HTTPS : la sécurité pour tous, mais à quel prix ?

	**HTTPS : la sécurité pour tous, mais à quel prix ?**

Réseaux : Plusieurs chercheurs ont présenté lors des conférences ACM CoNext à Sidney le résultat de leurs recherches sur le coût et les implications du déploiement de HTTPS. Un gain de sécurité pour l'utilisateur mais un choix qui implique d'envisager les conséquences.

Face aux écoutes de la NSA, les principaux constructeurs et acteurs du numérique semblent au moins tous d'accord sur un point : il faut tout chiffrer. Non pas que cela vous sauvera immédiatement des grandes oreilles de la NSA, qui est peut être déjà arrivé à bout des algorithmes de chiffrement les plus pointus, mais cela aura au moins un mérite : celui d'augmenter le « coût de la surveillance » pour les importuns, compliquer la tache des Five Eyes afin de décourager l'espionnage à grande échelle de nos communication.

Quel est le prix du S dans HTTPS ?

Chacun y va donc de son petit chiffrement mais pour le web, en attendant un http/2 qui se fait désirer, la plupart des principaux sites web ont progressivement basculé au déploiement de HTTPS, une couche de chiffrement sécurisant les connexions web. Mais quel est le coût réel de cette sécurité ? C'est la question que se sont posée plusieurs chercheurs de l'université de Carnegie Mellon, de Telefonica ou de l'école polytechnique de Turin.

Déployer le HTTPS suppose tout d'abord des coûts financiers non négligeables à travers l'achat et le maintien de certificats : l'étude se base sur les tarifs de Symantec mais les offres dans le domaine sont extrêmement variables en fonction du prestataire et des services associés. Mais plus que la question financière, c'est celle des performances qui intéresse les chercheurs.

L'utilisation de HTTPS présente plusieurs désavantages : tout d'abord une augmentation, minime mais sensible, de la latence et du temps nécessaire au chargement d'une page. Si celle-ci varie beaucoup en fonction de nombreux facteurs, les chercheurs constatent néanmoins une augmentation du temps de réponse, parfois de plus de 300ms. Un cout de performance « pas si négligeable que cela », rappellent les auteurs de l'étude, qui rappellent que chaque seconde compte pour les internautes.

Un réseau opaque

Si l'impact sur la batterie est jugé mineur, le déploiement du HTTPS pourrait en revanche se retourner contre les opérateurs en compliquant l'utilisation de solutions reposant sur le Deep Packet Inspection. Certes, c'est plus ou moins le but initial puisque le Deep Packet Inspection est utilisée par des applications de surveillance, mais cette technologie permet également à un opérateur de lutter contre le spam ou les attaques ddos.

Le DPI a mauvaise presse et cela se comprend, mais si le déploiement du HTTPS se poursuit, comme le supposent les auteurs de l'étude, alors les opérateurs vont devoir envisager de nouvelles solutions pour lutter contre ces problèmes. Moins polémique mais peut être plus problématique encore : le HTTPS empêche par exemple les opérateurs et fournisseurs d'accès d'avoir recours à du caching pour épargner leur bande passante.

Pourtant, malgré les problèmes relevés par l'étude, les chercheurs restent confiant et s'attendent à voir HTTPS de plus en plus présent au cours des années à venir : « le S est là pour rester » concluent ils, et ce malgré les désavantages liés au chiffrement sur les connexions web. Reste donc à trouver un moyen de minimiser l'impact, peut être grâce à http/2, dont les premières spécifications sont attendues cette année.

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

Source : http://www.zdnet.fr/actualites/https-la-securite-pour-tous-mais-a-quel-prix-39810969.htm
Par Louis Adam

SONY : Connexion impossible au PSN

SONY : Connexion impossible au PSN

Déjà responsable de la paralysie des serveurs du Xbox Live sur Xbox One et Xbox 360 dernièrement, le groupe de hacker Lizard Squad semble de nouveau être en train de complètement faire disjoncter le PSN, causant des messages de connexion impossible sur PS4, PS3 et PS Vita en ce lundi 8 décembre 2014. En effet, les joueurs se plaignent un peu partout de ne plus pouvoir jouer en ligne sur leur console PlayStation, et de ne plus avoir accès au PSN.

