Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « *judiciaire* ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « *Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges* ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une initiative franco-allemande contre le chiffrement numérique

---

Révélations sur de petits piratages informatiques entre alliés…

Révélations sur de petits piratages informatiques entre alliés…

C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.
Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »
Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »
Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Caméras IP installées par des incompétents ? Une aubaine pour les pirates

Caméras IP installées par des incompétents ? Une aubaine pour les pirates

---

Le piratage des caméras de vidéo surveillance, un jeu d'enfant pour les plus dégourdis du web. Sauf que ces pirates n'ont rien de génie, ils profitent uniquement de la fainéantise des utilisateurs.

Le piratage des caméras de vidéo surveillance n'est pas nouveau. Je vous parlais déjà de ces infiltrations de webcams en 2000. En novembre 2015, par exemple, je revenais sur un fichier contenant des centaines de webcams non sécurisées vendues dans le blackmarket ou encore de ce bébé réveillé par des hurlements d'un idiot du village ayant pris la main sur le baby phone de la famille.

En 2014, je vous révélais la création d'un site Internet Russe qui référencent plusieurs dizaines de milliers de webcams. Bref, un business juteux pour les commerçants du voyeurisme et autres vendeurs de données sensibles (La boutique est-elle vide ? Le hangar stocke en ce moment des téléphones portables ; la banque vient d'être livrée en billets frais…).

Je te soupçonne de taper dans la caisse ! (Boutique de la Ville de Rai)

La sécurité des caméras sur IP est souvent mise à la mal comme j'ai pu le montrer dans ZATAZWeb.tv de mars 2014. Il ne devrait pas être si facile, normalement, de regarder dans la chambre d'un étranger, et encore moins dans des centaines de chambres filmées par ces caméras de vidéo surveillance. Pourtant, cela reste possible comme je vais vous l'expliquer plus bas.

Montrez moi votre contrat, que je vous renseigne. (Boutique du 92)

Failles et mots de passe facilitent le piratage des caméras de vidéo de surveillance

Pour accéder à une caméra de vidéo surveillance rien de plus facile. D'abord avoir l'IP de la cible. Un détail pour les adeptes du social engineering. Autant dire que cette adresse n'est à communiquer à personne. Lisez le mode d'emploi de votre caméra. Chercher les options de sécurité proposées. Soyons honnête, plus votre webcam IP aura d'option, plus elle sera coûteuse. Mais la réflexion vaut, je pense, la sécurité de ce que vous souhaitez protéger. Ensuite, le malveillant va rechercher la marque de votre matériel. Pour cela, rien de plus simple une fois encore. La page d'accès à l'administration de votre matériel parle.

Mais tu vas le changer ce password… c'est marqué en GRAS ! (Hôtel du 77)

Un conseil, faites de manière à ce qu'elle ne soit pas lisible : un Htaccess par exemple, ou modifier le logo et toutes marques de reconnaissance pour le malveillant. Ensuite, le mot de passe. Trop de webcam IP, de caméras de vidéo surveillance gardent le mot de passe usine. Je vous laisse imaginer la facilité déconcertante que de retrouver ce sésame dans les notices et listes disponibles sur la toile. Un *admin:admin ; root:root et autre admin:0000* sont légions. Des clés qui se changent. Vous le faites bien quand vous perdez les clés de votre maison, faites le sur Internet. Enfin, les failles. Assurez-vous que votre cerbère ne soit pas référencé comme étant un outil « *open bar*« . Pour cela, un petit coup de Google ou ne soyez pas timide, posez la question !

La bijouterie est vide ! Le matériel, la caisse, le coffre sont repérés. Autant d'informations qui faciliteront l'action d'un malveillant. Vous aurez remarqué le petit « H@ck3D » en haut à gauche qui ne semble perturber personne !

Branleurs, voleurs, mateurs… même combat

Dans mon exemple, le pirate possède donc dorénavant l'IP, l'accès à la page d'administration de votre webcam IP, sa marque, vous n'avez pas changé le mot de passe usine et si c'est le cas, il vient de rechercher sur la toile les failles et accès « *pasvraimentprévudanslemodedemploi*« . Dernier exemple en date que ZATAZ a pu constater, l'alerte au sujet de la société AXIS. Un logiciel pirate, baptisé « *Hack AXIS* » permettait (permet toujours pour les caméras non mises à jour, NDR) d'accéder à la racine des périphériques sans avoir besoin de connaitre le mot de passe ; changer le mot de passe du matériel ; contrôler la caméra et, dans ce cas, lancer des attaques via la caméra transformée en Zombie/botnet. La caméra prise en main de la sorte par un pirate au fait de la faille, même mise à jour ensuite, restait dans le sac à malveillance de l'intrus. Une attaque d'autant plus gênante que l'exploit a été diffusé, en juillet 2016.

