Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

Les nouvelles règles de confidentialité de WhatsApp ne vont peut-être pas vous plaire.
Lorsque WhatsApp a annoncé son acquisition par Facebook en 2014, les utilisateurs et les défenseurs de la vie privée se sont inquiétés de ce qui allait advenir de leurs données. Pendant deux ans, les deux services sont restés indépendants. Cependant, aujourd'hui, WhatsApp a mis à jour ses règles de confidentialité, qui sont restées inchangées pendant 4 ans.
Et celles-ci n'excluent plus l'utilisation par Facebook des données du milliard de personnes utilisent WhatsApp pour optimiser ses publicités.

« […] en connectant votre numéro de téléphone avec les systèmes de Facebook, ce dernier peut vous offrir de meilleures suggestions d'amis et vous montrer des publicités plus pertinentes si vous avez un compte Facebook. Par exemple, vous pouvez voir une publicité d'une entreprise avec laquelle vous avez déjà travaillé au lieu de voir celle d'une entreprise dont vous n'avez jamais entendu parler », lit-on dans un communiqué de WhatsApp.

Cependant, le service explique aussi que cette « coordination » avec Facebook permettra également à WhatsApp de faire des choses comme « suivre des mesures de base sur la fréquence d'utilisation de nos services des gens et améliorer la lutte contre les spams ».

Et WhatsApp a bien clarifié que même si il va d'avantage collaborer avec Facebook, ses messages sont chiffrés de bout en bout, ce qui signifie que théoriquement, personne (ni Facebook, ni WhatsApp) ne peut accéder au contenu.

Le modèle économique de WhatsApp se précise

Pour rappel, WhatsApp était à l'origine une application payante, mais gratuite la première année. Cependant, le service a récemment décidé supprimer les frais annuels, pour devenir entièrement gratuit. Cependant, WhatsApp n'entend pas gagner de l'argent en affichant des bannières publicitaires, mais plutôt en misant sur des fonctionnalités pensées pour les relations entre clients et entreprises. Et les nouvelles règles de confidentialités reflètent aussi ce projet.
Article original de Setra

Réagissez à cet article

Original de l'article mis en page : WhatsApp va partager vos données avec Facebook

Alerte : Twitter pour Android infecté par un Cheval de Troie

	Alerte : Twitter pour Android infecté par un Cheval de Troie

ESET découvre le premier botnet sous Android qui contrôle Twitter

Les chercheurs ESET ont découvert une porte dérobée sous Android qui contient un Cheval de Troie et qui est contrôlée par des tweets. Détecté par ESET comme étant Android/Twitoor, **il s'agit de la première application malveillante utilisant Twitter** au lieu d'une commande et d'un contrôle traditionnel de serveur (C&C).
Après son lancement, le Cheval de Troie cache sa présence sur le système et vérifie le compte Twitter défini par intervalle régulier pour les commandes. Sur la base des commandes reçues, il peut soit télécharger des applications malveillantes, soit basculer le serveur C&C d'un compte Twitter à un autre.
« L'utilisation de Twitter pour contrôler un botnet est une étape innovante pour une plateforme Android », explique Lukáš Štefanko, malware researcher chez ESET et qui a découvert cette application malicieuse.
Selon Lukáš Štefanko, les canaux de communication basés sur des réseaux sociaux sont difficiles à découvrir et impossible à bloquer entièrement – alors qu'il est extrêmement facile pour les escrocs de rediriger les communications vers un autre compte de façon simultanée.

Twitter a d'abord été utilisé pour contrôler les botnets de Windows en 2009. « En ce qui concerne l'espace Android, ce moyen de dissimulation est resté inexploité jusqu'à présent. Cependant, nous pouvons nous attendre à l'avenir à ce que les cybercriminels essayent de faire usage des statuts de Facebook ou de déployer leurs attaques sur LinkedIn et autres réseaux sociaux » , prévoit Lukáš Štefanko.
Android/Twitoor est actif depuis juillet 2016.Il ne peut pas être trouvé sur l'un des app store officiels d'Android (selon Lukáš Štefanko) mais il est probable qu'il se propage par SMS ou via des URL malveillantes. Il prend l'apparence d'une application mobile pour adulte ou d'une application MMS mais sans fonctionnalité. Plusieurs versions de services bancaires mobiles infectés par un malware ont été téléchargées. Cependant, les opérateurs de botnet peuvent commencer à distribuer d'autres logiciels malveillants à tout moment, y compris des ransomwares selon Lukáš Štefanko.

Twitoor est le parfait exemple de l'innovation des cybercriminels pour leur business. Les utilisateurs d'Internet devraient continuer à protéger leurs activités avec de bonnes solutions de sécurité valables pour les ordinateurs et les appareils mobiles », conclut Lukáš Štefanko.
Source : ESET

Pour protéger vos équipements, nous recommandons l'application suivante :

Réagissez à cet article

Pokémon Go, le nouveau jeu

favori des spammeurs

Pokémon Go, le nouveau jeu favori des spammeurs

La distribution de malwares à travers Pokémon Go est aujourd'hui supplantée par des campagnes de spam par SMS.
Pokémon Go, le jeu star de l'été qui fait exploser les revenus de son concepteur Niantic et des stores d'applications (il aurait généré plus de 200 millions de dollars en un mois avec 100 millions de téléchargements), est une aubaine pour les pirates. Lesquels n'hésitent pas à profiter de la popularité du jeu de réalité augmentée pour multiplier les tentatives d'arnaques.