Il y a peu de temps, Lizard Squad avait annoncé une campagne visant à complètement mettre à terre les services online de Microsoft et Sony le jour de Noël 2014, et est déjà responsable de plusieurs épisodes de paralysie du PSN et du Xbox Live ces dernières semaines. Prendre en otage le PSN aujourd'hui même, alors que Sony est en pleine PlayStation Experience est-il un message d'avertissement aux deux constructeurs ? Difficile à dire, d'autant que rien n'est jamais demandé en retour. C'est alors les joueurs qui se retrouvent pénalisés avec des connexions impossible au PSN et Xbox Live. Cependant, dans l'ombre, Anonymous souhaite ne pas en rester là, et menace à son tour Lizard Squad dans une vidéo postée sur internet il y a deux jours, disponible ci-dessous.
Bien entendu, il est toujours assez délicat d'accorder de la légitimité aux nouvelles vidéos d'Anonymous, tant ce groupe est volatile, et peut être représenté par n'importe qui. Vont-ils essayer de voler dans les plumes d'un Lizard Squad qui multiplie les actions pour mettre à terre les services online de la PS4 et de la Xbox One régulièrement ? De son côté, Sony avoue être en ce moment même au travail pour rétablir les connexions à son PSN. Nous vous tiendrons bien entendu au courant de la situation, dans notre colonne d'actualité jeux vidéo, comme toujours.

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

Source : http://playerone.tv/news/v/6234/connexion-impossible-au-psn-lizard-squad-ddos-encore-les-services-playstation.html

Après le piratage, les

employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Une semaine après s'être fait pirater, la société Sony Pictures a indiqué que ses employés avaient reçu un email de menaces d'un groupe de pirates informatiques. Le FBI enquête sur le dossier.

Les attaques viennent de toutes parts. Des employés de Sony Pictures, qui a fait l'objet la semaine dernière d'une attaque informatique massive, ont reçu un email de menaces qui se dit être du groupe de pirates informatique GOP (« Guardians of Peace ») a indiqué un porte-parole de la société américaine.
Il assure par ailleurs être « au courant du problème et travailler avec les forces de l'ordre ». Le FBI, la police fédérale américaine, enquête sur le dossier.

Les familles des employés aussi menacées
L'attaque informatique, qui s'est traduite par le vol de données personnelles d'employés de Sony, dont leurs adresses, dates de naissance et numéro de sécurité sociale, et la mise en ligne illégalement de cinq films du studio, a touché quelque 47 000 personnes, selon des experts informatiques.

L'email adressé aux employés est reproduit par Variety. Il ordonne à son destinataire d'envoyer son nom à une adresse email « si vous ne voulez pas faire l'objet de représailles ». « Si vous ne le faites pas, non seulement vous mais votre famille serez en danger », précise le message.

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

Source : http://lexpansion.lexpress.fr/high-tech/apres-le-piratage-les-employes-de-sony-recoivent-un-email-de-menaces_1629800.html

---

L'attaque informatique de

Sony Pictures a touché 47.000 personnes

L'attaque informatique de Sony Pictures a touché 47.000 personnes

Les pirates informatiques responsables de la cyberattaque géante de Sony Pictures ont dévoilé des informations confidentielles de 47.000 individus dont des personnalités, ont affirmé vendredi des experts en sécurité informatique.

