Piratage du compte Twitter et de la page Facebook du Real Madrid

Piratage du compte Twitter et de la page Facebook du Real Madrid

Ce samedi matin, le compte Twitter et la page Facebook du Real Madrid ont été la cible d'un hacker, qui a notamment annoncé l'arrivée de Lionel Messi chez les Merengue. Une cyber-attaque qui survient quelques jours seulement après celle subie par le FC Barcelone.

Les supporters madrilènes ont dû avoir une drôle de surprise ce samedi matin en se rendant sur les réseaux sociaux. Sur Facebook comme sur Twitter, le Real a en effet été victime d'une cyber-attaque. Pendant une bonne heure, le hacker à l'origine de cette acteur a ainsi publié de fausses informations, parmi lesquelles l'arrivée de Lionel Messi sous le maillot merengue et la vente de Karim Benzema…[lire la suite]

Réagissez à cet article

Source : *Victimes d’un piratage, le compte Twitter et la page Facebook du Real Madrid ont annoncé la signature de Lionel Messi*

Les failles utilisées par les hackers ont plus de 10 ans

Les récentes attaques de malwares et de ransomwares survenues en 2017, dont WannaCry et Petya/NotPetya ont été les plus répandues et médiatisées, ont permis aux spécialistes de la cybersécurité d'avoir une vision plus claire des failles utilisées par les hackers.

Fortinet, spécialiste de la cybersécurité, a analysé les attaques dont ont été victimes ses clients, généralement des entreprises. Dans le rapport publié en août 2017, il est mis l'accent sur la vétusté des failles utilisées par les hackers : la très grande majorité des attaques n'aurait pas pu être menée à bien si les systèmes avaient été mis à jour.
Les chiffres sont éloquents : dans 90 % des cas, les victimes ont été attaquées par le biais de failles datant de plus de 3 ans et dans 60 % des cas, ces failles étaient vieilles de 10 ans voire plus. L'attaque WannaCry a utilisé la faille EternalBlue de Windows qui faisait partie des outils de la NSA pour espionner ses cibles. Cette faille avait été rendue publique par les hackers du groupe *The Shadow Brockers*…[lire la suite]

Réagissez à cet article

Source : *Les failles utilisées par les hackers ont plus de 10 ans*

Un nouveau ransomware, Defray, cible l’éducation et la santé

	Un nouveau ransomware, Defray, cible l’éducation et la santé

Les chercheurs Proofpoint ont récemment analysé un nouveau ransomware, nommé Defray. Durant le mois d'août, ils ont observé plusieurs attaques ciblées, visant notamment les secteurs de la santé, de l'éducation, de l'industrie et de l'informatique.

« Defray » a été choisi en rapport avec le nom d'hôte du serveur de commande et de contrôle (C&C) de la première attaque observée : defrayable-listings[.]000webhostapp[.]com Par coïncidence, le terme « defray » signifie fournir de l'argent pour payer une partie d'un coût, bien que ce dont les victimes doivent s'acquitter ne soit pas tout à fait clair.

La distribution de Defray présente plusieurs caractéristiques :

• Defray est diffusé via des documents Word dans des pièces jointes d'emails

• Les pièges sont conçus sur mesure pour attirer toutes les victimes potentielles

• Les destinataires sont des individus ou bien des groupes d'individus, par exemple, group@ ou websupport@

• Les pays les plus touchés sont le Royaume-Uni et les États-Unis

[Global Security Mag Online]

Réagissez à cet article

Source : *Defray, le nouveau ransomware qui cible l'éducation et la santé – Global Security Mag Online*

Mots de passe Wifi des espaces Lounges des principaux aéropors à travers le monde. Les conseils de Denis JACOPINI

Mots de passe Wifi des espaces Lounges des principaux aéropors à travers le monde. Les conseils de Denis JACOPINI

Une base de donnée de nombreux codes d'accès Wifi des principaux aéroports à travers le monde accessible librement sur une carte Google Maps. Toutefois, même si le service paraît très utile, il peut aussi devenir un piège à voyageurs. Denis JACOPINI nous en dit plus

Même si pour beaucoup les vacances sont terminées, pour d'autres le réflexe à peine descendu d'un vol lors d'une escale ou arrivé à destination est de vérifier ses mails pour certains, ses j'aime, ses stats ou flash pour d'autres.
Autant anticiper en consultant cette carte et récupérer les identifiants et mots de passe des aéroports qui seront visités (avant de partir).
[Accéder à la carte avec la liste des aéroports]

Attention toutefois à prendre vos précautions lorsque vous utiliserez ces réseaux Wifi inconnus, publics ou libres ! Des pirates peuvent traîner par là et récupérer vos codes, vos informations ou pire, infecter leurs voisins numériques. Protégez bien votre ordinateur avec un système de sécurité à jour et utilisez un VPN pour accéder à des informations sensibles.

