# Caméras IP installées par des incompétents ? Une aubaine pour les pirates

| | |
|---|---|
|  | Caméras IP installées par des incompétents ? Une aubaine pour les pirates |

**Le piratage des caméras de vidéo surveillance, un jeu d'enfant pour les plus dégourdis du web. Sauf que ces pirates n'ont rien de génie, ils profitent uniquement de la fainéantise des utilisateurs.**

Le piratage des caméras de vidéo surveillance n'est pas nouveau. Je vous parlais déjà de ces infiltrations de webcams en 2000. En novembre 2015, par exemple, je revenais sur un fichier contenant des centaines de webcams non sécurisées vendues dans le blackmarket ou encore de ce bébé réveillé par des hurlements d'un idiot du village ayant pris la main sur le baby phone de la famille.

En 2014, je vous révélais la création d'un site Internet Russe qui référencent plusieurs dizaines de milliers de webcams. Bref, un business juteux pour les commerçants du voyeurisme et autres vendeurs de données sensibles (La boutique est-elle vide ? Le hangar stocke en ce moment des téléphones portables ; la banque vient d'être livrée en billets frais…).

Je te soupçonne de taper dans la caisse ! (Boutique de la Ville de Rai)

La sécurité des caméras sur IP est souvent mise à la mal comme j'ai pu le montrer dans ZATAZWeb.tv de mars 2014. Il ne devrait pas être si facile, normalement, de regarder dans la chambre d'un étranger, et encore moins dans des centaines de chambres filmées par ces caméras de vidéo surveillance. Pourtant, cela reste possible comme je vais vous l'expliquer plus bas.

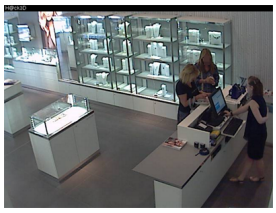
Montrez moi votre contrat, que je vous renseigne. (Boutique du 92)

**Failles et mots de passe facilitent le piratage des caméras de vidéo de surveillance**

Pour accéder à une caméra de vidéo surveillance rien de plus facile. D'abord avoir l'IP de la cible. Un détail pour les adeptes du social engineering. Autant dire que cette adresse n'est à communiquer à personne. Lisez le mode d'emploi de votre caméra. Chercher les options de sécurité proposées. Soyons honnête, plus votre webcam IP aura d'option, plus elle sera coûteuse. Mais la réflexion vaut, je pense, la sécurité de ce que vous souhaitez protéger. Ensuite, le malveillant va rechercher la marque de votre matériel. Pour cela, rien de plus simple une fois encore. La page d'accès à l'administration de votre matériel parle.


Mais tu vas le changer ce password… c'est marqué en GRAS ! (Hôtel du 77)

Un conseil, faites de manière à ce qu'elle ne soit pas lisible : un Htaccess par exemple, ou modifier le logo et toutes marques de reconnaissance pour le malveillant. Ensuite, le mot de passe. Trop de webcam IP, de caméras de vidéo surveillance gardent le mot de passe usine. Je vous laisse imaginer la facilité déconcertante que de retrouver ce sésame dans les notices et listes disponibles sur la toile. Un *admin:admin ; root:root et autre admin:0000* sont légions. Des clés qui se changent. Vous le faites bien quand vous perdez les clés de votre maison, faites le sur Internet. Enfin, les failles. Assurez-vous que votre cerbère ne soit pas référencé comme étant un outil « *open bar*« . Pour cela, un petit coup de Google ou ne soyez pas timide, posez la question !




La bijouterie est vide ! Le matériel, la caisse, le coffre sont repérés. Autant d'informations qui faciliteront l'action d'un malveillant. Vous aurez remarqué le petit « H@ck3D » en haut à gauche qui ne semble perturber personne !

**Branleurs, voleurs, mateurs… même combat**

Dans mon exemple, le pirate possède donc dorénavant l'IP, l'accès à la page d'administration de votre webcam IP, sa marque, vous n'avez pas changé le mot de passe usine et si c'est le cas, il vient de rechercher sur la toile les failles et accès « *pasvraimentprévudanslemodedemploi*« . Dernier exemple en date que ZATAZ a pu constater, l'alerte au sujet de la société AXIS. Un logiciel pirate, baptisé « *Hack AXIS* » permettait (permet toujours pour les caméras non mises à jour, NDR) d'accéder à la racine des périphériques sans avoir besoin de connaitre le mot de passe ; changer le mot de passe du matériel ; contrôler la caméra et, dans ce cas, lancer des attaques via la caméra transformée en Zombie/botnet. La caméra prise en main de la sorte par un pirate au fait de la faille, même mise à jour ensuite, restait dans le sac à malveillance de l'intrus. Une attaque d'autant plus gênante que l'exploit a été diffusé, en juillet 2016.