Les noms, adresses, numéros de sécurité sociale et dates de naissance ont ainsi été dérobés, autant d'informations permettant des usurpations d'identité, selon la société Identity Finder.
« Le plus inquiétant est le nombre très élevés de copies des numéros de sécurité sociale retrouvés dans les dossiers que nous avons analysés », a fait remarquer le président de cette société, Todd Feinman.
Il a précisé que ces numéros apparaissaient dans plus de 400 documents différents, « offrant aux pirates la possibilité de causer davantage de dégâts ». Selon lui, quelques 15.000 personnes, actuels ou anciens employés de Sony, ont eu leur numéro de sécurité sociale dérobé.
Sony Pictures a confirmé cette semaine avoir été victime d'un vol « très important de données confidentielles » fin novembre. En plus de ces informations confidentielles, cinq films, y compris des films pas encore sortis, avaient été piratés.

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

Source : http://www.jeanmarcmorandini.com/article-329895-l-attaque-informatique-de-sony-pictures-a-touche-47000-personnes.html

---

Sécurité des données : Quid des risques liés aux nouveaux usages ?

Sécurité des données : Quid des risques liés aux nouveaux usages ?

Une étude Hiscox/IFOP révèle que si 3/4 des actifs interrogés se considèrent bien sensibilisés à la protection des données professionnelles, une majorité d'entre eux ont toujours des pratiques risquées… Pourquoi ?

C'est un fait, les appareils mobiles sont complètement intégrés au sein des entreprises et les frontières entre le professionnel et le privé s'en trouvent fortement diminuées. Qu'en est-il de la sécurité des données des entreprises ? Hiscox s'est interrogé sur le sujet avec l'institut IFOP et les résultats sont pour le moins surprenants !

La sécurité des entreprises est exposée

Les salariés équipés d'au moins un appareil mobile professionnel sont les plus concernés par ces pratiques risquées puisqu'ils sont 77% à déclarer transporter des fichiers professionnels sur une clé USB ou un disque dur externe (contre 63% pour l'ensemble) et la moitié partage des fichiers en ligne via un service de cloud (contre 39% pour l'ensemble). 54% estiment que le partage de fichiers via le cloud n'a pas d'incidence sur la sécurité.
Si les salariés des petites structures sont les mieux équipés en appareils mobiles, ce sont ceux qui utilisent le plus leur matériel professionnel à titre personnel. 82% des salariés de ces entreprises se connectent à Internet au moins une fois par semaine pour des raisons personnelles à partir de leur appareil professionnel.

Des techniques de sécurisation non adaptées

Mais ce n'est pas tout ! Pour assurer leur protection, 9 entreprises sur 10 s'appuient sur un mot de passe. Et là, tout commence, 18% des actifs doivent changer leur mot de passe tous les mois alors que 34% déclarent devoir le changer moins de 2 fois par an. Quant à l'élaboration du mot de passe, 70% des entreprises imposent au moins une règle à leurs salariés pour le choix du mot de passe, on arrive à 51% dans les structures de moins de 10 salariés.
Parmi les autres techniques, 35% des actifs interrogés déclarent disposer d'outils de cryptage des données mais 22% ne savent pas s'ils peuvent bénéficier de cette technique dans leur entreprise.

Enfin, 63% laissent leur ordinateur allumé lorsqu'ils quittent le bureau en fin de journée ou ne le verrouillent pas en quittant leur poste.

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

Source : http://www.itpro.fr/n/securite-donnees-quid-risques-lies-nouveaux-usages-20899/

74% des réseaux domestiques français sont fortement exposés à la cybercriminalité

74% des réseaux domestiques français sont fortement exposés à la cybercriminalité

Près de trois ménages français sur quatre connectés à internet sont susceptibles d'être victimes d'une cyberattaque via leur routeur sans fil, estime Avast Software, qui vient de publier une étude sur ce domaine. La vulnérabilité des routeurs et la faiblesse des mots de passe permettent aux pirates informatiques d'accéder facilement aux réseaux domestiques.

