L’innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016

L’innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016

Deuil national en Belgique au lendemain des attaques qui ont fait 31 morts et 270 blessés tandis que l'enquête s'accélère.
Deux frères kamikazes, auteurs des tueries à l'aéroport et dans le métro, ont été identifiés grâce à leurs empreintes digitales. Alors, comment prévenir un nouvel attentat comme celui de Bruxelles ?

La lutte contre le terrorisme passe par le renseignement et la surveillance sur le terrain. Mais les effectifs semblent insuffisants et épuisés. Reconnaissance faciale, logiciels d'analyse comportementale… l'une des armes efficaces contre le terrorisme ne serait-il pas l'innovation ? — Avec: Gérôme Billois, membre et administrateur du CLUSIF. Frédéric Simottel, éditorialiste high-tech BFM Business. Matthieu Marquenet, COO de Smart Me Up. Jean-Baptiste Huet, BFM Business. Et Jean-Louis Missika, adjoint à la mairie de Paris en charge de l'innovation. — Les Décodeurs de l'éco, du mercredi 23 mars 2016, présenté par Fabrice Lundy, sur BFM Business.

Réagissez à cet article

Source : *L'innovation, une arme contre le terrorisme ? — 23/03*

Alerte : Faille Java à corriger d'urgence. Oui encore…

Alerte : Faille Java à corriger d'urgence. Oui encore…

Oracle a publié un patch en urgence pour son logiciel Java. Celui-ci corrige une faille critique dans Java permettant d'exécuter du code à distance sur une machine vulnérable.Dans une alerte de sécurité, Oracle confirme que la faille (CVE-2016-0636) est sévère avec une note de 9.3 sur une échelle qui grimpe jusqu'à 10 (Common Vulnerability Scoring System)… [Lire la suite]

Réagissez à cet article

Source : *Oracle corrige en urgence Java. Oui encore… – ZDNet*

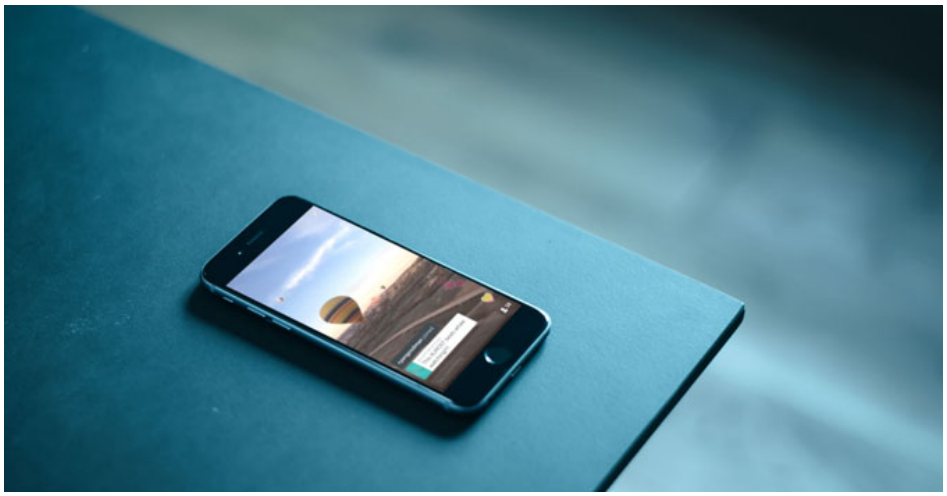
Un canular sur Periscope fait passer par la case prison ferme

	Un canular sur Periscope fait passer par la case prison ferme

Le tribunal correctionnel de Meaux a rendu son verdict dans l'affaire du canular sur Periscope. Les trois prévenus écopent d'une peine d'emprisonnement avec sursis, dont deux mois ferme pour l'un d'entre eux.

Les blagues les plus courtes sont les meilleures, surtout lorsqu'elles ne provoquent pas inutilement l'intervention des secours. Telle pourrait être la conclusion de ce fait divers un peu idiot, qui s'est heureusement avéré n'être qu'un canular qui a dérapé. Appréhendés en début de semaine pour une farce sur Periscope qui a déclenché le déploiement d'importants moyens d'intervention pour rien, trois hommes ont été condamnés mercredi par la justice.

