iOS 9 impose un code d’accès à 6 chiffres – Le Monde Informatique | Le Net Expert Informatique

	iOS 9 impose un code d’accès à 6 chiffres

Sous iOS 9, le verrouillage des terminaux se fera avec un code à six chiffres. « En passant d'une clef de 4 chiffres à une clef de 6 chiffres, le nombre de combinaisons possibles passe de 10 000 à 1 million », a déclaré Apple.

Il faudra des mots de passe à six chiffres pour déverrouiller les appareils mobiles d'Apple qui tourneront sous le futur système d'exploitation IOS 9. Et si iOS 8 permet déjà aux utilisateurs de choisir un mot de passe de plus de quatre chiffres, dont des symboles et des lettres, ce mode de codage reste optionnel, ce qui ne sera pas le cas du futur iOS. En exigeant un code d'accès à six chiffres, Apple multiplie par 100 le nombre de combinaisons possibles, « rendant ainsi les terminaux beaucoup plus difficiles à pirater », comme on peut le lire sur le site du constructeur.
Ce saut à un code d'accès plus long risque de ne pas plaire non plus aux autorités américaines qui craignent que le renforcement des mesures de sécurité et du cryptage complique leurs investigations et rende plus difficile l'accès à des informations sensibles où le facteur temps est important, notamment dans le cadre de la lutte antiterroriste. Apple avait déjà renforcé le chiffrement d'iOS 8 afin de protéger les données les plus sensibles, et la firme de Cupertino avait mis en œuvre davantage de protections matérielles pour rendre l'accès aux terminaux plus difficile. Mais les experts en sécurité avaient estimé que l'utilisation d'un mot de passe à quatre chiffres ne suffisait probablement pas à protéger les données malgré les remparts mis en place par Apple. D'autant que, même si les utilisateurs savent qu'ils sont mieux protégés par des mots de passe plus longs, notamment parce que les séquences peuvent être plus personnalisées, ils choisissent rarement les mots de passe les plus compliqués.
Le changement de mots de passe concernera les terminaux équipés de l'ID Touch, le système d'empreintes digitales intégré aux dernières versions d'iPhone et d'iPad. L'ID Touch permet de se passer du déblocage, parfois fastidieux, du mobile avec le code à quatre chiffres, mais Apple oblige l'utilisateur à déverrouiller le mobile avec son code en cas de redémarrage du terminal. Les appareils iOS offrent d'autres fonctions de protection. Par exemple, si l'utilisateur tape un mauvais code de déverrouillage, l'iPhone peut être bloqué pendant une minute et plus, si plusieurs mots de passe sont saisis à la suite. Il est également possible de programmer l'effacement complet des données après 10 tentatives infructueuses. Le passage à un code à six chiffres pourrait grandement compliquer le travail des enquêtes judiciaires, surtout si l'appareil sous iOS 9 est configuré pour effacer les données après plusieurs tentatives erronées.

Source :
http://www.lemondeinformatique.fr/actualites/lire-ios-9-impose-un-code-d-acces-a-6-chiffres-61419.html
Par Jean Elyan

Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ? | Le Net Expert Informatique

Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ?

Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. L'enquête se tourne désormais vers la Russie.

La piste jihadiste semble s'éloigner. L'enquête sur le piratage d'envergure subi le 8 avril par la chaîne de télévision francophone TV5 Monde s'oriente vers « un groupe de hackers russes », selon une source judiciaire, mardi 9 juin. Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. Des messages de propagande jihadiste avaient été diffusés sur le site de la chaîne, ainsi que sur ses comptes Facebook et Twitter.
Le parquet antiterroriste avait alors ouvert une enquête préliminaire. Dans ce cadre, « les investigations conduisent à ce stade vers un groupe de hackers russes désignés sous le nom APT28 », d'après la même source. Ce groupe serait aussi parfois désigné sous les noms de « Pawn Storm » et « Sofacy group ».
Selon un rapport de la société américaine FireEye, APT28 est « un groupe aguerri de développeurs et d'opérateurs qui collectent des données relatives aux problématiques de défense et de géopolitique, des données qui ne pourraient être mises à profit que par un gouvernement ». L'ampleur des moyens déployés et le fait que cette cellule mène des attaques avec régularité depuis « au moins 2007 » témoignent, selon FireEye, du fait qu'elle est « soutenue par un gouvernement, plus précisément un gouvernement basé à Moscou ».