Captures du SMS et du site vers lequel renvoie le lien.

AdaptiveMobile, société spécialisée dans la sécurité mobile, relève aujourd'hui une campagne de spam par SMS invitant les destinataires à se rendre sur un faux site baptisé Pokemonpromo.xxx. La campagne semble se concentrer pour l'heure sur les joueurs d'Amérique du Nord. *« Il s'agit d'un site de phishing sophistiqué qui imite fidèlement le vrai site Pokémon GO. Il prétend fournir à l'utilisateur des fonctionnalités supplémentaires au jeu s'il référence 10 de ses amis (susceptibles d'être à leur tour spammés) »*, indique AdaptiveMobile dans un billet de blog daté du 17 août. Le site, signalé pour ses activités de phishing, n'est plus actif aujourd'hui.

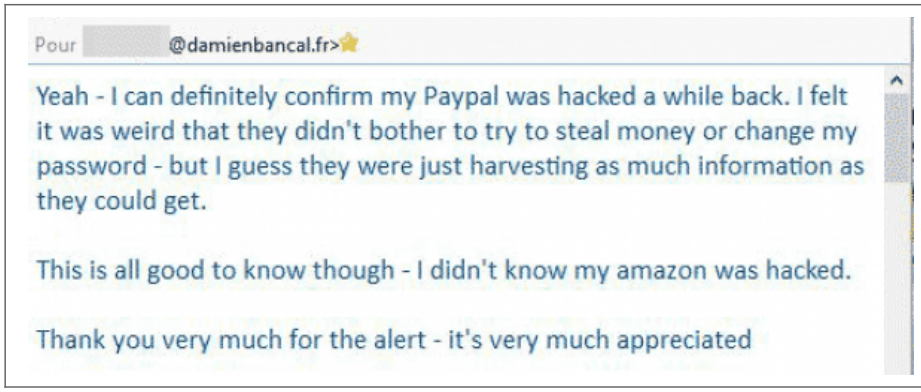
Multiplication des campagnes de spam

Mais ce n'est pas le seul dans le genre. Une autre campagne de phishing par SMS propose par exemple 14 500 Pokecoins (la monnaie virtuelle du jeu utilisée pour des achats internes) pour 100 points collectés et pointe vers d'autres sites de spam (dédiés ou non au jeu de Niantic) depuis une URL raccourcie. Citons par exemple Pokemon.vifppoints.xxxx ou Pokemon Generator… Autant de sites qui cherchent à leurrer l'utilisateur en l'invitant à fournir ses identifiants de connexion. Des sites promus par SMS comme depuis les réseaux sociaux et autres forums dédiés à Pokémon Go, précise le fournisseur de solutions de protection pour mobiles.
Autant de campagnes malveillantes qui ne se tariront pas avant que la popularité du jeu ne commence à décliner, estime AdaptiveMobile. D'ici là, les utilisateurs sont invités à redoubler de prudence, surtout s'ils reçoivent un message (SMS ou autre) accompagné d'un lien vers un site web. *« Méfiez-vous des messages SMS non sollicités que vous recevez et qui mentionnent l'application »*, rappelle l'entreprise dans son billet.
Les campagnes de spam ne sont pas les seuls dangers qui guettent les joueurs de Pokémon Go. Mi juillet, les cybercriminels profitaient de l'absence du jeu dans les stores de certains marchés, dont la France, pour distribuer le fichier .APK de la version Android de l'application. Fichier évidemment compromis par le malware DroidJack (ou SandroRAT) qui ouvrait grandes les portes du système infecté aux attaquants. Plus récemment, début août, l'Anssi (Agence nationale de la sécurité des systèmes d'information) y allait de son grain de sel en alertant sur les risques liés à Pokémon Go. De quoi nous gâcher l'envie de jouer…
Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Pokémon Go, le nouveau jeu favori des spammeurs

Votre vie privée numérique en danger sur Leakedsource



Votre vie privée numérique en danger sur Leakedsource

Depuis quelques semaines, le site leakedsource engrange des centaines de millions de données volées par des pirates informatiques. Un business juteux qui met en danger des millions d'internautes.

LeakedSource, nouvelle source d'informations pour pirates informatiques ? Souvenez-vous, on vous parlait en juillet, de données volées appartenant à un ancien garde du corps de Vladimir Poutine, le Président Russe, ou encore de Nicolas Sarkozy, ancien Président de la République Française. Son identité, ses données privées, des courriels… Un piratage qui semblait être particulièrement compliqué à orchestrer tant les sources d'informations concernant ce body guard étaient variés. Après enquête, j'ai découvert que si le résultat pouvait être particulièrement préjudiciable pour la cible, la mise en place et l'exécution de cette attaque était aussi simple que « *1 + 1 font 2*« .