Le tribunal correctionnel de Meaux a en effet rendu son jugement dans « l'affaire » de ce canular qui a simulé la torture et le meurtre d'un faux pédophile, le tout filmé via Periscope, une application pour smartphone qui permet à chacun de retransmettre en direct ce qu'il voit. Les conclusions des juges, rapportées par Le Parisien, incluent de la prison ferme et de la prison avec sursis.



Le personnage central de cette affaire a été condamné à dix mois de prison, dont deux qu'il devra effectivement passer derrière les barreaux. Il s'agit de la peine la plus lourde, puisque les deux comparses s'en tirent avec six mois de prison avec sursis. Le fait qu'il ait déjà un casier judiciaire bien garni, avec 12 condamnations incluant des fausses alertes à la bombe, a peut-être pesé dans la balance. D'autant qu'il doit encore être jugé pour une autre affaire, ajoutent nos confrères.

Le jugement a également permis d'évaluer le coût total de l'opération : 32 000 euros. Il faut dire que les moyens déployés alors étaient conséquents : des dizaines d'hommes mobilisés (policiers, plongeurs, pompiers), des véhicules (dont un hélicoptère équipé d'une caméra thermique et deux bateaux dotés de sonars)… [Lire la suite]

Réagissez à cet article

Source : *Prison ferme pour le sinistre canular sur Periscope – Politique – Numerama*

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

D’après Palo Alto Networks, un nouveau malware baptisé AceDeceiver, a déjà infecté près de 6 millions d’appareils iOS non jailbreakés appartenant à des utilisateurs Chinois.

Comme ont pu le constater les chercheurs, ce trojan infecte les appareils mobiles via des ordinateurs Windows et exploite des erreurs commises par Apple dans le système de gestion des droits numériques (DRM). A l’heure actuelle, AceDeceiver circule uniquement sur le territoire chinois ; d’après Palo Alto, il s’agirait du premier malware capable d’infecter les gadgets d’Apple qui utilisent le système imparfait DRM FairPlay. Et il n’est pas nécessaire que l’appareil soit débridé pour garantir l’infection.

« D’abord, il y a eu XcodeGhost, puis ZergHelper, et maintenant AceDeceiver » a rappellé Ryan Olson, directeur des études sur les virus chez Palo Alto, alors qu’il commentait la dernière découverte aux journalistes de Threatpost. « Ils contribuent tous à l’érosion continue de la protection du magasin d’applications d’Apple ». D’après l’expert, AceDeceiver permet d’obtenir un accès « homme au milieu » à l’appareil iOS et de forcer l’utilisateur à communiquer son identifiant Apple aux attaquants.

Ce nouveau malware iOS se distingue de ses prédécesseurs par le fait qu’il n’utilise pas de certificats légitimes Apple pour s’introduire dans un appareil non débridé. Il opte pour la technique FairPlay Man-In-The-Middle, utilisée déjà depuis deux ans pour diffuser des applications pirates. D’après les conclusions de Palo Alto, le trojan AceDeceiver est le premier cas où ce genre de modification est utilisé pour installer des malwares sous iOS à l’insu de l’utilisateur.

L’analyse a démontré que les auteurs d’AceDeceiver ont préparé cette campagne malveillante pendant de nombreux mois. Au deuxième semestre de l’année dernière, ils ont réussi à introduire dans l’App Store trois versions différentes de l’application AceDeceiver avec une fonction d’économiseur d’écran. Cette opération s’imposait afin d’obtenir les codes d’autorisation d’Apple sollicités via iTunes. Par la suite, les individus malintentionnés ont exploité ces codes avec l’application Windows Aisi Helper spécialement développée à cette fin pour procéder à l’installation des malwares sur les appareils mobiles à l’insu de l’utilisateur.

Aisi Helper est vendu uniquement en Chine et se présente comme un outil pour iOS qui permet de créer des copies de sauvegarde, de restaurer le système, de débrider les appareils, d’administrer l’appareil et de le purger. Toutefois, dans ce cas l’existance d’un client de ce genre sur le poste de travail Windows simplifie également la tâche de l’attaquant car le malware peut être installé sur les appareils iOS lorsque ceux-ci sont connectés à l’ordinateur. AceDeceive réalise l’installation en substituant la poigné de main FairFlay par son propre serveur d’autorisation. Il s’agit d’une attaque FairPlay Man-In-The-Middle, appliquée pour la première fois en 2014.

AceDeceiver a été porté à l’attention d’Apple le mois dernier et la société a déjà retiré les trois faux économiseurs d’écran de son magasin d’applications. Palo Alto indique toutefois que l’attaque est toujours possible. « Tant que les attaquants disposent du code d’autorisation, ils ne doivent pas obligatoirement accéder à l’App Store pour diffuser ses applications » expliquent les chercheurs dans leur blog. Ryan Olson, de son côté, a confirmé aux journalistes que de telles utilisationsdétournées étaient possibles car les résultats de l’analyse réalisée par le mécanisme DRM d’Apple sont valides en dehors de l’écosystème iTunes.

Une fois installé sur un appareil iOS, AceDeceiver peut fonctionner comme un magasin d’applications alternatifs. Il fonctionne sous le contrôle des individus malintentionnés et offre un large choix de jeux et d’utilitaires. L’utilisateur est également invité à saisir son identifiant Apple et son mot de passe pour pouvoir accéder à toutes les fonctions de l’application pirate gratuite.

Ryan Olso explique qu’il est difficile d’éliminer les problèmes provoqués par AceDeceiver. Dans le cas de ZergHelper cité ci-dessus, Apple avait simplement supprimé le malware de son magasin. Le nouveau trojan se distingue par le fait qu’il compte sur un client Windows et utilise un code d’autorisation obtenu antérieurement, ainsi que des lacunes dans le projet FairPlay DRM.

Au moment de la publication de ce billet, Apple n’avait pas encore réagi aux questions de Threatpost…. [Lire la suite]

Réagissez à cet article

Source : *Un Trojan Exploite Un Bogue Du DRM Pour Charger Des Malwares Dans IOS – Securelist*

Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

Les Anonymous ont publié une nouvelle vidéo dans laquelle ils entendent renforcer leurs offensives contre l'Etat islamique suite aux attentats ayant touché Bruxelles cette semaine.

Daesh a revendiqué les deux attentats survenus en Belgique dans la ville de Bruxelles. Face à cette menace terroriste, le groupe de hackeurs Anonymous a diffusé une nouvelle vidéo sur YouTube dans laquelle ils affirment vouloir renforcer leurs offensives contre les sites et infrastructures de l'Etat islamique.

Anonymous rappelle les actions précédemment menées après les attaques survenues à Paris en novembre dernier. Le groupe a ainsi fait fermer des milliers de comptes Twitter liés à des sympathisants de l'El. Ils ont hacké plusieurs sites de propagande et récupéré l'argent obtenu des Bitcoin.

« *Cependant, tant qu'il y aura des attaques à travers le monde, nous ne nous arrêterons pas (…) nous défendrons le droit à la liberté (…)*

Sympathisants de Daesh, nous vous traquerons, nous vous trouverons, nous sommes partout et nous sommes bien plus nombreux que ce que vous pouvez imaginer », affirme Anonymous dans cette nouvelle vidéo. Chacun est invité à rejoindre les efforts de ce groupe de hackeurs.

En novembre, 22 000 comptes Twitter liés à Daesh avaient été listés par Anonymous et un site de l'Etat islamique avait subi les foudres des hackeurs.

Un peu plus tôt ce mois-ci, Anonymous avait déclaré une guerre totale au candidat à la présidence des Etats-UnisDonald Trump pour ses diverses déclarations choc au sujet des femmes, des étrangers ou des handicapés…. [Lire la suite]

Réagissez à cet article

Source : *Terrorisme : les Anonymous déclarent la « guerre totale » à Daesh*

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Dans le cadre du projet de loi sur la réforme pénale, le rapporteur Michel Mercier veut instaurer en France un délit d'entrave au blocage des sites « terroristes ».