Un travail d'investigation sur les adresses IP
D'après ce même rapport, APT28 a notamment mené des attaques contre des ministères géorgiens. Selon un autre rapport de la société japonaise Trend Micro, Pawn Storm a aussi visé des dissidents russes ainsi que des intérêts américains, notamment des infrastructures militaires et des ambassades.
Les enquêteurs ont pu remonter la trace des hackers par « le travail d'investigation sur les adresses IP des ordinateurs d'où sont parties les attaques », selon une source proche du dossier. D'après les rapports des deux sociétés de cybersécurité, la cellule utilise des méthodes très sophistiquées, notamment pour recueillir mots de passe et codes d'accès. Ils enregistrent, par exemple, des noms de sites internet avec des adresses très proches de sites institutionnels reconnus afin de tromper leurs cibles.

Source : http://www.francetvinfo.fr/culture/tv/cyberattaque-de-tv5-monde-des-pirates-russes-a-la-manoeuvre_944085.html
Par Francetv info avec AFP

Piratage du site de l’US Army par l’armée électronique syrienne | Le Net Expert Informatique

Piratage du site de l’US Army par l’armée électronique syrienne

L’armée de terre américaine a annoncé lundi avoir temporairement fermé son site internet grand public, après un piratage revendiqué sur Twitter par l’armée électronique syrienne (SEA). Cette dernière soutient le président Bachar al-Assad.

Après avoir constaté qu’un contenu de son site avait été « compromis », l’armée de terre « a pris les mesures préventives appropriées pour s’assurer qu’il n’y avait pas de vol de données de l’armée, en fermant son site internet temporairement », a-t-elle déclaré dans un communiqué de presse. Le site (www.army.mil) n’était toujours pas accessible à 21h30 GMT (23h30 suisses) lundi.
L’attaque a été revendiquée par un compte Twitter s’identifiant comme un compte de l’Armée électronique syrienne. Cette dernière soutient le président Bachar al-Assad et a déjà mené des attaques contre les sites internet de presse dans le monde entier, dont ceux du New York Times ou du Washington Post.
Le compte Twitter du service photo de l’AFP et les réseaux sociaux de la BBC, d’Al Jazeera, du Financial Times ou du Guardian en ont aussi fait les frais.

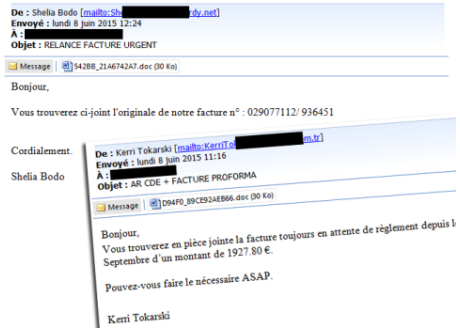
Message confus
Selon ce compte, @official_SEA16, les pirates avaient notamment laissé sur le site de l’US Army un message en anglais alambiqué dénonçant apparemment le programme de formation de rebelles syriens modérés par le gouvernement américain. « Vos responsables admettent qu’ils entraînent ceux contre qui ils vous envoient mourir au combat », littéralement, selon ce message.
En janvier, les comptes Twitter et YouTube du commandement de l’armée américaine au Moyen-Orient avait déjà été temporairement fermés, après avoir été piratés par des messages faisant la promotion du groupe Etat islamique. Les responsables militaires américains avaient qualifié ce piratage de « cybervandalisme », répétant qu’aucune donnée sensible n’avait été touchée.

