelles.

Comment éviter que ce type de scénario ne vire à la catastrophe ?
1 – Connaitre le déroulé d'une attaque Le phishing, également appelé hameçonnage, est une technique employée par les hackers pour obtenir des données personnelles, comme des identifiants ou des données bancaires.
Le déroulement est simple : le hacker envoie un email en usurpant l'identité d'un tiers de confiance, comme un partenaire, un organisme bancaire, un réseau social ou encore un site reconnu.
L'email contient une pièce jointe piégée ou un lien vers une fausse interface web, voire les deux.
Si le subterfuge fonctionne, la victime se connecte via le lien, et toutes les informations renseignées via la fausse interface web sont transmises directement au cybercriminel.
Autre possibilité : la pièce jointe est téléchargée et permet ainsi à un malware d'infester le réseau de l'entreprise.

2 – Comprendre la dangerosité d'une attaque pour l'entreprise
Pour les entreprises, le phishing peut s'avérer très coûteux. Il est bien évidemment possible que le hacker récupère les données bancaires pour effectuer des virements frauduleux.
Puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites, les informations recueillies sont parfois réutilisées pour pirater d'autres comptes, comme une messagerie, un site bancaire, ou autre.Mais – puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites – il est aussi possible que le hacker réutilise les informations recueillies pour pirater une boite mail, ou un compte cloud.
Le cybercriminel peut ainsi consulter l'ensemble de la boîte mail, ou des comptes de sauvegarde cloud, et mettre la main sur des documents confidentiels, comme des plans ou des brevets, pouvant nuire à l'entreprise.
Enfin, les hackers profitent du piratage des boîtes mails pour envoyer à tous les contacts un nouvel email de phishing. La crédibilité de l'entreprise peut ainsi être touchée et ses clients pourraient subir à leur tour des pertes.

3 – Se préparer et éduquer avant qu'il ne soit trop tard
Les emails de phishing ont bien souvent une notion « d'urgence », qu'il s'agisse d'une demande pressante de la part d'un organisme ou d'un partenaire, ou d'une participation à un jeu concours « express ». Le but étant bien évidemment de ne pas laisser le temps à la victime de prendre du recul.
Comprendre le procédé d'une attaque est la première étape pour organiser sa défense. Il faut donc éduquer les salariés et leur donner quelques astuces pour ne pas tomber dans le piège :
• faire attention aux fautes d'orthographe : bien que les emails de phishing soient de mieux en mieux conçus, on y retrouve régulièrement des erreurs de syntaxe ou d'orthographe.
• regarder l'adresse mail ou le lien URL : même lorsqu'un email ou une interface web est une parfaite copie de l'original, l'adresse de l'expéditeur ou l'URL n'est pas la bonne puisqu'elle ne provient pas du même nom de domaine.
Des salariés éduqués et conscients du danger sont le meilleur atout contre les cyber-attaques, en particulier contre le phishing.
Mais, cela n'est pas suffisant, notamment sur les terminaux mobiles où nous avons tous tendance à être plus spontanés et donc, à adopter des comportement à risques.
Il est donc important de mettre en place un filtre anti-phishing aussi bien sur les postes fixes que sur les terminaux mobiles. Ces filtres scannent automatiquement les expéditeurs et les contenus afin de bloquer les emails suspects.
Pour les PME, il est donc important d'éduquer l'ensemble du personnel, mais aussi de mettre en place des solutions de filtrage email et de sécurité complètes. Par ailleurs, garder une proximité avec son équipe informatique, ou ses fournisseurs de services, peut également jouer un rôle primordial pour limiter les dommages si un employé est tombé dans le piège.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-menace-du-phishing-plane-sur,20151123,57740.htm

Les hôtels Hilton victimes d’une cyber-attaque

	Les hôtels Hilton victimes d’une cyber-attaque

La chaîne hôtelière américaine Hilton a annoncé mardi avoir fait l'objet d'une attaque informatique destinée à voler les données bancaires de ses clients.

Cette cyber-attaque s'est déroulée en deux temps, précise le groupe dans un communiqué. Les hackers ont installé un logiciel malveillant du 18 novembre au 5 décembre 2014. Une nouvelle attaque a eu lieu du 21 avril au 27 juillet 2015, ajoute Hilton sans dire si les deux attaques ont été commises par les mêmes pirates informatiques.

« En collaboration avec des experts, des représentants de la loi et des émetteurs de cartes bancaires, Hilton Worldwide est parvenu à déterminer que le logiciel malveillant ciblait des informations spécifiques des cartes de paiement » dont les noms, les numéros, les codes de sécurité et les dates d'expiration.

Aucune adresse personnelle, ni de codes Pin n'ont été volés, assure le groupe hôtelier, qui préconise néanmoins par précaution aux personnes ayant séjourné dans ses établissements lors des périodes des attaques de vérifier leurs déclarations bancaires mensuelles. En cas d'irrégularité, Hilton demande aux clients victimes de contacter immédiatement leur banque.