« Les routeurs non-sécurisés sont des points d'entrée très faciles d'accès pour les hackeurs, qui sont dès lors capables de pirater des millions de réseaux domestiques en France, déclare Vince Steckler, Directeur Général d'Avast. Notre enquête révèle que la vaste majorité des routeurs domestiques en France ne sont pas sécurisés. Et si un routeur n'est pas correctement sécurisé, un cybercriminel pourra facilement accéder aux informations personnelles d'un particulier, comme par exemple à ses données financières, ses identifiants et mots de passe, ses photos et son historique de navigation. »

D'après l'étude, plus de la moitié des routeurs seraient mal sécurisés par défaut ou ne seraient équipés d'aucune protection, avec des combinaisons login/mot de passe beaucoup trop évidentes telles que admin/admin ou admin/mot de passe, voire admin/. Au terme de cette enquête réalisée auprès de plus de 20 000 ménages en France, Avast met également en avant que 24% des consommateurs utilisent comme mot de passe leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner.

L'un des principaux risques auxquels un réseau Wi-Fi est exposé est le piratage du système de noms de domaine (DNS). Les logiciels malveillants sont utilisés pour exploiter les failles de sécurité d'un routeur insuffisamment protégé et pour rediriger subrepticement l'utilisateur depuis un site connu, comme par exemple un site web bancaire, vers une fausse page identique à l'original. Lorsque l'utilisateur s'y connecte, le pirate peut ainsi capturer ses identifiants et les utiliser pour accéder à son compte sur le véritable site.

« Le manque de sécurisation actuel au niveau des routeurs rappelle fortement la situation des PC dans les années 1990, où les tendances laxistes des utilisateurs en matière de sécurité et l'explosion du nombre de menaces avaient rendu les environnements informatiques largement exploitables. La grande différence, c'est que les utilisateurs stockent aujourd'hui bien plus d'informations personnelles sur leurs appareils qu'ils n'en avaient auparavant. Les consommateurs ont besoin d'outils à la fois simples d'utilisation et capables de prévenir toute cyberattaque ciblant leurs données », explique Vince Steckler.

Toujours selon le sondage, moins de la moitié des français interrogés sont persuadés que leur réseau privé est sécurisé, tandis que 20% d'entre eux déclarent avoir déjà été victimes d'un pirate informatique. Les participants précisent être pleinement conscients de la gravité des conséquences d'une faille de sécurité, et confient que leurs principales craintes concernent le vol de leurs données bancaires ou financières (34%), la perte de leurs informations personnelles (34%), le piratage de leurs photos (17%) et le vol de leur historique de navigation (13%).

Afin de répondre à ces problèmes, Avast a récemment lancé Avast 2015, qui inclut la première solution de sécurisation de réseaux privés (Home Network Security), capable de protéger les utilisateurs face au piratage des réseaux domestiques, tant au niveau du système de noms de domaine que dans le cas de mots de passe trop simples. Avast 2015 est disponible gratuitement et en version payante via www.avast.com.
L' « internet des objets » est présent dans les ménages français : 96% des ménages français possèdent six appareils ou plus connectés à un réseau Wi-Fi. En marge des ordinateurs de bureau et portables, les utilisateurs possèdent des appareils mobiles (28%), des imprimantes et scanners (18%), des Smart TV (5%), et des lecteurs DVD ou Blu-ray (3%) connectés à leur réseau Wi-Fi.
Les utilisateurs craignent que des « espions » ne se cachent dans leur voisinage, mais certains aiment aussi épier les autres : 60% des répondants seraient très mal à l'aise s'ils apprenaient qu'un voisin ou une tierce personne se connecte en cachette à leur réseau Wi-Fi privé. 5% indiquent avoir eux-mêmes déjà utilisé le réseau Wi-Fi d'un voisin sans le lui avoir signalé ou lui en avoir demandé la permission…

Malgré leurs inquiétudes, les utilisateurs manquent de clairvoyance en matière de protection : 23% des répondants ignorent s'ils disposent d'une solution de protection sur leur réseau domestique, alors que 12% sont sûrs de ne pas en posséder une seule. 25% des personnes interrogées utilisent toujours le même nom d'utilisateur et le même mot de passe, aussi bien pour leur routeur que sur les sites web protégés par mot de passe. 34% ont conservé le mot de passe par défaut de leur routeur, tandis que 6% des utilisateurs sont incapables de répondre à cette question. Seuls 38% ont pris des mesures supplémentaires pour protéger leur réseau, en marge de leur pare-feu de base.