Maintenant, si c'est trop tard pour les utiliser lors des vacances de cette année pour certains, conservez précieusement ces informations pour l'année prochaine

Denis JACOPINI

Réagissez à cet article

Source : *Wireless Passwords From Airports And Lounges Around The World*

Vous êtes le maillon faible (en cybersécurité)

	Vous êtes le maillon faible (en cybersécurité)

Encore une fois, une étude pointe l'importance du facteur humain dans les problèmes de cybersécurité, cette fois réalisée par Kaspersky.

De HAL à Skynet, les ordinateurs n'ont-ils pas raison de vouloir éliminer les humains ? Les études pointant le facteur humain comme maillon faible de la cybersécurité se multiplient en effet. Celle qui vient d'être publiée par l'éditeur Kaspersky s'ajoute à la longue liste en pointant les principales causes d'incidents et les mauvaises pratiques.

Parmi les plus mauvaises pratiques, la dissimulation des incidents de cybersécurité est adoptée dans 40 % des entreprises. Or la dissimulation empêche la correction. Et 46 % des incidents sont eux-mêmes issus d'actions de collaborateurs internes. En présence d'un malware, un incident sera déclenché dans 53 % des cas par une action inappropriée d'un collaborateur.

Les attaques ciblées utilisent souvent les collaborateurs comme portes d'entrée

Les attaques ciblées restent dominées par l'action d'un tel malware (49 % des cas). L'exploitation des failles techniques ou des fuites via des terminaux mobiles représente 30 % Et l'ingénierie sociale (hameçonnage inclus) est la troisième cause d'infection avec 28 % des cas.

Les mauvaises pratiques sont nombreuses. Tomber dans le piège d'un phishing n'est qu'un des cas. Il y a aussi les mots de passe trop faibles, les faux appels du support technique, les clés USB abandonnées dans un parking qui sont systématiquement récupérées… Et la dissimulation d'incident est probablement le pire.

Source : cio-online.com *Vous êtes le maillon faible (en cybersécurité)*

Réagissez à cet article

Source : *Vous êtes le maillon faible (en cybersécurité)*

Mise à jour Apple pour résoudre la vulnérabilité d’exécution de code critique dans iOS et MacOS

	Mise à jour Apple pour résoudre la vulnérabilité d’exécution de code critique dans iOS et MacOS

La sécurité est toujours un point important dans nos appareils électroniques et encore plus lorsqu'il s'agit de nos objets connectés. Apple propose une mise à jour de sécurité capitale pour les utilisateurs d'iPhones, d'iPads et d'ordinateurs Mac. Une mise à jour en rapport avec Broadpwn.

La mise à jour corrige une vulnérabilité clé appelée Broadpwn qui permet aux pirates de "exécuter un code arbitraire" ou de prendre en charge votre appareil via des puces Wi-Fi intégrées au processeur principal de l'appareil.

Pour rappel, nous avions évoqué cette faille de sécurité il y a environ trois semaines. En effet, cette faille était liée principalement aux puces Wi-Fi de Broadcom BCM43xx en proie aux hackers.

Nitay Artenstein, un chercheur en sécurité dans le service de sécurité informatique américain Exodus Intelligence, avait exposé le défaut et avait déclaré qu'un pirate informatique pouvait être en mesure cibler ces appareils.

Une mise à jour qui vaut la peine d'être faite…[lire la suite]

Réagissez à cet article

Source : *Mise à jour Apple pour résoudre la vulnérabilité d'exécution de code critique dans iOS et MacOS. –*

Faille dans votre box :

désactivez d’urgence l’option WPS

Faille dans votre box : désactivez d’urgence l’option WPS

La rumeur était partie d’un réputé forum dédié au wifi et à sa sécurité. Une faille permet de bypasser l’authentification par le bouton WPS lancée par votre box…[lire la suite]

Réagissez à cet article

Source : *ZATAZ Faille dans votre box : désactivez d’urgence l’option WPS – ZATAZ*

