Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

	Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

Dévoilée au public lundi 16 octobre 2017, Krack Attacks est une faille qui permet aux pirates d'espionner votre connexion wifi. Que doit-on craindre ? Comment se protéger ? Denis JACOPINI nous apporte des éléments de réponse.

Que doit-on craindre de cette faille découverte dans le WPA2 ?

Mathy Vanhoef, chercheur à l'université KU Leuven, a découvert une faille permettant d'intercepter des données transmises sur un réseau Wi-Fi, même lorsqu'il est protégé par le protocole WPA2. Pire, il est également possible d'injecter des données, et donc des malwares, en utilisant la technique découverte. Les réseaux domestiques aussi bien que les réseaux d'entreprises sont concernés, c'est donc une découverte majeure dans le domaine de la sécurité informatique.

La technique décrite par Mathy Vanhoef est appelée Key Reinstallation AttaCK, ce qui donne KRACK.

Comment se protéger de cette faille ?

Il n'y a pas de meilleur protocole que le WPA2. Il ne faut surtout pas revenir au protocole WEP. Changer de mot de passe ne sert à rien non plus. Le seul moyen de se protéger de cette faille est de mettre à jour votre système d'exploitation et les appareils concernés. Les acteurs du marché, fabricants ou éditeurs, ont été notifiés de cette faille le 14 juillet 2017. Certains l'ont comblée par avance comme Windows.

Il faut combler la faille à la fois sur les points d'accès et sur les clients, c'est-à-dire que patcher vos ordinateurs et smartphones ne vous dispense pas de mettre à jour votre routeur ou votre box Wi-Fi.

Même si, en tant qu'utilisateur, vous n'avez pas grand chose à faire de plus que de mettre à jour votre système d'exploitation et le firmware de votre point d'accès pour vous protéger contre la faille Krack Attacks, nous vous énumérons une liste de préconisations qui mises bout à bout, rendront plus difficile aux pirates les plus répandus l'intrusion dans votre Wifi.

Les Conseils de Denis JACOPINI pour avoir un Wifi le plus protégé possible :

1. Mettez à jour les systèmes d'exploitation de vos ordinateurs, smartphones, tablettes et objets.
2. Mettez à jour votre point d'accès Wifi (le firmware de votre Box, routeur…)
3. Modifier le SSID ;
4. Modifier le mot de passe par défaut ;
5. Filtrage des adresses MAC (facultatif car peu efficace);
6. Désactiver DHCP ;
7. Désactiver le MultiCast (pour les appareils qui disposent de cette fonction) ;
8. Désactiver le broadcast SSID (pour les appareils qui disposent de cette fonction) ;
9. Désactiver le WPS (pour les appareils qui disposent de cette fonction) ;
10. Utilisez un VPN ou un accès http**s** pour envoyer ou recevoir des informations confidentielles
11. Choisissez un cryptage fort de votre Clé WIFI :

- Technologie WPA 2 (également connu sous le nom IEEE 802.11i-2004) ;
- **Protocole de chiffrement AES** (ou CCMP) : **Important !**

Des personnes peuvent accéder librement à votre Wifi ?

Condition exigée depuis plusieurs années par les touristes et les nomades, il y a de fortes chances que les clients de votre hôtel, de vos chambres d'hôtes, de vos gîtes ou tout simplement des amis vous demandent absolument de disposer du Wifi.

Je tiens à vous rappeler que selon l'article L335-12 du Code de la Propriété Intellectuelle, l'abonné Internet reste le seul responsable des usages de sa connexion.

Ainsi, je ne peux que vous conseiller d'être prudent concernant l'usage de votre connexion Wifi par des tiers et de vous munir de moyens technologiques permettant de conserver une trace de chaque personne se connectant sur votre Wifi afin que si votre responsabilité en tant qu'abonné à Internet était recherchée, vous pourriez non seulement vous disculper mais également fournir tous les éléments permettant l'identification de l'individu fraudeur.

Les personnes intéressées par les détails techniques, et pointus, concernant la découverte de la faille WPA2 peuvent se rendre sur le site du chercheur dédié à ce sujet.

Bulletin d'alerte du CERT-FR

Va-t-on aller vers un WPA 3 ?

Réagissez à cet article

Source : *KRACK Attacks: Breaking WPA2 / KRACK : faille du Wi-Fi WPA2, quels appareils sont touchés ? Comment se protéger ?*

Télétravail : gare aux failles de sécurité

Télétravail : gare aux failles de sécurité

Le télétravail fait entrer dans les systèmes d'information de l'entreprise des appareils dont le niveau de sécurité peut s'avérer à risque.

Les directeurs des systèmes d'information (DSI) s'arrachent déjà les cheveux. Si nombre de métiers, comme ceux des commerciaux ou des consultants, sont déjà équipés pour travailler à distance en toute sécurité, le télétravail pousse hors des murs de l'entreprise des salariés souvent peu sensibilisés aux risques de cybersécurité.

D'une part, travailler de chez soi pose la question de la sécurité du matériel. La connexion Internet est-elle sécurisée ? Le chiffrement du disque dur en cas de perte est-il actif ? L'identification par SMS ou par token est-elle en vigueur ? « *Autant de questions auxquelles les DSI doivent répondre pour sécuriser le travail à distance. Les mesures sont simples et souvent déjà déployées pour certains salariés mais il faut désormais les généraliser* »…[lire la suite]

Réagissez à cet article

Source : *Télétravail : gare aux failles de sécurité, Cybersécurité – Les Echos Business*

Une faille dans Windows 10 utilisée pour vous espionner !

	Une faille dans Windows 10 utilisée pour vous espionner !

Selon un rapport publié sur le blog de la firme de sécurité informatique FireEye, les pirates procédaient comme suit : un fichier Word ouvert innocemment par l'utilisateur activait la faille 0-Day -CVE-2017-8759- et permettait au maliciel d'installer à son insu un programme informatique destiné à vous espionner. L'ordinateur visé par la manoeuvre était alors contraint d'installer FinSpy – le spyware en question.

Ce malware est développé par une entreprise anglaise particulièrement controversée qui commercialise ses produits à des gouvernements partout dans le monde : **Gamma Group**. Selon le rapport de FireEye, **FinSpy a déjà été vendu à de multiples acheteurs,** il est donc plus que probable que ceux-ci s'en servent activement pour tenter d'infiltrer de nombreuses cibles.
Selon les experts en cybersécurité de Microsoft, les hackers en question font **partie du groupe NEODYMIUM**, déjà connu pour des pratiques de hacking similaires. Microsoft reste donc très vigilant par rapport à ces failles de sécurité : n'hésitez donc pas à télécharger les patchs proposés dès que possible !
On ne le répétera jamais assez, si vous recevez un fichier Word suspect sur votre boîte mail ne l'ouvrez pas, même s'il vous promet de vous révéler la suite de Game Of Thrones !…[lire la suite]

Réagissez à cet article

Source : *Windows 10 : une faille de sécurité permet aux*

pirates d’y installer un dangereux malware !

Alerte : CCleaner compromis par une backdoor

Piriform avertit que son logiciel CCleaner a été compromis. Avec des risques de fuites de données persos de 130 millions d'utilisateurs.

Piriform, l'éditeur de l'utilitaire CCleaner de nettoyage et d'optimisation de Windows, vient de reconnaître qu'il a fait l'objet d'une attaque.

Les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud de sa solution ont été compromises.

« Une activité suspecte a été identifiée le 12 septembre 2017, où nous avons vu une adresse IP inconnue recevant des données du logiciel trouvé dans CCleaner et CCleaner Cloud sur les systèmes Windows 32 bits », alerte Paul Yung, Vice-Président Produit de Piriform.

Selon l'éditeur, le logiciel a été illégalement modifié avant sa livraison publique. Le pirate a réussi à installer une backdoor à deux niveaux afin d'exécuter du code envoyé à partir d'une adresse IP sur les systèmes affectés…[lire la suite]

Réagissez à cet article

Source : *L'utilitaire CCleaner compromis par une backdoor*

Un demi-million de pacemakers menacés de piratage informatique rappelés

	Un demi-million de pacemakers menacés de piratage informatique rappelés

L'administration américaine a rappelé 465.000 stimulateurs cardiaques menacés d'un piratage potentiel à cause d'une vulnérabilité informatique. Un correctif « vital » de leur logiciel devra être installé en hôpital. Explications.

Jamais le terme « vital » ne s'était autant appliqué à un correctif logiciel. Un léger vent de panique souffle dans les départements de cardiologie des hôpitaux américains, car ils doivent se préparer à recevoir la visite de presque un demi-million de patients pour une mise à jour logicielle de leur stimulateur cardiaque.

La puissante US Food and Drugs Administration (FDA) est à l'origine de ce rappel. Son **alerte officielle** concerne 465.000 pacemakers exposés à une attaque informatique éventuelle en raison d'un « faille » décelée a posteriori.

Cette « vulnérabilité » permettrait à un pirate très mal intentionné se trouvant à proximité d'en altérer le fonctionnement en agissant à distance par onde radio pour, par exemple, vider la batterie ou modifier la fréquence cardiaque. Et mettre en danger la vie du porteur du stimulateur cardiaque…[lire la suite]

Réagissez à cet article

Source : *Un demi-million de pacemakers menacés de piratage informatique rappelés*

Faille de sécurité sur Instagram : les mails et numéros de 6 millions de comptes en vente libre ?

	Faille de sécurité sur Instagram : les mails et numéros de 6 millions de comptes en vente libre ?