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

Source : http://www.lavienumerique.com/articles/152544/74-reseaux-domestiques-francais-sont-fortement-exposes-cybercriminalite.html

Cybercriminalité : le jeu en vaut-il la chandelle ?

Crédit Photo : Shutterstock

Cybercriminalité : le jeu en vaut-il la chandelle ?

Faire réaliser une page web factice pour faire du hammeçonnage ne coûte que 150 dollars

Attention, il n'est pas là question de dire qu'être un cybercriminel c'est bien… comme toute activité criminelle elle est punie par la loi avec des amendes et des peines de prison, nous y reviendront. Mais, tout de même, selon une étude Kaspersky, il semblerait que le ratio investissement/gains soit plus qu'intéressant… ce qui explique l'augmentation exponentielle de ce nouveau type de criminalité 2.0 qui ne nécessite plus du tout de courage. Assis tranquillement devant un ordinateur, les criminels n'ont plus rien à voir avec les gangsters des années 30.

Mais avant tout, une petite précision : tous les cybercriminels ne sont pas des hackers… et tous les hackers ne sont pas des cybercriminels. Bon nombre de cybercriminels ne font qu'acheter des logiciels préconçus par des hackers, les « Black Hats »… et il y a des hackers, les « White Hats », qui luttent justement contre ce derniers.

Le vol de données : peu d'investissement pour beaucoup de gain
Les cybercriminels qui ne veulent pas investir beaucoup dans un logiciel malveillant peuvent tout simplement faire du phising (hammeçonnage) de données. Pour 150 dollars, selon Kaspersky Lab, il est possible de se faire créer une page web similaire à celle visée (réseau social, site institutionnel, société…), de l'héberger et d'envoyer des spams (du style « Insérez vos données pour qu'on vous rembourse 450 euros de trop payé sur vos factures » et autres…)

Ce type de campagne de phising est souvent facilement décelable puisque de grossières fautes de grammaire et d'orthographe se glissent dans le texte. Mais malgré tout ça peut rapporter gros : en revendant les données ainsi captées (ne serait-ce que nom, prénom et adresse), le pirate peut toucher 100 dollars par personne touchée… avec 100 personnes touchées, les gains montent en flèche : 10 000 dollars.

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

Source : http://www.economiematin.fr/news-cout-cybrecriminalite-enjeu-gain-piratage-revente-donnees

---

Quand les objets connectés contrôlent nos vies…

Quand les objets connectés contrôlent nos vies…

La sécurité est un enjeu majeur pour les objets connectés. Que ce soit dans le Quantified Self où les données relatives à la santé sont sensibles ou dans la domotique où les pirates peuvent prendre contrôle de la maison, les failles sont multiples.

Nous vous avions déjà parlé du hack du thermostat Nest lors de la Blackhat Conference, voici maintenant 5 autres cas avérés de piratage d'objets connectés. L'objectif n'est pas de vous faire peur, mais de simplement montrer que de nouveaux défis émergent pour toutes les sociétés qui s'y lancent.

Le compteur électrique qui coupe le courant
Une étude réalisée par deux experts en sécurité a montré de sérieuses lacunes dans les derniers compteurs d'électricités intelligents mis sur le marché pour répondre aux nouvelles normes du gouvernement espagnol. Les deux spécialistes ont ainsi démontré qu'il était possible de couper le courant chez les propriétaires (potentiellement pour créer un gros black out) ou trafiquer les compteurs pour fausser les factures. Grâce à un système d'infection en cascades, il serait même possible de remonter jusqu'aux centrales électriques. Sans donner le nom du fournisseur de compteurs chez qui la faille a été découverte, on sait cependant qu'il s'agirait d'un des gros acteurs du marché en Espagne que sont Endesa, Iberdrola ou E.ON.
L'Union Européenne a lancé un programme pour inciter les habitants à développer l'usage du compteur d'électricité intelligent, dans l'objectif d'économiser 3% d'énergie supplémentaires d'ici à 2020. A cette date, ce sont deux tiers des européens qui devraient en avoir installé un (sous condition qu'ils ne représentent pas de faille aussi importante…).