Comment transformer

l’enceinte Amazon Echo en espion

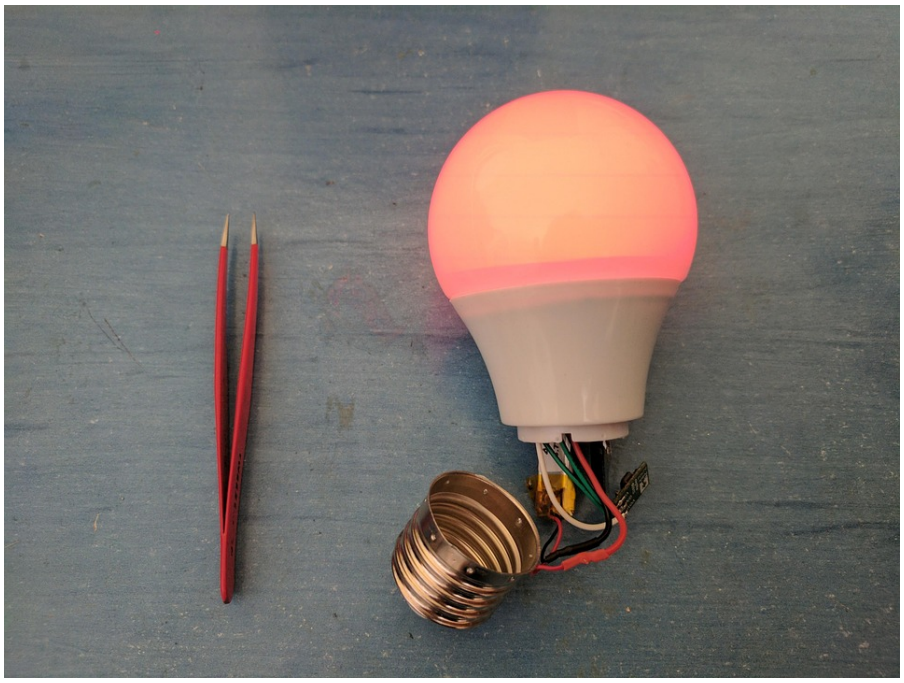
Comment transformer l’enceinte Amazon Echo en espion

Pour les spécialistes, ce n’est pas réellement une surprise, mais pour les premiers acheteurs d’Amazon Echo, cette enceinte sans-fil embarquant des fonctions d’assistant vocal, la pilule est difficile à avaler.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d’audits dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur sur cette page.

Réagissez à cet article

La problématique des objets connectés trop indiscrets



La problématique des objets connectés trop indiscrets

Brancher le baby phone, activer le thermostat, prendre sa tension ou sa température… Gestes loin d'être anodins dans l'internet des objets.

On a récemment évoqué dans les médias le danger potentiel d'un aspirateur automatique baptisé Roomba. Ses algorithmes et capteurs détectent les objets et obstacles, de manière à établir une cartographie des pièces où il est utilisé. Chez le fabricant, on précise que ces données servent à améliorer le matériel. Les détracteurs prétendent que les données récupérées sont vendues. Peu importe, la prudence s'impose avec les objets du quotidien connectés sur Internet.

Pas de budget pour la sécurité

Frigos, pacemakers, smartwatchs, babyphones et téléviseurs derniers cris peuvent désormais présenter un danger. Samsung conseille ainsi de désactiver la reconnaissance vocale sur ces Smart TV afin d'empêcher que vos conversations privées puissent être interceptées! Ces TV intelligentes disposent de deux microphones; un à l'intérieur du téléviseur, l'autre à l'intérieur de la télécommande afin d'interagir avec votre Smart TV à la voix. Un fournisseur de services tiers convertit vos commandes vocales interactives en texte et dans la mesure nécessaire pour vous fournir les fonctionnalités de reconnaissance vocale. Le fabricant insiste sur le fait qu'il utilise le cryptage standard de l'industrie pour sécuriser les données.

Multinationales ou start-up mettent aujourd'hui sur le marché des produits connectés où la sécurité pour protéger les données est reléguée au second plan pour des raisons de budget. Ces appareils disposent de petits processeurs capables de traiter un nombre d'instructions limité. Au point qu'aujourd'hui l'industrie récompense les personnes aidant à remonter des bugs de sécurité (sites, applications etc.) via les bug bounty qui mettent en contact ceux qui cherchent et trouvent les failles avec les développeurs de produits. Une stratégie préventive de sécurité qui en appelle d'autres…[lire la suite]

Réagissez à cet article

Source : *La problématique des objets connectés trop indiscrets*

Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed

Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed

Check Point Software Technologies Ltd révèle que 28 % des entreprises dans le monde ont été affectées par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

Check Point Software Technologies Ltd révèle que 28% des entreprises dans le monde ont été affectées de près ou de loin par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

RoughTed est une campagne de publicités malveillantes à grande échelle utilisée pour diffuser des sites web malveillants et des charges embarquées malveillantes telles que des escroqueries, des logiciels publicitaires, des kits d'exploitation de vulnérabilités et des logiciels rançonneurs. Elle a connu une forte poussée fin mai, puis a continué de se répandre en juin, touchant des entreprises dans 150 pays.

Large éventail

Les entreprises les plus touchées par RoughTed font partie des secteurs de la communication, de l'éducation, de la vente au détail et du commerce de gros… Les taux d'infection liés aux publicités malveillantes ont augmenté au cours des derniers mois, car il suffit aux pirates d'infecter une seule plate-forme de publicités en ligne pour atteindre un large éventail de victimes sans trop d'efforts, et il n'est pas nécessaire de se doter d'une infrastructure de diffusion lourde pour le logiciel…

En seconde place, Fireball, qui a touché 20% des entreprises en mai, a fortement reculé et n'a affecté que 5% des entreprises en juin. Le ver Slammer est la troisième variante la plus courante, touchant 4 % des entreprises…[lire la suite]

Réagissez à cet article

Source : *Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed*