Ballons, satellites, drones… Comment les milliardaires du web vont connecter le monde

Ballons, satellites, drones… Comment les milliardaires du web vont connecter le monde

Des connexions à très haut débit qui tomberaient du ciel, c'est presque un conte de fées pour quiconque habite dans un secteur où la 3G passe à peine et où l'ADSL arrive en bout de course.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article

Alerte Que Choisir sur les jouets connectés et nos données personnelles

	Alerte Que Choisir sur les jouets connectés et nos données personnelles

A l'approche de Noël et face à la multiplication des offres de jouets connectés pour enfants dans les rayons de magasins ou sur Internet, l'UFC-Que Choisir dénonce aujourd'hui, sur la base d'une analyse technique, des lacunes quant à la sécurité et la protection des données personnelles des enfants utilisateurs de la poupée connectée 'Mon amie Cayla' et du robot connecté 'i-Que' disponibles chez de nombreux vendeurs en France. Sur la base de ces inquiétants constats, l'association saisit la CNIL et la DGCCRF.

L'étude technique commanditée par notre homologue norvégien, Forbrukerradet, souligne que Cayla et i-Que, en apparence inoffensifs, ne garantissent pas le respect de la vie privée et de la sécurité des données personnelles de vos enfants.

Faille de sécurité du Bluetooth intégré

Ces jouets disposent d'un microphone intégré qui se connecte par Bluetooth à une application mobile, préalablement téléchargée par l'utilisateur sur son smartphone ou sa tablette. Le jouet peut alors comprendre ce que lui dit l'enfant et y répondre. Mais, les sociétés fabricantes, ont fait le choix d'implanter dans Cayla et i-Que, une technologie Bluetooth sujette à des risques de failles de sécurité élevées.

En effet, si les sociétés ont fait le choix d'une connexion simple et rapide, aucun code d'accès ou procédure d'association entre ces jouets et les téléphones/tablettes n'est exigé avant la connexion au jouet, ce qui garantirait pourtant que seul le propriétaire puisse s'y connecter. Résultat : un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom du Bluetooth, « Cayla » et « i-Que », permet très simplement d'identifier les poupées. Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.

Conditions contractuelles et utilisation des données personnelles

La protection des données personnelles des utilisateurs français est prévue par la loi Informatique et Libertés mais semble avoir été oubliée par les sociétés fabricantes.

Les conditions contractuelles les autorisent, sans consentement express, à collecter les données vocales enregistrées par Cayla et i-Que, et ce, pour des raisons étrangères au stricte fonctionnement du service. Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents: « aux Etats-Unis, ou vers les autres territoires concernés où les lois sur la protection de la vie privée ne sont peut-être pas aussi complètes que celles du pays où vous résidez et/ou dont vous êtes ressortissant»!

Matraquage publicitaire ciblé

Les sociétés fabricantes n'hésitent pas à faire de la publicité ciblée à destination de vos enfants. Les conditions contractuelles supposent que le simple fait de visualiser une publicité ciblée, constitue de votre part, un accord express à recevoir de telles publicités ciblées. L'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits – notamment des produits Disney ou des références aux dessins animés de Nickelodeon.

Loin d'être des cas isolés, Cayla et i-Que reflètent un problème général de sécurité et de données personnelles des jouets connectés. En effet, l'étude commanditée par nos homologues norvégiens souligne que la poupée Hello Barbie *(pas encore commercialisée en France)* est sujette aux mêmes griefs.

Au vu de ces éléments inquiétants, l'UFC-Que Choisir:

• appelle les parents à réfléchir à deux fois avant d'acheter la poupée Cayla et le robot i-Que ; rappelle qu'en cas de vente à distance, ils bénéficient d'un délai de rétractation de 14 jours. Pour ceux déjà équipés et qui souhaitent le conserver, l'association les invite à n'utiliser le jouet connecté qu'en leur présence, ou à défaut de l'éteindre.

• saisit d'une part la CNIL pour qu'elle diligente sans délai un contrôle du respect de la protection des données personnelles des utilisateurs de la poupée Cayla et du robot i-Que, et d'autre part, la DGCCRF afin que ses services enquêtent sur le niveau de sécurité des jouets connectés et sanctionnent tout manquement aux dispositions légales et réglementaires.

