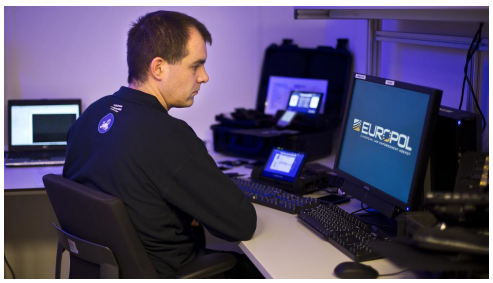
Une loi pour nous espionner sous couvert de la peur du terrorisme | Le Net Expert Informatique

Des manifestants contre le projet de loi sur le renseignement devant l'Assemblée nationale, à Paris, le 13 avril 2015. (MAXPPP)

Une loi pour nous espionner sous couvert de la peur du terrorisme…

Cybercriminalité : trois techniques en vogue chez les pirates | Le Net Expert Informatique

15



Cybercriminalité : trois techniques en vogue chez les pirates

Avez-vous déjà entendu parler de « rançongiciels » ? Le rapport annuel de la société américaine de sécurité informatique Symantec, publié mardi 14 avril, assure que le recours à ce type de programmes malveillants parmi d'autres est de plus en plus fréquent. « De manière générale, la cybercriminalité a encore crû en 2014, avec 317 millions de nouveaux programmes malveillants créés au niveau mondial, soit près d'un million par jour », explique à l'AFP Laurent Heslault, expert en cybersécurité de Symantec et Norton.

La France progresse d'une place et passe donc au 14e rang mondial (6e rang européen) des pays où la cybercriminalité est la plus active, selon le rapport. **Au niveau mondial, cinq grandes entreprises sur six ont été attaquées en 2014**, soit une progression de **40 % sur un an**, avance Symantec. Francetv info vous présente certaines techniques d'attaque remarquées en 2014.

Viser les éditeurs de logiciels

Les pirates ne sont pas toujours là où on les cherche. Alors que les entreprises se méfient de plus en plus des vols de mots de passe et des usurpations d'identité de leurs employés, les cybercriminels changent de tactique, selon le rapport de Symantec. Pour échapper à toute détection, ils détournent les infrastructures des grandes entreprises, pour les utiliser contre elles.

« Beaucoup sont capables de faire s'auto-infecter les infrastructures des entreprises, via des 'chevaux de Troie', lors de mises à jour de logiciels standards, et d'attendre ensuite patiemment que leurs cibles téléchargent ces mises à jour infectées, leur donnant ainsi libre accès au réseau de l'entreprise », détaille Laurent Heslault. Les cyberattaquants ciblent donc de plus en plus les fournisseurs des grandes entreprises, comme les éditeurs de logiciels.

Réclamer des rançons

Les « rançongiciels » ont plus que doublé dans le monde en 2014, selon le rapport de Symantec. Ces logiciels malveillants prennent le contrôle des PC, tablettes et smartphones et les utilisateurs se voient ensuite réclamer de l'argent pour pouvoir à nouveau utiliser leur machine. **L'an dernier, l'utilisation de ce type de programme (appelé en anglais « ransomware ») a augmenté de 113%**.

Sa variante, dite « cryptolocker », qui retient en otage les données personnelles, a fait 45 fois plus de victimes qu'en 2013. Dans ce système, si la rançon n'est pas payée au terme d'un compte à rebours, les données de la victime sont détruites. « Là où un particulier doit payer 300 euros, une entreprise française s'est vu réclamer 90 000 euros pour récupérer 17 téraoctets de données », relèvent Les Echos.

Miser sur les vulnérabilités encore non détectées

L'année 2014 aura connu un record avec 24 découvertes de vulnérabilités « zero day », c'est-à-dire des pirates qui utilisent des failles non détectées jusque-là dans un logiciel. Ces vulnérabilités entraînent un délai de réponse fortement accru et donc offrent plus de temps aux pirates pour s'en servir.

« Il aura fallu en moyenne 59 jours aux éditeurs de logiciels pour créer et déployer des correctifs [en 2014] alors qu'ils en avaient besoin de seulement quatre en 2013 », relève Laurent Heslault.