En préparation de l'examen en Commission des lois, le sénateur a déposé un amendement visant à condamner ceux qui viennent entraver les procédures de blocage des sites faisant l'apologie ou provocant au terrorisme. Celui qui viendrait extraire, reproduire et transmettre intentionnellement les données concernées par ces mesures, « en connaissance de cause », serait ainsi éligible à cinq ans de prison et 75 000 euros d'amende.
Cette mesure, puisée directement dans une proposition de loi sénatoriale contre le terrorisme (UDI/LR), viendra épauler les mesures de blocage administratif de ces sites, permises depuis la loi du 13 novembre 2014 sur le terrorisme, ou celles décidées par un juge en application de l'article 706-23 du code de procédure pénale.
« *Ces blocages, administratif ou judiciaire, ont pour but de lutter contre la diffusion de contenus faisant l'apologie d'actes de terrorisme,* explique l'auteur de l'amendement dans son exposé des motifs. *Néanmoins, ces blocages peuvent être entravés par certains comportements. Ces derniers, s'ils ne consistent pas en la diffusion publique de ces contenus, ne peuvent être appréhendés sous le délit d'apologie d'actes de terrorisme ou de provocation à de tels actes* ».
Cette mesure est rédigée en des termes suffisamment larges pour qu'on puisse imaginer la sanction de celui qui viendrait tweeter ou publier sur Facebook les données litigieuses, puisqu'il n'est pas possible de bloquer l'un ou l'autre de ces réseaux. Remarquons surtout que le texte n'exige pas nécessairement de diffusion publique. Il joue dès lors qu'on extrait, reproduit et transmet ces données d'une manière ou d'une autre, à destination par exemple d'un serveur distant. Du coup, l'amendement est également taillé pour frapper ceux qui multiplient des contre-mesures aux blocages par IP ou DNS… [Lire la suite]

Réagissez à cet article

Source : *Vers un délit d'entrave au blocage des sites faisant l'apologie du terrorisme ? – Next INpact*

Des millions de smartphones Android touchés par une faille critique

Des millions de smartphones Android touchés par une faille critique

Une faille figurant dans un nombre considérable de smartphones Android permet à des applications d'accéder au contrôle total du système d'exploitation.

La sécurité du système d'exploitation Android est une source régulière d'inquiétude et mobilise constamment l'attention des spécialistes, qui scrutent sans relâche l'OS open source porté par Google afin d'y déceler des vulnérabilités.
Si celles-ci ne manquent pas – les récents correctifs publiés par la firme de Mountain View sont là pour le prouver –, elles sont néanmoins corrigées avec une relative célérité. Toutefois, une faille repérée depuis un certain temps est parvenue à passer entre les mailles du filet. Et pour ne rien arranger, celle-ci s'avère très sérieuse.