Leakedsource, source quasi inépuisable de malveillances

Pour ce garde du corps, mais aussi pour de nombreuses personnalités, le risque est énorme. Tout débute par le piratage de centaines de bases de données de part le monde. Myspace, Adobe, Linkedin, Twitch , Xat , Badoo… ne sont que des exemples parmi d'autres. Je gère, avec le protocole d'alerte ZATAZ, des dizaines de fuites de données par mois concernant des PME et entreprises Françaises. Imaginez donc ce que brassent des sites comme leaked source.

Leakedsource.com, un espace web tenu par des Russes, a pour mission de regrouper les informations volées par des pirates et de permettre de consulter les informations en question. Les administrateurs du portail expliquent que leur service est fait pour s'assurer que les données volées ne vous concernent pas. Sauf que, des données, il y en a des centaines de millions, et vous pourriez bien vous y retrouver, comme Mark Zuckerberg, cofondateur et directeur général de Facebook, piraté en juin 2016 parce que son mot de passe « *DaDaDa* » était accessible dans une base de données piratées et stockées chez Leakedsource.

Vous ne risquez rien ? Vraiment ?

Cela n'arrive qu'aux autres ? Allez donc regarder du côté de vos données. C'est d'ailleurs ce qu'aurait dû faire l'auteur des jeux vidéo Garrysmod et de Rust, Garry Newman. J'ai pu avoir une longue conversation avec l'auteur de divertissements vidéo ludique qui ne s'attendaient pas à découvrir sa vie numérique mise en pâture de la sorte. Il faut dire aussi que plusieurs pirates ont contacté la rédaction de ZATAZ.COM pour se vanter d'avoir mis la main sur ses données Paypal, Amazon, gMail de ce créateur de jeux vidéo britannique. Bref, pour 4 dollars (le prix journalier d'un abonnement Leaked source pour accéder aux données) n'importe quel internaute peut se transformer en vulgaire violeur de vie 2.0. Il suffit de rentrer un mail, un pseudonyme ou encore une adresse IP et Leakedsource cherche dans ses bases de données la moindre concordance. Cerise sur le gâteau, quand le mot de passe est hashé, donc illisible à la première lecture, Leaked source propose la version du précieux sésame déchiffré. « ***Si les personnes [les pirates, NDR) sont malines, elles peuvent faire beaucoup de dégâts avec ce genre d'outil accessible à Monsieur tout le monde*** » me confirme un utilisateur.

Que faire pour éviter ce type de fuite de données ?

Je vais très rapidement être honnête avec vous, si vous mettez vos données en ligne, dites vous qu'elles ne sont plus en sécurité. Et ce n'est pas notre vénérable CNIL qui pourra vous aider. Avec plusieurs centaines de cas de fuite de données que je traite avec le protocole d'alerte de zataz par an, j'ai déjà pu croiser mes propres informations. Je vous parlais plus haut de Leakedsource, j'ai pu y retrouver mon compte Adobe. Pourtant, le géant du logiciel l'avait juré, il était « *secure* » [sécurisé, ndr].

Tellement « *secure* » qu'un de mes mails, et le mot de passe attenant, sont disponible dans ce big data du malveillant. Autant dire que l'adresse mail et le mot de passe en question ont été détruits et ne seront plus utilisés.

Que faire donc ? D'abord, un compte mail par service. Je sais, c'est long est fastidieux. Mais je pense qu'il va être beaucoup plus long et fastidieux pour Garry Newman de revalider l'ensemble de ses comptes « infiltrés », car il utilisait la même adresse électronique pour ses accès Paypal, Amazon…

Ensuite, ne mettez pas le même mot de passe pour l'ensemble de vos services en ligne. On a beau le répéter, cesser de vous croire plus malin que les 010101 qui nous régissent. Mark Zuckerberg et son « *DaDaDa* » lui ont coûté son Twitter et son Pinterest. Pour Garry, plus grave encore, son compte Amazon et Paypal, avec des données sensibles [adresses postales, données bancaires…] qui ne devraient pas être disponibles à la planètes web. Donc, oui, c'est fastidieux, mais un mot de passe par compte est une obligation.

Pour finir, en ce qui concerne l'IP, n'hésitez plus à utiliser un VPN. L'outil permet de cacher votre véritable adresse de connexion, en plus de chiffrer vos informations transitant sur la toile. Je vous invite à regarder du côté de nos partenaires et amis de chez **NoLimitVPN** ou encore HMA! pour blinder vos connexions PC, Mac et mobiles.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Leakedsource, le site qui met en danger votre vie privée – ZATAZ

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d’Ivoire à l’honneur au Maroc, du 21 au 24 septembre 2016

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d’Ivoire à l’honneur au Maroc, du 21 au 24 septembre 2016

Le Sénégal et la Côte d'Ivoire, qui compte parmi les pays d'Afrique subsaharienne à avoir engagé des projets de gouvernance électronique, seront à l'honneur au Maroc lors de la première édition du Salon de l'innovation et de la transformation digitale en Afrique, « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à Casablanca.

Dans un communiqué transmis à notre Rédaction, la **Fédération marocaine des technologies de l'information, des télécommunications et de l'Offshoring (APEBI),** chef d'orchestre de l'AFRICA IT EXPO, explique le choix du Sénégal et de la Côte d'Ivoire par le souci d'établir une connexion sud-sud des ressources du continent. Un défi majeur que le Royaume chérifien veut relever en commençant par ces deux pays qui sont la locomotive économique de la sous-région ouest-africaine. La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an. Une performance portée en partie par un secteur privé qui fait de la transformation numérique, un vecteur de compétitivité. Le Sénégal, deuxième économie de l'Afrique de l'Ouest francophone derrière la Côte d'Ivoire, est plébiscitée pour les efforts fournis dans le domaine du digital. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016. En choisissant ces deux pays, le Maroc veut leur apporter son « soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique ».