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

Source : http://www.francetvinfo.fr/internet/cybercriminalite-trois-techniques-en-vogue-chez-les-pirates_876373.html
Par Par Yann Thompson

Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ? | Le Net Expert Informatique

12

	Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ?

Le piratage à distance en 2020 du stimulateur cardiaque d'un dirigeant d'un grand pays est le point de départ de la nouvelle « Café, Wi-Fi et la Lune » de Nikolas Katsimpras, qui a été primée ce mardi 17 mars par le Conseil Atlantique. Les candidats étaient invités par ce think tank de Washington, à présenter des textes courts, fictifs, de « unes » de journaux, sur le déclenchement du prochain conflit majeur, en s'inspirant des événements qui ont emporté le monde dans la Grande Guerre en 1914.

Le choix du jury souligne deux consensus. En premier, nous devrions à très court terme être immergés dans une multitude d'Objets Connectés, senseurs et capteurs qui nous aideront sur de nombreux aspects de notre vie. En second, la sécurisation de cet Internet des Objets face à des actes de maladresse comme de malveillance, pose encore de nombreux problèmes techniques et politiques. Enfin, le Conseil Atlantique ouvre par cette initiative la question de la contribution de l'art et de la littérature à ce débat, en terme de communication ou pour faciliter la prise de conscience par le grand public du travail restant à faire dans le domaine de la cyber-sécurité et du respect de la sphère privée.

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

Source : http://www.bulletins-electroniques.com/actualites/78150.htm

Colloque international sur la Cybercriminalité à Montpellier

Colloque international sur la Cybercriminalité à Montpellier

Principalement organisé par Adel JOMNI, ce colloque a eut lieu les 8 et 9 avril 2015 à l'Université de Montpellier (Maison des étudiants- Richter) .

Objet du colloque

Présentation du projet Européen CAMINO (Comprehensive Approach to cyber roadMap CoordInation and develOpment),une conférence internationale sur l'innovation et la Cybercriminalité (draft programme joint à cette invitation)

Programme

Session 1 : Innovations numériques, Cybercriminalité et Cyber terrorisme : Enjeux et défis : quelles stratégies ?

– Lord Carlile of Berriew, Membre du Parlement du Royaume--Uni,
– Général Watin--Augouard, Directeur du centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)
– Andy Archibald, Directeur adjoint de l'unité nationale cybercriminalité de l'Agence Nationale de la Criminalité du Royaume--Uni
– Marco Lozano, Représentant INCIBE (Espagne)

Session 2: Les menaces cybernétiques : Analyse des risques et des stratégies

– Etat des lieux des cyber menaces par Jean--Dominique Nollet
– EC3--Europol L'investigation et la coopération entre les organisations internationales (Interpol, Europol,..) par Valérie Maldonado, OCLCTIC
– Analyse des réseaux sociaux et sécurité nationale par Thomas Delavallade, THALES – Comment améliorer la résilience face à la cybercriminalité et au cyber--terrorisme (Projet Européen CAMINO – FP7) Michal Choras, ITTI

Session 3: Enjeux et risques liés au développement des monnaies virtuelles; Irruption de l'innovation numérique dans la finance

– Flux illicites et monnaies virtuelles par Myriam Quéméner, Magistrate, cour d'appel de Versailles
– Crypto--monnaies et Blockchain : nouvelles opportunités d'investigation forensique sur le Darknet par Intervenant Camino ou Courage
– Monnaie virtuelle et crypto monnaie : quels enjeux et réponses réglementaires en Europe ? Quelles préconisations pour les utilisateurs et les entreprises? par Cathie--Rosalie Joly, Avocat, Barreau Paris et Bruxelles

---

Session 4: Big data, Internet des objets et sécurité : le pouvoir de l'anticipation au service de la cybersécurité par Adel Jomni, Enseignant-- chercheur, Université de Montpellier

– Le droit est--il un frein pour le développement du Big Data ? par Francesca Bosco, UNICRI
– Objets connectés et santé : l'innovation au service ou au détriment du citoyen par Corinne Thierache, Avocat associé
– Le Big Data pour lutter contre les attaques persistantes par Fraser Sampson, West Yorkshire Police