Source : http://www.bluewin.ch/fr/infos/international/2015/6/9/piratage-du-site-de-l-us-army-par-l-armee-electron.html

---

Alerte au Malware caché dans une pièce jointe Microsoft

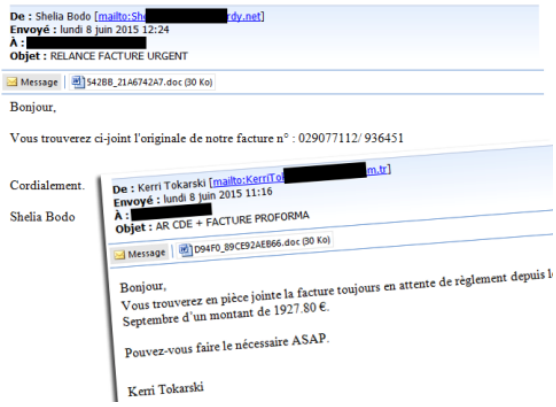
Office – Relayez l’info ! | Le Net Expert Informatique



Alerte au Malware caché dans une pièce jointe Microsoft, Office – Relayez l’info !

En ce début de semaine, de nombreuses entreprises ont reçu un e-mail alarmant les informant qu'une facture impayée était à régler rapidement. Attention ! Le document Microsoft Office en pièce jointe dissimule un code d'attaque.

Vous trouverez ci-joint l'originale de notre facture », « vous trouverez en pièce jointe la facture toujours en attente de règlement », « un montant de 1927,80€ », etc.
Les e-mails, écrits dans un français très correct, sans faute d'orthographe, se ressemblent tous et contiennent un document Microsoft Word en pièce jointe. La notion d'urgence dans le ton employé incite à l'ouverture du document.
Une fois exécuté, le document Word téléchargera via un script en Visual Basic un code malveillant-relai Drixed.



Sa présence en mémoire compromet la sécurité du poste et de ses transactions, celui-ci pourra en effet évoluer de diverses manières : trojan bancaire, logiciel espion ou encore un cryptoware.
Vous l'aurez compris, il ne faut surtout pas ouvrir la pièce jointe de cet e-mail, même s'il semble en tout point réaliste. Le fait que vous ne connaissez pas l'expéditeur devrait suffire à vous mettre en garde.
En cas d'ouverture, n'éteignez pas votre ordinateur, déconnectez-le d'Internet et appelez votre département informatique.
Bitdefender détecte le malware en tant que Trojan.Downloader.Drixed.C.

Source : http://www.globalsecuritymag.fr/Le-trojan-Drixed-revient-en-force,20150609,53337.html

Surveillance des salariés et logiciel de détection d’infractions pédopornographique | Le Net Expert Informatique

Surveillance des salariés et logiciel de détection d’infractions pédopornographique

Dans un arrêt du 11 mai 2015, le Conseil d’État confirme une délibération de la Cnil refusant à une entreprise la mise en place sur les postes informatiques d’un logiciel de recherche des infractions à caractère pédopornographique.

Si l’employeur peut exercer une surveillance sur les connexions internet des salariés sur leur poste de travail, de là à pouvoir mettre en œuvre un logiciel ayant pour objet de collecter des données relatives à la consultation par les salariés de sites à caractère pédopornographique, il y a un pas que n’a pas franchi la Cnil ni le Conseil d’État.
En effet, le Conseil d’État a été saisi par une entreprise d’une demande d’annulation de la décision de la Cnil lui refusant l’autorisation de mettre en place un tel logiciel.
La Haut juridiction n’a pas annulé la décision de la Cnil en considérant que la loi informatique et libertés ne permet à une entreprise privée de mettre en œuvre un traitement de données personnelles visant des infractions pénales ou qui peuvent en établir l’existence.

CE 11 mai 2015, n° 375669
Lire la suite….

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126327/Surveillance-des-salaries-et-logiciel-de-detection-dinfractions-pedopornographique.aspx
Par Dominique Jullien

Alerte ! Des images informatiques infectées, le

nouveau danger… | Le Net Expert Informatique

Alerte ! Des images informatiques infectées, le nouveau danger…

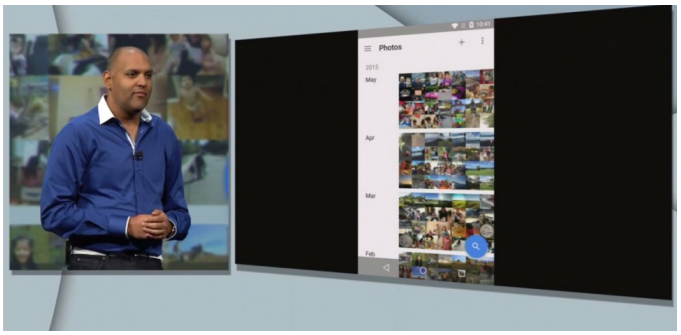
Lors de la conférence Hack In The Box d'Amsterdam, un chercheur en sécurité informatique présente Stegosploit, un outil qui permet de cacher un code malveillant dans une image.