Bref, voilà donc le pirate avec une nouvelle source d'information à votre sujet. Imaginez, le serveur et l'IP l'oriente sur votre situation numérique ; la caméra, et les informations qu'elle peut transporter, fournissent au malveillant les yeux qu'il n'avait pas. En France, c'est une liste de plusieurs milliers de webcams accessibles qui trainent sur la toile, que ce soit dans le blackmarket ou sur des sites offrant de regarder à travers ces « yeux » non sécurisés.

Auteur : Damien Bancal

---



Réagissez à cet article

Original de l’article mis en page : ZATAZ Vidéo surveillance : Vous n’en avez pas marre d’être des idiots du 2.0 – ZATAZ

---

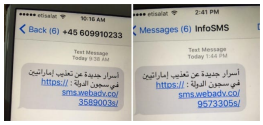
# Le malware Pegasus exploite 3 failles 0 day sur iPhone

Le malware Pegasus exploite 3 failles 0 day sur iPhone

---

**Les trois failles corrigées par Apple dans iOS 9.3.5 (ainsi que dans la dernière bêta d'iOS 10 livrée, contre toute attente, vendredi dernier) sont redoutables. Elles ont été exploitées par NSO Group, une société israélienne dont le fonds de commerce n'est autre que l'espionnage de journalistes et de militants. Le site Motherboard raconte la découverte de l'affaire qui relève du thriller…**

Ce 10 août, Ahmed Mansoor, un militant des droits de l'homme dans les Émirats Arabes Unis, reçoit sur son iPhone un message lui proposant d'en savoir plus sur de *«nouveaux secrets sur la torture dans les prisons d'État »*. Un lien accompagnait ce message, qu'il s'est bien gardé de lancer.




Les deux messages reçus par Mansoor — Cliquer pour agrandir

À la place, il a contacté un chercheur du Citizen Lab, un organisme de défense des droits numériques rattaché à l'université de Toronto. Aidé par Lookout, un spécialiste de la sécurité mobile, ils ont pu mettre au jour un mécanisme très élaboré de surveillance par iPhone interposé.
Si Mansoor avait touché le lien, il aurait provoqué le jailbreak de son iPhone et donné à NSO Group le plein contrôle de son smartphone. *« Un des logiciels de cyberespionnage parmi les plus sophistiqués que nous ayons jamais vus »*, expliquent les chercheurs.
NSO Group vient d'apparaitre sur les radars, mais cette entreprise très discrète (aucune présence sur internet) opère depuis 2010. Le malware qu'elle a mis au point, baptisé Pegasus, permet d'infecter un iPhone, d'intercepter et de voler les données et les communications. Une arme redoutable, qualifiée de *« fantôme »* par NSO pendant une de ses rares interventions publiques en 2013. Cette société vend Pegasus au plus offrant, notamment des gouvernements peu regardants sur les droits de l'homme.


Les données volées par Pegasus — Cliquer pour agrandir
NSO a visiblement pu pénétrer par effraction dans des iPhone depuis le modèle 5. Son malware est programmé avec des réglages qui remontent jusqu'à iOS 7.
Ces trois failles *zero day*, baptisées Trident par les chercheurs, ont été communiquées à Apple il y a dix jours. *« Nous avons été mis au courant de cette vulnérabilité et nous l'avons immédiatement corrigée avec iOS 9.3.5 »*, explique un porte-parole du constructeur. *« iOS reste toutefois le système d'exploitation mobile grand public le plus sécurisé disponible »*, rassure Dan Guido, patron de la société de sécurité informatique Trail Of Bits, qui travaille souvent avec la Pomme.
Il indique toutefois qu'il reste à améliorer le système de détection des vulnérabilités. Apple a annoncé début août un programme de chasse (rémunérée) aux failles.
Article original de Mickaël Bazoge

---



Réagissez à cet article

Original de l'article mis en page : Cyberspionnage : derrière les failles Trident d'iOS, le redoutable malware Pegasus | iGeneration

---

# Pokémon Go inquiète l'armée française !


Pokémon Go inquiète l'armée française !