---

Session 5 : Projets européens, coopération internationale, recherche et formation dans le domaine de la lutte contre la Cybercriminalité et le Cyberterrorisme

– Défis majeurs de la recherche dans le domaine de la cybercriminalité et le cyber terrorisme par Akhgar Babak, Projet Européen COURAGE
– Nouvelles méthodes d'investigation et de formation forensique dans un environnement virtuel (cloud) (projet D--FET) par Bill Buchanan, Professeur, Université Napier d'Edimbourg
– La coopération internationale pour renforcer les capacités de protection des infrastructures d'information critiques 2015--2020 (CIIP) par Jean--Christophe Letoquin, Expert auprès du Conseil de l'Europe, Président de SOCOGI
– Projet ePOOLICE par Estelle de Marco
– L'entraide judiciaire en matière de traitement judiciaire de la Cybercriminalité à l'échelle Européenne et internationale par Victoria CATLIFF

Cet événement organisé en partenariat avec les membres des projets européens CAMINO et COURAGE (Cybercrime and Cyberterrorism European Research Agenda), s'inscrit dans une démarche de réflexion et d'échange visant à promouvoir une

vision européenne de la cybersécurité et à renforcer la lutte contre la Cybercriminalité et le Cyberterrorisme, priorité de l'Union Européenne pour laquelle les deux projets ont été élaborés.

Source :
Adel JOMNI et Denis JACOPINI

Infectée par un cryptolocker, la police du Massachusetts paie 500$ de rançon | Le Net Expert Informatique

Infectée par un cryptolocker, la police du Massachusetts paie 500$ de rançon

La police de la ville de Tewksbury, dans le Massachusetts, victime d'un cryptolocker, a du régler 500$ pour déchiffrer les fichiers conservés sur un serveur afin de remettre ses équipes au travail.

Un Département de police du Massachusetts, celui de la ville de Tewksbury, a du verser 500 $ à un cyberpirate pour débloquer les fichiers chiffrés avec un cryptolocker, le ransomware qui verrouille les disques durs jusqu'à ce que les propriétaires paient une rançon. Après plusieurs jours d'essais infructueux, les services informatiques de la police de Tewksbury ont réalisé qu'ils ne pouvaient pas casser le chiffrement et payé la rançon pour obtenir la clef privée permettant d'accéder aux données.
« Ils ont rendu inopérant le logiciel que nous utilisons pour assurer le fonctionnement du Département de la police », a déclaré le chef de la police, Timothy Sheehan, au journal Tewksbury Town Crier. L'incident est survenu à la fin de l'année dernière, l'infection a démarré le 7 décembre sur un poste de travail.

Une attaque très ciblée
Les attaquants ont exploré le réseau jusqu'à corrompre le serveur principal du Département. Les services de Police sauvegardent leurs fichiers sur un disque dur externe qui a également été touché par le ransomware, de sorte qu'ils avaient le choix de payer 500 $ ou de perdre toutes les données.
La police de l'État et le FBI se sont penchés sur cette affaire, tout comme Delphi Technology Solutions et Stroz Friedberg, des sociétés spécialisées dans la police scientifique. Aucune des deux n'a réussi à casser le cryptage de sorte que le Département a payé, indique le journal local. Stroz Friedberg a converti les 500 $ de la rançon en bitcoins avant de l'envoyer de la part du Département de police.

Payer ou pas
Les applications affectées concernaient la répartition des tâches assignées aux différents agents, la gestion des documents, la main courante avec les arrestations et la conservation des appels au commissariat. La même mésaventure s'est déjà produite en 2013 dans un autre service de police à Swansea, toujours dans le Massachusetts ; 750$ avaient alors été réglés pour débloquer le système.
De nombreux experts estiment que les victimes auraient du refuser de payer, surtout s'ils s'agit des forces de l'ordre, mais après avoir examiné l'alternative, c'est-à-dire ne jamais revoir ses données, de nombreuses entreprises préfèrent payer afin de recommencer à travailler.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-infectee-par-un-cryptolocker-la-police-du-massachusetts-paie-500$-de-rancon-60783.html
Par Serge Leblal