Cette révélation tombe quatre jours seulement après que la chaîne hôtelière Starwood (Sheraton, St.Regis, W, Le Méridien…) a fait état d'une attaque informatique similaire.

Réagissez à cet article

Source : http://information.tv5monde.com/en-continu/les-hotels-hilton-victimes-d-une-cyber-attaque-69830

Comment protéger au mieux les données clients des

cyberattaques ?

Comment protéger au mieux les données clients des cyberattaques ?

Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison… Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité.
C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.
Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :
• Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître couteux à mettre en œuvre mais c'est une méthode de protection efficace.
• Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.
• Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail , d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.
• Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !

Réagissez à cet article
Source : http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html

---

Le nombre d'attaques sur Mac

a considérablement augmenté en 2015

Le nombre d'attaques sur Mac a considérablement augmenté en 2015

Selon l'étude d'un spécialiste de la sécurité, il y a eu plus d'attaques sur Mac en 2015 que durant ces cinq dernières années cumulées.

Jusqu'a présent, il s'agissait d'un archétype assez clair : les PC étaient plus vulnérables aux attaques que les Mac. Les détenteurs des ordinateurs Apple pouvaient alors se targuer de posséder un objet protégé des virus et autres logiciels malveillants.

Mais, selon une étude de Bit9 + CarbonBlack , spécialiste en sécurité informatique, cette idée est désormais mise à mal : « Jusqu'à présent, on a longtemps cru que les Mac faisaient face à beaucoup moins de risques de cyber-attaques que les PC et, jusqu'à très récemment, ce sentiment était plutôt correct. Les utilisateurs de Mac ont été, la plupart du temps, plus à l'abri que les utilisateurs Windows. Mais le vent est en train de tourner », indique la société qui affirme que le nombre de malwares ayant ciblé le système OS X d'Apple a bondit cette année.

En 2015, il y a même eu plus d'attaques sur OS X que durant les cinq dernières années cumulées.

948 malwares en 2015 Entre 2010 et 2014, l'OS d'Apple a été la cible de 180 logiciels malveillants, Bit9 + CarbonBlack indique qu'il y en a eu près de 948 cette année, soit « l'année la plus prolifique de toute l'histoire de l'OS X d'Apple ».

Si les attaques sont plus nombreuses sur le système Apple, c'est aussi parce qu'il y a de plus en plus de personnes qui ont acheté des Macs ces dernières années. Un revers de médaille en quelque sorte : ces engins sont devenus « mainstream » et se sont fortement implantés dans les entreprises.

Par exemple, le marché des OS sur desktop est certes dominé par Windows, mais Apple s'affiche désormais en 3e place parmi les systèmes les plus utilisés, avec 14,46% de parts de marché en 2015, contre 12,46% en 2014.

Si ces logiciels malveillants sont souvent découverts à temps par les entreprises et les chercheurs, il convient malgré tout aux utilisateurs de vérifier s'ils disposent d'un logiciel antivirus à jour, qu'ils soient des afficionados du PC ou du Mac.

Réagissez à cet article

Source : http://www.lesechos.fr/tech-medias/hightech/021447295747-le-nombre-dattaques-sur-mac-a-considerablement-augmente-en-2015-1171406.php

Les autorités s’inquiètent des piratages visant les avions

Les autorités s’inquiètent des piratages visant les avions

L’agence européenne chargée de la sécurité à bord des avions s’inquiète des possibilités de pirater les systèmes informatiques embarqués.

L’autorité a fait appel à un hacker, qui est parvenu à pénétrer plusieurs systèmes de communication.
L’Agence européenne de sécurité aérienne (AESA) insiste sur le manque de sécurité sur certains équipements embarqués dans les avions. Selon son directeur, Patrick Ky, des hackers pourraient facilement prendre le contrôle de plusieurs systèmes, en particulier lorsque les engins se trouvent encore au sol.
Le responsable appuie ses craintes par une expérience menée avec un hacker. Ce dernier serait parvenu à pénétrer en quelques minutes un réseau baptisé Acars (Aircraft Communication Addressing and Reporting System). Ce dernier sert aux compagnies aériennes à s’envoyer des messages automatiques entre les avions et le sol. Ces données communiquent des informations sur l’état de l’avion et ses éventuelles avaries sur ses installations critiques.
Le risque en termes de sécurité est avéré, selon les dires du responsable. Il convient toutefois de préciser que le système en cause n’est pas connecté avec les dispositifs contrôlant les avions. Il n’est donc pas question de prendre la main à distance sur un engin volant.Su
ite à ces révélations, l’AESA s’inquiète de la multiplication des systèmes de communication entre les avions mais également les satellites ou les installations présentes au sol. Cet accroissement pourrait tout aussi ajouter de nouveaux risques de piratages. C’est pourquoi l’organisme milite pour que les autorités américaines et européennes se rapprochent autour d’un projet commun d’analyse de données du trafic aérien.
