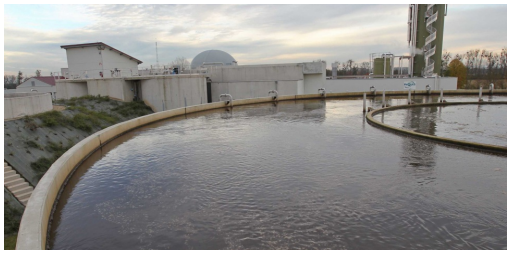
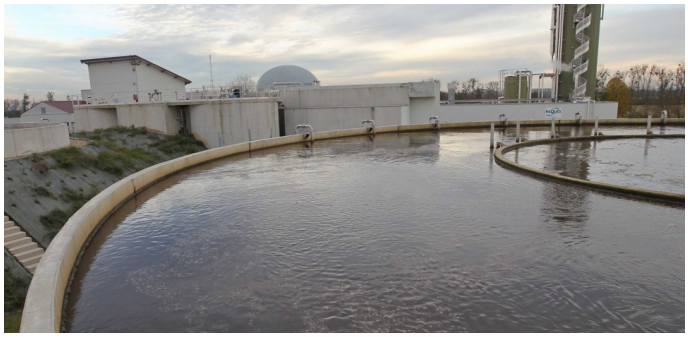
L’eau d’une station d’épuration manipulée par des hackers – Sciencesetavenir.fr

	L’eau d’une station d’épuration manipulée par des hackers

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.



Le bilan dressé par l'opérateur américain Verizon publié en mars 2016 et consacré aux fuites de données a de quoi faire frémir. Il recense pas moins de cinq cents incidents de cybersécurité dans quarante pays en 2015 (le rapport en anglais ici**).** Parmi eux, l'un attire tout particulièrement l'attention : il concerne la Kemuri Water Company (KWC), une station d'épuration bien réelle mais dont le nom a été changé et le pays d'implantation non divulgué pour éviter de la compromettre. Et pour cause ! Verizon relate la façon dont des hackers ont réussi, très facilement, à manipuler la composition chimique de l'eau qui est redistribuée aux habitants après traitement ! Le tout, sans même en avoir eu l'intention au départ…
L'affaire a été révélée lorsque la société a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information afin d'anticiper tout problème éventuel. Or, une fois sur place, les experts ont constaté avec stupeur que la station d'épuration était déjà la proie de pirates informatique depuis deux mois ! Et que ses responsables s'en doutaient… Des mouvements suspects de valves et de tuyauteries avaient été remarqués. Beaucoup plus grave ! Les gestionnaires avaient constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau pour la rendre portable. Sans conséquence désastreuse heureusement…

« Pour tout dire, KWC était un candidat tout trouvé pour une fuite de données. Son interface Internet présentait plusieurs failles à haut risque dont on sait qu'elles sont souvent exploitées» mentionne le rapport de Verizon. Et son système opérationnel, qui commande les applications industrielles (traitement des eaux, gestion du débit), reposait quant à lui sur une infrastructure informatique vieille de plusieurs dizaines d'années.
En outre, de nombreuses fonctions de ce système cohabitaient avec des applications « business » de l'entreprise sur un même et unique serveur, un AS/400 d'IBM, ordinateur commercialisé en… juin 1988. En clair, si des hackers pénétraient le système, ils pouvaient sans peine passer du contrôle du traitement des eaux aux informations financières et aux données de facturation de la compagnie. Et c'est exactement ce qui s'est passé.

L'opérateur liste une série de failles assez confondantes

Au cours de son enquête, Verizon s'est rendu compte que des adresses IP de hackers déjà rencontrées dans trois autres affaires s'étaient connectées au système de paiement en ligne de la KWC, cette interface permettant aux clients d'accéder à leur compte à distance (depuis un ordinateur, un mobile) ; c'est a priori par cette voie que les hackers sont passés, comme d'autres l'ont fait lors du piratage en octobre 2015 de l'hydrolienne Sabella.

2,5 MILLIONS. L'opérateur liste ensuite une série de failles confondantes : l'accès aux données clients n'était protégé que par un login/mot de passe, sans double authentification ; une « *connexion directe par câble* » existait entre l'application de paiement en ligne et l'AS/400, ce dernier ayant un accès ouvert à Internet, avec une adresse IP et des données d'identification administrative disponibles sur le serveur web de paiement, écrites en clair dans un fichier ! Au final, les pirates ont pu sortir du système 2,5 millions de dossiers clients avec leurs données de paiement. Pour l'heure, il semble qu'ils n'en aient pas fait usage.