Le communiqué :
« Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO » – 21 – 24 septembre 2016 à Casablanca
Le 1er salon de l'innovation et de la transformation digitale du continent met à l'honneur le Sénégal et la Côte d'Ivoire

La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI) organise la 1ère édition du Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à la foire internationale de Casablanca. « AITEX – AFRICA IT EXPO » est la première plateforme de l'innovation et de la transformation digitale en Afrique, qui va réunir 150 exposants – tous issus des entreprises référencées dans le domaine -, 200 donneurs d'ordre, mais aussi des experts et des utilisateurs venus d'Afrique, du Moyen Orient et d'Europe. Pour cette édition, l'APEBI met à l'honneur le Sénégal et la Côte d'Ivoire, deux pays amis avec lesquels le Royaume entretient des relations de longue date, qui constituent un modèle de coopération exemplaire, et qui jouent par ailleurs un rôle de locomotive en Afrique de l'Ouest dans le domaine des TIC.

Aujourd'hui, la transformation digitale est devenue un enjeu majeur pour les sociétés, une mutation indispensable pour les entreprises et l'économie. A l'ère du numérique, cette transformation constitue un avantage fort pour nos sociétés, qui crée de la valeur… L'évolution très rapide des TIC -Technologies de l'Information et de la Communication- a profondément façonné le changement de nos modes de vie. Face à la généralisation des TIC dans les pays industrialisés, l'intégration de ces compétences (mais surtout leur maîtrise et leur exploitation) est un enjeu stratégique, sociétal, culturel et technologique en Afrique.
Le continent, qui poursuit son processus de mondialisation et sa dynamique d'émergence doit se « mettre à niveau » pour améliorer l'efficience de son économie et « booster » sa compétitivité locale et internationale. Grâce à une approche bien encadrée, qui va intégrer tous les paramètres, les enjeux et aussi les risques induits, la transformation digitale est sans conteste un levier de croissance économique et de compétitivité, créateur de valeur ajoutée.
La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI), est un acteur régional stratégique en Afrique car elle regroupe des entreprises qui jouent un rôle clé dans l'économie et qui sont des références dans leur domaine.
Pendant trois jours, l'APEBI va être le catalyseur d'une dynamique nouvelle, qui va accélérer le développement du numérique dans le continent.

AITEX – AFRICA IT EXPO : Première plateforme de l'innovation et de la transformation digitale d'Afrique
Cette édition sera marquée par une forte présence d'experts de haut niveau, des opérateurs nationaux et internationaux reconnus, tous réunis autour d'un programme ambitieux qui a pour vocation d'être la première plateforme de l'innovation et de la transformation digitale en Afrique.
Organisé avec le soutien institutionnel de Maroc Export, le salon « AITEX – AFRICA IT EXPO » va accueillir principalement des distributeurs, des fournisseurs de technologie, des intégrateurs de solutions, éditeurs, opérateurs télécoms, ISP, ASP, délocalisation de fonctions de gestion, TMA, help desk conseil, offshoring, mobility, big data, Cloud, réseaux, e-Commerce… Vitrine de l'offre numérique et des dernières évolutions digitales, « AITEX – AFRICA IT EXPO » est une *plateforme* unique de rencontres, d'échanges et d'opportunités d'affaires.
Véritable révélateur des nouvelles tendances, le Salon «AITEX – AFRICA IT EXPO » est une occasion unique de rencontrer et d'échanger sur les problématiques quotidiennes des entrepreneurs, collectivités et de trouver les réponses appropriées grâce au concours de spécialistes, eux-mêmes engagés dans les processus de développement des économies émergentes et de la coopération sud-sud.
Placé sous le thème, «Transformation Digitale : Levier de développement en Afrique», le salon offre une nouvelle occasion de conscientiser et sensibiliser nos sociétés sur la formidable opportunité offerte par les technologies numériques pour accélérer le développement du continent. Des rencontres sont organisées au cours de ces trois journées pour débattre des problématiques actuelles et des enjeux sociétaux de ces mutations afin d'adopter les meilleures pratiques et ainsi anticiper les défis auxquels les entreprises et économies africaines sont confrontées.
«AITEX – AFRICA IT EXPO » va promouvoir les relations d'affaires et la mise en réseau des différents acteurs économiques du continent, à travers des coopérations sud-sud, nord-sud et public-privé.

