Protégez-vous gratuitement du Virus Locky avant qu'il ne soit trop tard !

Protégez-vous gratuitement du Virus Locky avant qu'il ne soit trop tard !

Voici une solution rapide et pratique et efficace uniquement avec les versions actuelles de Locky pour s'en protéger.
Rien ne garantit qu'une version ultérieure de Locky ne contournera pas le souci.

Comme Locky essaye de créer la clé **HKCUSoftwareLocky** dans la base de registre (regedit), il suffit de la créer avant lui…

et de refuser tous les droits d'accès sur celle-ci:

Et voilà ! Ainsi, en se lançant sur votre système, Locky se crashera comme une station Mir dans le jardin de Paco. Les autres solutions proposées par Lexsi sont un poil plus complexes, mais vraiment intéressantes. Je vous invite à les lire, ne serait-ce que pour votre culture personnelle.
Merci Korben d'avoir relayé et à Olivier pour le partage.

Réagissez à cet article

Source : *Locky – La solution pour s'en protéger – Korben*

Petya, le nouveau ransomware qui chiffre l'ensemble du disque

Petya, le nouveau ransomware qui chiffre l'ensemble du disque

---

Le G DATA Security Labs a détecté les premiers fichiers ce jeudi 24 mars, en Allemagne, d'un nouveau type de ransomware nommé Petya.

A la différence des codes actuels, tels que Locky, CryptoWall ou TeslaCrypt, qui chiffrent certains fichiers du système, Petya chiffre l'ensemble des disques durs installés.

.

La campagne actuellement en cours vise les entreprises

Dans un email au service des ressources humaines, il y a une référence à un CV se trouvant dans Dropbox. Le fichier stocké dans le partage Dropbox est un exécutable. Dès son exécution, l'ordinateur plante avec un écran bleu et redémarre. Mais avant cela, le MBR est manipulé afin que Petya prenne le contrôle sur le processus d'amorçage. Le système démarre à nouveau avec un message MS-Dos qui annonce une vérification CheckDisk. A défaut d'être vérifié, le système est chiffré et plus aucun accès n'est possible.

Le message est clair : le disque est chiffré et la victime doit payer une rançon en se connectant à une adresse disponible sur le réseau anonyme TOR. Sur la page concernée, il est affirmé que le disque dur est chiffré avec un algorithme fort. Après 7 jours, le prix de la rançon est doublé. Il n'y a pour le moment aucune certitude sur le fait que les données soient irrécupérables.

Il est donc recommandé aux entreprises et particuliers de redoubler de vigilance quant aux emails reçus… [Lire la suite]

Réagissez à cet article

Source : *Petya : un nouveau ransomware qui chiffre l'ensemble du disque*

Daech prend le contrôle d’une centrale nucléaire – Futuriste ?

	Daech prend le contrôle d’une centrale nucléaire. Futuriste ?

Le coordinateur de l'UE pour la lutte contre le terrorisme estime que les djihadistes seront bientôt capables de cyberattaques contre des sites sensibles.

La prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité « avant cinq ans », a admis samedi le coordinateur de l'Union européenne pour la lutte contre le terrorisme alors que la sécurité des sites nucléaires belges est pointée du doigt.
« Je ne serais pas étonné qu'avant cinq ans il y ait des tentatives d'utiliser l'Internet pour commettre des attentats », notamment en prenant le contrôle du « centre de gestion d'une centrale nucléaire, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer », estime Gilles de Kerchove dans une interview au quotidien La Libre Belgique.
« À un moment donné, il y aura bien un gars » au sein de l'organisation djihadiste État islamique « avec un doctorat en technologie de l'information qui sera capable d'entrer dans un système », a-t-il estimé.

La miniaturisation des explosifs mais également la connaissance accrue des combattants de l'État islamique dans les biotechnologies constituent de réelles menaces pour l'avenir, selon lui. « Que se passera-t-il quand on en sera à comment élaborer un virus dans la cuisine de sa mère ? » s'est-il demandé.
En revanche, M. de Kerchove a estimé que le département belge de la Défense était « assez bon » en matière de cybersécurité. « Ils n'ont, bien sûr, pas les capacités de représailles des Français, des Anglais ou des Américains, mais en cas d'attaque, je pense que notre département de la Défense est assez bon », a-t-il dit, précisant cependant qu'il ne savait pas « si le gouvernement » belge était « capable d'anticiper et de résoudre de grosses attaques ».