ALERTE. Mais le plus grave restait à venir. Une fois à l'intérieur du réseau, les pirates se sont en effet rendus compte qu'ils pouvaient accéder aux fonctions opérationnelles.
En se servant des données d'identification administrative, ils ont ainsi pu intervenir sur des fonctions clés : le débit de l'eau potable, son traitement chimique et le temps de remplissage des réserves. A priori – et c'est une chance – les hackers ne semblent pas avoir eu l'intention de nuire et ne poursuivaient pas un but précis, mais les autorités frémissent à l'idée des conséquences dramatiques qu'une telle ingérence aurait pu occasionner. « *Si les attaquants avaient eu un peu plus de temps et avaient été un peu plus familiers du système de contrôle industriel, la KWC et les populations locales auraient pu subir de sérieux dommages* » conclut le rapport… [Lire la suite]

Réagissez à cet article

Source : *L'eau d'une station d'épuration manipulée par des hackers – Sciencesetavenir.fr*

Cinq questions importantes à se poser en matière de cybersécurité

	Cinq questions importantes à se poser en matière de cybersécurité

Pas un jour ou presque ne se passe sans que le sujet de la cybersécurité ne soit traité dans les médias. Entre les « cyberattaques », les « cybermenaces » et la nécessité de « connaître son adversaire », on pourrait croire que les entreprises sont en état de siège permanent.

Les cybermenaces revêtent plusieurs formes : États-nations qui se livrent à des activités d'espionnage, cybercriminels qui cherchent à dérober de précieuses informations en vue de les exploiter, ou encore groupes aux motivations diverses qui cherchent à perpétrer des vols ou à causer des perturbations.

Il peut même s'agir d'une personne interne de confiance qui vole des données de clients ou d'entreprise ou d'un employé bien intentionné qui, en effectuant son travail, perd sans le vouloir de précieuses données de clients ou d'entreprise. Nul doute que les cybercriminels peuvent être très adaptables et innovants, mais le contexte de menace est un fait établi. C'est la manière dont vous gérez le risque qui est importante.
Dans un environnement cacophonique, il est important que les dirigeants d'entreprise gardent les choses en perspective. L'environnement est inondé de toutes sortes de solutions techniques, promettant de vous donner un avantage en matière de détection et de prévention. Toutefois, il est essentiel que tous les dirigeants d'entreprise prennent du recul et se rappellent que le cyber risque n'est pas un risque informatique, mais un risque d'entreprise et, à l'instar de tout autre risque d'entreprise, il doit être géré.

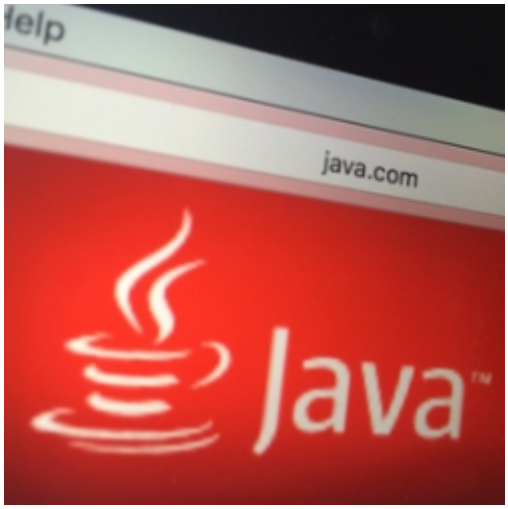
La menace ne peut pas être éliminée, mais le risque peut être géré

