Alerte : Faille dans TeamViewer permet de prendre le contrôle de votre ordinateur

	Alerte : Faille dans TeamViewer permet de prendre le contrôle de votre ordinateur

Plusieurs millions d'internautes utilisent, de part le monde, l'outil TeamViewer. Un problème de sécurité vient d'être découvert. Il pourrait permettre de détourner l'ordinateur des utilisateurs.

Le logiciel TeamViewer est une sorte de cheval de Troie légal. Je m'explique ! L'outil permet de prendre la main sur un ordinateur dont l'accès a été autorisé. Il permet aussi de filmer l'écran, capture écran, … Bref, un trojan licite. Seulement, un problème de taille vient d'être découvert dans ce logiciel utilisé par des millions d'entreprises et particuliers.

Tout d'abord, une vulnérabilité critique a été découverte dans le logiciel qui pourrait permettre aux utilisateurs partageant une session de prendre le contrôle total du PC de leur ,interlocuteur. Pour qu'une session à distance fonctionne sur les deux machines, il faut un présentateur, celui qui affiche son écran et un spectateur, celui qui regarde l'écran du présentateur…[lire la suite]

Lien vers le code et la démo de Gelin

Commentaire de Denis JACOPINI :

Dans la mesure du possible, ne laissez jamais un TeamViewer en l'attente. Autorisez l'accès manuellement. Si vous ne pouvez pas faire autrement, programmez le déclenchement d'une alerte lors des connexions automatiques. En attendant, que Teamviewer corrige cette vulnérabilité au plus vite, prudence !

Réagissez à cet article

Source : *ZATAZ Une faille dans TeamViewer permet de détourner l'ordinateur d'un utilisateur – ZATAZ*

Alerte : Mettez à jour votre Mac s’il a la High Sierra, version 10.13

	Alerte : Mettez à jour votre Mac s’il a la High Sierra, version 10.13

Une faille de sécurité préoccupante avait été détectée sur la dernière version, appelée « High Sierra », du système d'exploitation macOS d'Apple. La firme à la pomme a développé un correctif en urgence.

Comment savoir si vous êtes concerné ?

La vulnérabilité permettait d'obtenir un accès administrateur depuis un simple accès utilisateur, sans nécessairement nécessiter un accès physique à l'ordinateur : pour peu que des services à distance (comme par exemple VNC Viewer) soient activés, un intrus connecté à votre réseau local pouvait en prendre le contrôle. Il n'est toutefois pas possible de se *logger* par ce moyen sur une machine déjà allumée, dont l'écran est protégé par mot de passe. Apple avait rappelé la procédure permettant remédier temporairement au problème : il s'agit d'activer l'utilisateur « root » sur votre Mac et de définir un mot de passe.

VERSION.

Ce problème ne concerne que la dernière version du système d'exploitation (High Sierra, version 10.13). Pour savoir quelle est la version du système de votre Mac, il vous suffit de suivre le mode d'emploi mis en ligne par Apple : dans le menu Pomme situé dans le coin de l'écran, sélectionnez *« À propos de ce Mac »*. La version du système d'exploitation s'affiche dans la boîte de dialogue…[lire la suite]

Denis JACOPINI

Afin de connaître la version de Mac OS X installé sur votre ordinateur, veuillez suivre les manipulations suivantes :

1. Cliquez sur le menu Pomme en haut à gauche de votre écran.
2. Sélectionnez « A propos de ce Mac »
3. Une fenêtre va apparaître avec la version de votre système.

Réagissez à cet article

Source : *Une faille de sécurité critique détectée sur le système d'exploitation MacOS – Sciencesetavenir.fr*

70 % des attaques informatiques partent d’un problème humain. Il est urgent de sensibiliser votre personnel.

70 % des attaques informatiques partent d’un problème humain. Il est urgent de sensibiliser votre personnel.

En matière de cybersécurité, l'Europe a décidé de légiférer mais des disparités existent. Explications avec Julie Gommes, experte en cybersécurité lors de la SME Assembly 2017 (Assemblée annuelle des PME organisée par la Commission européenne) à Tallinn (Estonie). Pour elle, la première faille de sécurité est entre la chaise et l'ordinateur.

[Article source]

LE NET EXPERT

:

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **FORMATIONS / SENSIBILISATION** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Cybersécurité : 70 % des attaques partent d'un problème humain – Courrier cadres*

Vol de données chez Uber : L'état Français demande des explications

	Vol de données chez Uber : L'état Français demande des explications

---

Le secrétaire d'État au Numérique a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'usagers.
Le secrétaire d'État au Numérique Mounir Mahjoubi a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'usagers, pour lui demander des explications sur d'éventuelles victimes françaises.
« Face au danger que représente l'exploitation de ces données, je souhaite vous exprimer mon inquiétude quant à l'éventuelle présence en très grand nombre de clients et chauffeurs français » parmi les victimes, souligne Mounir Mahjoubi, dans un courrier. « Pouvez-vous à ce jour nous indiquer si des utilisateurs français sont concernés et si oui combien, et de quel type sont les données qui ont été dérobées », interroge-t-il. Le secrétaire d'État demande aussi « quelles mesures techniques et organisationnelles sont mises en place pour informer et accompagner les utilisateurs ».