Le Sénégal et la Côte d'Ivoire à l'honneur
Le défi numérique en Afrique passe inéluctablement par la connexion des ressources du continent. Un aspect *que l'APEBI a compris et intégré dans l'organisation de ce salon, c'est pourquoi la fédération a décidé de mettre à l'honneur, pour sa première édition, le Sénégal et la Côte d'Ivoire.* Ces deux pays, représentant deux premières puissances économiques de l'Afrique de l'ouest francophone engagés dans une dynamique de croissance depuis plusieurs années, ont à cœur de poursuivent respectivement leurs ambitions numériques.
La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an et le développement du numérique est devenu un enjeu majeur, créateur de richesses. Le numérique constitue un potentiel énorme, présent dans tous les esprits, aussi bien du côté du gouvernement que des dirigeants d'entreprise. Selon une étude publiée par le cabinet Deloitte en mai 2016, seulement 36 % des entreprises estiment avoir atteint la maturité numérique.
Le Sénégal, quatrième économie de la sous-région ouest africaine après le Nigéria, la Côte d'Ivoire et le Ghana, et deuxième économie en Afrique de l'Ouest francophone derrière la Côte d'Ivoire s'est largement distingué dans l'évolution de l'économie numérique, premier levier de la transformation digitale. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016.
Le *Sénégal et la Côte d'Ivoire font partie des premiers pays africains à initier des* projets de gouvernance électronique (e-Gouv). Ils ont réalisé au fil des années des progrès importants dans les domaines tels l'économie numérique, la monétique, le courrier hybride, ou encore le taux de connectivité internet, etc.) Néanmoins, les disparités qui existent entre les différents pays du continent peuvent être réduites si un effort de coopération est accompli.
En mettant en avant ces deux pays amis, qui constituent un modèle important d'exemplarité sur le continent africain (et en particulier de ses voisins ouest-africains), le Maroc apporte son soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique. »
Article original de Cio-Mag

Original de l'article mis en page : « AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016 | CIO MAG

Certification des objets connectés de santé – Web des

Objets

Certification des objets connectés de santé

De l'objet connecté de bien-être à l'objet connecté de santé : une certification qui a du sens

Très répandus sur le marché, les objets connectés de bien-être ont pour vocation de développer un état de satisfaction morale ou physique, sans obligation de mesurabilité ni de résultats cliniques. Les données de bien-être peuvent être observées sur le long terme pour mieux déterminer l'état de santé d'un patient. De nombreux objets connectés de santé sont en développement, afin de fournir des données quantifiables et médicalement fiables. L'usage de ces objets se fait notamment dans un but nommé le « quantified self ». C'est une collaboration entre utilisateurs et fabricants d'outils qui partagent un intérêt pour la connaissance de soi à travers la mesure et la traçabilité de soi. Des objets connectés tels que la balance Polar connectée pour suivre son poids ou le capteur Withings Go permettant de mesurer son activité physique et de suivre ses cycles de sommeil sont des outils qui s'intégrent dans cette démarche.

« La frontière entre les domaines du bien-être et de la santé va s'estomper. L'objectif est que demain, les gens disent que c'est eux qui prennent soin de leur santé, avec l'aide de leur médecin et non plus leur médecin seul. Le patient devient expert, le médecin va devoir le prendre comme un partenaire. »
Cédric Hutchings, PDG de Withings ***(Cahiers IP n°2 : Le corps, nouvel objet connecté)****.*

L'objet connecté de santé en tant que dispositif médical, qu'est-ce que c'est ?

Les objets connectés de santé sont classés dans la catégorie des ***dispositifs médicaux*** *pour l'ANSM et la CNIL. Adrien Rousseaux, expert en protection des données à caractère privé à la CNIL, apporte des éléments permettant de mieux comprendre les enjeux de la certification.*
Selon l'ANSM*, est considéré comme* ***dispositif médical*** *« tout instrument, appareil, équipement, logiciel, matière ou autre article, utilisé seul ou en association, y compris le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostique et/ou thérapeutique, et nécessaire au bon fonctionnement de celui-ci. Le dispositif médical est destiné par le fabricant à être utilisé chez l'homme à des fins de diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie, d'une blessure ou d'un handicap ; mais aussi d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique. Son action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais sa fonction peut être assistée par de tels moyens » (directive européenne 93/42/CEE).*
Pour la CNIL*, c'est l'utilisation ou l'exploitation des données recueillies par les objets connectés de santé, ou de bien être, qui fait intervenir la loi Informatique et Libertés.*

Il n'y a pas de définition dans la loi française d'une donnée de santé permettant de la distinguer de la donnée de bien-être. Mais le ***règlement européen relatif à la protection des données personnelles****, adopté le 14 avril dernier, et qui sera applicable en 2018, apporte une définition légale qui toutefois n'est pas opposable (ne peut être utilisée comme argument juridique) mais le sera d'ici son application.* ***L'article 4 de ce règlement européen définit les données de santé*** *comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris les prestations de services, de soins de santé qui révèlent des informations sur l'état de santé de cette personne. »*
Des objets connectés de santé sont déjà commercialisés en tant que dispositifs médicaux :
Le Tensiomètre Bluetooth de Withings *se connecte aux smartphones et mesure la pression systolique, diastolique ainsi que le rythme cardiaque. Cet appareil a obtenu la certification européenne CE, il est donc certifié comme dispositif médical.*
L'électro-stimulateur connecté MyTens *de BewellConnect développé avec le laboratoire Visiomed se connecte aux smartphones et stimule des zones précises du corps avec des électrodes pour réduire les douleurs. Il est remboursé par la sécurité sociale, donc reconnu comme dispositif médical.*
MyECG, l'électrocardiogramme connecté *de BewellConnect développé avec le laboratoire Visiomed se connecte au smartphone et mesure la fréquence cardiaque. Il a reçu le marquage CE, ce qui en fait également un dispositif médical certifié.*

Tensiomètre sans fil de Withings, MyTens et MyECG de BewellConnect (Visiomed)

Quelles étapes pour certifier un objet de santé, dispositif médical ?

