Trouver une faille de sécurité peut rapporter jusqu’à 500 000 dollars

	Trouver une faille de sécurité peut rapporter jusqu’à 500 000 dollars

La société Zerodium, spécialisée dans le commerce de failles zero-day, revient avec un nouvel appel d'offre : un demi million de dollars à quiconque apportera sur un plateau une vulnérabilité inconnue dans les applis de messagerie WhatsApp et Signal.

Quel est le prix de votre vie privée ? 499 999 dollars, ça vous semble correct ? Parce qu'à vrai dire, elle pourrait être bientôt être vendue pour seulement un dollar de plus. L'entreprise Zerodium, spécialisée dans l'achat et la revente de vulnérabilités zero-day, vient de proposer la rondelette somme de 500 000 dollars à celui qui sera capable mettre au point les outils nécessaires au piratage des applications de messagerie cryptée Signal et WhatsApp. Déjà, en octobre 2016, elle avait proposé 1,5 millions de dollars pour une faille dans iOS 10…[lire la suite]

Réagissez à cet article

Source : *Une entreprise offre 500 000 dollars à celui qui trouvera une faille de sécurité exploitable sur WhatsApp et Signal*

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*

La stéganographie pour cacher des informations volées dans les images

	La stéganographie pour cacher des informations volées dans les images

En analysant de multiples campagnes de cyberespionnage et de cybercriminalité, les chercheurs de Kaspersky Lab ont identifié une nouvelle tendance inquiétante : des pirates emploient de plus en plus la stéganographie, une version numérique d'un stratagème ancien consistant à dissimuler des messages à l'intérieur d'images, afin de masquer les traces de leur activité malveillante sur un ordinateur attaqué. Un certain nombre de malwares espions ainsi que plusieurs autres destinés au vol d'informations financières ont récemment été repérés utilisant cette technique.

Dans le cadre d'une cyberattaque ciblée type, un acteur malveillant – une fois infiltré dans le réseau attaqué – établit une tête de pont puis collecte des informations de valeur afin de les transférer par la suite à un serveur de commande et de contrôle (C&C). Dans la plupart des cas, des solutions de sécurité ou des outils analytiques professionnels éprouvés sont en mesure de détecter la présence de l'intrus sur le réseau à chaque phase d'une attaque, notamment au moment de l'exfiltration des données volées. En effet, cette exfiltration laisse généralement des traces, par exemple l'enregistrement de connexions à une adresse IP inconnue ou inscrite en liste noire. Or le recours à la stéganographie rend cette détection difficile….[lire la suite]

Réagissez à cet article

Source : *Plusieurs groupes de pirates utilisent de plus en plus la technique de la stéganographie pour cacher des informations volées dans les images – Global Security Mag Online*

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)*

Faire face aux cyberattaques

Faire face aux cyberattaques

Notre niveau de défense informatique doit se hisser au niveau d'expertise des attaquants. Il faut veiller à la sensibilisation des salariés et des citoyens.

WannaCry et Pethia prouvent que nous entrons dans l'ère de la cyberguerre marquée par la volonté des pirates de nuire pour nuire sans forcément chercher à extorquer des rançons. Le scénario actuel avait été anticipé par l'Etat français. La création de l'Agence nationale de la sécurité des systèmes d'information, dès 2009, démontre qu'en France, nous étions pionniers. Nous savions que plus la technologie progressait, plus l'entrée en cyberguerre était inévitable…[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

Réagissez à cet article

Source : *Faire face aux cyberattaques*

Pourquoi les mots de passe compliqués sont finalement une mauvaise idée ?

	Pourquoi les mots de passe compliqués sont finalement une mauvaise idée ?

Ponctuer son mot de passe de chiffres et de caractères spéciaux est inutile. Celui qui avait prodigué ces conseils voici 14 ans, vient de faire son mea culpa . Et il en livre de nouveaux qui devraient vous ravir.

Quatorze ans après avoir publié ce qui était considéré comme la bible de la création de mots de passe, l'auteur du document révise sa position dans une interview au ***Wall Street Journal*.**

En 2003, Bill Burr conseillait dans une annexe d'un document publié par le **National Institute of Standards and Technology** (agence américaine notamment chargée de développer des normes technologiques) de créer un mot de passe contenant majuscules, minuscules, chiffres et signes de ponctuation et d'en changer régulièrement (tous les 90 jours).

Des combinaisons trop compliquées à retenir

Mais ces conseils n'étaient finalement pas si judicieux. Pour une raison simple: de tels mots de passe sont non seulement compliqués à retenir pour les utilisateurs… mais aussi très faciles à casser par d'éventuels pirates. En effet, d'innombrables internautes choisissent un simple mot, qu'ils vont légèrement modifier et/ou compléter par des caractères spéciaux pour en faire leur sésame.

Exemple? Un amateur d'oursins pourrait par exemple choisir de sécuriser son compte avec le mot de passe « HouR-s1N$! ». Or malgré sa complexité apparente, cette suite de caractères demeure facilement cassable par une attaque hybride combinant dictionnaire et force brute…[lire la suite]

Réagissez à cet article

Source : *Oubliez tout ce qu'on vous a dit sur la sécurisation des mots de passe*

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. –*