Imaginez, vous êtes en train de surfer quand soudain votre machine devient folle ! Un code malveillant vient d'être installé alors que vous avez un antivirus et vos logiciels à jour. Une image, affichait par un site que vous veniez de visiter vient de lancer l'attaque. De la science-fiction ? Pas avec les preuves de Saumil Shah, un chercheur en sécurité informatique.
L'ingénieur a expliqué lors de la conférence (HiP) Hack In The Box que des pirates étaient très certainement en train d'exploiter sa découverte. L'idée, cacher un code malveillant dans une image en utilisant la stéganographie (cacher une information dans un autre document, NDR). Des recherches de Shah est sorti Stegosploit, un logiciel qui code en Javascript un logiciel malveillant dans les pixels d'une image au format JPEG ou PNG.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.datasecuritybreach.fr/stegosploit-loutil-qui-cache-un-code-malveillant-dans-une-image/#axzz3cN0qvWLQ

Et maintenant Google veut vos photos. Toutes vos photos… | Le Net Expert Informatique



Ani Sabharwal, responsable de l'application Photos chez Google, lors de sa présentation au Google I/O le 29 mai 2015. Google

Et maintenant Google veut vos photos. Toutes vos photos…

Après les courriers électroniques, Google veut héberger toutes les photos des internautes. Et bien sûr, analyser leur contenu.

A peine quelques jours avant Apple, c'est Google qui a organisé sa grand-messe annuelle à l'attention des développeurs. L'occasion de se faire une idée des prochains développements sur lesquels mise le géant américain. Parmi eux, une application qui a de bonnes chances de faire mouche auprès du grand public : Google Photos. A première vue, rien de révolutionnaire, car il s'agit d'une application de stockage et de partage de ses photos. Mais avec le petit détail dont Google s'est fait une spécialité : le stockage illimité et gratuit. Et la taille du stockage, c'est ce qui avait assuré par le passé le succès de Gmail face aux messageries déjà implantées.

Un stockage gratuit et illimité

Pour la première fois, le grand public a donc une solution gratuite de sauvegarde de l'ensemble de ses photos et même de ses vidéos. Avec une limitation technique qui ne devrait pas poser de problème aux non-professionnels : la qualité des photos est limitée à 16 mégapixels et celle des vidéos à 1080p (limitation dont on peut se défaire pour 10 dollars par mois et par teraoctet de données). L'interface est soignée, très épurée, dans la droite ligne des produits maison. On peut classer les photos, les retoucher, faire des montages. Google a aussi mis à disposition de chacun ses algorithmes de fouille d'image. Ainsi, toutes les photos sont analysées et l'application y reconnaît toute seule les visages ou des éléments comme par exemple de la nourriture. On peut théoriquement ainsi retrouver des photos en tapant des mots-clés dans le moteur de recherche sans jamais avoir « taggé » ses photos. Démonstration sur scène avec une recherche instantanée des photos après avoir dicté « tempête de neige à Toronto ». La recherche combine sans doute les éléments de neige sur l'image avec la géolocalisation de la ville.

La mort de Google+

Cette nouvelle application marque le premier signe du repositionnement de Google sur les réseaux sociaux. En effet, elle découle du début de démantèlement de Google+, qui n'a jamais su s'imposer face à Facebook. En séparant la partie photos de son réseau social, Google va essayer de reprendre du terrain sur les images. D'autant que l'application n'existe pas que sur le web ou les appareils Android : elle est aussi disponible sur iOS (le système d'exploitation d'Apple), ce qui en fait un grand concurrent du stockage des photos sur le cloud d'Apple, qui lui est facturé au prix fort : de 0,99 € par mois pour 20 Go à 19,99 € pour 1 To. Avec ce nouveau service, Google semble bien armé pour réussir ce qu'il a fait avec Gmail : garder l'internaute dans son propre univers en hébergeant ses données personnelles, afin de pouvoir par la suite se rémunérer avec la publicité. En sachant en plus cette fois tout ce qu'il y a dans ses photos et où et quand elles ont été prises.