---

**Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.**

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

*TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE*

*Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :*

- *« sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;*
- *les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;*
- *ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »*


*Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.*

*La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».*

*Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?*

*On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.*

*Article original de Omar Belkaab*

---

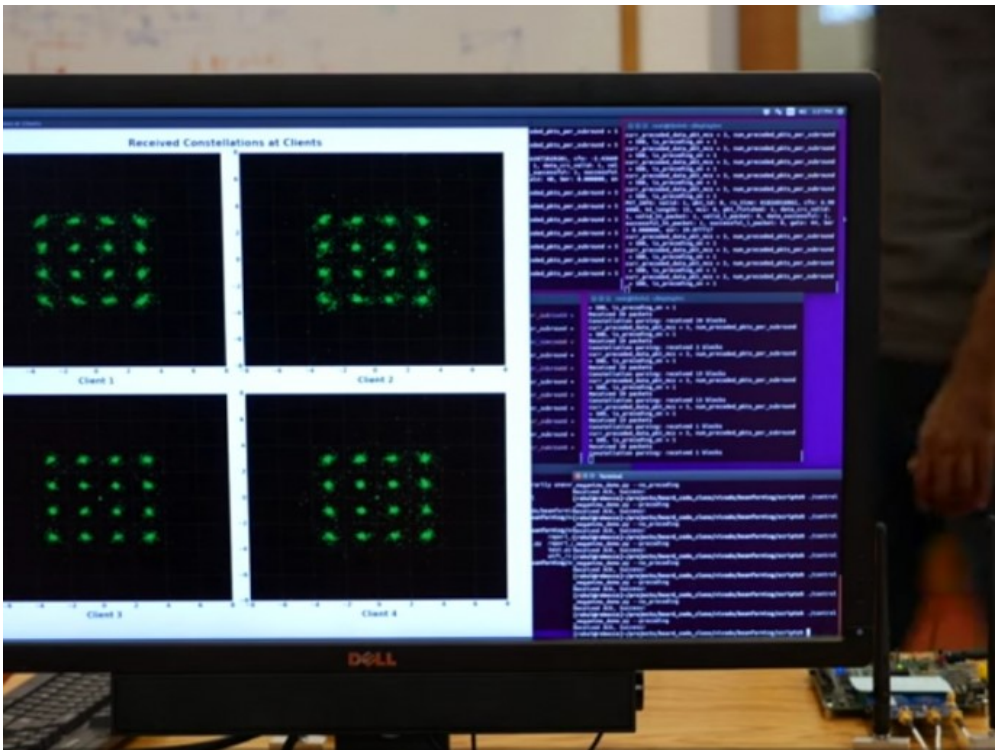


Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

# La vitesse de votre Wi-Fi

# sera bientôt multipliée par 3




**La vitesse de votre Wi-Fi sera bientôt multipliée par 3**

**Des chercheurs du MIT ont mis au point un système qui coordonne différents points d'accès Wifi environnants pour palier la congestion du trafic.**

Des chercheurs du CSAIL (Computer Science and Artificial Intelligence Lab au Massachussetts Institute of Technology) ont développé une technique qui améliore grandement les performances du Wifi et des communications sans fil plus généralement.

Ezzeldin Hamed, Hariharan Rahul, Mohammed Abdelghany et Dina Katabi présentent leurs travaux dans le cadre du ACM SIGCOMM 16 (Association for Computing Machinery's Special Interest Group on Data Communications), qui se tient au Brésil (à Florianópolis) jusqu'au 26 août. Ils entendent palier les risques de congestion qui peuvent survenir dans un réseau sans fil traditionnel quand deux points d'accès rapprochés émettant à la même fréquence risquent de causer des interférences.

Aujourd'hui, la solution pour éviter ces interférences consiste à traiter les requêtes les unes après les autres, ce qui restreint inévitablement l'envoi des données (même si, à haute fréquence de traitement, cela ne se perçoit pas tant que le point d'accès n'est pas saturé de connexions). Un peu comme si les supermarchés n'étaient équipés que d'une seule caisse obligeant les consommateurs à d'interminables queues pour payer leurs achats (même si la caissière est super rapide…). Les scientifiques du MIT ont donc envisagé une autre approche visant à coordonner de multiples points d'accès sans fil à la même fréquence sans créer d'interférences.