Le bug d'API qu'Instagram a corrigé cette semaine n'aurait pas seulement permis à des internautes de récupérer les numéros de téléphone et les adresses mail de plusieurs célébrités. Selon Ars Technica, 6 millions de comptes seraient concernés si l'authenticité des données proposées à la vente sur le web est confirmée.

e bug d'API qui a permis un accès aux données personnelles – adresse mail et numéro de téléphone – de plusieurs célébrités présentes sur Instagram a peut-être eu des conséquences plus importantes que ne le laissait entendre le réseau social. Une base de données contenant 10 000 identifiants Instagram a en effet été mise en ligne jeudi 31 août, comme le rapporte Ars Technica.

Dans un mail en date du 30 août adressé à tous les comptes certifiés « *par excès de prudence* », Instagram affirmait avoir corrigé le bug d'API, sans toutefois indiquer la portée de cette intrusion – qui n'aurait donc pas seulement touché les célébrités, appelées à renforcer la sécurité de leur compte.

Depuis, un internaute – qui a contacté Ars Technica – affirme avoir récolté les données personnelles de 6 millions d'utilisateurs. Il les propose librement à la vente sur un site, moyennant 10 dollars par compte…[lire la suite]

Réagissez à cet article

Source : *Faille de sécurité sur Instagram : les mails et*

numéros de 6 millions de comptes en vente libre ? – Tech – Numerama

---

Plus de 100 000 smartphones Android infectés par un botnet DDoS

	Plus de 100 000 smartphones Android infectés par un botnet DDoS

Les victimes étaient infectées par des centaines d'applications en apparence inoffensives, diffusées par le Google Play Store.

On ne cesse de le répéter : attention aux applications que vous téléchargez, y compris sur le Google Play Store. Des chercheurs en sécurité viennent de démanteler WireX, un botnet spécialisé en attaques par déni de service distribuées (DDoS) et qui regroupait jusqu'à 120.000 smartphones zombies répartis dans plus de 100 pays. Ce n'est pas la première fois qu'un tel botnet est détecté. En septembre 2016, les chercheurs d'Imperva avait déjà mis le doigt sur un réseau de smartphones Android zombies destiné au DDoS et composé de plus de 26.000 nœuds…[lire la suite]

Réagissez à cet article

Source : *Plus de 100 000 smartphones Android esclaves d'un botnet DDoS*

Des hackers utilisent des

spoilers de «Game of Thrones» pour propager un logiciel malveillant

	Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant

En règle générale mieux vaut éviter les spoilers. Surtout, quand ceux-ci proviennent d'un email suspect. D'après un article Proofpoint, une entreprise américaine de cybersécurité, une «campagne d'emails ciblées» qui utilise des spoilers des prochains épisode de «Game of Thrones» comme appât est actuellement en cours. À la clef, pour les internautes malchanceux qui cliqueraient sur la pièce jointe, un logiciel malveillant.

L'entreprise de cyber-sécurité explique avoir repéré un de ces emails le 10 août dernier, à la suite du piratage de HBO par des hackers. Intitulé *«Vous voulez voir «Game of Thrones» en avance ?»*, le courrier contient quelques détails concernant les prochains épisodes de la série ainsi qu'une pièce jointe word contenant un maliciel. Une fois téléchargé, celui-ci tente d'installer un Remote Access Trojan (cheval de Troie à distance) qui est ensuite capable d'envoyer des informations et des données à un serveur.
D'après The Verge, ce genre d'attaque a été associée par le passé avec le gouvernement chinois et il serait possible *«que cette attaque provienne des mêmes acteurs»*. Cet email fait suite au hack massif de HBO. La chaîne américaine, qui diffuse «Game of Thrones», s'était fait voler 1,5 To de données en juillet dernier, dont des informations sur la saison de la série. Une demande de rançon avait rapidement suivi ce hack…[lire la suite]

Réagissez à cet article

Source : *Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant | Slate.fr*

Une faille dangereuse découverte sur les hoverboards

	Une faille dangereuse découverte sur les hoverboards

Des experts chez Alibaba Security se sont penchés sur le niveau de sécurité des hoverboards. Résultat, ils sont parvenus à mettre à jour une faille qui pourrait être dangereuse pour les utilisateurs. Les tests menés par les spécialistes ont démontré qu'il était possible de brouiller les capteurs de mouvement des hoverboards. L'usager pourrait alors tomber et se blesser.

Les démonstrations, faites lors de la conférence Black Hat Security en juillet, ont révélé que la faiblesse des hoverboards n'était autre que les ondes sonores. Projetées sur les capteurs, elles peuvent perturber les mesures et données collectées par ces derniers, déséquilibrant du même coup l'hoverboard et son utilisateur…[lire la suite]

Réagissez à cet article

Source : *Les hoverboards ont un talon d'Achille, les ondes sonores*

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