Il est également important de comprendre que cette menace ne peut pas être éliminée, mais que le risque peut être géré. Il est facile de se laisser tenter par une « structure du risque », mais comme de nombreuses structures, elle peut nécessiter d'investir beaucoup de temps et d'efforts pour des résultats de sécurité négligeables.
Trop souvent, la cybersécurité est évoquée à l'aide de jargon technique ou militaire, mais cela ne fait que dissiper l'attention et la compréhension des dirigeants. Il est vital que les professionnels de la sécurité expliquent le contexte de menace et le défi de la cybersécurité dans un langage accessible. C'est pourquoi il est important de comprendre le cyber risque auquel votre entreprise est confrontée. Tous les dirigeants doivent pouvoir poser les questions simples et non techniques suivantes et obtenir des réponses.
1. **Connaissez la valeur de vos données :** savez-vous de quelles données de valeur dispose votre entreprise ? Sont à inclure les données qui ont de la valeur non seulement pour vous, mais aussi pour les cybercriminels qui peuvent vouloir les voler. Quelles sont les données qui vous causeraient le plus grand préjudice si vous deviez les perdre ? Vous devez avoir une liste de vos données de valeur.
2. **Sachez qui a accès à ces données de valeur :** qui possède les droits d'administration ou l'accès aux informations ? Toutes vos « personnes internes de confiance » ont-elles besoin d'avoir accès aux données de valeur pour effectuer leur travail ? Cette question est essentielle, car l'accès aux données de valeur doit être étroitement surveillé. Vous ne confieriez pas les clés de votre domicile à n'importe qui, alors surveillez de près les personnes qui ont accès à vos données de valeur.
3. **Sachez où se trouvent vos données de valeur :** vous devez savoir où elles sont stockées et comment vous y accédez. Vos données de valeur sont-elles délocalisées au loin, dans le pays, dans le cloud ou même stockées chez un tiers ? Allez plus loin et demandez-vous si vos fournisseurs ont partagé vos données de valeur avec des sous-traitants.
4. **Sachez qui protège vos données :** vous devez savoir qui protège vos données de valeur. Cet aspect est extrêmement important. Où se trouvent ces personnes ?
5. **Sachez dans quelle mesure vos données sont protégées :** vous devez savoir ce qui est fait par les professionnels de la sécurité pour protéger vos données 24 h/24 et 7 j/7. Les tiers qui ont accès à vos données les protègent-ils de manière adéquate ?
C'est seulement une fois que vous aurez la réponse à ces questions que votre entreprise sera préparée à comprendre le niveau de cyber risque et l'efficacité avec laquelle il est géré… [Lire la suite]

Réagissez à cet article

Source : *Cinq questions importantes à se poser en matière de cybersécurité – ZDNet*

Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013



Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013

Oracle vient de livrer un correctif de sécurité pour combler une faille critique dans Java remontant à 2013. Cette dernière avait été découverte seulement en début d'année.

Oracle a publié une mise à jour de sécurité **urgente** pour corriger une vulnérabilité critique dans Java permettant à des attaquants de compromettre les ordinateurs d'internautes se rendant sur des sites web spécialement conçus pour les piéger. L'identifiant de cette vulnérabilité est CVE-2016-0636, suggérant qu'il s'agit d'une nouvelle mais cela n'est pas vraiment le cas. Dans un mail, la société de sécurité polonaise Security Explorations a confirmé que cette mise à jour patche une faille originellement rapportée à Oracle en 2013.
En début de mois, cette même société avait indiqué qu'un correctif publié par Oracle en octobre 2013 pour une vulnérabilité critique, portant l'identifiant CVE-2013-5838, s'était révélé inefficace et pouvait être contourné en changeant seulement 4 caractères de l'exploit original. Cela signifie que la vulnérabilité était toujours exploitable dans les dernières versions de Java. Or, dans son dernier bulletin, Oracle n'a fait aucune mention à l'ancienne faille trouvée par Security Explorations. Etrange renvoi d'ascenseur, non ?

L'update 77 pour Java SE 8 indispensable

Oracle recommande d'installer dès que possible cette nouvelle mise à jour Java, compte-tenu du degré de sévérité de la vulnérabilité et des détails techniques de contournement désormais rendus publics. Les utilisateurs de Java SE 8 sont prévenus d'installer l'update 77 (8u77), sachant que pour les possesseurs de Java 6 et 7, la mise à jour n'est proposée qu'en cas de support long terme, ces versions n'étant plus supportées … [Lire la suite]

Réagissez à cet article

Source : *Une vulnérabilité critique de 2013 patchée dans Java – Le Monde Informatique*

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*

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 ».

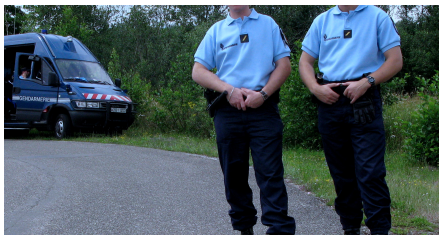
Sécurité renforcée
Des médias belges et internationaux ont rapporté vendredi que la cellule terroriste bruxelloise responsable des attentats de mardi avait prévu une attaque à l'arme de guerre dans les rues de Bruxelles, type 13 novembre à Paris, et la fabrication d'une « bombe sale » radioactive après 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*

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.

