Le malware Pegasus exploite 3 failles 0 day sur iPhone

	Le malware Pegasus exploite 3 failles 0 day sur iPhone

Les trois failles corrigées par Apple dans iOS 9.3.5 (ainsi que dans la dernière bêta d'iOS 10 livrée, contre toute attente, vendredi dernier) sont redoutables. Elles ont été exploitées par NSO Group, une société israélienne dont le fonds de commerce n'est autre que l'espionnage de journalistes et de militants. Le site Motherboard raconte la découverte de l'affaire qui relève du thriller…

Ce 10 août, Ahmed Mansoor, un militant des droits de l'homme dans les Émirats Arabes Unis, reçoit sur son iPhone un message lui proposant d'en savoir plus sur de «*nouveaux secrets sur la torture dans les prisons d'État* ». Un lien accompagnait ce message, qu'il s'est bien gardé de lancer.

Les deux messages reçus par Mansoor – Cliquer pour agrandir

À la place, il a contacté un chercheur du Citizen Lab, un organisme de défense des droits numériques rattaché à l'université de Toronto. Aidé par Lookout, un spécialiste de la sécurité mobile, ils ont pu mettre au jour un mécanisme très élaboré de surveillance par iPhone interposé.

Si Mansoor avait touché le lien, il aurait provoqué le jailbreak de son iPhone et donné à NSO Group le plein contrôle de son smartphone. « *Un des logiciels de cyberespionnage parmi les plus sophistiqués que nous ayons jamais vus* », expliquent les chercheurs.

NSO Group vient d'apparaitre sur les radars, mais cette entreprise très discrète (aucune présence sur internet) opère depuis 2010. Le malware qu'elle a mis au point, baptisé Pegasus, permet d'infecter un iPhone, d'intercepter et de voler les données et les communications. Une arme redoutable, qualifiée de « *fantôme* » par NSO pendant une de ses rares interventions publiques en 2013. Cette société vend Pegasus au plus offrant, notamment des gouvernements peu regardants sur les droits de l'homme.

Les données volées par Pegasus – Cliquer pour agrandir

NSO a visiblement pu pénétrer par effraction dans des iPhone depuis le modèle 5. Son malware est programmé avec des réglages qui remontent jusqu'à iOS 7.

Ces trois failles *zero day*, baptisées Trident par les chercheurs, ont été communiquées à Apple il y a dix jours. « *Nous avons été mis au courant de cette vulnérabilité et nous l'avons immédiatement corrigée avec iOS 9.3.5* », explique un porte-parole du constructeur. « *iOS reste toutefois le système d'exploitation mobile grand public le plus sécurisé disponible* », rassure Dan Guido, patron de la société de sécurité informatique Trail Of Bits, qui travaille souvent avec la Pomme.

Il indique toutefois qu'il reste à améliorer le système de détection des vulnérabilités. Apple a annoncé début août un programme de chasse (rémunérée) aux failles.

Article original de Mickaël Bazoge

Réagissez à cet article

Original de l’article mis en page : Cyberspionnage : derrière les failles Trident d’iOS, le redoutable malware Pegasus | iGeneration

---

Pokémon Go inquiète l’armée française !

Pokémon Go inquiète l’armée française !

Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE

Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :

• « sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;

• les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;

• ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »

Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.

La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».

Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?

On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

Des systèmes biométriques piratés à partir de vos

photos Facebook

Des systèmes biométriques piratés à partir de vos photos Facebook

Des chercheurs découvrent comment pirater des systèmes biométriques grâce à Facebook. Les photographies sauvegardées dans les pages de Facebook peuvent permettre de vous espionner.