TOUTE LA GAMME NEXUS EST CONCERNÉE

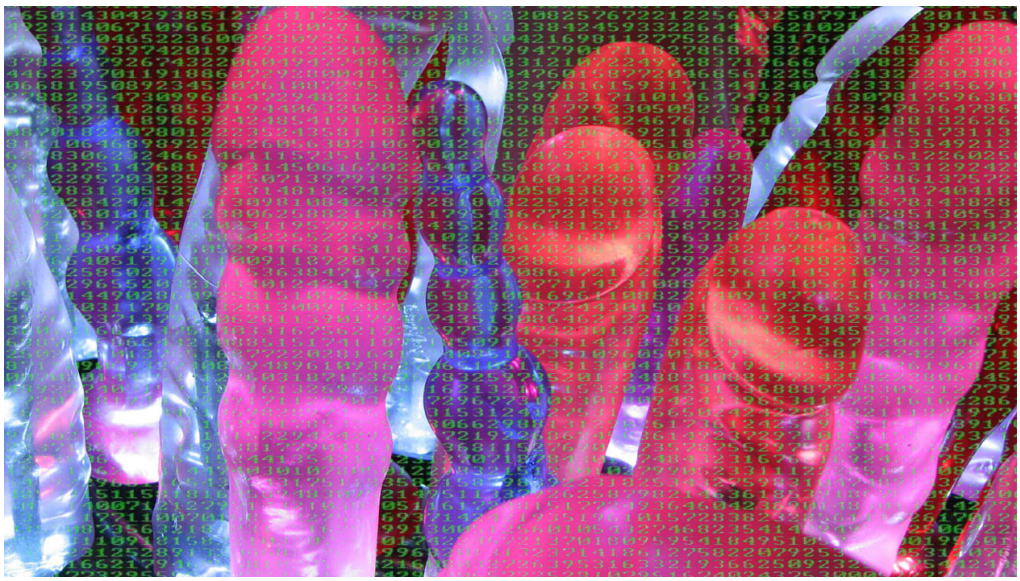
Depuis 2014, une vulnérabilité permettait à une application d'accéder aux privilèges root sur un grand nombre de téléphones Android, dont toute la gamme Nexus. Sur un téléphone rooté, il est possible d'accéder au contrôle total du système d'exploitation et ainsi effectuer des actions normalement bloquées par le constructeur pour des raisons de sécurité.
En l'occurrence, avec cette brèche, une application pouvait accéder à des fonctionnalités bloquées de l'OS et installer du code malveillant. « Une vulnérabilité du noyau qui permet l'élévation des privilèges pourrait permettre à une application nuisible d'exécuter du code arbitraire [sans l'accord du propriétaire, nlr] dans le noyau », explique Google.
Les noyaux Linux 3.4, 3.10 et 3.14 sont touchés, mais ceux plus récents (à partir de 3.18) sont hors de danger.
Cette faille a été identifiée depuis février 2015 sous la référence CVE-2015-180 et un patch est en préparation depuis le mois dernier, après la notification envoyée à Google par la CORE Team, un regroupement d'experts en sécurité informatique. En mars, Zimperium, une startup également spécialisée dans ce domaine, a notifié Google de la présence d'une application profitant de cette faille sur le Google Play.

Dans son bulletin de sécurité, Google explique que l'application en question a été retirée du Google Play. « Les clients qui installent une application qui cherche à exploiter cette faille prennent des risques.
Les applications de root sont interdites sur le Google Play et nous allons bloquer l'installation de cette application en dehors du Google Play grâce à la vérification d'applications », tranche l'entreprise.
Cela étant dit, un utilisateur qui aurait désactivé la vérification d'application peut toujours installer manuellement une application profitant de l'exploit sur son appareil via le fichier APK ou sur un magasin d'application alternatif.
Pour corriger ce problème, Google va déployer un patch sur l'ensemble de la gamme Nexus dans les prochains jours. Celui-ci a été transmis aux différents constructeurs, mais à cause de la fragmentation d'Android, il pourrait se passer plusieurs semaines, voire mois, avant que les fabricants n'appliquent le correctif sur leurs appareils… [Lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité critique touche des millions de smartphones Android – Tech – Numerama*

Piratage de sextoys ! Que faut il craindre ?



Piratage de sextoys ! Que faut il craindre ?

Un éditeur de logiciels de sécurité a mis en lumière le danger que représentent les objets connectés en piratant un vibromasseur. De quoi limiter le potentiel ludique de l'engin!

Les hackers pourront peut-être pourrir nos vies jusque dans notre plus stricte intimité… c'est en tous les cas ce qu'ont essayé de démontrer des ingénieurs de l'éditeur de logiciels de sécurité Trend Micro au salon informatique allemand CeBit qui vient de s'achever à Hanovre.

Les attaques récentes contre les données informatiques d'un… hôpital nous ont mis en garde sur l'impact que peut avoir le piratage sur les systèmes professionnels connectés, mais la menace concerne tous les objets connectés. Y compris les sextoys !

