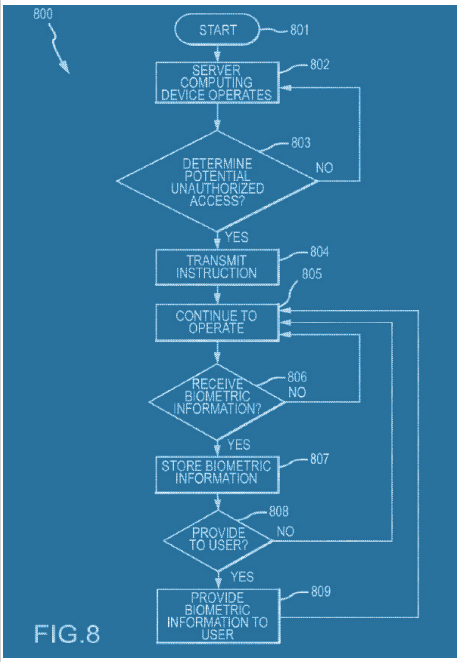
Les futurs iPhone pourraient renvoyer des données biométriques de leurs voleurs

Les futurs iPhone pourraient renvoyer des données biométriques de leurs voleurs

Apple a déposé un brevet sur une méthode qui permettrait de glaner un maximum d'informations sur les voleurs d'iPhone, dont leur photo et une image de leur empreinte digitale.

Apple fait tout pour éviter que ses clients se fassent voler leur iPhone, et imagine donc un ensemble de stratégie pour décourager les voleurs. La firme de Cupertino permet déjà de localiser un téléphone à distance, de le verrouiller, ou encore d'effacer les données depuis son ordinateur. Mais prochainement, Apple pourrait aussi permettre à ses clients d'obtenir des informations biométriques et d'autres données liées au voleur potentiel d'un téléphone.
Comme le remarque Apple Insider, le groupe a en effet obtenu cette semaine la publication par le bureau des brevets américain d'un nouveau brevet portant sur la « capture biométrique pour l'identification d'un utilisateur non utilisé ». Apple y explique que les différents capteurs d'un iPhone ou d'un iPad pourraient être utilisés pour rassembler un maximum d'informations sur le voleur, et les envoyer vers un ordinateur associé au compte Apple de la victime.
La firme de Cupertino explique ainsi qu'il serait possible de reconstituer des empreintes digitales du voleur ou de toute personne qui tente d'accéder illégalement à l'iPhone, au besoin en combinant jusqu'à une quinzaine d'essais de lectures d'empreintes via son capteur Touch ID. Cette hypothèse est toutefois surprenante de la part d'Apple, qui avait rassuré sur le fait que le capteur qu'il avait conçu ne serait pas capable de restituer sur demande une image de l'empreinte digitale.

« *Aucune image de votre empreinte n'est conservée par la fonctionnalité Touch ID. Celle-ci en stocke uniquement la représentation mathématique, et personne ne peut déterminer votre empreinte à partir de cette dernière* », peut-on lire sur le site d'Apple. Il précise :
« *La puce de votre appareil profite également d'une architecture de sécurité avancée, appelée Enclave sécurisée. Celle-ci permet de protéger codes d'accès et données liées aux empreintes. Ces dernières sont chiffrées et protégées par une clé, uniquement accessible via l'enclave sécurisée, qui utilise les données en question pour vérifier que votre empreinte correspond aux informations enregistrées sur l'appareil.*
L'enclave sécurisée est totalement indépendante des autres composants de la puce et des autres fonctionnalités d'iOS. Ainsi, iOS et toute autre application n'ont jamais accès aux données liées aux empreintes, et celles-ci ne sont ni enregistrées sur les serveurs Apple, ni sauvegardées dans iCloud ou ailleurs. Seule la fonctionnalité Touch ID a accès à ces données, qui sont incompatibles avec les autres bases de données d'empreintes. »
Dans ces conditions, il faudrait qu'Apple revoit l'architecture de ses iPhone et de Touch ID pour permettre la capture de l'empreinte d'un éventuel voleur, au risque de troubler l'image de protectrice de la vie privée qu'elle a mis du temps à construire.
Ce n'est pas tout. Apple imagine aussi capter des photos de celui qui cherche à débloquer un iPhone sans en avoir les droits, du son, des coordonnées GPS ou même des indications comme la pression de l'air, pour rassembler un maximum d'informations qui permettraient d'identifier avec certitude le coupable. Selon les configurations, les données pourraient être collectées et envoyées systématiquement, ou selon des scénarios plus fins (par exemple au bout de 5 essais infructueux, si l'iPhone est à un plus de 10 km de tel lieu, etc.).
Rien ne dit néanmoins qu'Apple souhaite véritablement mettre en œuvre ce brevet, qui ne traduit à ce stade qu'une idée et pas une intention de commercialisation. L'avenir le dira.



Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Les futurs iPhone pourraient renvoyer des données biométriques de leurs voleurs – Tech – 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

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

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

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

---

Ransomware : Locky se fait passer pour un fichier système Windows

Alerte : le Ransomware Locky se fait passer pour un fichier système Windows

Une variante du ransomware Locky se fait passer pour un fichier DLL dans l'espoir de tromper les filtres de sécurité.

Toujours plus vicieux. Le ou les groupes de cybercriminels qui se cachent derrière le Locky ne cessent de faire évoluer l'un des plus populaires ransomware de la Toile. Objectif : déjouer les dernières mises à jour des solutions de protection et attraper toujours plus de victimes dans les filets. Victimes qui, rappelons-le, n'auront d'autre choix que de payer une rançon (généralement en bitcoin) pour récupérer leurs données si elles n'ont pas pris soin de faire des sauvegardes.
Aux dernières nouvelles, la dernière variante de Locky se distingue en se cachant derrière un fichier .DLL et non plus derrière un .EXE comme précédemment. Les DLL (Dynamic Link Library) sont des bibliothèques logicielles exploitées par Windows pour exécuter une application. « Ce que nous trouvons le plus intéressant dans cette dernière vague Locky est qu'au lieu de télécharger un binaire EXE, ce composant ransomware arrive maintenant en tant que binaire DLL, soulignent les chercheurs en sécurité de Cyren. Qui plus est, le fichier DLL ainsi téléchargé est personnalisé pour empêcher les scanners de virus de le détecter facilement. »

Attention au zip
Si le DLL parvient à passer les filtres de sécurité, son exécution reste identique à celle constatée jusqu'à présent, à savoir que le rançongiciel part à la recherche de fichiers à chiffrer avant de rediriger ses victimes vers une page affichant la facture (et la méthodologie du mode de paiement). Petite variante, le mécanisme d'attaque attribue l'extension .zepto aux fichiers devenus illisibles. « Comparé aux précédentes, cette nouvelle variante ajoute un autre niveau d'obscurcissement qui déchiffre et exécute le réel script chargé du téléchargement de Locky », constatent toutefois les chercheurs.
Le mode de distribution et d'infection de JS/Locky.AT!Eldorado, nom de cette nouvelle variante de Locky, n'a, lui, pas changé : il tente toujours de se propager par l'envoi d'un e-mail trompeur invitant à cliquer sur une pièce jointe au format ZIP renfermant le code Javascript qui va déclencher la décompression des fichiers et l'exécution des commandes de téléchargement de l'agent infectieux proprement dit. Etre doublement attentif lors de la réception de ce genre d'e-mail (et éviter de cliquer sur des fichiers ZIP sans être absolument certain de leur origine) reste le meilleur moyen d'éviter de l'infection.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Ransomware : Locky se fait passer pour un fichier système Windows

---

Où en est la protection des lanceurs d’alerte ?

	Où en est la protection des lanceurs d’alerte ?

Lanceurs d'alerte : nullité du licenciement d'un salarié ayant dénoncé de bonne foi des faits susceptibles de recevoir une qualification pénale.
Pour la première fois, par un arrêt du 30 juin 2016 (n°15-10.557), la Cour de cassation s'est prononcée sur la sanction du licenciement d'un salarié lanceur d'alerte.
Dans cette affaire, le directeur administratif et financier d'une association qui assurait la gestion d'un centre d'examen de santé avait été licencié pour faute lourde en mars 2011 après avoir dénoncé auprès du procureur de la République des faits susceptibles de constituer une escroquerie et un détournement de fonds de la part d'un membre du conseil d'administration et du président de l'association.
(Cass. Soc. 30 juin 2016, n°15-10.557)