De nombreuses entreprises de haute technologie considèrent le système de reconnaissance faciale comme l'une des méthodes fiables pour être reconnu par votre ordinateur. J'utilise moi-même la reconnaissance biométrique digitale, rétinienne et du visage pour certaines de mes machines. C'est clairement un des moyens simples et fiables de vérification d'une identité. Cependant, des chercheurs prouvent que la biométrie peut se contourner, dans certains cas, avec une photo, de la colle…

Une nouvelle découverte vient de mettre à mal, cette fois, la reconnaissance faciale mise en place par Facebook. Comme je pouvais vous en parler en 2014, Facebook met en place une reconnaissance faciale que des commerçants Américains ont pu tester avec succès. Des chercheurs ont découvert que cette prouesse technologique n'est pas encore parfaite et sujette au piratage. Des pirates peuvent utiliser votre profil Facebook, et les photos sauvegarder.

Systèmes biométriques

Des étudiants de l'Université de Caroline du Nord ont expliqué lors de la conférence d'Usenix, à Austin, avoir découvert une nouvelle technique particulièrement exaspérante pour intercepter l'intégralité d'un visage, via Facebook. Le rendu 3D et certaines « lumières » peuvent permettre de cartographier votre visage en deux clics de souris. Les chercheurs ont présenté un système qui créé des modèles 3D du visage via les photos trouvées sur Facebook. Leur modèle 3D va réussir ensuite à tromper quatre systèmes de reconnaissance faciale… sur 5 testés : KeyLemon, Mobius, TrueKey, BioID, et 1D.

Pour leur étude, 20 cobayes volontaires ont participé à l'expérience. Leurs photos sont tirées d'espaces publiques comme Facebook, mais aussi LinkedIn et Google+. La modélisation des visages à partir de 27 images différentes va permettre de créer des modèles en 3D, avec des animations faciales : bouches, yeux… Les chercheurs ont reconstruit les visages via les bouts trouvés sur les différentes photographies.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Pirater des systèmes biométriques à partir de vos photos Facebook – Data Security BreachData Security Breach

---

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

---

Le géant de l’informatique Hewlett-Packard s’associe avec 3M pour préinstaller sur ses prochains ordinateurs portables professionnels un filtre anti espion.
Quoi de plus courant que de croiser à la terrasse d’un café, dans le train ou dans un aéroport ces fiers commerciaux pressés de travailler, même dans un lieu non sécurisé. Autant dire que collecter des données privées, sensibles, en regardant juste l’écran de ces professionnels du « c’est quoi la sécurité informatique ? » est un jeu d’enfant.
Hewlett-Packard (HP), en partenariat avec 3M, se prépare à commercialiser des ordinateurs portables (Elitebook 1040 et Elitebook 840) dont les écrans seront équipés d’un filtre anti voyeur. Un filtre intégré directement dans la machine. Plus besoin d’utiliser une protection extérieure.
Une sécurité supplémentaire pour les utilisateurs, et un argument de vente loin d’être négligeable pour le constructeur. Selon Mike Nash, ancien chef de la division de sécurité de Microsoft et actuellement vice-président de Hewlett-Packard, il est possible de croiser, partout, des utilisateurs d’ordinateurs portables sans aucune protection écran. Bilan, les informations affichés à l’écran peuvent être lues, filmées, photographiées.
Le filtre pourra être activé et désactivé à loisir.
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Filtre anti espion sur les prochains Hewlett-Packard – Data Security BreachData Security Breach

---

La neutralité du Net triomphe en Europe

En publiant ses lignes directrices sur la neutralité du net qui s'imposent à tous les régulateurs européens, le BEREC a donné pleinement satisfaction aux organisations qui plaidaient pour une obligation la plus ferme possible de respecter le principe par lequel Internet s'est développé.

Le BEREC, qui regroupe les différents régulateurs des communications électroniques en Europe (dont l'Arcep en France), a publié mardi ses lignes directrices très attendues, sur l'implémentation par les autorités nationales des règles de neutralité du net prévues par la régulation adoptée par le Parlement européen en fin d'année 2015.

Le cadre général laissait quelques zones d'ombre, que le BEREC est venu combler au bénéfice d'une consultation publique menée cet été, qui a vu la société civile se mobiliser massivement. Plus de 500 000 réponses ont été envoyées à l'organisation.