Afin de certifier un objet connecté comme dispositif médical, le fabricant doit d'abord constituer un dossier auprès d'un ***organisme notifié****. Ce dernier évalue la conformité aux exigences essentielles et délivre le certificat européen de marquage CE.*
La donnée de santé cible un risque de maladie. Les données issues d'un dispositif médical certifié peuvent être utilisées par un professionnel de santé. Les formalités auprès de la CNIL ne sont pas les mêmes pour un traitement de données de bien-être et un traitement de données de santé. En effet, les données de santé sont dites "sensibles" d'après l'article 8 de la loi Informatique et Libertés. Pour un objet connecté de bien-être, ne comportant donc pas de données de santé ou pour lequel le consentement de l'utilisateur est demandé, ***les formalités sont déclaratives****. Même si le traitement des données doit respecter la loi Informatique et Libertés (notamment le respect des droits des personnes à pouvoir s'opposer, à pouvoir rectifier ou tout simplement à pouvoir être informé et la mise en place de mesures de sécurité adaptées), l'entreprise doit simplement signaler les modalités d'usage à la CNIL. Pour les objets connectés de santé, ou de bien-être utilisant des données de santé, les* ***formalités nécessitent une autorisation de la CNIL*** *avant de pouvoir proposer le service délivré par l'objet connecté. En moyenne, les procédures prennent de 2 à 6 mois selon la disponibilité du responsable de traitement. Ce dernier est la personne ou l'entité qui définit le service proposé par un dispositif médical, et donc qui gère la transmission de données générées par ce dispositif médical à un serveur, le stockage des données, etc. Un certain nombre d'informations sont à fournir à l'usager d'après* ***l'article 32 de la loi informatique et libertés****. « La personne auprès de laquelle sont recueillies les données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le* ***responsable de traitement*** *ou son représentant :*
• De l'identité du responsable de traitement (qui va effectuer les traitements sur les données)
• Des finalités poursuivies par le traitement
• Du caractère obligatoire ou facultatif des réponses
• Des conséquences éventuelles d'un défaut de réponses (par exemple le service ne pourra pas être rendu dans son intégralité)
• Des destinataires ou catégories de destinataires des données
• Des droits de l'utilisateur sur ces données »
Le site de la CNIL propose un ***générateur de mentions "informatique et libertés"*** *équivalent aux mentions légales.*

Les intérêts de la certification pour l'utilisateur et le distributeur

Toutes ces démarches visent à protéger l'utilisateur de tout mésusage des dispositifs médicaux. C'est cette « digitalovigilance » qui garantit une communication maîtrisée des données de santé aux personnes souhaitées. L'usager ayant enregistré des données doit avoir connaissance des destinataires s'il y a transmission et il doit pouvoir maîtriser à qui il envoie quelles données.
*Sur de nombreux appareils, le système d'****API (Application Programming Interface = interface pour l'accès programmé aux applications)*** *permet à l'utilisateur de partager la donnée qui a été générée par un capteur avec un nouveau service, une application. Il peut à tout moment déconnecter les applications pour que les données cessent d'être transmises.*
*De nombreuses données transmises par les dispositifs médicaux peuvent être très utiles, dans le cadre de la recherche notamment. L'intérêt majeur de la certification des données de santé est donc qu'****elles peuvent être utilisées par des professionnels de santé****. De plus, un objet certifié dispositif médical peut être vendu en pharmacie : il peut être prescrit par un professionnel de santé et donc potentiellement pris en charge par la sécurité sociale.*

Bluetens et Beta-bioled : deux objets connectés vers la certification

Électrostimulateur connecté Bluetens / Test sanguin portable connecté Beta-Bioled

