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

---

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

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/

La police judiciaire découvre une escroquerie à la carte bancaire inédite

La police judiciaire découvre une escroquerie à la carte bancaire inédite

L'office anti cyber-criminalité de la police judiciaire a annoncé vendredi avoir démantelé un réseau d'une quinzaine d'escrocs à la carte bancaire utilisant une méthode nouvelle. Ils auraient fait plus d'une centaine de victimes.

Ils pensaient avoir trouvé un système imparable pour s'enrichir à distance. Mais malgré leur inventivité et après avoir fait des centaines de victimes en France, une quinzaine d'escrocs à la carte bancaire ont été interpellés par l'office anti cyber-criminalité de la direction centrale de la police judiciaire (DCPJ).

Des escrocs créatifs… et bricoleurs
Les cyber-escrocs qui comptaient dans leurs rangs des petits commerçants, n'avaient pourtant rien laissé au hasard mais surtout, ils avaient innové.
Leur méthode consistait à fabriquer eux-même des « TPE » (les terminaux de paiements électriques que l'on trouve dans la plupart des magasins) permettant d'enregistrer le code de la victime ainsi que les données associées à sa carte bancaire. Ces informations en main, les escrocs débitaient les cartes depuis l'étranger, échappant à tous les filtres habituels.
Les victimes elles, ne se doutaient de rien. Au terme de la transaction sur le « TPE » frauduleux elles recevaient même le reçu habituel leur garantissant que leur carte avait bien été débité du montant indiqué sur l'appareil.

« Eviter l'effet « boule de neige » »
« Nous avons enquêté pendant un an il fallait agir avant que cette méthode ne fasse « boule de neige » en France » a affirmé Valérie Maldonado, directrice de l'office anti cyber-criminalité de la PJ (**OCLCTIC**).
Reste maintenant à retrouver les victimes. Leur nombre pourrait dépasser la centaine. Quant au préjudice total il reste lui aussi à déterminer mais pourrait atteindre des centaines de milliers d'euros.

Des escroqueries qui se multiplient
La fraude à la carte bancaire n'a cessée de progresser ces dernières années en France, selon un rapport de l'Observatoire national de la délinquance et des réponses pénales (ONDRP). Entre 2010 et 2012, le volume de ces fraudes a augmenté de 44%. En 2012, on estimait le préjudice total à plus de 450 millions d'euros. Dans plus des deux tiers des cas, les victimes ne sont débitées qu'une seule fois pour un montant moyen de 900 euros. On estime que le nombre d'escroqueries à la carte bancaire augmente deux plus vite que le nombre de cartes mises en circulation.

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

Source : http://www.franceinfo.fr/actu/justice/article/la-police-judiciaire-decouvre-une-escroquerie-la-carte-bancaire-inedite-609719

La reconnaissance juridique du vol de données

La reconnaissance juridique du vol de données

Pour assurer la protection des droits fondamentaux des citoyens, aussi bien les droits positifs que sa protection contre les abus, le Conseil d'Etat préconise 50 mesures à prendre d'urgence.

Le vol de données, une notion mal définie. On entend régulièrement parler dans la presse aussi bien de « vols de données personnelles » de clients, commis au détriment d'opérateurs ou de grandes entreprises, que de « vols de données confidentielles » qui s'apparentent plutôt à de l'espionnage industriel. Dans ces dossiers, le terme de « vol » est utilisé par commodité de langage, mais il n'est pas toujours la qualification retenue juridiquement. En effet, pour qu'il y ait vol, selon la définition du Code pénal (article 311-1), il faut constater la « soustraction frauduleuse de la chose d'autrui ». Or dans un vol de données, celles-ci ne sont pas « soustraites », mais recopiées ; elles demeurent à la disposition de leur légitime propriétaire qui ne peut donc pas déposer plainte pour « vol ».