Réagissez à cet article

Original de l'article mis en page : Jouets connectés et données personnelles – UFC-Que Choisir

---

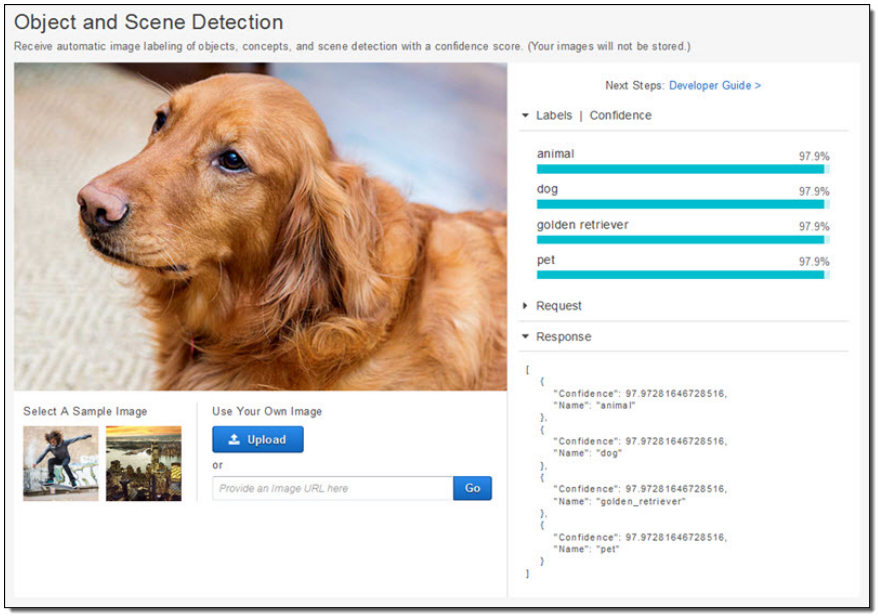
Intelligence artificielle : un programme capable de voir deux secondes dans le futur

Une innovation surprenante ce matin, puisqu'il s'agit d'une intelligence artificielle capable de voir deux secondes dans le futur.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article

Amazon lance Rekognition, une IA de reconnaissance d'image



Amazon lance Rekognition, une IA de reconnaissance d'image

Amazon vient de lancer Rekognition, une intelligence artificielle capable de reconnaître de nombreux éléments sur une image. Le groupe continue ses avancées en matière d'IA.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi

et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

Réagissez à cet article

---

900 000 routeurs de Deutsche Telekom infectés par un malware

900 000 routeurs de Deutsche Telekom infectés par un malware

Deutsche Telekom a confirmé la thèse d'un malware ayant infecté plus de 900.000 de ses routeurs. Selon Flashpoint, environ 5 millions de routeurs à travers le monde seraient vulnérables à la faille exploitée par cette variante de Mirai.

Le Cert-FR alerte les utilisateurs français sur cette attaque. L'équipe rappelle ainsi que « plusieurs version du binaire malveillant sont en circulation ». Le Cert-FR recommande de changer les mots de passe par défaut, de restreindre l'accès aux outils d'administration et de désactiver « les services inutilement lancés sur les équipements exposés sur le réseau. »
Mirai se tourne vers de nouvelles cibles et la nouvelle version du ver informatique s'attaque maintenant aux routeurs. On avait déjà constaté par le passé des variantes de ce malware modifiées afin de s'attaquer à de nouveaux appareils. Mais l'attaque ayant visé Deutsche Telekom montre que les opérateurs de cette nouvelle variante entendent maintenant changer de cible et délaisser les objets connectés pour s'attaquer aux routeurs.

