Le site de la BBC victime d’une cyber-attaque

Le site de la BBC victime d’une cyber-attaque

Ce jeudi matin, tous les sites de la BBC étaient inaccessibles à cause d'une attaque par déni de service…

Une cyber-attaque de grande ampleur. Le fonctionnement du site Internet de la BBC a été perturbé jeudi matin par une attaque par déni de services, rendant la consultation des informations impossible, selon un article du groupe britannique d'audiovisuel public.

« Une attaque par déni de service »

« Tous les sites Internet de la BBC étaient inaccessibles jeudi matin en raison d'une importante cyber-attaque », a indiqué la chaîne dans un article publié dans la section technologie de son site Internet attaqué qui était consultable par intermittence dans la matinée.
« Des sources au sein de la BBC ont indiqué que les sites étaient inaccessibles à cause d'une attaque par déni de service », ajoute l'article qui précise que l'attaque a porté sur le site et des services associés comme le service iPlayer pour revoir les émissions et l'application iPlayer Radio.

La situation est revenue à la normale

« Le site de la BBC est maintenant de retour et fonctionne normalement. Nous nous excusons pour le désagrément », a indiqué peu après 12h GMT une porte-parole de la chaîne dans un communiqué.
Ce type d'attaques a pour but de rendre un service indisponible en inondant un réseau ou en perturbant les connexions à un serveur.

La BBC déjà victime d'une cyber-attaque

En juillet 2014, une précédente attaque avait paralysé le service iPlayer de la BBC pendant un week-end entier, précise le groupe britannique d'audiovisuel public.
En septembre dernier, c'était le site Internet de l'Agence britannique de lutte contre le crime (NCA) qui avait été perturbé en raison d'une attaque équivalente, dans ce qui s'apparentait à une riposte d'un groupe de pirates après une série d'arrestations.
Selon la police, quelque 30 % des entreprises britanniques ont signalé avoir subi des attaques par déni de service en 2014.

Réagissez à cet article

Source : *Le site de la BBC victime d'une cyber-attaque*

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Selon Valve, l'éditeur du service cloud de jeux vidéo Steam, c'est la combinaison d'une attaque par déni de service visant le Steam Store et d'un problème de cache qui est à l'origine de l'exposition des données personnelles de 34 000 clients.
Valve s'est finalement expliqué plus en détails sur ce qui s'est passé le jour de Noël sur sa plateforme Steam. Rappelons que des utilisateurs du service de distribution de jeux vidéo ont remarqué avoir accès depuis leurs comptes à des données personnelles d'autres utilisateurs, comme leurs adresses mail, leurs historiques d'achats, ou encore leurs numéros (incomplets) de cartes de crédit.

Dans un communiqué diffusé hier, Valve explique que ce bug est le résultat de deux facteurs : une attaque par déni de service qui a touché son magasin en ligne, le Steam Store, et une erreur dans le système de cache qui fut déployé pour la contrer. "Au cours de la deuxième vague de cette attaque, la seconde configuration de cache déployée a mal géré le trafic web en cache pour les utilisateurs authentifiés. Cette erreur de configuration s'est traduite pour certains utilisateurs capables de voir des réponses du Steam Store qui étaient générées pour d'autres usagers."

Valve a indiqué que les données personnelles de 34 000 clients ont ainsi été exposées. L'entreprise dit travailler avec son partenaire gérant la mise en cache afin d'identifier chaque client affecté pour pouvoir le contacter directement. (Eureka Presse)