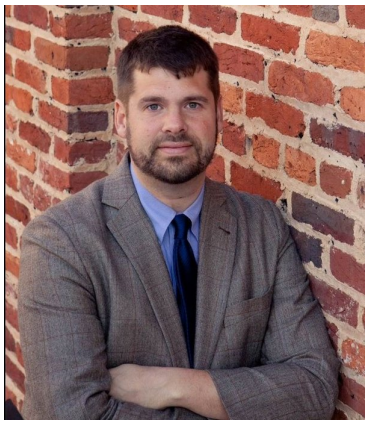
La personne recrutée « *devra mettre en place les outils d'analyse de données permettant au département INL d'exploiter au mieux les informations à sa disposition* ». « *Il devra pour ce faire être en mesure d'analyser les supports informatiques et réaliser des dossiers d'expertise comme soutenir techniquement 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

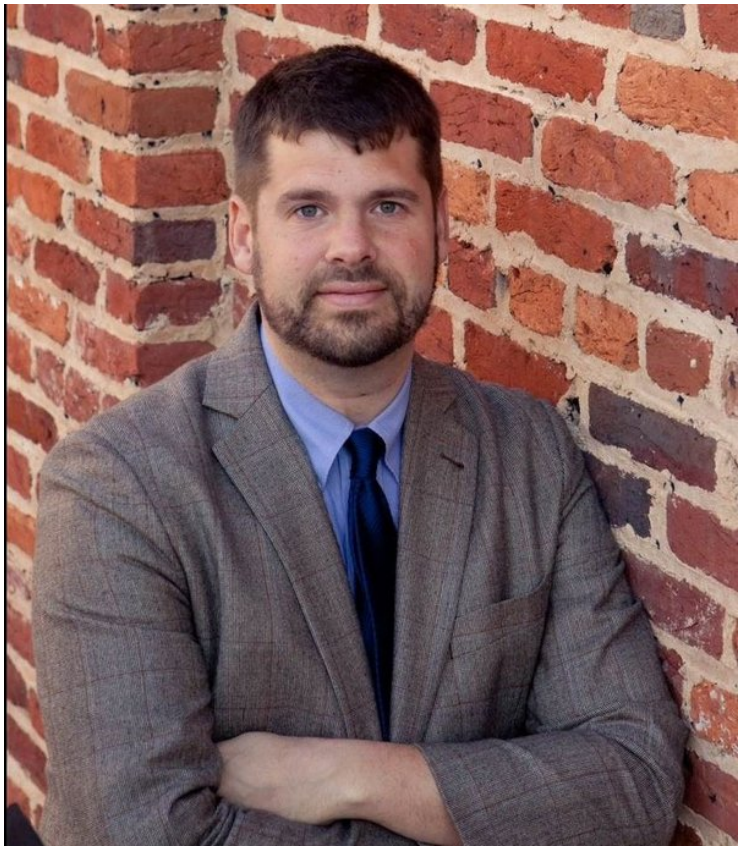
---

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

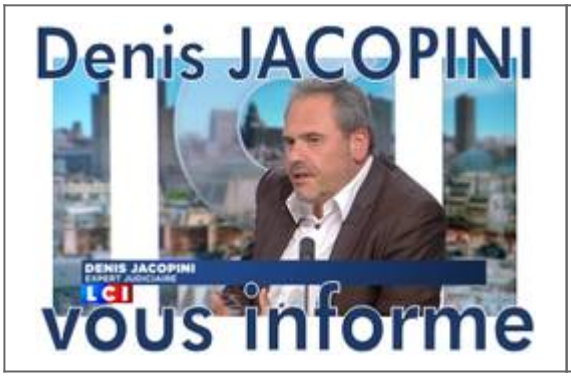
Pour intercepter le fichier, les étudiants auraient conçu un logiciel qui imite les serveurs d'Apple. La communication qu'ils ont attaquée par la suite contenait selon eux un lien vers une photo stockée sur l'iCloud d'Apple, ainsi que sa clé de déchiffrement de 64 bits.

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*

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*

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.

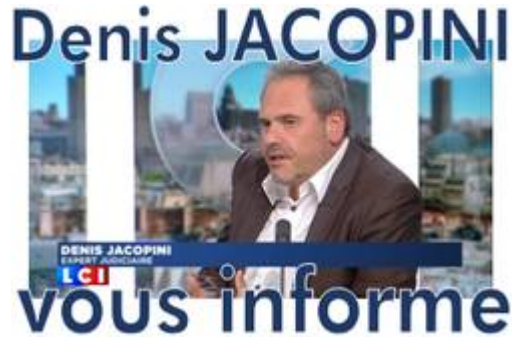
Ryan Olso explique qu’il est difficile d’éliminer les problèmes provoqués par AceDeceiver. Dans le cas de ZergHelper cité ci-dessus, Apple avait simplement supprimé le malware de son magasin. Le nouveau trojan se distingue par le fait qu’il compte sur un client Windows et utilise un code d’autorisation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

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*