Bref, voilà donc le pirate avec une nouvelle source d'information à votre sujet. Imaginez, le serveur et l'IP l'oriente sur votre situation numérique ; la caméra, et les informations qu'elle peut transporter, fournissent au malveillant les yeux qu'il n'avait pas. En France, c'est une liste de plusieurs milliers de webcams accessibles qui trainent sur la toile, que ce soit dans le blackmarket ou sur des sites offrant de regarder à travers ces « yeux » non sécurisés.

Auteur : Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Vidéo surveillance : Vous n’en avez pas marre d’être des idiots du 2.0 – ZATAZ

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

---

Privacy Shield adopté, nouveau fondement pour les transferts de données outre-atlantique

Privacy Shield adopté, nouveau fondement pour les transferts de données outre-atlantique

---

La Commission européenne a adopté mardi 12 juillet dernier le Privacy Shield. Ce nouvel accord remplace le Safe Harbor, et aura pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis adhérant à ce dispositif.

L'adoption de ce nouveau « bouclier de protection des données personnelles » est l'aboutissement d'un long processus, commencé dès 2014, avec la révélation par l'ancien agent de la CIA Edward Snowden de la surveillance de masse effectuée par les services de renseignements américains puis par le refus, sur ce motif, d'un citoyen autrichien de transférer ses données vers les Etats-Unis. La Cour de Justice de l'Union Européenne a ainsi dans une décision du 6 octobre 2015 déclaré invalide la décision de la Commission du 26 juillet 2000 constatant que les Etats-Unis assurent un niveau de protection adéquat aux données caractère personnel transférées. En effet la Cour a considéré que les Etats-Unis n'apportaient pas les garanties suffisantes pour protéger les données des citoyens Européens au motif que les pouvoirs des services de renseignements américains s'étendaient à toutes données exportées depuis l'Europe dès lors que l'intérêt de sécurité publique était en cause. La CJUE a considéré que ces intrusions étaient disproportionnées et heurtaient les principes de la Charte des droits fondamentaux de l'Union Européenne.
A la suite de cette décision, l'ensemble des transferts de données personnelles vers des entités situés aux Etats-Unis sur le fondement du Safe Harbor ont dû être suspendus et des solutions alternatives mises en place. Le Groupe de travail de l'article 29, qui est constitué des différents autorités de protection des données à caractère personnel au sein de l'UE (le G29), a assuré les organisations souhaitant poursuivre le transfert de données de l'UE vers les Etats-Unis qu'elles pouvaient se fonder sur les mécanismes alternatifs prévus par la directive de 1995 relative à la protection des données, telles que les clauses contractuelles types et les règles d'entreprise contraignantes (BCR).
En parallèle la Commission européenne et le gouvernement américain engageaient des discussions afin de trouver un nouvel accord sur le transfert des données personnelles des citoyens européens vers les Etats-Unis.
Le 2 février 2016, la Commission européenne et le gouvernement des États-Unis sont parvenus à un premier accord politique. La Commission a présenté le projet d'accord le 29 février 2016. Le groupe de travail « Article 29˝ a ensuite rendu un premier avis le 13 avril 2016 assez critique en particulier sur l'insuffisance des gardes fous accordés aux citoyens européens pour contrôler l'usage de leurs données.
Une résolution a été adoptée le 26 mai par le Parlement européen, et la Commission a clôturé la procédure d'adoption du nouvel accord le 12 juillet 2016 en adoptant une décision d'adéquation visant à reconnaitre au mécanisme « EU-U.S. Privacy Shield » un niveau de protection « essentiellement équivalent » aux exigences européennes. .

Le nouveau dispositif : Comment ça marche ?

Le Privacy Shield vise à permettre aux entreprises de transférer plus facilement vers les Etats Unis des données personnelles collectées dans l'Union européenne, tout en protégeant les droits des personnes concernées.