Réagissez à cet article

Source : *Steam : plus de 30 000 utilisateurs concernés par le*

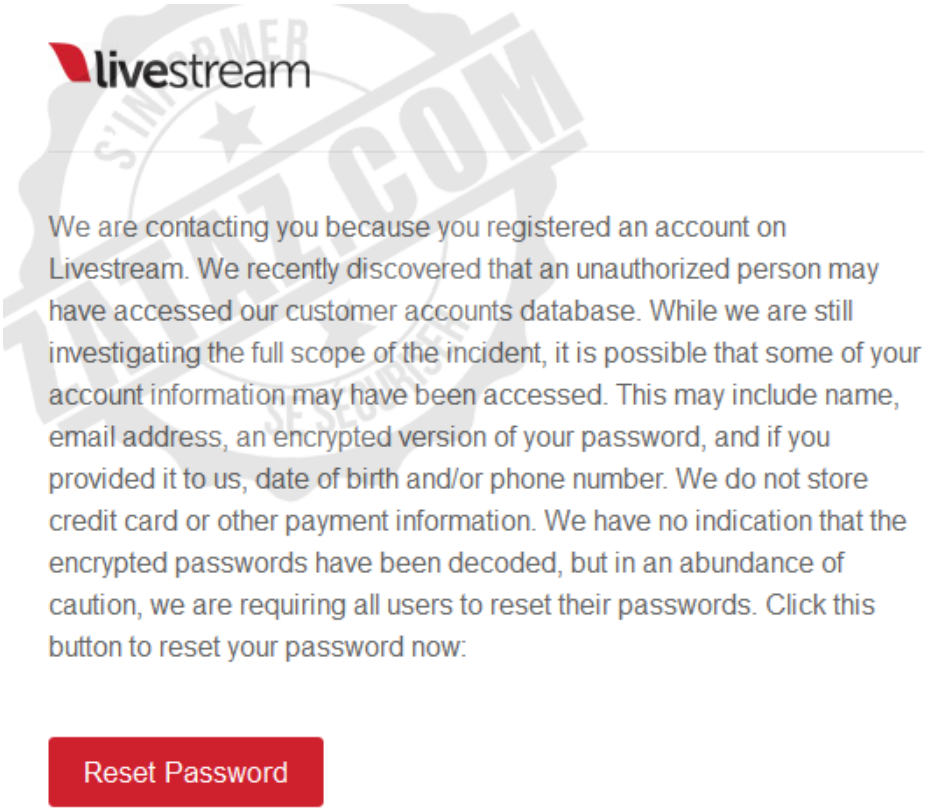
piratage de données

Alerte : livestream.com victime d’un vol de données

	**Alerte : livestream.com victime d’un vol de données**

Le site Internet dédié aux concerts en live sur Internet, livestream.com, visé par un piratage informatique.

C'est via un courrier électronique laconique, envoyé après le réveillon de Noël, que le site Internet dédié aux concerts en live sur Internet, livestream.com, indique avoir été visé par un piratage informatique. « ***Nous vous contactons parce que vous avez enregistré un compte sur Livestream,*** explique la missive. ***Nous avons récemment découvert qu'une personne non autorisée a pu avoir accès à nos comptes clients.***«


livestream

We are contacting you because you registered an account on Livestream. We recently discovered that an unauthorized person may have accessed our customer accounts database. While we are still investigating the full scope of the incident, it is possible that some of your account information may have been accessed. This may include name, email address, an encrypted version of your password, and if you provided it to us, date of birth and/or phone number. We do not store credit card or other payment information. We have no indication that the encrypted passwords have been decoded, but in an abundance of caution, we are requiring all users to reset their passwords. Click this button to reset your password now:

Reset Password

Bilan, une faille qui a donné accès à la base de données et aux informations des utilisateurs. « ***Cela peut inclure le nom, l'adresse électronique, une version chiffrée de votre mot de passe.*** » Bref, toutes les informations que les clients ont pu sauvegarder. Aucunes données de carte de crédit ou autres informations de paiement ont pu être lues par le pirate, la base de données impactées ne concernées par ce secteur numérique de livestream.com. « ***Dans un souci de prudence, nous conseillons aux utilisateurs de réinitialiser leur mot de passe***« .

Réagissez à cet article

Source : *ZATAZ Magazine » Piratage de données pour livestream.com*

URGENT : Phishing Free Mobile, ne vous faites pas avoir !

URGENT : #Phishing Free Mobile, ne vous faites pas avoir !