## Utiliser efficacement le spectre disponible

*« Dans le monde sans fil d'aujourd'hui, vous ne pouvez pas résoudre le problème de la contraction du spectre en multipliant les émetteurs, car ils continueront d'interférer les uns avec les autres*, explique Ezzeldin Hamed, selon des propos repris par le site de news du MIT. *La réponse tient dans une coordination de tous les points d'accès afin d'utiliser efficacement le spectre disponible. »* Et cette réponse se traduit par la mise au point du **dispositif MegaMIMO 2.0**, un boîtier de la taille d'un routeur traditionnel qui embarque processeur, système de traitement radio temps réel, émetteur-récepteur et, surtout, algorithmes maison.

Ces derniers génèrent un signal qui permet à de multiples émetteurs indépendants de transmettre des données sur la même ressource hertzienne à plusieurs points d'accès indépendants sans interférer les uns avec les autres grâce à une synchronisation de leur phase d'ondes. Autrement dit, une sorte de réseau MIMO distribué que nombre d'ingénieurs tenaient jusqu'à présent pour difficile à mettre au point. Mais l'équipe du CSAIL a fait une démonstration de l'efficacité du MegaMIMO 2.0, via une simulation de quatre ordinateurs portables en mouvement dans une salle de réunion. Il en ressort une augmentation des débits de 330 % par rapport à un système Wifi traditionnel (et même par rapport à leurs premiers travaux, MegaMIMO, présentés en 2012 et dans lesquels l'utilisateur devait fournir manuellement les informations sur les différentes fréquences). Sans oublier un doublement de la portée du signal. MegaMIMO permet même d'adapter le signal en fonction des obstacles environnants (par exemple lorsque quelqu'un se positionne entre l'émetteur et le récepteur).

## Applicable aux réseaux mobiles

Les chercheurs entendent poursuivre leurs travaux pour parvenir à coordonner des dizaines de routeurs sans fil afin de gérer toutes ces ressources comme une seule, ce qui devrait encore démultiplier les performances. Mais le système vise avant tout à palier les risques de congestion du réseau alors que ses usages progressent beaucoup plus vite que la disponibilité des ressources hertziennes.

Dans l'absolu, le MegaMIMO pourrait en effet parfaitement s'appliquer aux réseaux cellulaires. Et permettrait d'assurer des services mobiles de qualité dans les endroits particulièrement fréquentés, comme les stades lors des événements sportifs, les gares les jours de grève ou lors d'incidents de circulation des transports, etc. En attendant, les campus et grandes entreprises pourraient être les premiers à adopter le MegaMIMO pour fournir des accès Wifi efficaces… si le système est commercialisé un jour.

---



Original de l'article mis en page : MegaMIMO 2.0, le système qui multiplie par 3 les performances du Wi-Fi

# 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

# 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

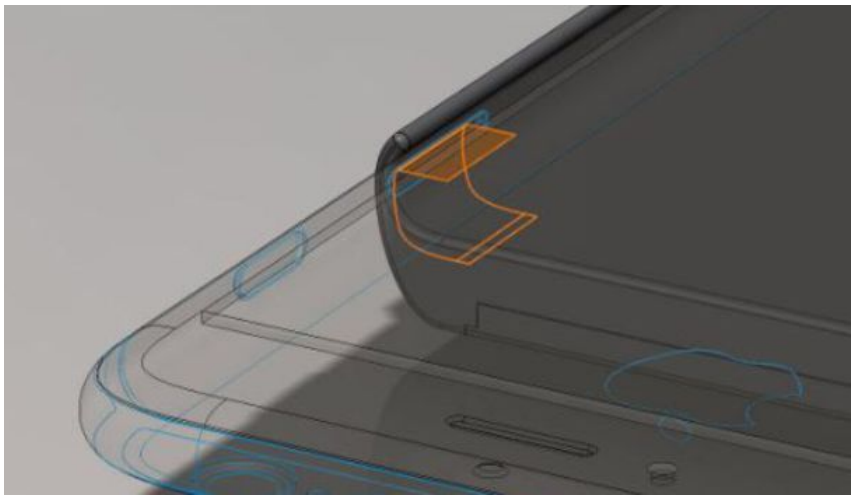
Contactez-nous


*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

---

# Attention à l’application « Rio Olympics 2016 «

## Attention à l’application « Rio Olympics 2016 «

---

**Avec l'approche des jeux Olympiques de Rio, le téléchargement d'applications thématiques va battre son plein. Gare aux applications dangereuses !**
**Rio Olympics 2016 Keyboard, un clavier publicitaire dangereux !**