Sécurité renforcée
Des médias belges et internationaux ont rapporté vendredi que la cellule terroriste bruxelloise responsable des attentats de mardi avait prévu une attaque à l'arme de guerre dans les rues de Bruxelles, type 13 novembre à Paris, et la fabrication d'une « bombe sale » radioactive après une surveillance vidéo par deux des kamikazes, les frères El Bakraoui, d'un « expert nucléaire » belge.
À la suite des attaques survenues mardi à Bruxelles qui ont fait 31 morts, la sécurité avait été renforcée autour des deux centrales nucléaires de Belgique.
C'est dans ce contexte de suspicion sur la sécurité des sites nucléaires qu'un agent de sécurité dans le nucléaire a été abattu et son badge volé jeudi soir dans la région de Charleroi, dans le sud de la Belgique, selon le journal La Dernière Heure. Samedi, la piste terroriste a été écartée, par la justice belge. La piste terroriste est formellement démentie, rapporte l'agence de presse Belga, citant le parquet de Charleroi, dans le sud du pays. Le juge d'instruction spécialisé dans les matières terroristes n'a pas été saisi. Les raisons de la mort de la victime, abattue, tout comme son chien, de plusieurs balles à son domicile, ne sont pas encore connues mais les enquêteurs pensent à un cambriolage qui aurait mal tourné ou à un crime pour des raisons privées.
Le parquet de Charleroi a démenti le vol de son badge d'accès de centrale nucléaire… [Lire la suite]

-

Réagissez à cet article

Source : *Quand Daech prendra le contrôle d'une centrale nucléaire – Le Point*

Les notaires marocains sensibilisés à la protection des données personnelles

	Les notaires marocains sensibilisés à la protection des données personnelles

L’accent a été mis sur les dispositions de la loi 09-08, mais aussi sur le rôle et les missions de la Commission nationale de contrôle de la protection des données à caractère personnel.

Les notaires ont été invités le 23 mars dernier, à prendre part à un séminaire placé sous le thème «Le notaire, quel rôle en matière de protection des données personnelles ?».

La rencontre organisée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), en partenariat avec le Conseil national de l’ordre des notaires du Maroc (CNONM) avait pour but de mettre la lumière sur les dispositions de la loi 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel, mais aussi sur le rôle et les missions de la CNDP.

Ainsi, les notaires ont eu l’occasion de mieux appréhender les enjeux liés à la protection des données personnelles dans l’exercice de leur mission. Le séminaire leur a aussi permis de situer leur rôle dans la consécration des droits des citoyens à la protection de la vie privée et des données personnelles, et de prendre connaissance des obligations légales en vigueur.

Les deux organisateurs soulignent, par ailleurs, que cette initiative «constitue également un premier pas vers une coopération plus étroite entre la CNDP et le Conseil national de l’ordre des notaires»… [Lire la suite]

Réagissez à cet article

Source : *:: Le Matin :: Les notaires sensibilisés à la protection des données personnelles*

La gendarmerie cherche un expert en « déprotection » logicielle et matérielle

	**La gendarmerie cherche un expert en « déprotection » logicielle et matérielle**

La gendarmerie recrute un expert de haut niveau pour « déprotéger » des matériels ou des données auxquels les enquêteurs cherchent à accéder.

La gendarmerie nationale a fait publier ce jeudi au Journal Officiel deux petites annonces d'emploi, dont l'intitulé résonne fortement avec le conflit qui oppose Apple au FBI aux États-Unis.
La première concerne un « *emploi d'expert de haut niveau en technologies numériques chargé de projet et développement de techniques de déprotection matérielle à la division ingénierie numérique* » de l'Institut de recherche criminelle, au pôle judiciaire de la gendarmerie nationale, à Pontoise (95).
La seconde est très proche dans son intitulé mais concerne les « *techniques de dé-protection logicielle* ».

Les deux postes sont ouverts aux titulaires d'un diplôme d'ingénieur ou au moins d'un master 2 en informatique, électronique cryptologie ou mathématique.

Selon le descriptif, « *le candidat retenu aura pour mission principale de développer des méthodes et outils nécessaires à la dé-protection matérielle (smartphones, disques durs…) et assurer la pertinence, la robustesse de ses méthodes* ». En clair, il s'agira par exemple d'essayer de contourner le chiffrement des iPhone ou lechiffrement sous Android, pour accéder au contenu des appareils bloqués. C'est une attente forte du parquet, et plus généralement des enquêteurs qui souhaitent obtenir toutes les preuves potentiellement accessibles sur les matériels saisis chez des suspects.

UN HACKER CHERCHEUR

Le candidat idéal, qui devra aussi « *disposer de capacités avérées à acquérir de nouvelles compétences* », doit déjà avoir dans ses bagages :
• maîtrise de la structure des systèmes électroniques ;
• expérience de conception et de rétro-conception de circuits électroniques ;
• capacités de développement (langages C/C++, Java, Python…) ;
• connaissance d'un ou plusieurs domaines innovants nécessaires au développement de l'activité du département ;
• excellente connaissance des technologies numériques ;
• maîtrise écrite et parlée de la langue anglaise ;
• une connaissance de la criminalité liée aux nouvelles technologies est également recherchée.