Noms, adresses électroniques et numéros de téléphone.
Uber n'a pas détaillé qui sont les victimes de cette fuite d'informations remontant à la fin 2016, et qu'il avait dissimulée, mais de nombreux Français sont vraisemblablement concernés. Le chiffre de 57 millions est en effet énorme, quand l'ancien patron Travis Kalanick déclarait en octobre 2016 -plus ou moins au moment des faits- compter 40 millions d'utilisateurs actifs dans le monde. Selon Uber, les noms, adresses électroniques et numéros de téléphone des victimes ont été subtilisés. Le groupe américain de réservation de voitures avec chauffeur affirme qu'aucune information bancaire n'a été exfiltrée, pas plus que les dates de naissance et les historiques de trajets.

Le secrétaire d'État s'étonne qu'Uber n'ait « pas signalé cet incident ». Mounir Mahjoubi s'étonne également de ce qu'Uber n'ait « pas signalé cet incident » auprès de la Commission nationale de l'informatique et des libertés (Cnil) et de l'Agence nationale de la sécurité des systèmes d'information (Anssi), responsables respectivement de la protection des citoyens et de la coordination de la défense française contre les pirates informatiques, qui ont été mises en copie de son courrier. Il aurait également apprécié que le groupe américain se signale « auprès des utilisateurs concernés ».

Mahjoubi souhaite que l'entreprise informe les utilisateurs concernés et les autorités. « Au regard du nombre de vos clients, vous avez une importance qui vous donne des responsabilités », souligne Mounir Mahjoubi, rappelant qu'un règlement européen rendra en mai prochain les entreprises responsables des données personnelles qu'elles détiennent, et leur imposera de signaler rapidement les incidents. « Au regard du danger existant, nous aimerions que vous informiez volontairement les utilisateurs concernés ainsi que les autorités françaises », insiste le secrétaire d'État au Numérique…[lire la suite]

Réagissez à cet article

Source : *Piratage d'Uber : Mahjoubi demande des explications*

Une faille permet d'écouter 77 % des smartphones Android

Une faille permet d'écouter 77 % des smartphones Android

Voilà qui risque d'augmenter la paranoïa de celles et ceux qui pensent qu'ils sont écoutés, via leur smartphone, à tout moment de la journée : les chercheurs de MWR Labs ont découvert une nouvelle faille majeure qui toucherait plus des trois quarts des smartphones Android en circulation. Une faille que Google a comblée, mais seulement dans Android 8.0 Oreo.

Le problème de cette nouvelle faille, c'est qu'elle est très facilement exploitable par un développeur malintentionné : il ne s'agit pas d'une attaque à proprement parler mais d'un souci dans les autorisations données aux applications.

Le service Android MediaProjection au centre de cette nouvelle faille

Les chercheurs de MWR Labs ont découvert que Google, qui développe Android, a réalisé un changement majeur dans les autorisations d'un des services les plus anciens d'Android : MediaProjection. Ce service est en mesure d'enregistrer l'audio ainsi que l'écran du smartphone et est utilisé par certaines applications….[lire la suite]

Réagissez à cet article

Source : *Une faille permet d'écouter 77 % des smartphones Android*

Alerte : Une faille de sécurité sur des jouets connectés expose les enfants

	Alerte : Une faille de sécurité sur des jouets connectés expose les enfants

---

Une association de consommateurs britannique alerte sur une faille de sécurité liée à la connexion Bluetooth de certains jouets connectés et appelle à ce que ces derniers soient retirés de la vente.

Alors que certains ont déjà effectué les premiers achats de Noël, l'association britannique de consommateurs **Why ?** alerte les consommateurs sur le risque présenté par plusieurs jouets connectés : la peluche Furby Connect, le robot i-Que, le petit chien Toy-Fi Teddy et les animaux CloudPets.
En cause : **une faille de sécurité** qui permet à toute personne ayant une connexion Bluetooth et ayant téléchargé l'application de ces jouets de se connecter à ces derniers, sans mot de passe ou étape de sécurité.
Une situation rendue possible par la **non-sécurisation de la connexion Bluetooth** de ces jouets, selon les tests réalisés par Why ? avec l'aide de Stiftung Warentest, l'équivalent allemand de l'UFC Que choisir…[lire la suite]

Réagissez à cet article

Source : *VIDÉO – Une faille de sécurité sur des jouets connectés expose les enfants*

Internet : les machines-zombies inquiètent les spécialistes

	Internet : les machines-zombies inquiètent les spécialistes

Après la contamination de plus d'un million d'objets connectés à travers la planète, les experts en cybersécurité tirent la sonnette d'alarme.