Comme l'explique Flashpoint dans une note de blog, la mise à disposition du code source de Mirai par son créateur a entraîné une guerre entre les cybercriminels, alors que plusieurs groupes tentaient d'utiliser Mirai pour prendre le contrôle du maximum d'objets connectés vulnérables. « L'évolution logique pour ce malware était de découpler le mécanisme d'infection de la charge utile du malware, en exploitant un nouveau vecteur d'attaque » précise ainsi Flashpoint sur son blog.
La dernière déclinaison de Mirai n'exploite donc plus simplement Telnet pour tenter de se connecter à des objets connectés en utilisant les identifiants par défaut. Selon Flashpoint, celle-ci exploite des vulnérabilités connues au sein des protocoles TR-064 et TR-069, des protocoles de maintenance utilisés par les opérateurs. C'est grâce à cette faille que les opérateurs du réseau botnet sont parvenus à infecter plus de 900.000 routeurs livrés par Deutsche Telekom à ses clients. Mais selon Flashpoint, l'opérateur allemand n'est pas le seul à devoir s'inquiéter de ce type d'attaques. Flashpoint évoque ainsi le fait que des appareils infectés ont également été détectés au Brésil et en Grande-Bretagne. Selon Flashpoint, environ 5 millions de routeurs à travers le monde sont vulnérables à cette nouvelle variante.
Reste à déterminer l'origine de l'attaque contre l'opérateur. Flashpoint précise que les administrateurs de cette variante semblent être des habitués de Mirai, puisque le nouveau malware présente plusieurs points communs (notamment des serveurs de command and control) avec des Botnets déjà identifiés lors d'attaques précédentes effectuées grâce à Mirai.
Selon le journal allemand Tagesspiegel, les soupçons se tournent vers la Russie. Dans une prise de parole, la chancelière Angela Merkel s'est refusée à confirmer cette thèse, mais précise néanmoins que de nombreuses cyberattaques ont été constatées en Europe et appelle ses citoyens à s'habituer à ce type d'attaques. Cité par la presse locale, le directeur de l'équivalent allemand de l'Anssi, le BSI, évoque de son côté « le crime organisé » à l'origine de l'attaque, mais rappelle que l'attaque n'a pas fonctionné. Le malware a bien déconnecté les routeurs des abonnés, mais celui-ci n'est pas parvenu à s'installer correctement. Plus de peur que de mal donc…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Deutsche Telekom : 5 millions de routeurs vulnérables au malware – ZDNet

---

iCloud indiscret sur nos journaux d’appels…

iCloud indiscret sur nos journaux d’appels…

La synchronisation iCloud envoie sur les serveurs d'Apple le journal des appels d'un appareil sous iOS, en remontant jusqu'à quatre mois. Une option sur laquelle l'utilisateur ne peut pas influer directement et qui nécessite une désactivation complète d'iCloud Drive pour être coupée. Pour la société, il ne s'agit que de simplifier la vie des clients.

iCloud, quand il est actif sur un appareil Apple, synchronise et sauvegarde de nombreux éléments : contacts, agendas, messages, réglages et ainsi de suite. L'idée est de simplifier la vie de l'utilisateur s'il vient à perdre son appareil ou tout simplement s'il en utilise plusieurs. La « réserve » de données est ainsi la même et il ne s'embarrasse pas de doublons et autres.

Une synchronisation active, même quand la sauvegarde iCloud est coupée

Mais iCloud synchronise aussi le journal des appels, ce qui n'est en fait mentionné nulle part. La découverte a été faite par Elcomsoft, à qui l'on doit déjà les révélations sur la fragilité du chiffrement dans les sauvegardes faites par iOS 10. Toutes les informations du journal d'appel sont présentes : les appels classiques émis et reçus, les appels FaceTime, et globalement tout ce qui peut y inscrire des évènements depuis iOS, comme Skype et WhatsApp.

Selon Elcomsoft, la seule manière de couper cette synchronisation, qui remonte le journal jusqu'à quatre mois en arrière, est de désactiver complètement iCloud Drive, un choix que l'on trouve dans les options du service dans iOS et macOS. Désactiver iCloud lui-même ne suffit pas.

Mais ce faisant, d'autres services peuvent ne plus fonctionner. WhatsApp, justement, se sert de Drive pour stocker ses sauvegardes. D'autres applications l'utilisent pour entreposer leurs documents et les synchroniser entre les machines de l'utilisateur. Il reste bien entendu le cas où cette révélation ne dérange pas l'utilisateur.