Face à un panel de journalistes, un ingénieur de Trend Micro a en effet piraté un vibromasseur en l'allumant à distance, une action qui a s'abord provoqué l'hilarité, selon l'agence Reuters qui rapporte les faits. Cité par l'agence, le responsable de la technologie de l'éditeur a affirmé que si un « hacker un vibromasseur est amusant […] mais si j'accède au back end (le logiciel de contrôle, ndr) je peux faire chanter le constructeur ».

Un individu mal intentionné et assez qualifié pourrait tout à fait contrôler la vitesse du moteur de l'appareil, accélération qui pourrait potentiellement mener à sa destruction… limitant ainsi son potentiel ludique !

Si nous commençons à nous habituer aux piratages d'infrastructures, le fait que de plus en plus d'objets soient connectés – à nos smartphones voire directement à internet – ne va faire qu'augmenter le périmètre des menaces potentielles.

Espérons que les constructeurs n'attendent pas d'incidents graves pour prendre les mesures de sécurité qui s'imposent…. [Lire la suite]

Réagissez à cet article

Source : *Tout ce qui est connecté peut être piraté, y compris… les sextoys!*

Téléphone, SMS et Internet coupés au Congo pendant les présidentielles…

Téléphone, SMS et Internet coupés au Congo pendant les présidentielles…

Ce n'est pas une rumeur. Les réseaux de téléphonie mobile et d'Internet sont coupés sur toute l'étendue du territoire de la République du Congo (Brazzaville).
Intervenue ce dimanche 20 mars, jour des élections présidentielles, cette mesure court jusqu'à ce lundi 21 mars.
Blackout. La coupure des télécommunications a plongé le pays dans un blackout sans précédent que les autorités justifient par la nécessité de sécuriser le Congo en cette période électorale. Ainsi, pour des « raisons de sécurité et de sureté nationales », le pays a été coupé du reste du monde pendant deux jours. Ce qui n'est pas fait pour rassurer la population, dans la mesure où ces élections se déroulent dans un climat tendu.
Les opposants et la communauté internationale pointent une mauvaise organisation de ce scrutin. Celui-ci met aux prises le Président sortant Dénis Sassou Nguesso (32 ans au pouvoir) face à huit challengers… [Lire la suite]

Réagissez à cet article

Source : *Présidentielles au Congo Brazzaville : téléphone, SMS et Internet coupés dans tout le pays | CIO-MAG*

La Côte d’Ivoire va exiger des passeports biométriques aux frontières

La Côte d’Ivoire va exiger des passeports biométriques aux frontières

---

Bientôt, la Côte d'Ivoire va exiger des passeports biométriques et des cartes d'identités sécurisées à ses frontières. « Sans ces documents, on ne pourra plus entrer en Côte d'Ivoire », a prévenu le ministre d'Etat, ministre de l'Intérieur et de la Sécurité, Hamed Bakayoko.

C'était au cours de la conférence de presse qu'il a co-animée mardi après-midi avec le Procureur général Adou Kouamé Richard, sur l'attentat terroriste de Grand-Bassam, survenu le dimanche 13 mars dernier.
Des propos du Procureur général Adou Kouamé Richard, il ressort que « *l'exploitation efficiente des documents électroniques* » trouvés sur la plage de Grand-Bassam a permis de remonter jusqu'au nommé Kounta Dallah. Cet individu, dont on ignore pour l'instant l'identité et la nationalité, a été présenté par les conférenciers comme le cerveau des attentats qui ont fait 19 victimes et 33 blessés.

A en croire le ministre d'Etat, Hamed Bakayoko, l'enquête se poursuit pour identifier certains individus. Déjà, il faut noter que les preuves numériques ont permis d'interpeller 15 personnes, qui sont à ce stade de l'enquête considérées comme des prévenus. Dans cette affaire, la Côte d'Ivoire bénéficie du soutien du Bureau régional du FBI basé au Sénégal, d'Interpol, de la France, du Mali et du Maroc… [Lire la suite]

Réagissez à cet article

Source : *Attentat de Grand-Bassam : la Côte d'Ivoire va exiger des passeports biométriques aux frontières | CIO-MAG*