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

Comment combattre la cyber-violence à l’école ?

Comment combattre la cyber-violence à l’école ?

La cyber-violence en milieu scolaire se développe, au collège comme au lycée. Selon une enquête du ministère de l'éducation nationale, un collégien sur cinq a déjà été la cible d'insultes, d'humiliations et de brimades par SMS ou sur les réseaux sociaux.

Catherine Blaya, professeure en sciences de l'éducation et présidente de l'Observatoire international de la violence à l'école, explique l'existence de ce phénomène et la manière de lutter contre.

Qu'est-ce que la cyber-violence ?
Catherine Blaya : La cyber-violence est une forme de harcèlement réalisé, non plus uniquement dans la cour d'école ou dans la rue, mais par le biais des nouvelles technologies et des réseaux sociaux. Il peut prendre des formes multiples : du détournement de photo à la vidéo humiliante, en passant par des brimades, des moqueries, des intimidations par SMS. La spécificité de ce harcèlement est son caractère public, amplifié par le Web, qui agit ici comme une caisse de résonance.

Avez-vous des exemples concrets de ce type de harcèlement ?
Les victimes que j'ai rencontrées ont fait état de situations diverses. Des filles prises à partie sur leur apparence physique. D'autres qui sont ostracisées par des camarades qui jalousent leur succès ou désirent briser leur popularité. Les revanches à la suite de ruptures sont nombreuses aussi, comme les humiliations pour assurer la position dominante de l'agresseur.

Les filles sont-elles plus souvent visées que les garçons ?
Elles ont 1,3 fois plus de risque d'être victimes que les garçons, car elles ont une plus grande propension à mettre en scène leur corps, en postant des photos d'elles. Cela attire les commentaires malveillants et la raillerie. Soumettre son estime de soi au regard d'autrui, c'est s'exposer au harcèlement.

Le machisme n'est-il pas la cause première ?
Bien sûr ! Un machisme auquel elles participent aussi. En critiquant leurs congénères et en utilisant le même type d'arguments que les garçons. C'est le phénomène du « slut shaming ». Elles se font, elles-mêmes, l'instrument de la domination masculine.

Pourquoi les auteurs de ces violences privilégient-ils le Web ?
Les auteurs ont besoin d'un auditoire, de spectateurs pour leur violence. Ils veulent se venger ou acquérir un statut social au sein d'un groupe. Ils cherchent donc des témoins pour faire du « buzz » et gagner des « like », afin d'asseoir leur popularité. C'est pourquoi il faut pousser les jeunes témoins à intervenir. La cyber-violence ne doit pas être banalisée. Sur les réseaux sociaux, le problème est démultiplié par un effet de viralité. Le danger supplémentaire d'Internet est que l'agresseur qui lance une rumeur sur la Toile ne peut plus la maîtriser après coup, même s'il se rétracte. Le mal est fait pour durer.

Comment réagir face aux agresseurs ?
Il ne faut pas oublier que les agresseurs sont aussi des victimes dans la plupart des cas. C'est pourquoi il est important d'expliquer aux victimes que répondre à la violence par la violence, c'est prendre le risque de devenir soi-même agresseur. Ces derniers sont souvent des jeunes en quête de popularité qui n'ont pas confiance en eux, ou sont dans une détresse psychologique. J'ai récemment eu le cas d'un jeune homme qui après une rupture difficile s'est mis à harceler son ex-compagne.

Au quotidien, comment empêcher ces violences et harcèlement ?
Il faut beaucoup informer sur le rôle primordial des témoins dans la dénonciation de ces violences. L'enquête du ministère de l'éducation nationale indique qu'un collégien sur cinq est concerné par la cyber-violence. Mais selon mes propres études, c'est plutôt 42 % des jeunes qui sont atteints au moins une fois dans l'année. Et près de la moitié d'entre eux sont à la fois victimes en ligne et dans la cour d'école. La majorité de la population collégienne est concernée par le phénomène, en tant qu'auteur, témoin ou victime.

Lire la synthèse : Un collégien sur cinq a été victime de « cyber-violence »
http://campus.lemonde.fr/campus/article/2014/11/27/un-collegien-sur-cinq-a-ete-victime-de-cyber-violence_4530528_4401467.html

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

Source et la suite sur :
http://campus.lemonde.fr/campus/article/2014/12/02/comment-combattre-la-cyber-violence-a-l-ecole_4532343_4401467.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.