Une commodité, et pas seulement pour les utilisateurs

Pour Apple, il n'y a pas vraiment de problème, comme la firme l'a indiqué à *Forbes* : « *Nous offrons la synchronisation du journal d'appels comme une commodité à nos clients, pour qu'ils puissent rappeler depuis n'importe lequel de leurs appareils.* […]*L'accès aux données iCloud – y compris les sauvegardes – requiert l'identifiant Apple et le mot de passe. Nous recommandons à tous nos clients de choisir des mots de passe forts et d'utiliser l'authentification à deux facteurs* ».

Tout irait bien donc à partir du moment où le mot de passe serait assez fort. Cependant, ce n'est pas aussi simple. L'affaire de l'iPhone 5c a certes montré qu'Apple ne pouvait pas déverrouiller par la force un appareil et récupérer les données (le code de verrouillage participe à la clé de chiffrement), mais iCloud, même s'il communique de manière chiffrée, dépose des données sur les serveurs de l'entreprise.

Or, comme pour iMessage, ces données sont disponibles sur demandes si les forces de l'ordre les réclament, dument armées d'un mandat. Une situation similaire à ce que l'on retrouve dans le domaine de la téléphonie mobile « classique » depuis des années.

L'expert Jonathan Zdziarski, interrogé par Forbes, a indiqué que rien n'empêchait en théorie Apple de basculer dans le chiffrement intégral pour l'ensemble de ses services. « *Mais d'un point de vue politique* » ajoute-t-il, « *cela pourrait déclencher une guerre avec certaines agences fédérales qui utilisent ces données quotidiennement* ». Une situation à ce qu'on a pu voir avec WhatsApp lors de son passage au chiffrement de bout-en-bout.

Réagissez à cet article

Original de l’article mis en page : Apple : iCloud synchronise sans accord les journaux d’appels

---

Une clé de déchiffrement gratuite pour le ransomware Crysis

	Une clé de déchiffrement gratuite pour le ransomware Crysis

ESET fournit une clé de déchiffrement pour toutes les personnes victimes du ransomware Crysis (détecté par ESET comme Win32/Filecoder.Crysis). L'outil a été mis au point grâce aux clés de déchiffrement maîtres récemment publiées via le forum BleepingComputer.com.

Le ransomware Crysis a commencé à s'étendre une fois que l'un de ses principaux « concurrents », TeslaCrypt, ait cessé ses opérations plus tôt cette année. Se propageant par plusieurs canaux, Crysis a été détecté par nos systèmes des milliers de fois partout dans le monde.
Si vous avez été victime du ransomware Crysis, téléchargez la clé de déchiffrement depuis notre page dédiée en cliquant ici. Si vous avez besoin d'informations supplémentaires sur la façon d'utiliser l'outil, consultez ESET Knowledgebase.
Veuillez noter que les nouvelles variantes de cette famille de ransomware peuvent utiliser de nouvelles clés, ce qui rend les fichiers concernés indéchiffrables.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Lecture sur les lèvres : l'IA fait désormais mieux que l'homme

Lecture sur les lèvres : l'IA fait désormais mieux que l'homme

L'IA plus performante que les spécialistes de la lecture sur

les lèvres ? C'est en tout cas que laisse entendre une étude menée conjointement par Google DeepMind (une entreprise britannique rachetée par Google en 2014 et à l'origine d'AlphaGo) et l'université d'Oxford.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article

Lecture sur les lèvres : l'IA fait désormais mieux que l'homme

Lecture sur les lèvres : l'IA fait désormais mieux que l'homme

L'IA plus performante que les spécialistes de la lecture sur les lèvres ? C'est en tout cas que laisse entendre une étude menée conjointement par Google DeepMind (une entreprise britannique rachetée par Google en 2014 et à l'origine d'AlphaGo) et l'université d'Oxford.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article

De l'intelligence artificielle pour épauler les experts en cybersécurité

Arrêtons de taper tout le temps sur la tête des utilisateurs et de citer la faiblesse de l'humain comme la principale

faille en matière de cybersécurité.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article