Le Privacy Shield est fondé sur les principes suivants:
• Des obligations strictes pour les entreprises qui traitent des données : dans le cadre du nouveau dispositif, le ministère américain du commerce procédera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes, afin de veiller à ce qu'elles observent les règles auxquelles elles ont souscrit. Les entreprises dont la pratique ne sera pas conforme aux nouvelles règles s'exposeront à des sanctions et à une radiation de la liste des entreprises adhérant au dispositif.
• Un accès des pouvoirs publics américains soumis à des conditions claires et à des obligations de transparence : les États-Unis ont donné à l'Union européenne l'assurance que l'accès des pouvoirs publics aux données à des fins d'ordre public et de sécurité nationale serait soumis à des limitations, à des conditions et à des mécanismes de surveillance bien définis. De même, tous les citoyens de l'Union bénéficieront pour la première fois de mécanismes de recours dans ce domaine. Les États-Unis ont exclu toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire dans le cadre du bouclier de protection des données UE-États-Unis. Le secrétaire d'État américain a instauré une possibilité de recours pour les Européens dans le domaine du renseignement national en créant un mécanisme de médiation au sein du département d'État ;
• Une protection effective des droits individuels : tout citoyen estimant que les données le concernant ont fait l'objet d'une utilisation abusive dans le cadre du Privacy Shield bénéficiera de plusieurs mécanismes accessibles et abordables de règlement des litiges. Lorsqu'un litige n'aura pas été réglé par l'un de ces moyens, un mécanisme d'arbitrage sera disponible, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouvert aux citoyens de l'UE passera par un médiateur indépendant des services de renseignement des États-Unis ;
• Un mécanisme de réexamen annuel conjoint : ce mécanisme permettra de contrôler le fonctionnement du Privacy Shield, et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale. Le réexamen sera mené par la Commission européenne et le ministère américain du commerce, lesquels y associeront des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données. La Commission s'appuiera sur toutes les autres sources d'information disponibles et adressera un rapport public au Parlement européen et au Conseil.

Le Privacy Shield reste donc un mécanisme souple, à l'instar du Safe Harbor sous-tendu par une nécessité d'auto-certification des entreprises américaines. Pour bénéficier de l'accord et faciliter les transferts de données personnelles entre l'Europe et les Etats Unis, les entreprises américaines adhérant au dispositif devront s'engager à respecter les obligations de protection des données du Privacy Shield.
La décision « Privacy Shield » entrera en vigueur à compter de sa notification à chacun des Etats membres de l'Union européenne et sera contraignante pour ceux-ci. L'applicabilité de ce cadre juridique aux entreprises concernées sera ensuite subordonnée à l'enregistrement de celles-ci auprès des autorités américaines en charge de la mise en œuvre du dispositif. Les entreprises américaines pourront obtenir la certification Privacy Shield à partir du 1er août 2016.
Si un des objectifs poursuivi par le Privacy Shield est d'exclure tout traitement massif des données européennes transatlantique la collecte massive de données pourra cependant être effectuée si elle est limitée à des objectifs de sécurité nationale prédéfinis : espionnage, terrorisme, armes de destruction massive, menaces sur la cyber-sécurité, sur les armées, ou menaces criminelles transnationales.

Un accord déjà critiqué

En dépit de son objectif d'amélioration de la protection des données personnelles, le nouveau cadre fait pourtant l'objet de nombreuses critiques.
Le G29 dans son avis d'avril 2016 avait notamment fait part de ses préoccupations sur un certain nombre de points manquants, incomplets ou peu clairs. Le G29 avait en particulier regretté l'absence de plusieurs principes tels que la limitation de la durée de conservation et l'interdiction des décisions automatisées. En ce qui concerne l'accès par les autorités publiques aux données, le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. Enfin, le G29 avait émis des doutes sur l'indépendance du médiateur (Ombudsperson) et sur le fait qu'il dispose de pouvoirs suffisants pour exercer son rôle efficacement et permettre d'obtenir un recours satisfaisant en cas de désaccord avec l'administration.
Il n'est pas certain que la nouvelle rédaction satisfasse pleinement le G29.
De même le 30 mai 2016, le contrôleur européen de la protection des données (EDPS en anglais), Giovanni Buttarelli, dans un Avis sur le Privacy Shield, demandait des améliorations « significatives » avant son adoption par la Commission européenne (CE). Selon l'Avis de l'EDPS: « La proposition de Privacy Shield est un pas dans la bonne direction, mais dans sa rédaction actuelle elle ne prend pas suffisamment en compte, de notre point de vue, toutes les garanties appropriées pour protéger les droits européens des individus à la vie privée et à la protection des données notamment en ce qui concerne le recours juridictionnel. Des améliorations significatives sont nécessaires dans l'hypothèse où la Commission européenne souhaiterait adopter une décision d'adéquation ».
Le G29 mène actuellement une analyse de la décision de la Commission et se réunira le 25 juillet 2016 afin de finaliser sa position.
Article original de DLA PIPER

Réagissez à cet article

Original de l'article mis en page : Adoption du Privacy Shield par la Commission européenne : un nouveau fondement pour les transferts de données outre-atlantique, Partenaire – Les Echos Business

---

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

---

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

---

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

	Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.
En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « *si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace* » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.

Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.
Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « *alors même qu'aucune infraction n'est constatée* ».
L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.
Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».
Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence – Politique – Numerama