1) La nullité du licenciement du salarié lanceur d'alerte prononcé en violation de la liberté d'expression
A l'époque des faits donc, la loi n°2013-1117 du 6 décembre 2013 qui prévoit que le licenciement d'un salarié fondé sur le fait qu'il témoigne ou dénonce, de bonne foi, des faits susceptibles de recevoir une qualification pénale est nul, n'était donc pas applicable.
Aussi, la cour d'appel avait estimé que le licenciement du directeur administratif et financier était certes dépourvu de cause réelle et sérieuse puisqu'il avait dénoncé les faits en parfaite bonne foi, mais elle avait refusé de prononcer la nullité du licenciement.
La cour d'appel avait ainsi fait une stricte application de la règle selon laquelle il n'y a « pas de nullité sans texte » hors les cas d'atteinte à une liberté fondamentale et avait relevé la loi du 6 décembre 2013 n'était pas applicable au moment des faits.
Pourtant, la chambre sociale, saisie d'un pourvoi formé par le salarié contre cette décision, a estimé, au visa de l'article 10§1 de la Convention européenne des droits de l'Homme, que le licenciement du lanceur d'alerte était nul car prononcé en violation de la liberté d'expression :
« Vu l'article 10 § 1 de la de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ;
Attendu qu'en raison de l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, de bonne foi, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est frappé de nullité ;
Attendu que pour dire qu'il n'y avait pas lieu d'annuler le licenciement et débouter le salarié de sa demande de réintégration, l'arrêt retient que la nullité ne peut être prononcée en l'absence de texte la prévoyant puisque les articles L. 1132-3-3 et L. 1132-4 du code du travail issus de la loi n° 2013-1117 du 6 décembre 2013, n'étaient pas applicables à l'époque du licenciement et que les faits dénoncés par le salarié ne se rattachaient pas à des faits de corruption, ce qui exclut l'application de l'article L. 1161-1 du code du travail ;
Qu'en statuant ainsi, alors qu'elle avait constaté que le licenciement était motivé par le fait que le salarié, dont la bonne foi ne pouvait être mise en doute, avait dénoncé au procureur de la République des faits pouvant être qualifiés de délictueux commis au sein de l'association, la cour d'appel qui n'a pas tiré les conséquences légales de ses constatations, a violé le texte susvisé. »
Ce faisant, la chambre sociale de la Cour de cassation se conforme à l'approche adoptée par la Cour européenne des droits de l'Homme (*CEDH, 12 février 2008, Guja c. Moldova, n°14277/04*).

2) Une protection contre le licenciement conditionnée à la seule bonne foi du lanceur d'alerte
La nullité du licenciement est toutefois soumise à la condition que le salarié qui a dénoncé des faits susceptibles de recevoir une qualification pénale l'ait fait de bonne foi.
La bonne foi doit ici être interprétée comme la croyance légitime du salarié en la commission desdits faits.
Aussi, le salarié qui dénoncerait une infraction pénale de manière parfaitement mensongère simplement pour se protéger d'un licenciement qu'il sentirait approcher, ne pourrait pas bénéficier de cette solution.
En revanche, la protection s'appliquerait à un salarié qui dénonce de bonne foi des faits susceptibles de recevoir une qualification pénale même s'il s'avère ensuite que le salarié s'est trompé et qu'aucune infraction n'a finalement été commise.
En effet, l'attendu de principe de l'arrêt du 30 juin 2016 ne laisse aucune place au doute à cet égard puisqu'il est formulé ainsi :
« *Attendu qu'en raison de l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, **de bonne foi**, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est frappé de nullité* ; »
En outre, par cet arrêt la chambre sociale va encore plus loin que son homologue européen puisque contrairement à la Cour européenne des droits de l'Homme, elle ne fait aucune référence à l'intérêt général comme condition d'application de la protection.
Enfin, la chambre sociale ne subordonne pas non plus le bénéfice de cette protection à la nécessité de respecter la graduation de la procédure d'alerte. En effet, pour la Cour de cassation, peu importe que le salarié ait averti sa hiérarchie préalablement à la dénonciation auprès de l'autorité judiciaire ou qu'il ait directement informé le procureur de la République.
De même, si en l'espèce, le directeur administratif et financier avait porté sa dénonciation auprès du procureur de la République, la Cour de cassation, dans son communiqué relatif à l'arrêt, précise que : *« Une telle décision est de nature à protéger les lanceurs d'alerte, dans la mesure où, la chambre sociale instaure cette immunité non seulement lorsque les faits sont portés à la connaissance du procureur de la République mais également, de façon plus générale, dès lors qu'ils sont dénoncés à des tiers ».*
Par cette décision, la Cour de cassation consacre donc la solution retenue par le législateur dans la loi du 6 décembre 2013 et étend ainsi la protection contre le licenciement à l'ensemble des lanceurs d'alerte, peu important la date des faits ayant donné lieu au licenciement.
Elle fait ainsi primer la liberté d'expression sur toute autre considération et rappelle donc que toute sanction prise en violation de cette liberté fondamentale doit être frappée de nullité.
La Cour de cassation entend d'ailleurs donner une résonance toute particulière à cet arrêt qu'elle publiera au sein de son rapport annuel.
Pour cause, le sujet des lanceurs d'alerte est plus que d'actualité puisque la loi Sapin 2 telle que modifiée par le Sénat qui l'a adoptée le 8 juillet dernier doit passer en commission mixte paritaire prochainement avant d'être votée définitivement.
Article original de Frédéric Chhum, Avocat.