Beaucoup craignaient que le BEREC ne laisse quelques trous béants dans les règles imposées aux opérateurs, d'autant plus après le coup de pression donné par ces derniers au prétexte du passage à la 5G vers 2020. Orange avait même affirmé qu'il n'y aurait pas de 5G avec la neutralité du net, la prochaine génération de réseaux mobiles imposant d'attribuer des droits d'utilisation de certaines fréquences ou certains protocoles en fonction des applications.

Mais le **texte publié mardi** obtient un satisfecit d'une limpidité rarissime de la part du lobby de la société civile European Digital Rights (EDRi). « *L'Europe fait désormais office de créateur de standard mondial dans la défense d'un internet ouvert, concurrentiel et neutre* », se réjouit dans un communiqué Joe McNamee, le directeur exécutif de l'association, en félicitant le BEREC.
Thomas Lohninger, de l'organisation SaveTheInternet.eu créé pour faire pression sur le BEREC, parle même de « *triomphe pour le mouvement européen des droits numériques* », obtenu après « une très longue bataille, et avec le soutien d'un demi million de personnes ». Il assure qu'avec les lignes directrices publiées mardi, l'Europe affirme des « *principes qui font d'Internet une plateforme ouverte pour le changement, la liberté et la prospérité* ».

INTERDICTION DU ZERO-RATING

Les règles adoptées par le BEREC prévoient notamment de donner à l'Arcep et à ses homologues le pouvoir d'imposer des sanctions lorsque les FAI dégradent la qualité d'accès à des services, ou favorisent indûment un type de services par rapport à d'autres.
Elles interdisent aux opérateurs de créer des « services spécialisés » (proposés directement par les FAI, notamment via leurs box), qui ne respectent pas les règles de la neutralité du net, lorsqu'ils ont des équivalents en tant que services proposés normalement sur Internet, ou lorsqu'ils conduisent à minimiser la bande passante accordée à l'internet ouvert.
Aussi, les lignes directrices interdisent quasiment dans les faits la pratique du « zero rating », qui consiste pour un opérateur à ne pas bloquer ou facturer la bande passante consommée par une application spécifique (par exemple des forfaits qui incluent Facebook et YouTube mais pas Twitter et Dailymotion, ou qui permettent un accès illimité au cloud de l'opérateur mais pas à celui de Google ou Apple), ou par certains types d'applications. Ces pratiques contestées n'étaient pas interdites explicitement par le règlement européen. Elles ne le sont toujours pas formellement par le BEREC, mais les conditions fixées sont tellement strictes qu'il sera très difficile pour un opérateur de continuer à avoir recours au zero-rating.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Un « triomphe » pour la neutralité du Net en Europe — Politique — Numerama

---

La cybercriminalité a de belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.

Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.

Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.

Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.

Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.

Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.

Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!

Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.

Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.

Article original de branchez-vous.com

Réagissez à cet article

Original de l’article mis en page : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Une initiative franco-allemande va tenter de convaincre les acteurs internationaux d'Internet et de l'informatique de la nécessité d'ouvrir leurs codes et leurs chiffrements pour lutter contre le terrorisme. Des voix s'élèvent au nom de la sécurité et des libertés.

Après le conseil restreint de Défense à l'Élysée le 4 août 2016, le ministre de l'Intérieur, Bernard Cazeneuve, a parlé chiffre. Avec son homologue allemand, Thomas de Maizière, il a proposé le 23 août une initiative européenne à vocation internationale pour « faire face au défi du chiffrement, une question centrale dans la lutte antiterroriste ». Le sujet est brûlant. Pas seulement depuis l'assassinat du père Hamel par des usagers de Telegram , d'ailleurs pas considéré comme la solution la plus hermétique d'un marché en plein essor.