Réagissez à cet article

Source : *URGENT : Phishing Free Mobile, ne vous faites pas avoir ! – Le Blog du Hacker*

Cyber-attaque contre le

ministère des Habous et des affaires islamiques

Cyber-attaque contre le ministère des Habous et des affaires islamiques

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »
Une fois piraté, le site est devenu inaccessible pour les fonctionnaires ainsi que le grand public.
D'après « Le360 », l'attaque est confirmée, et l'ouverture d'une enquête est indispensable pour déterminer les raisons de ce piratage ainsi que l'identité des hackers à l'origine de cet acte qualifié d'irresponsable.

Réagissez à cet article

Source : *Cyber-attaque contre le ministère des Habous et des affaires islamiques – Article 19*

Les données personnelles de 191 millions d'électeurs en accès libre sur la Toile

Les données personnelles de 191 millions d'électeurs en accès libre sur la Toile

---

Un spécialiste en cybersécurité a découvert l'existence d'une base de données contenant les informations personnelles détaillées de 191 millions d'électeurs nord-américains. La fuite serait due à une erreur de configuration de la base de données.

Des données personnelles concernant près de 60% des citoyens des États-Unis se sont retrouvées en libre accès sur la Toile en raison d'un base de données mal configurée. C'est la découverte faite récemment par Chris Vickery, un expert en cybersécurité. La base de données en question n'était apparemment pas sécurisée et serait même toujours active.
Elle contient le nom complet de chaque personne, son sexe, sa date de naissance, son adresse, numéro de téléphone, numéro d'électeur, l'Etat dans lequel elle vote, l'affiliation politique ainsi qu'un historique de ses choix électoraux depuis 2010. Une véritable mine d'or en somme, et Vickery n'a pas indiqué où il avait déniché cette base de données, ni qui en était le créateur.

Réagissez à cet article

Source : *États-Unis : les données personnelles de 191 millions d’électeurs en accès libre sur la Toile*

Sputnik France visé par une cyberattaque

Sputnik France visé par une cyberattaque

Le 25 décembre, une attaque de type DDoS a fait bloquer l'accès au fil d'actualités Sputnik France. Les spécialistes techniques sont en train de régler le problème d'accès au site.

Les attaques par déni de service (Distributed Denial of Service ou DDoS) sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en exécution et de leur efficacité contre une cible non préparée. Une attaque DDoS vise à envoyer une multitude de requêtes à un serveur afin de provoquer un déni de service, c'est à dire un arrêt total du service attaqué.

Ce n'est pas la première fois que Sputnik est victime d'une telle attaque. Le 7 décembre dernier, le site de Sputnik Turquie a été attaqué par des pirates informatiques. En octobre 2015, les fils d'actualité de l'agence russe Rossiya Segodnya, et notamment ceux de Sputnik, avaient été bloqués.

Réagissez à cet article

Source : *Sputnik France à nouveau visé par une cyberattaque*

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

La chaine d'hôtels Hyatt vient d'annoncer avoir découvert un logiciel malveillant dans son système de paiement. Il est désormais éradiqué, mais l'étendue des dégâts n'est pas connue. Hyatt n'est que le dernier d'une longue liste d'hôtels dont la sécurité a été mise à mal.

Alors que l'histoire de la porte dérobée dans les pare-feu de Juniper n'est pas encore terminée, une nouvelle affaire de sécurité informatique remonte à la surface. La chaine d'hôtels Hyatt vient en effet d'annoncer officiellement qu'elle a « identifié un logiciel malveillant sur les ordinateurs qui gèrent les systèmes de paiements ».

Le groupe ne donne pas d'informations supplémentaires sur les tenants et aboutissants de cette histoire, pas plus que sur le nombre de clients potentiellement touchés ou sur les données dérobées. Il est simplement demandé aux clients de scruter attentivement leurs relevés bancaires afin de vérifier qu'aucune transaction suspecte n'a été effectuée.