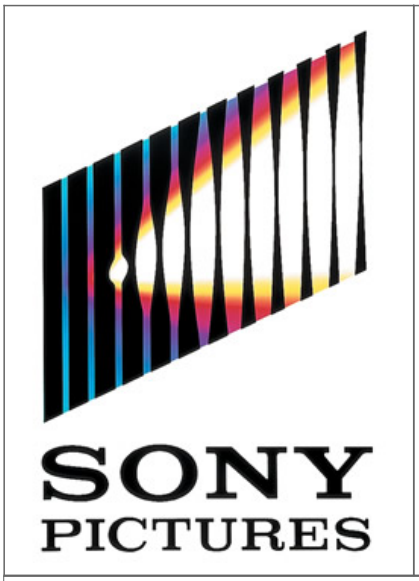
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

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

---

Piratage de Sony Pictures : le FBI met en garde contre un

malware « destructeur »



Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »

Le piratage massif de Sony Pictures Entertainment la semaine dernière a motivé le FBI à tirer la sonnette d'alarme. Le bureau fédéral, qui enquête sur l'affaire, met en garde les entreprises concernant un logiciel malveillant « destructeur » utilisé par les pirates.

De toute évidence, le FBI ne prend pas le piratage de Sony Pictures à la légère. Le bureau fédéral d'investigation a communiqué par voie de presse pour mettre en garde les entreprises contre un nouveau malware. Ce dernier est décrit comme étant « destructeur », et serait à l'origine des déboires de Sony, dont plusieurs films encore inédits aux Etats-Unis ont été mis en ligne dans des versions piratées. Il faut cependant préciser que, dans son rapport d'alerte, le FBI ne cite jamais le nom de Sony. Néanmoins, pour des experts en sécurité interrogés par l'agence Reuters, il ne fait aucun doute que les autorités évoquent bien cette affaire.
Selon le FBI, « il s'agit de la première cyber-attaque destructrice menée contre une entreprise sur le sol américain ». Des manœuvres similaires ont été constatées en Asie et au Moyen-Orient, mais jamais aux USA jusqu'à aujourd'hui.

Concrètement, le logiciel malveillant remplace petit à petit les données présentes sur le disque dur, y compris dans les secteurs d'amorçages qui permettent à l'ordinateur de démarrer. Le système se retrouve donc bloqué, à la merci des pirates qui contrôlent le malware.
« Le FBI conseille régulièrement le secteur privé de divers indicateurs de cyber-menaces observés au cours de ses enquêtes » explique le porte-parole du bureau, Joshua Campbell. « Ces données sont fournies afin d'aider les administrateurs systèmes à se protéger des actions permanentes des cyber-criminels. » Les entreprises victimes de ce type d'attaques sont invitées à contacter les autorités au plus vite.

Du côté de Sony, si un porte-parole a récemment déclaré que l'entreprise avait d'ores et déjà restauré « un certain nombre de services importants », de nombreux documents ont été récupérés par les pirates durant l'intrusion, et pas seulement des films du studio. Des contrats de tournage et des papiers d'identité de certains comédiens font partie des fichiers volés. Quant à l'origine de l'attaque, elle reste toujours à confirmer, même si les soupçons sont tournés vers la Corée du Nord, qui n'aurait pas apprécié la sortie du film « L'Interview qui tue », comédie qui prend pour cible le régime politique du pays.

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

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-742501-piratage-sony-fbi-garde-malware-destructeur.html?estat_svc=s%3D223023201608%26crmID%3D639453874_766966538

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 éffarant 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

---

Faire carrière dans la cybercriminalité ?

Faire carrière dans la cybercriminalité ?

The People’s Voice

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

Source : https://www.facebook.com/thepeoplesvoicetv/photos/a.287874141360034.1073741844.219195584894557/386748201472627/?type=1

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

Le pirate Informatique ayant attaqué Sony enfin démasqué ?

Le pirate Informatique ayant attaqué Sony enfin démasqué ?