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat

Islamique | Le Net Expert Informatique

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique

Stupeur à TV5 Monde. La chaîne publique francophone internationale est victime, mercredi 8 avril au soir, d'une importante attaque informatique menée par des militants islamistes se revendiquant de l'organisation Etat islamique (EI), a confirmé son directeur général Yves Bigot. « Nous ne sommes plus en état d'émettre aucune de nos chaînes. Nos sites et nos réseaux sociaux ne sont plus sous notre contrôle et ils affichent tous des revendications de l'Etat islamique », a-t-il indiqué

Propagande et documents postés sur Facebook

Les pirates ont posté des contenus de propagande sur la page Facebook de la chaîne, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI. Après près de deux heures, les équipes de la chaîne ont pu reprendre la main sur la page de le TV5 Monde sur le réseau social. Les programmes ont par ailleurs été interrompus, tandis que le site internet de TV5 Monde est toujours indisponible.

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 protection juridique du chef d'entreprise.
Contactez-nous

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

S o u r c e
http://www.francetvinfo.fr/monde/proche-orient/offensive-jihadiste-en-irak/la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789.html#xtor=EPR-51-la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789-20150408-bouton

---

Nouvelles formes d'attaques informatiques | Le Net Expert Informatique

Nouvelle formes d'attaques informatiques

Sévissant depuis l'année dernière, ce malware de nouvelle génération combine techniques informatiques sophistiquées, ingénierie sociale et intervention humaine pour que la fraude soit effective. Nom de code : Dyre Wolf

Entre 500 000 et 1,5 million de dollars par attaque. Tel est le butin ramassé lors de l'attaque réalisée à l'aide du malware Dyre qui sévit depuis le mois d'octobre dernier. Mais les criminels derrière ce programme ont récemment franchi une nouvelle étape qui permet au programme de retrouver une nouvelle jeunesse, au grand dam des entreprises qui en sont victimes.
L'attaque se déroule en plusieurs étapes. Dans un premier temps, des utilisateurs reçoivent un mail contenant une pièce jointe, elle-même infectée par le logiciel Upatre. Le but de ce logiciel est uniquement de permettre le téléchargement de Dyre, un programme beaucoup plus dangereux. Lorsque Dyre est téléchargé, il va essayer de se répandre le plus largement possible chez les autres employés de l'entreprise ou les amis de la personne infectée au travers du programme de messagerie Outlook. En parallèle, le logiciel va surveiller le travail de la personne infectée et attendre qu'elle se connecte à un parmi des centaines de sites bancaires que le maliciel est programmé pour surveiller.

Le voleur au bout du fil
Et c'est là que cela devient tout à fait nouveau. Lors de la tentative de connexion au site, Dyre va afficher un message indiquant que la connexion et le compte posent un problème et va inviter la personne à contacter un numéro de téléphone. Précisons que ceci se passe indépendamment du navigateur utilisé : Chrome, Firefox ou Internet Explorer. En effet, les trois navigateurs ont été usurpés.
En composant le numéro de téléphone, la victime ne va pas tomber sur un centre d'appel mais sur une vraie personne qui va se proposer de « l'aider » à régler son problème. Cette personne en apparence tout à fait bien intentionnée va donc vous demander des informations sur votre compte et pendant que vous discutez avec elle, elle procédera à un transfert de fonds depuis le compte bancaire de l'entreprise vers les propres comptes des criminels. « L'intervention d'un opérateur au téléphone en direct est unique», précise Caleb Barlow, vice-président d'IBM.

Et un petit DDOS pour bien masquer le tout
Enfin, simultanément au transfert de fonds, le site web de l'entreprise qui vient d'être pillée va être victime d'une attaque en DDOS. Le but de cette attaque est de détourner l'attention des services IT et de sécurité qui seront trop occupés à endiguer cette attaque pour s'occuper d'une escroquerie financière, du moins dans les premiers jours.
On le voit : l'imagination des cybercriminels est débordante. Comme à l'habitude, IBM répète une série de conseils, notamment de ne jamais fournir des informations bancaires à quiconque, les « vraies » banques ne demandant jamais ce type d'informations.