Outre Telegram, les terroristes, des criminels et des gens très soucieux de l'intégrité de leurs communications utilisent pléthore de dispositifs de chiffrement comme ChatSecure, Conversations, Kontalk, Signal, Threema ou WhatsApp (même s'il appartient à Facebook depuis 2014), sans parler des anonymes Tor (réseau décentralisé) ou ToX (pair à pair). Là n'est d'ailleurs pas la question centrale. L'ennemi pourrait émigrer vers d'autres cieux numériques voire créer son propre outil chiffré…

Incapable de casser le code

Depuis l'audition à l'Assemblée le 10 mai de Patrick Calvar, le directeur général de la sécurité intérieure, la pression monte. Pour les attentats de Bruxelles, le DGSI avoue que « même une interception n'aurait pas permis de mettre au jour les projets envisagés puisque les communications étaient chiffrées sans que personne soit capable de casser le chiffrement ». Face au chiffrement aléatoire et autres complications futures, le DGSI a une réponse martiale : « Je crois que la seule façon de résoudre ce problème est de contraindre les opérateurs. » Nous y voilà. En février, le FBI s'est heurté au refus d'Apple de livrer les données de l'iPhone d'un des meurtriers de Daech qui a tué 14 personnes à San Bernardino le 2 décembre 2015. Avant que le FBI n'annonce avoir réussi à casser le chiffre de la pomme…

Bernard Cazeneuve ne dit pas autre chose. Il prend pour exemple sa négociation avec les majors d'Internet en février 2015 qui a permis d'élaborer une charte sur le retrait des contenus et le blocage des sites haineux. « Sur le chiffrement, il faut que nous ayons la même méthode, la même volonté, le sujet est crucial. »

Sauf qu'un courrier, publié par Libération, du directeur de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et lui-même cryptologue, Guillaume Poupard, affirme le contraire aux autorités : « Un affaiblissement généralisé serait attentatoire à la sécurité numérique et aux libertés de l'immense majorité des utilisateurs. » Permettre une intrusion des services de renseignement (par des « portes dérobées ») pourrait profiter à des gens ou des États (pas seulement islamiques) mal intentionnés. Quelle tendance va l'emporter ? En cette époque sécuritaire, de l'état d'urgence éternel et du désarroi politique…

Article original de Olivier Berger

Réagissez à cet article

Original de l'article mis en page : Lutte contre le terrorisme : Faut-il ouvrir la porte du chiffrement aux services de renseignement ? – La Voix du Nord

---

Peur d'être surveillés ?

mettez à jour votre iPhone

Peur d’être surveillés ? mettez à jour votre iPhone

Apple corrige en urgence iOS, touché par trois failles sévères. Ces dernières étaient exploitées de concert par un spyware de haut vol, Pegasus, vendu par la société israélienne NSO à des gouvernements.

La mésaventure qui vient d'arriver à Apple, obligé de déployer en urgence un correctif pour son OS mobile iOS, ne manquera pas d'alimenter le débat sur l'utilisation des vulnérabilités logicielles par les gouvernements. Et sur le bien-fondé de l'activité de très discrètes petites sociétés spécialisées dans la vente de failles zero day. Avec sa version 9.3.5 d'iOS, la firme de Cupertino vient en effet combler 3 vulnérabilités sévères exploitées probablement depuis des années pour dérober des informations sur les terminaux de la marque.

Selon les chercheurs en sécurité de Lookout, société spécialisée dans la sécurité des terminaux mobiles, et du Citizen Lab, une émanation de l'université de Toronto (Canada), ces failles étaient exploitées conjointement par un logiciel espion. Cette menace, que les chercheurs ont appelée Pegasus, aurait été développé par NSO Group, société basée en Israël et passée, en 2014, sous le contrôle de Francisco Partners Management, un fonds d'investissement américain, pour 120 millions de dollars. L'enquête des chercheurs a pu déterminer que Pegasus a été utilisé pour espionner un dissident aux Emirats Arabes Unis, Ahmed Mansoor. Au-delà de ce cas particulier, le spyware pourrait avoir été utilisé par d'autres gouvernements ou entreprises afin d'espionner des dissidents, des journalistes, des concurrents, des partenaires… Le kit d'attaque est vendu environ 8 millions de dollars pour 300 licences. Cher mais pas hors de portée d'un Etat ou d'une grande entreprise.