L'ampoule connectée qui découvre les mots de passe Wi-Fi
La société Context a exposé une faille de sécurité dans une ampoule connectée : la Lifx Wi-Fi. En parvenant à accéder à l'ampoule, elle a réussi à récupérer et décrypter les informations de configuration du réseau. L'équipe qui avait déjà trouvé des failles dans des imprimantes ou des moniteurs pour bébés a accédé au firmware de l'ampoule en étudiant le microcontrôleur afin de comprendre le mécanisme de cryptage de l'ampoule.
Le responsable recherche chez Context a déclaré « Pirater l'ampoule n'est pas simple, mais ne nécessite pas non plus d'avoir des connaissances trop complexes en matière de hack ». Il précise que ces vulnérabilités peuvent facilement être comblées en travaillant avec les développeurs Lifx. Il a déjà vu des cas plus complexes…

Le moniteur vidéo qui insulte bébé
Un couple américain habitant de l'Ohio a entendu une voix inconnue dans la chambre de leur bébé en août 2013. Il s'agissait d'un hacker qui avait réussi à prendre le contrôle de la caméra pour surveiller le bébé. Selon ABC News, la voix proférait des insultes au bébé.
Le père du bébé avait pourtant pris des précautions, notamment en donnant des mots de passe à son routeur et la caméra et en utilisant un pare-feu. La caméra était une Foscam. La société a rapidement sorti une mise à jour permettant d'éviter de nouveaux désagréments. Malheureusement, tous les utilisateurs n'ont pas mis à jour leur caméra de surveillance de bébé, à l'instar de la famille Schreck chez qui l'incident s'est reproduit en avril 2014. Les réactions en vidéo :

La box TV qui menace les grands-mères
A croire que cela ne se passe qu'aux Etats-Unis, voici l'histoire d'une grand-mère de la ville d'Indianapolis qui a eu la mauvaise surprise de voir des messages vulgaires apparaître sur sa télévision après que sa box TV AT&T ait été piratée. Alana Meeks a rapidement changé de box en n'espérant plus jamais revoir ces messages menaçants, rien n'y a fait. La police est intervenue et a pris notes des injures proférées à son encontre sur la télévision.
AT&T a immédiatement déclaré rechercher les causes de ce piratage, mais aucune nouvelle information n'a été officialisée depuis. On ne sait finalement pas si Mme Meeks a rallumé une télévision depuis.

Le frigo connecté spammeur
Le premier cas de frigo qui envoi du spam a été découvert en Californie au début de l'année. Il faisait partie d'un parc de plus de 100 000 appareils dont les pirates se servaient pour leur spam, avec des ordinateurs, des smart TV et des médias center. Plus de 750 000 emails ont été envoyés depuis ces appareils, dont 75% par les ordinateurs et le reste par des objets pour la maison reliés à internet.
Bref, autant d'exemple pour montrer que les objets connectés sont aujourd'hui vulnérables à ce genre d'attaques. Evidemment, avec le nombre de ces appareils qui va en s'accroissant, il faudra que les fournisseurs de technologie redoublent de vigilance pour assurer la sécurité de leurs clients. On se rappelle que HP a publié il y a quelques mois une étude qui montrait des résultats effarant sur les objets connectés : ce ne seraient pas moins de 250 vulnérabilités qui auraient été découvertes dans les 10 objets connectés les plus populaires du moment.