La société ***Bluetens*** *a développé un* ***électrostimulateur connecté*** *pour* ***soulager la douleur et se relaxer****. Son objectif premier est de créer un objet de santé qui se définit par sa fonction et son utilité. Il doit apporter plus que de l'analyse ou de la collecte de données. L'objectif est un réel changement d'état de l'utilisateur, l'objet doit avoir un impact remarquable sur la santé. L'électrostimulateur Bluetens est certifié ISO 13485 par une société de certification qui effectue un audit d'une part auprès de l'entreprise Bluetens, et d'autre part sur l'objet connecté de santé. Dans ce cas, c'est l'entreprise allemande TÜV agréée par les autorités européennes qui a certifié l'objet. L'ISO 13485 atteste que l'entreprise Bluetens respecte bien les normes nécessaires à l'élaboration de dispositifs médicaux. Cet appareil est donc certifié d'utilité médicale. Le but de l'entreprise étant de le distribuer le plus largement possible, il est vendu dans les enseignes de grande distribution spécialisées telles que Darty ou la Fnac.*
De son côté, la société ***Archimej Technology*** *est en train de développer* ***Beta-Bioled****,* ***un test sanguin portable et connecté****. Cette entreprise cherche à insérer sur le marché des dispositifs médicaux en franchissant toutes les étapes de la certification jusqu'à obtenir les agréments de la sécurité sociale pour que l'appareil puisse être remboursé. Cette démarche s'inscrit dans une volonté d'asseoir la crédibilité de Beta-Bioled face aux utilisateurs et au corps médical. Le processus de certification passe ici par 3 étapes dont la première est la formation auprès d'organismes spécialisés. Le biocluster Genopole leur apporte les conseils sur les questions des biotechnologies et Medicen facilite l'insertion d'innovations dans le domaine de la santé humaine vers les marchés industriels. La seconde étape, une fois l'objet conceptualisé et réalisé, consiste à réaliser des essais cliniques avec quelques milliers de tests dans des structures médicales. Enfin, l'objet sera certifié uniquement lorsque la Haute Autorité de Santé (HAS) aura validé toute la procédure. Et pour assurer une diffusion optimale dans le parcours médical, Archimej Technology souhaite obtenir l'agrément LPPR (Liste des Produits et Prestations Remboursables), qui permettra un remboursement de Beta-Bioled par l'Assurance Maladie. Ce parcours du combattant assurant une crédibilité et une valeur médicale peut prendre plusieurs années : l'objectif de mise sur le marché est fixé à 2018. En premier lieu, il sera distribué aux professionnels de santé (urgences, SAMU, maisons de retraite…). Ensuite la vente sera ouverte au grand public pour les malades chroniques, invalides légers ou séniors ne pouvant se déplacer en laboratoires. A terme l'objectif est de cibler les pharmacies comme canaux de distribution.*

Article original de Charles Deyrieux

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

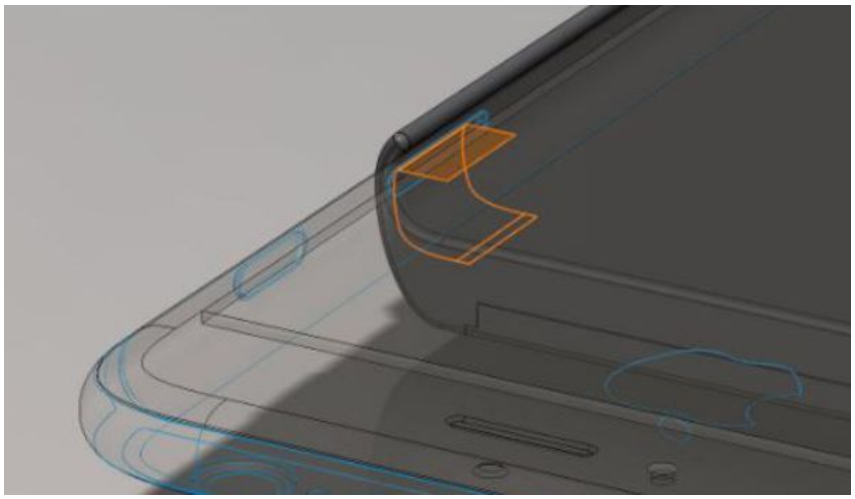
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Certification des objets connectés de santé – Web des Objets

---

Snowden conçoit une coque d’iPhone anti-espionnage – L’Express L’Expansion

	**Snowden conçoit une coque d’iPhone anti-espionnage**

Cette coque a pour objectif de protéger les données de nos smartphones. Un premier prototype sera rendu public d'ici un an.

Edward Snowden continue son combat contre la surveillance. L'ancien analyste de la NSA et lanceur d'alerte, qui a levé le voile sur les pratiques d'écoute massive à travers le monde, travaille à la réalisation d'une nouvelle coque d'iPhone. Son atout: elle est capable de protéger les données du téléphone qu'elle abrite.

Pour ce projet, Edward Snowden s'est associé au hacker Andrew « Bunnie » Huang. Dans un rapport, les deux hommes précisent que le mode avion est loin d'être efficace contre le piratage. « Croire au mode avion d'un téléphone hacké équivaut à laisser une personne ivre juger de sa capacité à conduire », indiquent-ils.

Contrôler les signaux envoyés à l'iPhone

Le système, encore au stade d'étude, a été présenté à l'occasion d'une conférence le 21 juillet. L'objet est un périphérique sous logiciel libre qui se pose à l'emplacement de la carte SIM. Il permet ensuite de contrôler les signaux électriques envoyés aux antennes internes du téléphone et donc de savoir si le téléphone partage des informations avec des tiers, sans que vous en soyez conscients.

Une alerte est envoyée dès lors qu'une transmission anormale est détectée.
Mashable explique que « lorsque le mode avion est activé et que les connexions réseaux sont supposées être désactivées, une alerte est envoyée dès lors qu'une transmission anormale est détectée ». L'anomalie repérée, le périphérique peut même éteindre le téléphone immédiatement.

Journaliste, activiste et lanceur d'alerte

L'outil, dont le premier prototype devrait être rendu public d'ici un an, a été pensé pour venir en aide aux journalistes, activistes et lanceurs d'alerte « pour détecter quand leurs smartphones sont surveillés et trahissent leurs localisations ».