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

Source : http://www.mag-securs.com/news/articletype/articleview/articleid/34604/dyre-wolf-nouvelle-etape-dans-la-cybercriminalite.aspx
Par Raphaël Stencher

Une faille permet de pirater les drones Parrot à distance

| Le Net Expert Informatique

Une faille permet de pirater les drones Parrot à distance

Les drones sont des objets fascinants, et tout particulièrement pour les hackers. Le chercheur en sécurité indien Rahul Sasi vient d'en décortiquer un provenant du fabricant français Parrot, à savoir le Parrot AR Drone 2.0.

Après de longues heures de rétro-ingénierie, il a trouvé une faille permettant d'installer une porte dérobée – baptisée Maldrone – au cœur même du système de l'appareil, à savoir dans le logiciel de pilotage et de navigation. Cette partie du code, totalement propriétaire, permet à l'appareil de voler et de rester stable dans les airs.
Dans une vidéo, le hacker montre comment il installe cette porte dérobée à distance puis prend le contrôle de l'appareil, y compris de sa caméra. Le plus effrayant, c'est que cette porte dérobée est persistante dans le temps. Une mise à zéro de l'appareil (« reset ») ne permettra pas de l'enlever. Il faudra donc réinstaller le firmware, ce qui n'est pas forcément aisé.
Rahul Sasi a présenté les détails techniques de son hack lors de la conférence Nullcon, qui s'est doulée à Goa début février. Ce n'est pas la première fois que des hackers se penchent sur les drones de Parrot. Fin 2013, le hacker Samy Kamkar avait déjà trouvé une manière de pirater ces appareils, en interceptant les commandes radio.

Un drone dans le jardin de la Maison Blanche
Les drones posent aussi des questions de sécurité physique. Hier, un drone grand public (DJI Phantom) s'est écrasé sur la pelouse de la Maison Blanche, créant un certain affolement chez les responsables de la sécurité du président américain. La France connait également une psychose similaire, avec le survol répété de plusieurs centrales nucléaires par des drones. Cette affaire est toujours en cours.

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

Source : http://www.01net.com/editorial/642968/une-faille-permet-de-pirater-les-drones-parrot-a-distance
Par Gilbert Kallenborn

Ce mardi, attaque numérique lancée contre Israël jusqu’à sa disparition de l’espace informatique | Le Net Expert Informatique

	Ce mardi, attaque numérique lancée contre Israël jusqu’à sa disparition de l’espace informatique

Ces pirates informatiques, prétendant appartenir à Anonymous, se lancent dans une guerre virtuelle contre Israël.
Anonymous, toujours prêt à l'attaque informatique
La prochaine attaque informatique contre Israël est qualifiée de « shoah électronique » par le groupe de hackers. Ceux-ci se disent révoltés par la terreur infligée au peuple palestinien dont les crimes, les tortures et les enlèvements. Ils crient aujourd'hui vengeance à travers un outil qu'ils maitrisent: la Toile!

En effet, dans une vidéo postée sur Youtube, on peut y voir un membre du groupe Anonymous faire l'apologie du terrorisme informatique et menacer ouvertement Israël de cyberattaques…
La personne dit clairement: « **Le 7 avril prochain, les élites du cyberespace s'uniront solidairement pour soutenir les Palestiniens contre Israël… Nous allons faire disparaître l'état d'Israël de l'espace informatique** ».
Tout cela est dit en illustration d'une vidéo en arrière-plan montrant une scène de conflit entre Palestiniens et Israéliens. L'homme sur la vidéo tient une posture solennelle, comme s'il s'agissait d'un chef d'Etat qui faisait une déclaration officielle à ses citoyens. Il porte aussi un costume et le fameux masque de Vendetta. Sa voix a été changée pour la circonstance et son discours en anglais a été sous-titré en arabe. Il s'adresse aussi au Premier ministre israélien réélu dernièrement, le traitant d'imbécile et lui promettant d'attaquer le pays électroniquement jusqu'à ce que le peuple palestinien soit libre.
Il est évident que la date de la cyber-attaque n'ait pas été choisie au hasard puisque cela tombe juste quelques jours avant la journée de commémoration de la Shoah.
L'Etat d'Israël semble toutefois insensible à ces menaces et préfère en rire et ne pas les prendre au sérieux.
En effet, Mr Benjamin T. Decker, membre des services secrets et basé à Tel Aviv, s'est exprimé dans les colonnes de Newsweek, disant que c'est plus une blague de bas étage et que cela fait la quatrième année que ce groupe demande à ses supporters de mener une attaque pour effacer Israël du cyber espace. Il poursuit disant que leurs attaques ne portent pas toujours les fruits attendus puisque Israël se protège en menant des contre-attaques et se protégeant informatiquement en amont.
Lire la suite….