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

Source : http://www.stuffi.fr/objets-connectes-exemples-piratages-insolites/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Stuffi+(Stuffi+-+L%27actualit%C3%A9+des+objets+connect%C3%A9s

---

Pickpocket numérique, une nouvelle activité saisonnière

« Pickpocket » numérique, une nouvelle activité saisonnière

La cybercriminalité est un marché… comme un autre. Avec ses foires, ses codes et même ses monnaies.

« Pickpockets » numériques

Appelons les « pickpockets » numériques. Le soi-disant « hameçonnage » numérique, ou phishing. Le premier marché pour ce type de cybercriminalité est l'Amérique du Nord, à savoir États-Unis et Canada. Suivi par le Royaume-Uni. Ce marché, en plus de son organisation, est un marché saisonnier. En novembre, les attaques augmentent ; l'activité diminue à partir de décembre, au moment de Noël. Il y a une explication très simple à ce phénomène étrange : une fois les données volées… les criminels doivent aller faire du shopping ! Selon Daniel Cohen, un des responsables de cette question chez RSA (la division sécurité d'EMC), les attaques augmentent de nouveau en avril, saison du paiement des taxes aux États-Unis et, bien évidemment, en août, pour les vacances.

La complexité de ce marché ne fait que s'accroître. Ainsi, les pirates, les cybercriminels qui volent des données, ne savent la plupart du temps pas quoi faire desdites données, et les vendent à des experts qui savent comment les utiliser et les transformer en argent réel. « Il faut savoir comment faire des emplettes dans le monde numérique sans laisser de traces », explique Daniel Cohen. En effet, ce marché est si organisé qu'il existe des 'places de marché' undeground où on peut trouver des données de cartes de crédit. Avec des garanties. Si la carte de crédit a expiré ou a été annulée par l'utilisateur, la place de marché va rembourser l'acheteur ou remplacer la carte inutilisable.

Ces sites ont même des centres d'appels pour aider les escrocs utilisant de cartes frauduleuses à appeler la banque du possesseur légal de la carte, afin de changer d'adresse par exemple. Imaginez que vous achetiez une carte dans ce monde souterrain et que vous vouliez modifier l'adresse qui y est associée. Évidemment, la banque se montrerait suspicieuse si la carte était émise au Texas par exemple, et que votre accent semblait plutôt correspondre à la Caroline du Nord. Ou à l'Angleterre. Un des services offerts par les magasins du crime online est précisément de mettre à disposition des hommes et femmes avec des accents différents afin d'appeler – et de tromper – les banques. Et ceci n'est qu'un exemple des services fournis…

En savoir plus sur http://www.silicon.fr/plongee-monde-cybercriminels-103081.html

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

Source : http://www.silicon.fr/plongee-monde-cybercriminels-103081.html#dV0OWrskHOYXcst5.99

Les experts de Symantec présentent leurs prédictions de sécurité pour 2015 – Global Security Mag Online

Des experts présentent leurs prédictions de sécurité pour 2015

Compte tenu du nombre d'incidents survenus cette année, depuis les campagnes de cyber-espionnage et de cyber-sabotage jusqu'aux vulnérabilités identifiées dans les fondements mêmes du Web, il est difficile de hiérarchiser les événements marquants de l'année 2014. On peut cependant s'interroger sur la signification de certains d'entre eux et sur ce qu'ils laissent présager pour l'année à venir.

L'équipe Symantec Security Response a récemment listé les 4 événements marquants de l'année 2014 en matière de sécurité. Laurent Heslault, directeur des stratégies de sécurité chez Symantec, s'est penché sur ce que 2015 nous réserve et présente aujourd'hui ses conclusions.

Les moyens de paiements électroniques en ligne de mire
Il est peu probable que des attaques à grande échelle similaires à celles qui ont ciblé les équipements de points de vente aux États-Unis se produisent en Europe. En effet, notre système de carte à puce associé à un code confidentiel ne facilite pas la récupération des données de carte bancaire. Cela dit, ces cartes à puce et à code confidentiel peuvent être subtilisées et utilisées pour effectuer des achats sur Internet. L'adoption grandissante des cartes de paiements sans contact, accompagnée du paiement sans contact via les mobiles, augmentera le risque d'attaques ponctuelles.