La conférence est à revoir en intégralité ici :

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.sciencesetavenir.fr/high-tech/20150529.OBS9810/et-maintenant-google-veut-vos-photos-toutes-vos-photos.html?cm_mmc=EMV-_-SEA-_-20150531_NLSEAACTU-_-et-maintenant-google-veut-vos-photos-toutes-vos-photos##xtor=EPR-6-ActuSciences17h-20150531

La NSA écoute nos disques

durs ?

	La NSA écoute nos disques durs ?

Kaspersky Lab a découvert une plate-forme de cyber-espionnage dont l'une des composantes, très certainement exploitée par la NSA, permet de surveiller des disques durs.

Iran, Russie, Pakistan, Afghanistan, Chine, Mali, Syrie, Yémen, Algérie… Les gouvernements, organes militaires, sociétés télécoms, banques, médias, chercheurs et activistes d'une trentaine de pays auraient été exposés à des logiciels espions cachés dans des disques durs.
Les équipes de Kaspersky Lab en sont arrivées à cette conclusion après plusieurs années d'enquête sur ce qu'elles considèrent aujourd'hui comme le dispositif de surveillance électronique « le plus complexe et le plus sophistiqué » découvert à date*.
Encore activement exploitée, cette plate-forme serait opérationnelle depuis au moins 2001, voire 1996, si on se fie à la date d'enregistrement de certains serveurs utilisés pour contrôler les malware.
Elle hébergerait notamment un ver très proche de Stuxnet. Ce virus complexe et polymorphe dont la conception est attribuée à l'Agence américaine de sécurité nationale (NSA) avec la collaboration de l'unité 8200 de l'armée israélienne (cyberdéfense) avait mis à mal un site d'enrichissement d'uranium implanté en Iran, endommageant un millier de centrifugeuses.
Mais c'est bien le module de piratage des disques durs qui retient l'attention de Kaspersky. Dans son rapport publié lundi (document PDF sur http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf, 44 pages), l'éditeur russe note que la quasi-totalité des produits du marché sont affectés : Seagate, Western Digital, Toshiba, IBM, Micron, Samsung…
Il est d'autant plus difficile de détecter l'infection qu'elle se loge dans le firmware des disques durs. Ce qui lui permet aussi de s'activer presque instantanément au démarrage (la seule étape qui précède dans la séquence d'amorçage est l'initialisation du BIOS) et d'ouvrir discrètement des portes dérobées permettant de récupérer des données à foison.
Pour Kaspersky Lab, réussir à implanter un logiciel malveillant dans le firmware d'un disque dur est une prouesse. A moins que les pirates aient eu accès au code dudit firmware. Du côté de Western Digital, on assure ne pas avoir communiqué ce genre de données. Chez Seagate, on estime avoir intégré des couches de sécurité pour éviter les modifications non sollicitées du micrologiciel, ainsi que son étude par reverse engineering.

A qui la faute ?
Le problème remonte peut-être à 2009. Dans le cadre d'une vague de cyber-attaques contre des sociétés high-tech américaines, les pirates avaient eu accès à du code source qualifié de « très précieux » car hébergé sur les serveurs de multinationales et d'organes gouvernementaux.

Dans ce butin figuraient probablement des copies du firmware des différentes marques de disques durs. Et pour cause : lorsqu'elles acquièrent un équipement informatique, les agences classées « sensibles » peuvent demander, pour le compte du gouvernement américain, un audit de sécurité des produits pour s'assurer de l'intégrité du code source… lequel est certainement sauvegardé au passage.

Kaspersky Lab n'affirme pas que la NSA est à l'origine de ce « mouchard à disques durs ». Ses chercheurs disposent toutefois de nombreux indices, comme ce mot-clé GROK trouvé dans le code d'un enregistreur de frappe et déjà présent dans un outil d'espionnage dévoilé en 2013 par Edward Snowden.

