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*

La Cnil veille sur vos données de e-santé

La Cnil veille sur vos données de e-santé

Chercheurs et médecins ont de plus en plus recours à des objets connectés pour suivre les patients ou collecter des informations. La protection de ces données est devenu un enjeu de taille.

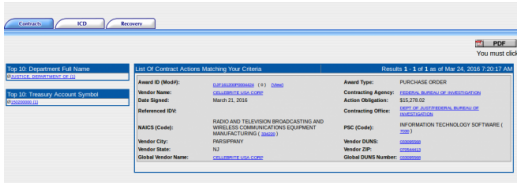
L'utilisation des technologies de l'information et de la communication dans le domaine de la santé pose un problème majeur : celui de la sécurisation des données. Portant sur la santé, elles sont dites « sensibles » au regard de la loi et donc soumises à une protection particulière.
En France, c'est la Commission nationale de l'informatique et des libertés (Cnil) qui y veille, en s'assurant de l'application de loi Informatique et Libertés de 1978.
Dans une étude de mai 2014, la Cnil a constaté que l'information sur l'utilisation des données personnelles par les éditeurs d'objets connectés et applications santé était insuffisante.

700 projets par an
Par ailleurs, la loi Informatique et Libertés impose que la sécurité porte « sur le fait que des tiers ne puissent pas accéder aux données, mais aussi sur l'intégrité des données », énonce Délia Rahal-Lofksög, responsable du service santé à la Cnil.
Il s'agit donc pour un éditeur de s'assurer qu'en cas de bug, piratage ou autre problème technique, les informations médicales délivrées ne seront pas erronées (diagnostic d'hyperglycémie au lieu d'hypoglycémie, par exemple).
Afin de renforcer et homogénéiser cette protection, un règlement européen en cours d'adoption, prévoit que des analyses d'impact sur la vie privée soient mises en place par les responsables de fichier afin d'évaluer, par exemple, les conséquences d'un piratage de données.
Enfin, tous les projets de recherches utilisant des données personnelles doivent préalablement faire l'objet d'une validation par la Cnil, qui en autorise en moyenne 700 par an, parmi lesquels figurent des projets impliquant des objets connectés… [Lire la suite]

Réagissez à cet article

Source : *E-santé : la Cnil veille sur vos données*

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*

L'Europe renforce la pression sur Apple pour ouvrir l'accès aux données personnelles des utilisateurs

L'Europe renforce la pression sur Apple pour ouvrir l'accès aux données personnelles des utilisateurs

---

Suite aux attaques terroristes de Bruxelles, les autorités européennes envisagent de forcer Apple et d'autres sociétés à ouvrir l'accès aux données personnelles des utilisateurs aux services spéciaux.

Les parlementaires français ont déjà commencé les débats sur le projet de loi à ce sujet. Ils sont convaincus qu'en choisissant entre l'élargissement des pouvoirs des services de sécurité en vue de prévenir des attentats terroristes et le respect de la vie privée, il est raisonnable d'opter pour le premier choix, lit-on dans le New York Times.
Les députés proposent de sanctionner les chefs des sociétés spécialisées dans les technologies de pointe, qui refusent de fournir des informations aux enquêteurs, d'une peine privative de liberté de cinq ans au maximum et d'une amende de 350.000 euros. Selon le New York Times, telle est également la position adoptée par le Royaume Uni.
Les sociétés en question quant à elles essayent de faire de leur mieux pour éviter un tel scénario. Ces derniers temps, le président d'Apple Tim Cook a personnellement rencontré plusieurs politiciens européens, y compris le premier ministre français Manuel Valls et la chef de la diplomatie britannique Theresa Mary May afin de s'assurer leur appui.Auparavant, le tribunal de Californie avait ordonné à Apple de fournir aux enquêteurs du FBI, dans l'affaire de l'attaque terroriste de San Bernardino, des données chiffrées sur l'iPhone du terroriste tué, après que l'entreprise ait refusé de coopérer volontairement avec les autorités.
Le directeur général d'Apple, Tim Cook, avait rétorqué que cette exigence présentait une menace pour la sécurité de ses clients, tandis que ses conséquences « étaient hors du cadre légal ». La société a refusé de se conformer à la décision du tribunal, déclarant avoir l'intention de faire appel… [Lire la suite]

Réagissez à cet article

Source : *Après Bruxelles, l'Europe renforce la pression sur Apple*

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

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

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*

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*