NSO : un discret et lucratif business

En novembre dernier, un article de *Reuters* se penchait sur l'activité de la très secrète société NSO, spécialisée dans l'assistance technique aux gouvernements pour l'espionnage de terminaux mobiles. Une société qui a plusieurs fois changé de nom et que Francisco Partners espérait revendre pas moins d'un milliard de dollars. Selon *Reuters*, la société israélienne, fondée en 2010 par Omri Lavie et Shalev Hulio, afficherait 75 M$ de bénéfices opérationnels par an.

Les fonctions de Pegasus. Une image qui serait issue de la documentation de NSO et ui a fuité lors du piratage de Hacking Team.

L'analyse du code semble faire remonter Pegasus à 2013, l'année de la sortie d'iOS 7 ; le malware renfermant des réglages adaptés à cette version de l'OS de Cupertino. « *Pegasus est l'attaque la plus sophistiquée ciblant un terminal que nous ayons jamais rencontrée parce qu'elle exploite la façon dont les terminaux mobiles s'intègrent dans nos vies et tire parti de la combinaison de fonctionnalités présente uniquement sur les mobiles : connexion permanente (WiFi, 3G/4G), communications vocales, caméra, e-mail, messages, GPS, mots de passe et liste de contacts* », écrivent les chercheurs de Lookout et de l'université de Toronto. Modulaire et exploitant le chiffrement pour éviter d'être repéré, Pegasus déroule une séquence d'attaque classique : envoi d'un message texte, ouverture d'un navigateur, chargement d'une page contrefaite (la Croix Rouge, le service de visa britannique, des médias, des sites d'entreprises IT…), exploitation des trois vulnérabilités et installation de codes permettant une surveillance de la cible (avec récupération de données tous azimuts, y compris des données de localisation, l'activation du micro ou de la caméra à distance, selon la documentation de NSO Group !).

Ahmed Mansoor : cible à répétition

C'est la prudence d'Ahmed Mansoor qui a permis la mise au jour de Pegasus : le 10 août, le dissident reçoit un message sur son iPhone accompagné d'un lien lui promettant d'en savoir plus sur les tortures dans les prisons de son pays. Plutôt que de cliquer, Mansoor fait suivre ce message à un chercheur du Citizen Lab, un laboratoire travaillant sur les sujets à la croisée des droits de l'homme et de la cybersécurité. Selon ce labo, c'est la troisième fois qu'Ahmed Mansoor est la cible d'un spyware (après d'autres attaques menées avec des outils conçus par le Britannique Gamma Group en 2011 et par l'Italien Hacking Team en 2012).

Selon les chercheurs du Citizen Lab et de Lookout, Pegasus serait « *hautement configurable* » afin de s'adapter aux spécificités de chaque cible et à l'épaisseur du porte-feuille des 'clients' de NSO. « *En fonction du pays concerné et des fonctions achetées par les utilisateurs, les capacités du spyware peuvent inclure les messages, les appels, les e-mails, les logs et d'autres données issues d'apps comme Gmail, Skype, WhatApp, Viber, FaceTime, Calendar, Line, Mail.ru, WeChat, Tango et d'autres* », écrivent les chercheurs, qui précise que le malware semble en mesure de résister à une montée de version de l'OS (sauf évidemment celle vers iOS 9.3.5) et se montre capable de se mettre à jour pour remplacer des parties de code devenues inopérantes. Selon les premières recherches du Citizen Lab, Pegasus a aussi servi à espionner un journaliste mexicain, travaillant sur la corruption dans son pays, et une personne non identifiée au Kenya.

iOS hyper-sécurisé ? Voire

Au passage, la sécurité légendaire des iPhone est passablement égratignée. Les trois failles, baptisées Trident par les chercheurs de Lookout et du Citizen Lab, montrent que le système d'Apple n'est pas hors de portée des hackers de haut vol. L'installation de Pegasus repose sur l'exploitation d'une vulnérabilité de Safari (corruption de mémoire avec CVE-2016-4655) et de deux failles du noyau d'iOS (CVE-2016-4656 & CVE-2016-4657), détaillent Lookout dans un rapport (PDF).