Les multiples révélations du lanceur d'alertes pèsent sur l'activité des sociétés high-tech américaines : les ventes de solutions – aussi bien matérielles que logicielles – chutent. A tel point que Peter Swire, membre du groupe de réflexion «Renseignement et Nouvelles technologies» monté par Barack Obama, reconnaît qu'il est «plus que jamais indispensable, pour les Etats-Unis, de mesurer l'impact que chaque décision d'exploiter une faille de sécurité pourrait avoir sur les relations commerciales […] et diplomatiques».

* Malgré sa puissance, il semble que la plate-forme ne soit exploitée que contre un nombre restreint de «cibles d'intérêt» localisées hors des Etats-Unis.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itespresso.fr/cyber-espionnage-nsa-ecoute-disques-durs-88684.html
Par Clément Bohic

La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ? | Le Net Expert Informatique

	La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ?

Depuis le début de l'examen, à l'Assemblée nationale puis au Sénat, du projet de loi sur le renseignement, une disposition du texte concentre les critiques et les débats. Il s'agit d'une partie de son article 2, qui permettra aux services de renseignement d'installer des appareils analysant le trafic Internet pour détecter des comportements suspects de terrorisme. Le terme de « boîte noire », d'abord avancé par le gouvernement, est devenu leur nom officieux.

Les détracteurs de la loi y voient, par son caractère systématique et indistinct, l'introduction dans la loi française de la surveillance de masse. Ses partisans refusent le terme. Au Sénat, mardi 2 juin, ils ne sont pas parvenus à trancher ce débat, qui est loin d'être seulement sémantique.

Que dit le projet de loi ?

Le projet de loi sur le renseignement prévoit, en l'état, dans le seul cadre de la lutte contre le terrorisme, la mise en place de « traitements automatisés » sur les réseaux des fournisseurs d'accès à Internet français. Cela signifie que des matériels seront physiquement installés chez les opérateurs, dans lesquels des logiciels – les fameux algorithmes – vont inspecter les flux de données des internautes à la recherche de signaux que les services estiment être avant-coureurs d'un acte terroriste.

Pour les opposants, cela ne fait pas de doute. Si des algorithmes inspectent, automatiquement, l'intégralité des flux qui transitent chez les fournisseurs d'accès à Internet (FAI) à la recherche de comportement suspects, il s'agit d'une mesure de surveillance de masse ; et ce, même s'ils ne sont destinés qu'au repérage de quelques personnes. C'est le cas du sénateur Claude Malhuret (Allier, Les Républicains), joint par Le Monde :

« Ceux qui disent qu'il ne s'agit pas de surveillance de masse disent, à la phrase suivante, qu'il s'agit de chercher une aiguille dans une botte de foin. Mais la botte de foin, c'est l'Internet français ! Les boîtes noires installées chez les FAI analyseront l'intégralité du trafic Internet français. C'est comme les radars sur les principales autoroutes : au bout de quelque temps, tous les Français seront passés devant. Elles cherchent des critères précis, mais en surveillant tout le monde ! »

Difficile en effet de qualifier autrement que « de masse » ce dispositif de surveillance, qui, au minimum, inspectera de très grandes quantités de données pour n'y repérer que quelques activités suspectes.

Ce qualificatif est pourtant violemment récusé par les défenseurs du texte. Le premier ministre, Manuel Valls, a assuré au Sénat mardi 2 juin que le projet de loi « n'exerçait pas de surveillance de masse des Français ». « Le texte n'autorise que de la surveillance ciblée, pas de surveillance de masse » a renchéri son collègue de la défense, Jean-Yves Le Drian.

Pas « d'atteinte à la vie privée »

Le sénateur socialiste du Loiret Jean-Pierre Sueur est du même avis :

« Il ne faut pas faire dire à la loi ce qu'elle ne dit pas. Certains disent que nous pompons les données comme le Patriot Act. C'est faux, c'est quelque chose contre lequel on a toujours été opposés. »

Lorsqu'on lui fait remarquer que pour repérer les suspects dans le flot des connexions, il faudra bien passer en revue toutes les connexions des internautes français, le sénateur dément : « Il ne s'agit pas de tout l'Internet français, mais seulement ceux qui se connectent aux sites terroristes. Notre objectif n'est pas de porter atteinte à la vie privée. » Un exemple d'utilisation des « boîtes noires » qui n'est cependant pas le seul avancé par les promoteurs du dispositif.