La personne recrutée « *devra mettre en place les outils d'analyse de données permettant au département INL d'exploiter au mieux les informations à sa disposition* ». « *Il devra pour ce faire être en mesure d'analyser les supports informatiques et réaliser des dossiers d'expertise comme soutenir techniquement les enquêteurs de la gendarmerie spécialisés en nouvelle technologie* », précise la gendarmerie.
Celle-ci attend par ailleurs de son expert de haut niveau qu'il s'engage dans la communauté internationale de la sécurité informatique, pour apporter ses propres travaux et bénéficier des avancées des autres. Ainsi, « *il sera également chargé de définir et conduire la politique de veille technologique dans son domaine de compétence et de valoriser son action à un niveau national ou international en participant à des publications dans des revues ou en recherchant des partenaires* ».
Enfin, précise l'annonce, « *il sera aussi chargé de l'animation de l'activité scientifique et technique du département en faisant preuve d'innovation et en suivant différents projets de recherches et de développement, en dispensant des cours et en développant des relations entre les acteurs français et étrangers du domaine de l'expertise en technologie numérique* ».

Il n'y a plus qu'à envoyer vos CV.
… [Lire la suite]

Réagissez à cet article

Source : *La gendarmerie cherche un expert en « déprotection » logicielle et matérielle – Tech – Numerama*

Des chercheurs trouvent une faille dans le chiffrement d’Apple

Des chercheurs trouvent une faille dans le chiffrement d’Apple

---

Des chercheurs de l'université Johns Hopkins révèlent une faille dans le chiffrement de l'application iMessage. Celle-là pourrait permettre à des pirates d'accéder aux photos et vidéos envoyées.

Issu du *Washington Post*, l'article aurait été retiré juste après sa publication ce matin, selon certains blogueurs qui réussissent néanmoins à retrouver sur Google des bribes de l'article. De nouveau visible sur le site du journal, la nouvelle pourrait faire grand bruit. Car ce matin des universitaires américains prétendent avoir décelé une faille dans le chiffrement d'iMessage, l'application de messagerie instantanée d'Apple.

La compagnie vante justement sa capacité de chiffrement « de bout en bout », qui chiffre le message au moment même de son envoi, et garantit normalement qu'aucun tiers (y compris Apple) ne puisse obtenir la clé de déchiffrement du message. Pourtant le chercheur Matthew D. Green qui a dirigé l'équipe universitaire affirme qu'une faille permettrait d'intercepter les images et vidéos. « *Cela n'aurait en rien aidé le FBI à débloquer l'iPhone du tueur de San Bernardino* », affirme-t-il, « *mais cela démontre que la notion selon laquelle ce type d'application serait infaillible est erronée.* »

Selon Green, il était insensé de demander à une société comme Apple de créer des versions modifiées de leurs produits, puisque des failles peuvent d'ores et déjà être trouvées : « *Même Apple, qui compte dans ses rangs les meilleurs cryptographes du monde, ne sont pas en mesure de créer un chiffrement 100% fiable. C'est bien ce qui me rend inquiet quand j'entends qu'en plus on parle de créer des failles volontaires dans leurs produits alors que nous ne sommes déjà pas capables de créer des sécurités imparables.* »

Le professeur Matthew D. Green, de l'université Johns Hopkins

Pour intercepter le fichier, les étudiants auraient conçu un logiciel qui imite les serveurs d'Apple. La communication qu'ils ont attaquée par la suite contenait selon eux un lien vers une photo stockée sur l'iCloud d'Apple, ainsi que sa clé de déchiffrement de 64 bits.

Matthew D. Green et son équipe ont fait savoir qu'ils publieront les détails de leur attaque dès qu'Apple aura trouvé un remède à la faille découverte. Ils affirment aussi que des attaques similaires sont régulièrement pratiquées par les services de renseignement américains… [Lire la suite]

Réagissez à cet article

Source : *Des chercheurs trouvent une faille dans le chiffrement d'Apple*

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*

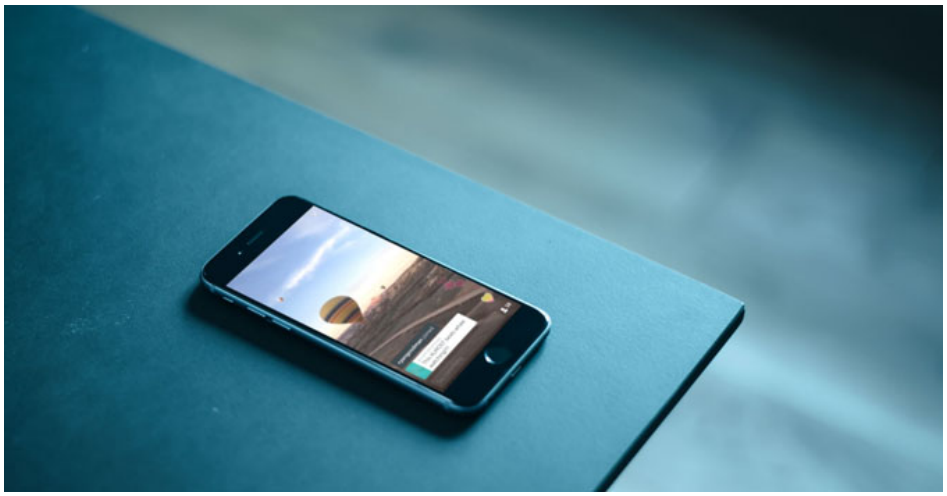
Un canular sur Periscope fait passer par la case prison ferme

	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*