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

Source : http://fr.blastingnews.com/international/2015/04/des-hackers-sortent-une-bombe-informatique-face-a-israel-00332177.html

---

Europol met en garde contre les communications chiffrées | Le Net Expert Informatique

Europol met en garde contre les communications chiffrées

Europol, la police criminelle intergouvernementale, s'est récemment exprimée au sujet des communications chiffrées. Selon les autorités, cela représenterait un réel danger face à la menace terroriste.

Les informations partagés par Edward Snowden, ancien analyste à la NSA, sur les pratiques de surveillance massive orchestrées par les agences de renseignements ont fait l'effet d'une onde de choc. Du jour au lendemain, les plus grosses sociétés Internet ont été directement impliquées dans des affaires de cyber-surveillance. Autant dire que la confiance des internautes vis-à-vis des entreprises, mais également celle de ces dernières face aux gouvernements, en a pris un sacré coup.
Microsoft, Yahoo, Apple ou encore Google ont renforcé leur infrastructure et de plus en plus d'outils surgissent sur la Toile pour sécuriser les communications et la vie privée des internautes. En d'autres termes, la notion de vie privée a le vent en poupe, et ce n'est pas pour plaire à tout le monde. Pour Europol, l'existence de ces technologies est un frein à la lutte contre le terrorisme.

Dans une interview recueillie par la BBC, Rob Wainwright, directeur d'Europol, affirme que les efforts visant à chiffrer les communications par les grandes sociétés high-tech devient problématique. « C'est probablement devenu le plus gros problème pour la police et pour les services de sécurité dans leur lutte contre le terrorisme », affirme-t-il. Et d'ajouter « cela a changé la nature-même du travail contre le terrorisme lequel était jusqu'à présent fiable avec des communications que nous pouvions gérer à un autre qui ne fournit plus rien ».
Apple et Google ont pris le parti de chiffrer leurs systèmes d'exploitation mobiles, au grand dam du FBI. Aussi, Yahoo! a annoncé qu'un dispositif de chiffrement des emails serait proposé d'ici la fin de l'année sur son Webmail. Un mécanisme similaire est déjà disponible avec l'extension Mailvelope pour Chrome et Firefox. Le service sécurisé ProtonMail vient de lever 2 millions de dollars tandis que la messagerie instantanée CryptoCat gagne en popularité.
Pour M. Wainwright, les efforts des sociétés de la Sillicon Valley seraient « motivés par des impératifs commerciaux parce qu'ils perçoivent une demande des consommateurs souhaitant une meilleure vie privée pour leur communications ». D'emblée, ce n'est donc pas la vie privée des internautes qui prime mais les dangers potentiels d'une communication entre terroristes. D'emblée, les efforts des sociétés pour protéger leurs infrastructures et leurs services sont donc replacés à une campagne marketing…
Entre les agences de renseignement et les prestataires de services, le bras de fer ne fait que commencer. Le mois dernier Alex Stamos, responsable de la sécurité chez Yahoo! est monté au créneau contre le directeur de la NSA, lequel souhaite voire la mise en place d'une porte d'accès aux données de l'internaute de manière légale. Les géants du Web se sont rassemblés pour lancer un appel au Congrès américain afin que les services de renseignement cessent leurs collectes de données.

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

S o u r c e :
http://pro.clubic.com/technologie-et-politique/actualite-761041-europol-garde-communications-chiffree.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_31/03/2015&partner=-&svc_position=916696908&svc_misc=-&crmID=639453874_916696908&estat_url=http%3A%2F%2Fpro.clubic.com%2Ftechnologie-et-politique%2Factualite-761041-europol-garde-communications-chiffree.html