Original de l'article mis en page : Lanceurs d'alerte : nullité du licenciement d'un salarié ayant dénoncé de bonne foi des faits susceptibles de recevoir une qualification pénale. Par Frédéric Chhum, Avocat.

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

Le FBI remonte une Cyberattaque jusqu’à Abidjan

Le FBI remonte une Cyberattaque jusqu’à Abidjan

La Banque centrale des Etats-Unis d'Amérique reçoit sur son système d'information (SI) un flux important de données provenant d'un réseau de machines inconnues. Lorsque les cyberdétectives du Bureau fédéral d'investigation (FBI) essaient de remonter jusqu'à l'origine de l'offensive, ils sont dirigés vers plusieurs continents, via des serveurs informatiques qui interagissent entre eux. Autant de rebonds sur des machines, rendant la piste des attaquants difficile à suivre.

Toutefois, des empreintes laissées sur internet permettent aux agents du FBI de localiser des serveurs situés en Côte d'Ivoire. Signe de la gravité de la cyberattaque, les fins limiers du web américain débarquent à Abidjan.

Sur place, après une séance de travail avec l'équipe d'experts en sécurité informatique du**CI-CERT (Côte d'Ivoire – Computer emergency response team)**, le FBI parvient à identifier à partir d'une liste d'adresses IP, des entreprises ivoiriennes, dont les machines infectées, sont utilisées à leur insu par des hackers basés en Thaïlande, pour lancer des offensives contre le SI de la Banque centrale des Etats-Unis d'Amérique.

Ce n'est pas le scénario d'un film américain, mais une réelle attaque informatique qui s'est déroulée dans le premier trimestre de l'année 2013, et qui a été décrite à CIO Mag par Jean-Marie Nicaise Yapoga, chef de service du CI-CERT, alors responsable technique adjoint. Pointant la vulnérabilité des entreprises qui s'exposent à des risques dus au non-respect des bonnes pratiques en matière de cybersécurité (Cf. CIO Mag N°29 – décembre 2013/janvier 2014).

L'expertise du CERT ivoirien dans cette affaire a permis aux entreprises infiltrées de limiter les dégâts et de réduire le coût du retour à un fonctionnement normal. Mais elle rappelle surtout l'essentiel de sa mission : assurer, au niveau local, la fonction de point focal pour toutes les questions de cybersécurité.

Des couches de sécurité sans protection suffisante

Vu l'ampleur des menaces sur les fleurons de l'économie ivoirienne, un pan de la mission de sensibilisation du CI-CERT est toujours orientée vers les chefs d'entreprise. Moins réceptives à l'idée d'investir dans le recrutement d'un responsable de la sécurité des systèmes d'information (RSSI), nombre d'entreprises empilent en effet des couches de sécurité (pare-feu, anti-virus, etc.), qui n'offrent souvent pas de protection suffisante.

Une situation que le chef de service déplore dans la parution de CIO Mag susmentionnée : « C'est lorsqu'elles (ces entreprises) doivent faire face à des incidents informatiques qu'elles se rendent compte de l'importance de la cybersécurité. Malheureusement, entre l'alerte et le temps mis pour rétablir le réseau, l'entreprise peut avoir déjà perdu plusieurs millions de FCFA. »

Partenariat public/privé

Côte d'Ivoire – Computer emergency response team.

Aujourd'hui, le CI-CERT peut se vanter d'avoir favorisé le recrutement de RSSI dans des entreprises de télécommunications. « On en retrouve également au sein des banques et de plusieurs groupes d'entreprises », révélait l'analyste-administrateur de sécurité des SI.