Le programme d'espionnage américain de la NSA, révélé par Edward Snowden a, permis la collecte de données personnelles de millions de citoyens, ainsi que des institutions et chefs d'Etats étrangers. Ces révélations ont montré que ces collectes dépassaient le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques.

Article original de l'express

Réagissez à cet article

Original de l’article mis en page : Snowden conçoit une coque d’iPhone anti-espionnage – L’Express L’Expansion

---

Ma vie disséquée à travers mes données personnelles

	Ma vie disséquée à travers mes données personnelles

---

Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

150 Go de données médicales volées seraient dans la nature !

150 Go de données médicales volées seraient dans la nature !

Un pirate (ou un groupe) aurait mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie américain, contenant des données précises sur le suivi de patients. Une tendance de plus en plus répandue outre-Atlantique.

Les données médicales semblent prisées des pirates. Un (groupe de) pirate(s), nommé Pravvy Sector, aurait ainsi mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie de l'Ohio, rapportait hier Motherboard. Le contenu trouvé concernerait à la fois les cliniques elles-mêmes (avec des données sur ses ressources humaines) et les patients, avec des indications précises sur leur suivi médical, leur traitement ou encore leurs informations d'assurance.

Motherboard a contacté trois patients présents dans le fichier identifié, dont deux ont pu confirmer que les informations publiées étaient exactes pour eux. L'origine des données, qui semblent bien venir du réseau de cliniques lui-même, n'a pas pu être confirmée. Contactée par le site américain, l'organisation n'a pas encore répondu à ses demandes de commentaires.

Bien avant cette publication, Pravvy Sector aurait été en quête de reconnaissance, contactant directement certains médias avec les contenus de « fuites » précédentes. Mais le plus important est la tendance que deviennent les incidents liés aux données médicales. Comme le relève The Verge, 49 intrusions affectant plus de 500 personnes ont été signalées dans le secteur médical, depuis le début de l'année.

En juin, une autre fuite présumée concernait 655 000 enregistements médicaux, via plusieurs organismes. Si l'ensemble des données n'a pas pu être authentifié, un échantillon l'avait été à l'époque par Motherboard. Contrairement à la publication de Pravvy Sector, les informations étaient cette fois vendues sur un site spécialisé.

Article original de Guénaël Pépin

Réagissez à cet article

Original de l'article mis en page : États-Unis : 150 Go de données médicales seraient dans la nature

L’ANSSI alerte sur les risques liés à Pokémon Go

L’ANSSI alerte sur les risques liés à Pokémon Go

Face au phénomène Pokémon Go, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) a publié un bulletin de sécurité sur l'installation et l'usage de cette application.

Devant l'ampleur du phénomène (près de 100 millions de téléchargements), l'application Pokémon Go pose quelques problèmes de sécurité. L'ANSSI (en quelque sorte le Gardien de la sécurité des Systèmes d'Information des Organisme d'Importance Vitale, des Organes et Entreprise de l'état Français selon Denis JACOPINI expert Informatique assermenté spécialisé en cybercriminalité) ne pouvait pas rester sourde à cette question et vient de publier via le CERT-FR un bulletin de sécurité dédié aux « *cyber-risques liés à l'installation et l'usage de l'application Pokémon Go* ».

Applications malveillantes et collectes de données

Dans ce bulletin, il est rappelé qu'avec le succès, de nombreuses fausses applications se sont créées. Le CERT-FR en a recensé 215 au 15 juillet 2016. Elles sont surtout présentes dans les pays où le jeu n'est pas présent. Il recommande donc de ne pas télécharger cette application sur des sites tiers, et de n'installer que les versions originales disponibles sur Google Play ou l'Apple Store. Nous nous étions fait l'écho de la disponibilité d'APK Pokémon Go pour Android qui contenait des malwares. Le bulletin constate aussi que Niantic a résolu le problème de permission qui exigeait un accès complet au profil Google de l'utilisateur.

Sur les données personnelles, l'ANSSI observe comme beaucoup d'autres organisations que Pokémon Go collecte en permanence de nombreuses données personnelles. Informations d'identité liées à un compte Google, position du joueur par GPS, etc. L'UFC-Que Choisir avait récemment alerté sur cette question de la collecte des données. La semaine dernière la CNIL a publié un document concernant « jeux sur votre smartphone, quand c'est gratuit… » où elle constatait que ce type d'application était très gourmande en données. L'ANSSI préconise la désactivation du mode « réalité augmentée » lors de la phase de capture d'un Pokémon.

BYOD et Pokémon Go, le pouvoir de dire non

L'ANSSI répond sur le lien qu'il peut y avoir entre le BYOD (Bring Your Own Device), c'est-à-dire l'utilisation de son terminal personnel dans un cadre professionnel et Pokémon Go. Le CERT-FR constate qu'il est « *tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capturer un Ronflex (un Pokémon rare à trouver)* ». Surtout quand la demande émane d'un VIP et qu'il est souvent difficile de refuser. Eh bien comme Patrick Pailloux (prédécesseur de Guillaume Poupard à la tête de l'ANSSI) l'avait dit en son temps, il faut avoir le pouvoir de dire non à l'installation de ce type d'application dans un environnement professionnel.

Toujours dans le cadre du travail, l'agence déconseille l'usage de l'application dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles).

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : L’ANSSI alerte sur les risques liés à Pokémon Go