Rappelons que l'image de l'OS des iPhone et iPad avait bénéficié de la bataille qui avait opposé Apple au FBI concernant une demande de déblocage d'un smartphone frappé de la pomme ayant appartenu à un des auteurs de la tuerie de San Bernardino, aux Etats-Unis. Idem avec le bug bounty lancé l'année dernière par la société Zerodium, un autre de ces prestataires vendant des failles zero day au plus offrant, qui offrait alors un million de dollars pour un code d'exploitation permettant de prendre le contrôle total d'un iPhone. Rappelons que, de son côté, Apple va lancer son propre programme de chasse aux bugs, mais n'offrira au maximum que 200 000 $ de récompense. Vu les tarifs pratiqués par NSO Group et autres sociétés vendeuses de zero day, pas sûr que ce maigre pactole suffise…

Article original de Reynald Fléchaux

Sans information sur l'existence de dysfonctionnements consécutifs à l'installation de IOS 9.3.5 lors de l'écriture de ces lignes, Denis JACOPINI vous recommande fortement l'installation de cette mise à jour si votre téléphone en a les capacités.

Réagissez à cet article

Original de l'article mis en page : Trois failles zero day d'iOS servaient à espionner des dissidents

Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

	Seriez vous d’accord pour que WhatsApp partage vos données avec Facebook ?

Les nouvelles règles de confidentialité de WhatsApp ne vont peut-être pas vous plaire.
Lorsque WhatsApp a annoncé son acquisition par Facebook en 2014, les utilisateurs et les défenseurs de la vie privée se sont inquiétés de ce qui allait advenir de leurs données. Pendant deux ans, les deux services sont restés indépendants. Cependant, aujourd'hui, WhatsApp a mis à jour ses règles de confidentialité, qui sont restées inchangées pendant 4 ans.
Et celles-ci n'excluent plus l'utilisation par Facebook des données du milliard de personnes utilisent WhatsApp pour optimiser ses publicités.

« […] en connectant votre numéro de téléphone avec les systèmes de Facebook, ce dernier peut vous offrir de meilleures suggestions d'amis et vous montrer des publicités plus pertinentes si vous avez un compte Facebook. Par exemple, vous pouvez voir une publicité d'une entreprise avec laquelle vous avez déjà travaillé au lieu de voir celle d'une entreprise dont vous n'avez jamais entendu parler », lit-on dans un communiqué de WhatsApp.

Cependant, le service explique aussi que cette « coordination » avec Facebook permettra également à WhatsApp de faire des choses comme « suivre des mesures de base sur la fréquence d'utilisation de nos services des gens et améliorer la lutte contre les spams ».

Et WhatsApp a bien clarifié que même si il va d'avantage collaborer avec Facebook, ses messages sont chiffrés de bout en bout, ce qui signifie que théoriquement, personne (ni Facebook, ni WhatsApp) ne peut accéder au contenu.