Cette définition du vol par la « soustraction » date du Code Napoléon (1804). Remarquons que le droit romain était peut-être paradoxalement mieux adapté au vol de données, car les Institutes de l'empereur Justinien, publiées en 529, définissaient plus largement le vol (furtum) comme « contractatio rei fraudulosa » : la manipulation frauduleuse d'une chose (livre IV, titre I, 1). Et de préciser « furtum autem fit, non solum cum quis intercipiendi causa rem alienam amovet, sed generaliter cum quis alienam rem invito domino contractat » : il y a vol, non seulement quand on déplace la chose d'autrui pour la dérober, mais de manière générale quand on en dispose sans la volonté du propriétaire (IV, I, 6).

Mais notre Code pénal moderne lie le vol à la disparition matérielle. Ainsi en avait jugé récemment le tribunal de grande instance de Créteil (23 avril 2013), qui rappelait que « en l'absence de toute soustraction matérielle de documents (…), le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques (du légitime propriétaire) qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose ».

Toutefois, la Cour d'appel de Paris a infirmé ce jugement (5 février 2014), et a considéré au contraire que le vol de données était bien caractérisé par le fait de réaliser « des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ». Suite à ces appréciations divergentes de l'applicabilité de l'incrimination de vol, ce dossier se retrouve désormais devant la Cour de cassation, dont la mission est justement de dire comment on doit appliquer le droit.
Il est à noter que la même Cour de cassation avait validé le 9 septembre 2003 une condamnation pour vol, basée sur le fait « d'avoir en sa possession, à son domicile, après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support du logiciel Self Card, sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire ». Elle a de nouveau validé le 4 mars 2008 une condamnation pour vol de données informatiques. Mais dans ces deux dossiers, la Cour n'a pas explicité comment l'incrimination de vol de données devait s'appliquer.

D'autres solutions juridiques
Lorsque l'on est victime d'un vol de données, d'autres solutions juridiques existent pour déposer plainte. Si les données copiées sont des données personnelles (relatives à des personnes identifiées ou identifiables), le recours à l'article 226-18 du code pénal (collecte frauduleuse de données personnelles) est possible.
Si le vol a été effectué via un accès frauduleux au système informatique (cas du hacking, du vol de mot de passe, du phishing…), l'article 323-1 du code pénal trouvera à s'appliquer.
Si c'est une base de données qui a été recopiée, son propriétaire peut réclamer la protection accordée par l'article L341-1 du code de la propriété intellectuelle, mais seulement si la constitution de la base a nécessité un investissement substantiel. La Cour de cassation a ainsi confirmé le 19 juin 2013 un arrêt refusant la protection d'une base de données en raison du caractère non substantiel des investissements réalisés.
Nouveaux éléments. L'arsenal juridique vient récemment de s'enrichir de deux nouveautés. Le 22 octobre 2014, dans une affaire de détournement de fichiers par un salarié, la Cour de cassation a validé la condamnation pour abus de confiance. Or l'article 314-1 du code pénal définit l'abus de confiance comme « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé ». N'étant pas des fonds ou des valeurs, on en déduit que pour la Cour de cassation les données sont des biens. Ce qui nous ramène à l'idée de vol : si les données sont des biens, la notion de vol de données devient plus naturelle.
Mais le législateur vient peut-être de rendre ces discussions inutiles. En effet, la loi antiterroriste du 13 novembre 2014 modifie l'article 323-3 du code pénal. Cet article, créé par la loi Godfrain de 1988, réprimait jusqu'ici l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression. Désormais, sont également interdits les faits « d'extraire, de détenir, de reproduire ou de transmettre » frauduleusement des données. La sanction encourue est de cinq ans de prison et 75.000 euros d'amende, et est portée à sept ans et 100.000 euros s'il s'agit de données personnelles volées dans un système d'information de l'Etat.
La nouvelle rédaction de l'article 323-3 permet donc de réprimer efficacement à l'avenir les vols de données. Elle rend inutile le recours à l'article 311-1 et les débats sur son applicabilité, d'autant plus que la sanction du vol « traditionnel » n'est que de trois ans de prison et 45.000 euros d'amende (article 311-3), soit moins que ce qui est prévu par le nouvel article 323-3 consacré aux données.