Bien évidemment, Hyatt ajoute avoir pris des mesures pour renforcer sa sécurité informatique (notamment avec l'aide d'une société spécialisée dans ce domaine) et indique que, désormais, ses « clients peuvent utiliser en toute confiance des cartes de paiement dans les hôtels Hyatt dans le monde entier ».
Mais il faut également rappeler que cette brèche dans la sécurité d'un hôtel n'est que la dernière d'une longue série pour 2015. En effet, il y a tout juste un mois, c'était la chaine Hilton qui annonçait avoir découvert un logiciel malveillant dans certains terminaux de paiements. Sur son blog, Krebs dresse une triste liste d'hôtels ayant fait face à une importante brèche dans leur sécurité informatique en 2015 : Starwood, Mandarin Oriental, White Lodgging et Trump Collection.

Réagissez à cet article

Source : *Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant*

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

---

Plus de 2 millions de personnes doivent recevoir ces jours-ci une prime de Noël de la part de la Caf et Pôle emploi. Des escrocs profitent de l'occasion pour envoyer de faux mail provenant soi-disant de ces organismes. Objectif : vous soutirer des données personnelles.

La prime de Noël est versée à partir de ce mercredi 16 décembre 2015. La période parfaite pour des cyber-escrocs de tenter de vous soutirer des informations personnelles en se faisant passer pour des administrations ou des grands organismes. Leur objectif : usurper votre identité voire se servir sur vos comptes bancaires.

La police nationale alerte en effet sur les faux mails prétendument envoyés par la Caf ou Pôle emploi, qui sont chargés de verser cette aide à plus de 2 millions de bénéficiaires. Cette technique est appelée phishing, ou hameçonnage. Pour mieux la reconnaître et donc ne pas tomber dans le piège, voici en quoi elle consiste et comment réagir :

Logos qui semblent vrais ⇒ Vous recevez un courrier électronique qui reprend les intitulés, les couleurs et les logos bien connus pour ne pas éveiller vos soupçons.

Liens vers des sites piégés ⇒ Ce mail mail comporte un lien ou une pièce jointe. En cliquant dessus, vous êtes redirigé sur un site piégé qui vous invite à saisir des données personnelles (login, mot de passe, numéro de compte client, coordonnées bancaires…) soi-disant pour confirmation ou une vérification.

Fautes d'orthographe ⇒ Ne cliquez pas si vous avez un doute. Un indice : ces faux messages comportent souvent des fautes d'orthographe. Sachez également qu'aucun opérateur ou organisme ne vous demande de venir vérifier sur leur site des informations confidentielles en vous les faisant retaper en ligne. Vous pouvez si vous le souhaitez signaler l'email douteux **ici** sur la plateforme Pharos.

Réagissez à cet article

Source : *Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews*

L’agence météorologique australienne victime d’une cyber-attaque chinoise

L’agence météorologique australienne victime d’une cyber-attaque chinoise

L’équivalent australien de Météo France aurait été frappé par une cyber-attaque émanant de Chine. La faille serait très importante, impacterait jusqu’au ministère de la Défense australien, et coûterait plusieurs millions de dollars à réparer.

Le Bureau of Meteorology (BOM), l’agence nationale de météorologique australienne, a souffert d’une cyberattaque « massive »,rapporte la Australian Broadcasting Corporation le 2 décembre. D’une ampleur sans précédent en Australie, elle a été attribuée au gouvernement chinois par l’un des représentants gouvernementaux avec lequel la chaîne d’information s’est entretenue.

Le BOM héberge entre autres un centre de calcul à haute performance baptisé Solar, construit par Oracle sur la base d’une architecture Fujitsu. Outre le BOM, il est utilisé par de nombreuses agences gouvernementales australiennes, y compris le département de la Défense. D’après ce même représentant, sécuriser la faille de sécurité qui a permis cette attaque coûtera plusieurs millions de dollars.

Le gouvernement australien s’est refusé à confirmer l’information officiellement. La Chine de son côté nie toute responsabilité et juge les accusations sans fondement.

Réagissez à cet article

Source : http://www.usine-digitale.fr/article/l-agence-meteorologique-australienne-victime-d-une-cyber-attaque-chinoise.N368378