Ce serait la première fois qu'un studio d'Hollywood – en l'occurence Sony – soit la victime d'une cyberattaque venue de la Corée du Nord, et pourtant. Selon le site d'informations technologiques Re/code, Pyongyang a mené une attaque informatique pour pirater les bureaux de Sony Pictures à Los Angeles.

La vengeance est un plat qui se mange froid, même en Corée du Nord. En juin dernier, les autorités de Pyongyang avaient annoncé qu'une réponse sans merci serait adressée à «l'acte de guerre» que constituait la sortie du film «L'interview qui tue!» d'Evan Goldberg, dans laquelle deux agents de la CIA se font passer pour des journalistes afin d'assassiner le dictateur nord-coréen Kim Jong-un.

Les menaces n'avaient pas été prises au sérieux: le film est une comédie avec Seth Rogen dans le rôle principal, et personne ne se doutait que la Corée du Nord puisse réellement prendre la mouche devant ce qui n'est qu'une parodie potache. C'était oublier le caractère absurde de la dictature nord-coréen. De mystérieux «Gardiens de la paix» ont mené une attaque informatique en début de semaine dernière contre le réseau informatique de Sony Pictures – qui distribue le film. Les employés du studio américano-nippon (deux pays ennemis de la Corée du Nord, Ndlr) ont été renvoyés chez eux, mardi avec la consigne de ne pas se connecter au réseau informatique de la société, selon Next web.

CINQ FILMS PIRATÉS

Cinq films ont été piratés et puis jetés en pâture sur le Web: «Annie», nouvelle version de la comédie musicale, avec Quvenzhané Wallis et Jamie Foxx, «Mr. Turner» de Mike Leigh, «Still Alice», drame avec Julianne Moore and Alec Baldwin, ou encore «Fury» avec Brad Pitt, déjà sorti en salles. Selon «Variety», les films ont été téléchargés illégalement par plus de 1,2 millions d'utilisateurs… Les pirates auraient pu également volés de nombreuses données personnelles de stars liées à Sony comme Angelina Jolie, Cameron Diaz et Jonah Hill. Pas sûr que cet épisode de guerre cyber se retrouve dans le bonus DVD de «L'interview qui tue!».

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

Source : http://www.parismatch.com/Culture/Cinema/Kim-Jong-un-dictateur-susceptible-660458

Sony : plusieurs films piratés avant même leur sortie dans les salles

Sony : plusieurs films piratés avant même leur sortie dans les salles

Victime d'une attaque informatique d'envergure, Sony Pictures a vu ses activités tourner au ralenti la semaine dernière. Dimanche, des hackers publiaient plusieurs copies des grosses productions à venir sur la toile, compromettant le lancement de plusieurs films.

Victime de plusieurs attaques informatiques la semaine passée, l'intranet de Sony Pictures est tombé peu après que la sécurité de l'un des serveurs de la firme ait été compromise. Les hackers, qui ont pénétré dans le système, ont menacé Sony Pictures de diffuser les dernières superproductions de Sony sur la toile si le distributeur ne répondait pas aux exigences des pirates, lesquelles n'ont pas été dévoilées publiquement.
Dimanche, le groupe de pirates menait ses menaces à exécution en diffusant plusieurs copies de films récents ou à venir comme Fury, Annie, Mr. Turner ou encore Still Alice, en version DVD.
En quelques heures, Fury, le dernier film de Brad Pitt, était déjà le second film le plus téléchargé sur Pirate Bay.
La diffusion de ces copies DVD de films pas encore sortis ou tout juste disponibles dans les salles est une grande première sur la toile. Si plusieurs films ont déjà fait les frais d'une diffusion à grande échelle avant leur sortie, comme The Expendables 3 ou X-Men, c'est la première fois que tout le catalogue de films d'un distributeur est diffusé simultanément. Un fiasco qui pourrait bien sûr affecter les résultats de Sony Pictures au cours des prochains mois mais aussi pousser les distributeurs à investir davantage dans la sécurité informatique.
Le distributeur, qui a très peu communiqué sur le piratage de son intranet, a réagi à la diffusion de son catalogue de films sur Pirate Bay en évoquant un "crime". Elle a également indiqué travailler avec les forces de l'ordre pour retrouver les auteurs des attaques.

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

Source : http://geeko.lesoir.be/2014/12/01/sony-plusieurs-films-pirates-avant-meme-leur-sortie-dans-les-salles/