Un ouragan se prépare sur Internet. C'est du moins ce qu'affirment depuis quelques jours les experts en cybersécurité de la société CheckPoint. Ces ingénieurs informatiques sont convaincus que la contamination, à bas bruit depuis l'été, de plus d'un million d'objets connectés et d'ordinateurs à travers le monde… est le préalable à une vaste attaque par botnet, comme on désigne les réseaux de machines-zombies, prises « en otage » par des hackers.
Si la plupart des botnets sont relativement inoffensifs en ce qu'ils visent juste à réaliser des clics artificiels pour doper la fréquentation de certains sites et augmenter ainsi, de manière indue, la valeur de leurs bandeaux publicitaires, d'autres peuvent se révéler plus dangereux en permettant de bombarder des serveurs, via l'accumulation de requêtes, dans le but de les faire « tomber »…[lire la suite]

Réagissez à cet article

Source : *Internet : les machines-zombies inquiètent les spécialistes – Le Point*

Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés

	Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés

La faille de sécurité « HomeHack » permettait de prendre le contrôle de n'importe quel objet connecté du fabricant coréen LG. Mais appliquée aux robots aspirateurs, elle serait un moyen offert aux hackers d'observer l'intérieur des maisons.

Pratiques parce qu'ils nous simplifient la vie et qu'on peut les piloter depuis une simple application mobile, les objets connectés sont aussi potentiellement de véritables chevaux de Troie dans notre intimité.
Les experts de l'entreprise de cybersécurité Check Point ont révélé une faille de sécurité, « HomeHack », via laquelle il était possible de prendre le contrôle à distance d'un aspirateur LG Hom-Bot et d'espionner l'intérieur d'une maison au moyen de la caméra intégrée, comme le montre cette vidéo :
http://www.youtube.com/embed/BnAHfZWPaCs
Communiqué à LG en juillet dernier, le problème a depuis été corrigé par le constructeur en septembre, mais une question demeure : comment être certain que les objets connectés qui nous entourent sont assez sécurisés ? En effet, il est régulièrement proposé aux clients de synchroniser l'ensemble de leurs appareils sur un même système, ici l'application mobile SmartThinQ de LG, disponible sur Android et iOS…[lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés*

Faille de sécurité dans des caméras de vidéosurveillance FLIR

	Faille de sécurité dans des caméras de vidéosurveillance FLIR

Un chercheur en sécurité informatique découvre comment accéder aux images de caméras de vidéosurveillance thermiques FLIR.

Infiltration possible dans des caméras de vidéosurveillance ! Étonnante révélation, fin septembre, par un internaute du nom de LiquidWorm. Ce chercheur en sécurité informatique a diffusé un code qui permet de découvrir que les caméras thermiques de vidéo surveillance de marque FLIR pouvaient être espionnées. FLIR Systems a des identifiants de connexion SSH codés en dur dans sa version distribuée sous Linux.

Bref, un accès aux images, via cet accès caché qui ne peut être modifié !

Cette backdoor est dénoncée quelques jours avant le salon Milipol qui se déroulera en novembre à Paris. Flir Systems y sera présent pour présenter son matériel.

Selon l'information diffusée par « Zero science« , les modèles de caméras incriminées sont les 10.0.2.43 (logiciel F/FC/PT/D) et les versions du micrologiciel 8.0.0.64: □□1.4.1, 1.4, 1.3.4 GA, 1.3.3 GA et 1.3.2 sont concernés par cette porte cachée…[lire la suite]

Réagissez à cet article

Source : *ZATAZ Une porte cachée dans des caméras de vidéosurveillance FLIR – ZATAZ*

Une faille dans le Wifi pourrait compromettre vos données personnelles

	Une faille dans le Wifi pourrait compromettre vos données personnelles

Les réseaux WiFi du monde entier pourraient être piratés par le biais d'une faille de sécurité majeure, ont mis en garde lundi les autorités américaines et des chercheurs en Belgique.

C'est le protocole de chiffrement WPA2, utilisé par quasiment tous les réseaux WiFi pour se protéger des intrusions, qui est vulnérable: il est possible grâce à cette faille de décrypter toutes les données transmises en WiFi depuis des téléphones mobiles, ordinateurs, tablettes, etc.

Cette annonce vient confirmer la vulnérabilité des réseaux WiFi signalée depuis longtemps par les experts en cybersécurité. Mais, pour l'heure, on ne sait pas si des pirates ont effectivement utilisé cette faille à des fins malveillantes.

D'après des chercheurs de l'université belge de Louvain à l'origine de cette découverte, elle rend possible «le vol d'informations sensibles comme les numéros de cartes bancaires, les mots de passe, les messages instantanés, courriels, photos, etc.».

Selon la configuration du réseau, il est aussi possible d'injecter et de manipuler les données.

Par exemple, «un pirate pourrait insérer des « ransomware » (rançongiciels, NDLR) ou d'autres logiciels malveillants dans des sites internet», poursuivent les universitaires, qui ont baptisé la faille «KRACK» (Key Reinstallation Attack), car elle permet aux pirates d'insérer une nouvelle clé de sécurité dans les connexions WiFi…[lire la suite]

Réagissez à cet article

Source : *WiFi: une faille qui pourrait compromettre vos données personnelles | TVA Nouvelles*