La société Lookout Mobile Security vient d'alerter ZATAZ de certains problèmes de confidentialité et des enjeux rencontrés par les utilisateurs et les entreprises avec l'application Rio Olympics 2016 Keyboard. Une APP disponible en version iOS et Android.
L'application officielle de l'entreprise américaine NBC Universal Media, Rio 2016 Olympics keyboard est en apparence une simple extension de clavier pour les personnes qui suivent les jeux Olympics. Cependant, il a identifié que cette application était capable de compiler plus d'information qu'initialement prévu par son développeur, exposant ainsi la confidentialité des données des amateurs des JO de RIO et possiblement des entreprises pour lesquelles ils travaillent.
Finalement, l'équipe de recherche a informé NBCUniversal des enjeux de confidentialité identifiés dans les versions Android et iOS de l'application officielle Rio 2016 Keyboard. NBCUniversal a réagi rapidement pour résoudre les problèmes identifiés et s'assurer que les versions disponibles seraient sécurisées avant l'ouverture des Jeux Olympiques d'été de Rio. Si vous avez téléchargé l'application, effacez là. A vous de décider, ensuite, si vous installez la nouvelle version.

---



Réagissez à cet article

Original de l'article mis en page : ZATAZ L'appli Rio Olympics 2016 Keyboard dangereuse – ZATAZ

# Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

**Les deux experts qui avaient piraté une Jeep Cherokee récidivent dans le cadre de la Black Hat en démontrant une attaque sur le même véhicule.**

En 2015, la Black Hat avait vu deux spécialistes en sécurité, Charlie Miller et Chris Valasek, prendre le contrôle à distance d'une Jeep Cherokee de 2014. Un exploit qui a obligé Chrysler, propriétaire de Jeep, à procéder à un rappel de près de 1,4 million de véhicules. Une opération de mise à jour coûteuse pour le constructeur automobile. Il en a profité aussi pour lancer un Bug Bounty, avec des primes allant de 150 à 1500 dollars.

Un programme auquel les deux experts ne pourront pas concourir. Car ils démontrent à la Black Hat 2016 que la sécurité des voitures connectées n'est toujours pas optimale, malgré les récentes mises à jour. Dans une présentation, ils présentent une attaque contre la même Jeep Cherokee de 2014. A la différence de l'année dernière, cette attaque n'est pas menée à distance, mais avec un accès physique à la voiture. Néanmoins, le duo précise qu'avec du temps elle pourrait être réalisée via un terminal embarqué ou à distance via une liaison sans fil.

## Blocage des freins et coup de volant intempestif

Une fois dans la voiture, Charlie Miller a branché son ordinateur sur le réseau du véhicule, nommé bus CAN, via un port situé sous le tableau de bord. Ce réseau envoie des instructions aux différents capteurs (consommation, confort, détection de panne, etc). L'accès à ce réseau est normalement sécurisé avec le patch de sécurité élaboré l'année dernière à la suite du premier piratage de la Jeep. Il semble que des failles subsistent et les deux spécialistes ont pu contourner certains garde-fous.

Parmi les actions réalisées, ils ont bloqué les freins. Charlie Miller s'est servi du mode maintenance pour rendre inopérant le freinage. D'habitude ce blocage des freins ne peut s'opérer qu'à une faible vitesse soit 5 miles par heure. Dans une vidéo, le duo roule sur une route de campagne et d'un coup (après un compte à rebours) le volant se met à tourner à 90 degrés plantant la Jeep dans le fossé. Pour se faire, Charlie Miller s'est servi de la fonction tourner le volant dans la fonction parking automatique (qui se fait habituellement en marche arrière et à faible vitesse). Concrètement pour réaliser leur piratage, les deux experts se sont attaqués à la fois aux bus CAN, mais surtout en ciblant directement les ECU (electronic control units) dont un a été placé en mode maintenance et un autre utilisé pour envoyer des commandes malveillantes.

Interrogé par nos confrères de Wired, Chrysler ne considère pas cette attaque comme un danger pour la sécurité des véhicules. En premier lieu, elle nécessite un accès physique à la voiture. De plus, les experts ont utilisé une Jeep Cherokee ne disposant pas de la dernière version du logiciel embarqué d'infotainment (vecteur de leur première attaque en 2015). Les experts précisent que même avec la dernière version, cette attaque est toujours possible.

Article original de Jacques Cheminat

---



Réagissez à cet article

Original de l'article mis en page : Direction, frein : les hackers de Jeep récidivent à la Black Hat