Les attaques de cyber-espionnage et de cyber-sabotage ne devraient pas faiblir en 2015
En 2015, les campagnes de cyber-espionnage et de cyber-sabotage financées par des États, telles que les opérations DragonFly et Turla observées en 2014, ou encore le spyware très récemment analysé et rendu public Regin, constitueront toujours des menaces pour la sécurité des infrastructures nationales et stratégiques dans le monde entier. Face à de telles campagnes visant à soutirer des renseignements et/ou à saboter des opérations, les entreprises et administrations devront revoir leur politique de cyber-sécurité et donner la priorité à la sécurité, qui deviendra un investissement stratégique plutôt que tactique.

Les secteurs publics et privés devront davantage collaborer pour lutter contre la cyber-criminalité
Fortes des différents démantèlements de groupes de cyber-criminels tels que les opérations Gameover Zeus, Cryptolocker ou encore Blackshades menées en 2014 , les autorités internationales adoptent une approche plus active et plus agressive vis-à-vis de la cyber-criminalité en renforçant leur collaboration avec l'industrie de la sécurité en ligne. Cette collaboration entre le secteur privé et les forces de police se poursuivra en 2015 afin d'avoir un impact durable et de stopper les cyber-criminels dans leur élan.

De nouvelles réglementations pour les entreprises européennes
À l'heure où l'Europe souhaite appliquer sa nouvelle législation sur la protection des données, la confidentialité et l'utilisation des informations demeureront au centre des préoccupations en 2015. Contraintes de garantir le respect des nouvelles réglementations, mais aussi de suivre le rythme de l'économie mondiale en exploitant leurs énormes volumes de données pour créer de nouveaux services et de trouver d'autres sources de revenu, les entreprises européennes vont devoir relever un certain nombre de défis en 2015.

En 2015, les plates-formes Open Source seront le maillon faible
L'année 2015 apportera son lot de vulnérabilités dans les bases de données Open Source et les plates-formes de services Web, que les pirates exploiteront en toute impunité. À l'instar de Heartbleed et Shellshock, ces vulnérabilités constituent une cible potentiellement juteuse pour les pirates, le plus gros risque continuant d'être lié aux failles connues ; entreprises et particuliers n'appliquent pas toujours les patchs correctifs appropriés.

L'Internet des objets restera l'Internet des vulnérabilités, mais les attaques seront limitées et ponctuelles
L'« Internet des objets » étant essentiellement lié à la génération de données, les cyber-criminels redoubleront d'imagination pour exploiter les failles logicielles des appareils connectés. Seront notamment concernés les technologies portatives, les équipements domestiques connectés, comme les téléviseurs connectés et les routeurs, et les applications automobiles connectées. Cela dit, nous ne devrions pas observer d'attaques à grande échelle sur l'Internet des objets, seulement des attaques ponctuelles.

Les organisations reconnaîtront que le système identifiant/mot de passe classique a ses limites
À une époque où les organisations cherchent des solutions pour prévenir les intrusions et protéger leurs utilisateurs, elles seront heureuses d'apprendre que des alternatives à l'ancien système se profilent à l'horizon. Notamment, l'authentification à deux facteurs, qui n'exige pas seulement une information que seul le véritable propriétaire connaît (mot de passe, etc.), mais aussi une information que lui seul est censé détenir (numéro de téléphone portable, etc.). Toutefois, alors que chaque service commence à prendre ce genre de mesures, le consommateur va devoir de plus en plus composer avec des applications, numéros de téléphone et questions de sécurité multiples (et ce sur différentes plates-formes), risquant ainsi de lui compliquer la tâche.

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

Source : http://www.globalsecuritymag.fr/Les-experts-de-Symantec-presentent,20141201,49146.html