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

Source : http://pro.01net.com/editorial/633857/vers-la-reconnaissance-juridique-du-vol-de-donnees/
par Fabrice Mattatia

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un

chantage

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

Les employés de la filiale du groupe japonais Sony Pictures Entertainment basée à Los Angeles ont eu une surprise des plus désagréables ce lundi 24 novembre 2014. En allumant leurs ordinateurs, une image représentant un squelette avec comme titre en rouge « Hacked By #GOP » (Gardians of Peace) apparaissait sur leurs écrans. Par la suite, les pirates passaient leur message : « nous vous avons déjà prévenu, et ceci n'est que le commencement. Nous continuerons jusqu'à ce que nos exigences soient satisfaites .» En cas de refus d'obtempérer, les pirates menacent de dévoiler à la face du monde des documents obtenus.

Depuis l'expiration de ce délai le 24 novembre 2014 à 23h GMT, plusieurs archives ont été publiées sur divers sites. Même si la plupart des liens ne fonctionnent pas, il est toujours possible de récupérer, sur Thammasatpress, un fichier au format zip de 207 Mo qui contient trois fichiers intitulés LIST1, LIST2 et « Readme ». Ce dernier se présente sous le format texte et contient des adresses électroniques. Pour les deux autres, ils semblent regrouper des documents financiers ainsi que des codes sources et des bases de données. Une analyse avec la commande GREP, dont le rôle est de rechercher un mot dans un fichier et d'afficher les lignes dans lesquelles ce mot a été trouvé, permet d'identifier des clés de chiffrement, mais aussi ce qui ressemble à des documents d'identité relatifs à certaines stars hollywoodiennes à l'instar d'Angelina Jolie.

La société n'était pas joignable pour commenter ces informations, mais un communiqué adressé au Hollywood Reporter indique que « Sony Pictures Entertainment a connu une perturbation de son réseau, et nous travaillons d'arrache-pied pour la résoudre ». Une source a confirmé « qu'un seul serveur a été compromis et l'attaque s'est propagée à partir de là ». Les employés ont été invités à rentrer chez eux après l'attaque : « nous allons tous travailler de la maison. Nous ne pouvons même pas aller sur internet » a déclaré un employé sous le couvert de l'anonymat. Ce dernier a confirmé que le département informatique de l'entreprise a demandé aux employés d'éteindre leurs ordinateurs et de désactiver le WiFi de leurs appareils mobiles, mais également qu'un message adressé aux employés a précisé que la résolution de cet incident pourrait prendre jusqu'à trois semaines.

Outre le blocage des ordinateurs de Sony Pictures, ce sont de nombreux comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.

Cependant, le magazine spécialisé The Verge avance avoir reçu un courriel de la part des hackers responsables de cette attaque qui dit « nous voulons l'égalité [sic]. Sony ne le veut pas. C'est une bataille ascendante ». D'ailleurs un tweet cinglant de la part de GOP a été adressé à Michael Lynton, le PDG de Sony Entertainments, sur le compte de Starship Trooper's où lui et le reste du staff ont été traités de « criminels ».

Selon The Verge, les pirates ont affirmé avoir réussi à infiltrer la société en travaillant « avec d'autres employés ayant des intérêts similaires » parce que « Sony ne verrouille pas ses portes, physiquement, ». Pour The Verge, cela peut impliquer que les pirates ont réussi à pénétrer les serveurs de l'entreprise avec l'aide de personnes ayant accès aux serveurs internes de Sony.
Sony Pictures quant à lui a choisi de rester sobre dans sa communication en se contentant de dire que « nous enquêtons sur un incident informatique ».