Le modèle économique de WhatsApp se précise

Pour rappel, WhatsApp était à l'origine une application payante, mais gratuite la première année. Cependant, le service a récemment décidé supprimer les frais annuels, pour devenir entièrement gratuit.
Cependant, WhatsApp n'entend pas gagner de l'argent en affichant des bannières publicitaires, mais plutôt en misant sur des fonctionnalités pensées pour les relations entre clients et entreprises. Et les nouvelles règles de confidentialités reflètent aussi ce projet.
Article original de Setra

Réagissez à cet article

Original de l’article mis en page : WhatsApp va partager vos données avec Facebook

---

Les réseaux SDN ouverts à tous les vents (mauvais)

Les réseaux SDN ouverts à tous les vents (mauvais)

Des scientifiques italiens démontrent une vulnérabilité de sécurité propre au fonctionnement intrinsèque des réseaux SDN. Inquiétant alors que les déploiements ont déjà démarré…

Et si l'un des principes de base du fonctionnement des SDN masquait une inquiétante faille de sécurité ? Les contrôleurs des Software Defined Networks, pilotés de manière logicielle, configurent le réseau en attribuant de nouvelles règles de traitement des flux aux switches. Et c'est ce fonctionnement même qui poserait problème.

C'est du moins le résultat des travaux de trois chercheurs italiens, Mauro Conti (de l'université de Padoue), Fabio De Gaspari et Luigi V. Mancini (tous deux de l'université de Sapienza). *« Nous pensons que des aspects importants de la sécurité des SDN restent encore inexplorés »*, notent-ils dans leur rapport. Pour en convaincre la communauté, ils ont mis au point une nouvelle forme d'attaque, baptisée Know Your Enemy (KYE), au moyen de laquelle un attaquant peut recueillir des informations vitales sur la configuration du réseau.

Moisson d'informations de configuration

A travers leurs travaux, ils entendent démontrer comment un attaquant peut recueillir des informations sur la configuration des outils de sécurité du réseau (dont les seuils de détection d'attaque par scan), sa politique de qualité de service ou encore sa virtualisation. Et d'ajouter qu'une seule table de routage d'un commutateur peut fournir ces informations tout en servant de canal d'attaque. Cerise sur le gâteau : *« nous montrons qu'un attaquant peut effectuer une attaque KYE dans un mode furtif, à savoir sans risquer d'être détecté »*, expliquent-*ils*.

Selon les universitaires, un attaquant pourrait se connecter aux ports d'écoute passive qu'intègrent la plupart des commutateurs pour le débogage à distance afin de récupérer le plan de routage (notamment avec la commande 'dpctl' sur les HP Procurve qu'ils ont utilisés au cours de leurs travaux), en déduire des informations sur la table de routage, espionner le contrôle du trafic en cas d'absence de protection de ce dernier (par chiffrement TLS ou usage de certificats d'authentification), exploiter les vulnérabilités connues dans les systèmes d'exploitation des switches pour introduire une backdoor, ou encore extraire la table de routage ou le contenu de la mémoire du commutateur pour la copier vers un support externe au réseau.

Obscurcir pour limiter les risques

Autant d'informations qui permettent une attaque ou un espionnage plus massif ou plus ciblé du SI dans l'absolu. Les conclusions des chercheurs italiens sont d'autant plus inquiétantes que, en apportant une flexibilité optimale de gestion des réseaux, les technologies SDN sont de plus en plus adoptées par les opérateurs et grandes entreprises. Le rapport insiste bien sur le fait que ces possibilités d'espionnage ne sont pas liées aux systèmes matériels présents sur le réseau, mais bien à son fonctionnement intrinsèque.

Pour limiter les risques d'attaque, les scientifiques détaillent une contremesure basée sur un « *obscurcissement* » des flux entrants. *« S'il était possible d'empêcher l'attachant de comprendre quel flux est responsable de l'application des règles de routage, l'attaque KYE serait irréalisable »*, indiquent-ils. Ce qu'ils ont réussi à faire en exploitant la possibilité de modification du transit des flux dont dispose un switch OpenFlow. Et les chercheurs de rappeler que les risques décrit dans leur travail ne touchent que les réseaux SDN, les structures « traditionnelles » étant par défaut épargnées. Ce qui ne les empêche pas d'avoir leurs propres soucis de sécurité.

Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Sécurité : les réseaux SDN ouverts à tous les vents (mauvais) | Silicon