Pour limiter les incidents informatiques, le CERT ivoirien organise des ateliers et séminaires de formation, notamment avec les directeurs de système d'information (DSI) et les RSSI. Objectif ? Créer un partenariat public/privé destiné à poser des actions de prévention. C'est-à-dire, diffuser des bulletins d'information et des avertissements, et établir un réseau d'information et d'alerte gouvernementale sur les attaques et les menaces.

Au cours de ces rencontres, les responsables informatiques et de cybersécurité sont briffés sur les menaces répertoriées sur le cyber espace national mais également sur les types d'attaques rapportées au CI-CERT par ses partenaires internationaux : IMPACT (Organisation internationale de lutte contre les cyber-menaces) et la communauté des CERT étrangers.

La nécessité de se doter d'un CERT

En Côte d'Ivoire, la nécessité de se doter d'un CERT (Computer incident response team) a été perçue dès 2009. Dans un contexte où l'image du pays était fortement écorchée sur le plan international du fait des nombreux cas de défacement de sites web gouvernementaux et de cyberescroquerie.

Hormis les pertes financières provoquées par ces actes de piratage avérés, d'autres conséquences majeures ont été enregistrées : « Adresse IP ivoiriennes mises sur des listes noires ; achats en ligne interdits avec IP des FAI ivoiriens sur les plateformes telles que PayPal et Yahoo », peut-on lire dans un document dont CIO Mag a reçu copie.

C'est donc pour faire face à la récurrence de ces incidents qui constituent une menace, à la fois sur l'économie et la notoriété du pays que le CI-CERT a vu le jour, en 2009. Depuis leurs bureaux situés à l'époque dans la commune du Plateau, en plein centre des affaires, cinq ingénieurs informaticiens se sont activés à écrire les premières pages du CI-CERT.

Sous tutelle de **l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI)**, leurs actions consistaient à lutter contre la cyberescroquerie et à émettre des alertes et annonces de sécurité.

Plus de 40 000 incidents traités au 1er semestre 2015

Aujourd'hui, cette structure joue pleinement son rôle de cyber pompier de l'Etat avec une quinzaine d'ingénieurs menant une série d'activités regroupées en deux axes:

• Protection du cyber espace national avec un portefeuille de services réactifs (alertes et avertissements, traitement d'incidents, coordination de traitement de vulnérabilité, etc.) et proactifs (annonces, veille technologique, détection d'intrusion, partage d'informations), ainsi qu'un service de management de la qualité de la sécurité orienté sur la sensibilisation, la formation et la consultance.

• Lutte contre la cybercriminalité dans le cadre de la Plateforme de lutte contre la cybercriminalité (PLCC) grâce à une convention de partenariat entre l'ARTCI et la Police nationale.

Au cours du premier semestre de 2015, le CI-CERT a collecté et traité 40 264 incidents de sécurité informatique, envoyé 145 bulletins et avis de sécurité et participé aux cyberdrill UIT-IMPACT et OIC-CERT, traduisant son leadership sur le cyber espace national.

Article original de CIO-Mag

Réagissez à cet article

Original de l'article mis en page : Cyberattaque : quand le FBI débarque à Abidjan | CIO MAG

La Loi de Programmation

militaire au secours de la sécurité des systèmes d’information des opérateurs d’importance vitale

La Loi de Programmation militaire au secours de la sécurité des systèmes d’information des opérateurs d’importance vitale

Pour faire face aux nouvelles menaces cyber et répondre aux besoins de la sécurité nationale, les opérateurs d'importance vitale (OIV), dont le bon fonctionnement est indispensable à celui de la Nation, ont mis en œuvre depuis le 1er juillet 2016, pour les premiers d'entre eux, des mesures relatives à la sécurisation de leurs systèmes d'information. Ces mesures sont définies par l'article 22 de la Loi de Programmation militaire (LPM) qui a introduit les articles L. 1332-6-1, L. 1332-6-2, L. 1332-6-3, L. 1332-6-4, L. 1332-6-5, L. 1332-6-6 du Code de la défense.

La France est le premier pays à s'appuyer sur la réglementation pour définir un dispositif efficace de cybersécurité de ses infrastructures critiques, qui sont indispensables au bon fonctionnement et à la survie de la Nation.