En août dernier, les pirates ont affirmé être venus à bout de PlayStation Network via une attaque par déni de service qui a inondé le système de données réseau erronées. Toutefois, l'entreprise a tenu à rassurer les utilisateurs en affirmant qu'aucune des données personnelles des 53 millions d'utilisateurs de la plateforme PlayStation Network n'a été compromise suite à l'incident daté du 24 août. D'ailleurs, les ingénieurs ont pu à nouveau rendre l'accès disponible dès le lendemain. En 2011, une brèche dans la sécurité de la même plateforme exposait les identifiants (noms d'utilisateur et mots de passe) des utilisateurs.
Source : bloomberg, the verge

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

Source : http://www.developpez.com/actu/77586/Sony-Pictures-victime-d-une-attaque-informatique-les-pirates-ont-publie-certaines-donnees-sensibles-apres-un-chantage/

Cyberattaque contre le département d’Etat américain

Cyberattaque contre le département d’Etat américain

Après des attaques contre le réseau informatique de la Maison Blanche le mois dernier et celui de la Poste américaine il y a quelques jours, ce serait désormais le département d’Etat américain qui aurait été victime de piratage.

Le département d’Etat américain a dû déconnecter ce week-end son réseau informatique non confidentiel après des soupçons de piratage, ont rapporté les médias américains. Vendredi, le département d’Etat avait invoqué une opération de maintenance de routine sur son principal réseau non confidentiel, affectant le trafic de courriels et l’accès aux sites internet publics.

Mais, selon des informations de presse publiées dimanche soir, un pirate informatique est soupçonné d’avoir franchi certaines barrières de sécurité du système gérant les courriels non classifiés. Selon un haut responsable cité par le Washington Post, une « activité inquiétante » a bien été constatée mais aucun des systèmes confidentiels n’a été touché.

Série de cyberattaques contre les organismes publics

Si elle se confirme, cette attaque informatique contre le département d’Etat serait la dernière d’une série de cyberattaques visant les organismes publics américains. La semaine dernière, la Poste américaine (USPS) avait annoncé que des pirates informatiques avaient volé des informations sur leurs employés et sans doute sur certains clients.

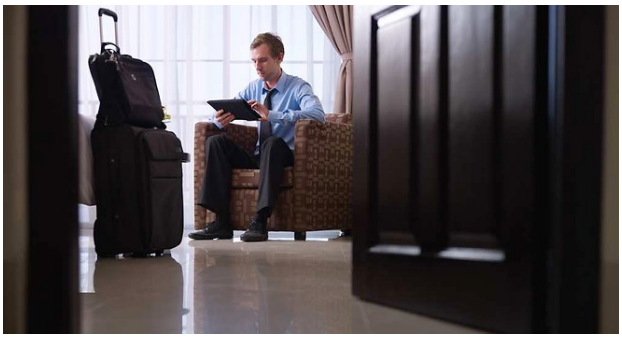
Jusqu’à environ 800.000 personnes rémunérées par la Poste américaine, y compris les sous-traitants, pourraient être concernées par ce piratage, selon un porte-parole de l’entreprise publique. Les pirates se seraient aussi introduits dans le système de paiement des bureaux de poste et en ligne, ce qui impliquerait aussi des clients, selon l’USPS. Le FBI a annoncé l’ouverture d’une enquête.

Le mois dernier, la Maison Blanche avait elle aussi fait état d’une « intrusion » dans son réseau informatique non confidentiel. Selon le Washington Post, des hackers russes sont soupçonnés d’en être à l’origine.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://lci.tf1.fr/monde/amerique/le-departement-d-etat-americain-victime-d-une-cyber-attaque-8519395.html

Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »



Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »

« Dark hotel » : ces hackers qui exploitent les réseaux Wi-fi des hôtels de luxe.
Des hackers ont pris pour cible des directeurs généraux et autres cadres dirigeants d’entreprises lorsqu’ils voyagent à l’étranger. Un phénomène qui durerait depuis quatre ans.
Nom de code « Dark Hotel ». Ce nouvel acteur dans le monde du cyberespionnage sévit depuis au moins quatre ans, révèle la société de sécurité russe Kaspersky Lab. **Ses cibles appartiennent à l’élite économique internationale : directeurs généraux, vice-présidents, directeurs des ventes et marketing de grosses entreprises américaines et asiatiques**. Pour les piéger et leur dérober des données sensibles, ces hackers mettent à profit les réseaux Wi-fi des hôtels de luxe dans lesquels ils voyagent.