La loi ne précise pas les modalités exactes du déploiement de ces « traitements automatisés ». Elle ne limite d'ailleurs pas leur activité à la détection des visiteurs de sites terroristes (dont le blocage est par ailleurs prévu par la loi sur le terrorisme adoptée à la fin de 2014) mais, plus largement, des « connexions susceptibles de révéler une menace terroriste ».

De multiples amendements de suppression des algorithmes

La délicate question des algorithmes dans la loi sur le renseignement a été abordée mercredi soir au Sénat. Des députés issus de tous les groupes politiques, de la gauche à la droite, ont déposé des amendements de suppression du dispositif de « boîtes noires ».

La commission des lois du Sénat a apporté quelques modestes retouches : la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'organisme administratif de contrôle que crée la loi, pourra désormais se prononcer sur les « paramètres » des algorithmes, et non plus sur leurs « critères ». La commission a aussi précisé que l'autorisation du premier ministre, dont la validité sera ramenée de quatre à deux mois, devra préciser les paramètres des algorithmes. L'accès de la CNCTR aux algorithmes ne sera, enfin, pas seulement « permanent », mais également « direct ».

Source : http://www.lemonde.fr/pixels/article/2015/06/03/la-loi-sur-le-renseignement-mettra-t-elle-en-place-une-surveillance-de-masse_4646733_4408996.html
Par Martin Untersinger

Les Etats-Unis victimes d’une nouvelle cyber-attaque | Le Net Expert Informatique

Les Etats-Unis victimes d’une nouvelle cyber-attaque

Des pirates chinois seraient à l’origine d’une nouvelle cyber-attaque visant les données de fonctionnaires américains © Reuters/Pichi Chuang

Les données de millions de fonctionnaires américains ont été piratées ces derniers mois, aux Etats-Unis. Des cyber-pirates chinois seraient à l’origine de l’attaque, ils ont réussi selon des officiels américains à s’introduire dans les serveurs de l’Office of Personal Management, qui stocke notamment les profils des employés fédéraux.
Une nouvelle cyber-attaque d’envergure aux Etats-Unis. Les données personnelles de fonctionnaires ont été piratées depuis décembre 2014. Des hackers, apparement chinois, ont réussi à s’introduire dans les serveurs de l’Office of Personal Management (OPM), une agence qui vérifie notamment les profils des employés fédéraux pour le compte de la sécurité nationale.

4 millions de victimes, peut-être plus
Pas moins de quatre millions d’agents fédéraux, en activité ou à la retraite, ont été victimes de cette cyber-attaque. Ils vont devoir s’assurer auprès de leur banque que leurs données privées n’ont pas été utilisés par les pirates. D’autres éléments, comme les numéros de sécurité sociale et autres identifiants personnels sont également tombées aux mains des hackers.
Dans son communiqué, l’OPM n’exclut pas que d’autres personnes aient pu être victimes de cette attaque en ligne, menée au moment même où l’agence se dotait d’un nouveau système de sécurité. Vol de données ou espionnage, l’objectif des pirates reste en revanche incertain.
Le FBI, qui enquête sur l’affaire, dit « prendre au sérieux toutes les attaques potentielles contre les systèmes du secteur public et privé ».

Vulnérabilité du réseau informatique américain
L’attaque a été découverte en avril, mais la pêche aux informations aurait débuté dès la fin 2014. Une affaire de plus qui confirme la vulnérabilité du réseau informatique de l’administration américaine, fragilité dénoncée par le Government Accountability Office (GAO), l’équivalent de la Cour des comptes française.
Il y a quelques jours encore, on apprenait qu’une cybermafia avait réussi à récupérer les déclarations fiscales de plus de 100.000 contribuables. L’an dernier, le Département d’Etat et la Maison Blanche faisaient les frais d’intrusions attribuées à des Russes. A l’époque les courriels du président Barack Obama avaient été compromis.

Source : http://www.franceinfo.fr/vie-quotidienne/high-tech/article/les-etats-unis-victimes-d-une-nouvelle-cyber-attaque-des-hackers-chinois-soupconnes-688588
par Arnaud Racapé