A partir du **1er juillet 2016**, l'entrée en vigueur d'une première vague d'arrêtés a marqué la mise en place effective de ce dispositif pour les secteurs d'activité suivants « produits de santé », « gestion de l'eau » et « alimentation ». D'autres arrêtés seront progressivement publiés au cours de l'année 2016.
Ces arrêtés sectoriels, signés par le Secrétaire général de la défense et de la sécurité nationale par délégation du Premier ministre, fixent les critères d'application des mesures relatives à la sécurité des systèmes d'information des OIV [J. Barnu Quelles conséquences pour les OIV] notamment :
• les règles de sécurité, à la fois organisationnelles et techniques, sécurisent l'accès et la gestion des systèmes d'information ciblés. Elles prennent aussi en compte les spécificités de chaque secteur, leurs enjeux et contraintes ainsi que leur niveau de maturité en matière de sécurité du numérique.
• les modalités d'application des autres mesures avec l'identification des systèmes d'information d'importance vitale (SIIV), la notification d'incidents de sécurité et les contrôles pour suivre la mise en place du dispositif.

Tout savoir sur la sécurité des systèmes d'information des OIV avec une nouvelle rubrique dédiée.
Un nouvel espace d'information dédié à la sécurité des systèmes d'information des OIV est dès aujourd'hui en ligne sur le site Internet de l'ANSSI.
Cette rubrique « OIV » est accessible depuis l'onglet « administration » et « entreprise », en page d'accueil.
Elle a été conçue pour être à la fois :
• un espace de ressources pratiques pour les opérateurs impactés, directement ou indirectement, par le dispositif français de cybersécurité des OIV ;
• un espace d'information pour un public intéressé par le dispositif français de cybersécurité des infrastructures critiques.
Article original de ANSSI

Réagissez à cet article

Original de l'article mis en page : Renforcer la sécurité des systèmes d'information des opérateurs d'importance vitale avec la publication des premiers arrêtés sectoriels | Agence

nationale de la sécurité des systèmes d’information

Alerte : un malware Android commandé par… Twitter

Alerte : un malware Android commandé par… Twitter

Les concepteurs du malware Android Twittor se servent du réseau social pour envoyer des instructions à la souche infectieuse. Une technique plus furtive que les classiques serveurs de commande et contrôle.

L'éditeur d'antivirus Eset affirme avoir découvert le premier malware commandé… par des tweets. Selon la société slovaque, Android/Twittor est une application Android malveillante, probablement diffusée par SMS ou via des URL piégées, qui masque sa présence et se connecte à un compte Twitter dans l'attente d'instructions. Ces dernières peuvent le conduire à télécharger une autre app malveillante ou à changer de compte Twitter de contrôle. Actuellement, selon Eset, Twittor sert à importer différentes versions d'un malware bancaire. Mais pourrait tout aussi bien passer au ransomware…

« *Utiliser Twitter plutôt que des serveurs de commande et contrôle (C&C) est plutôt innovant pour un botnet Android* », souligne Lukas Stefanko, le chercheur d'Eset qui a mis au jour cette nouvelle souche infectieuse. L'objectif des cybercriminels est, comme l'indique ce chercheur, de constituer un réseau de machines esclaves, soit un botnet. Le point faible des constructions de ce type réside souvent dans l'envoi régulier d'instructions aux éléments de ce réseau, des communications susceptibles de révéler l'existence du botnet. Par ailleurs, les serveurs C&C constituent le maillon faible des botnets : si les autorités les localisent et parviennent à les fermer, c'est tout le réseau criminel qui s'effondre.

Passer d'un compte Twitter à un autre

Autant de raisons qui pourraient avoir poussé les concepteurs de Twittor à complexifier les techniques de communication entre les machines esclaves et l'entité les contrôlant, selon Eset. En plus de l'emploi de Twitter, les cybercriminels chiffrent leurs messages et utilisent des topologies complexes pour leur architecture de C&C, avance l'éditeur. « *Ces canaux de communication sont difficiles à mettre au jour et encore plus difficiles à bloquer totalement*, reprend Lukas Stefanko. *De l'autre côté, il est très simple pour les escrocs de rediriger les communications vers un compte nouvellement créé.* » Et pas de risque de voir la police fermer purement et simplement Twitter pour ce motif…

Dans l'univers Windows, dès 2009, un botnet a eu recours à Twitter, fondé seulement 3 ans auparavant, pour envoyer des instructions. Mais Twittor est bien le premier malware créateur de bot commandé via le réseau social.

Article original de Reynald Fléchaux

Réagissez à cet article

Original de l’article mis en page : Inédit : un malware Android commandé par… Twitter