Ces hackers sans visage ont un mot d’ordre : ne jamais frapper deux fois la même cible. Leur mode opératoire ? Un faux logiciel, de type Adore Reader ou Google Toolbar, que le visiteur est invité à télécharger après s’être connecté au réseau Wi-fi de son hôtel. Un cheval de Troie permet ensuite au hacker de recueillir des données privées, y compris les mots de passe sur Firefox, Chrome, Internet Explorer ainsi que les identifiants sur Gmail, Yahoo,Facebook et Twitter.

Les victimes se font ainsi voler des données qui relèvent du domaine de la propriété intellectuelle des entreprises qui les emploient. Après l’opération, toute trace est effacée du réseau de l’hôtel, le hacker retournant dans l’ombre. Une « précision chirurgicale », souligne Kaspersky Lab.

Selon l’unité de recherche de la société russe, une empreinte laissée par les hackers suggère que les cybercriminels parlent coréen. Le plus haut volume d’activité a été détecté entre août 2010 et 2013. 90 % des cyberattaques étaient localisées au Japon, Taïwan, en Chine, en Russie et en Corée du Sud. Depuis 2008, elles se comptent par milliers. Kaspersky Lab n’est, pour l’heure, pas parvenu à tracer ces hackers.

A partager sans modération

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lesechos.fr/tech-medias/hightech/0203938482430-dark-hotel-ces-hackers-qui-exploitent-les-reseaux-wi-fi-des-hotels-de-luxe-1064496.php
Aurélie Abadie

JP Morgan piraté : les données de 83 millions de clients exposées

JP Morgan piraté : les données de 83 millions de clients exposées

Cet été, JP Morgan a été victime d'une attaque informatique de grande envergure. La banque américaine admet que les données de 83 millions de clients ont pu être exposées. Toutefois, il ne s'agirait pas d'informations sensibles pour la porte-parole de la société.

76 millions de foyers et 7 millions de PME seraient concernés par ce qui pourrait être l'une des plus grandes fuites de données de l'histoire. Cet été, les systèmes informatiques de la banque JP Morgan ont été compromis par une attaque ayant permis aux pirates d'accéder aux noms, adresses, numéros de téléphone, et adresses e-mail de 83 millions de clients, annonce JP Morgan dans un document transmis à la SEC, le gendarme américain de la bourse.

La banque ajoute qu'il n'y a « pas de preuve » que des données sensibles comme les numéros de comptes, mots de passe, identifiants, dates de naissance ou numéros de sécurité sociale aient été compromises. Les responsables de l'attaque n'auraient pas eu accès à ce type de données sensibles, pense Patricia Wexler, porte-parole de JP Morgan. Il ne serait donc pas nécessaire que les clients changent leurs mots de passe.

Pour le moment, la banque n'aurait pas constaté de fraude relative à cet incident.
Mais l'attaque, très sophistiquée, aurait tout de même permis aux pirates d'accéder « au plus haut niveau des droits administrateurs » selon le New York Times qui s'appuie sur des sources proches du dossier. Puis, les informations exposées restent potentiellement utiles aux cyber criminels : « ils pourraient littéralement utiliser l'identité de ces 83 millions de personnes et entreprises », affirme Tal Klein, de la société de sécurité informatique Adallom, à l'agence Reuters.
La banque avait annoncé en août qu'elle enquêtait avec les autorités sur une attaque informatique. Le FBI soupçonnait des pirates russes en raison de la crise ukrainienne et des sanctions économiques à l'encontre du régime de Moscou. Le New York Times affirmait que JP Morgan n'était pas la seule banque concernée mais qu'en tout, cinq banques auraient été visées le même mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-730905-clients-jp-morgan-pirates.html