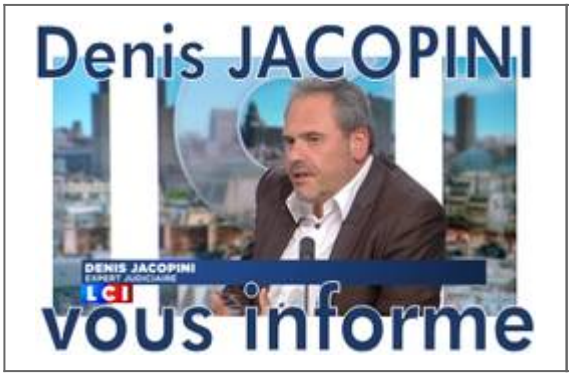
Les solutions VPN touchées par une faille sur la redirection de ports



Les solutions VPN touchées par une faille sur la redirection de ports

---

Suivre
nVpn.net @nVpnNet
Fixed a possibility to exploit a VPNs PF feature revealing a user’s real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy
01:07 – 27 Nov 2015
4 4 Retweets 2 2 j’aime

La société de sécurité Perfect Privacy a averti hier dans un billet de blog que bon nombre de solutions VPN étaient vulnérables à des attaques par redirection de port. De fait, un grand nombre d'utilisateurs pourraient voir leurs adresses IP réelles être dévoilées par des pirates utilisant les mêmes réseaux.

Les VPN, ou réseaux privés virtuels, sont conçus pour permettre laccès à des ordinateurs distants. Ils sont également souvent utilisés pour masquer les adresses IP dorigine. Mais il n'est finalement pas très compliqué d'obtenir quand même cette information, surtout quand les solutions existantes autorisent la redirection de port et qu'elles ne sont protégées contre des attaques utilisant cette fonctionnalité.

La faille « #VPN Fail »

Hier, la société Perfect Privacy a averti qu'un grand nombre de solutions VPN pouvaient révéler ces adresses IP si un pirate savait où chercher.

Pour que l'attaque fonctionne, il doit se trouver sur le même réseau virtuel que sa victime et connaître son adresse IP de sortie.

Comme l'indique The Hacker News, cette étape est assez simple puisqu'il suffit d'attirer l'utilisateur sur un site évidemment contrôlé par le pirate. Si la redirection de port est activée, le pirate pourra obtenir l'adresse IP réelle de la victime en l'amenant à ouvrir par exemple une image. À partir de là, il devient possible de rediriger le trafic vers un port là encore contrôlé par le pirate, d'où le nom de l'attaque.

Cette faille de sécurité, nommée « VPN Fail » par Perfect Privacy, a donné lieu à un avertissement lancé à de nombreux éditeurs. La plupart sont donc informés et le tir a été corrigé pour des solutions comme Private Internet Access, Ovpn.to et nVPN. Ce dernier est pour le moment le seul à avoir confirmé officiellement que cétait le cas, comme en atteste le tweet ci-dessous.

Perfect Privacy indique cependant que toutes les solutions n'ont pas été testées et que le nombre de produits vulnérables est donc sans doute important.

Clients VPN, systèmes dexploitation, BitTorrentLa faille pose évidemment un vrai problème de sécurité et de vie privée. Les VPN sont très utilisés dans les pays par exemple où la censure est importante, notamment parce qu'ils bloquent le repérage de la géolocalisation.

En conséquence, une faille qui laisserait apparaître la véritable adresse IP ne peut que briser tout l'intérêt de ces solutions et on peut espérer que des correctifs seront rapidement déployés.

La dangerosité de la faille est grande selon Perfect Privacy, puisqu'à cause de la nature même de la faille, on risque de la retrouver dans un très nombre de produits, dont les systèmes d'exploitation.

Elle peut également être utilisée pour piéger des internautes qui se serviraient de BitTorrent. La technique s'exploite d'ailleurs plus rapidement puisque le pirate n'a pas besoin d'amener l'utilisateur sur un site. Il doit simplement se trouver sur le même VPN et avoir activé la redirection de port.

nVpn.net @nVpnNet

Fixed a possibility to exploit a VPNs PF feature revealing a user's real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy

01:07 – 27 Nov 2015

4 4 Retweets 2 2 j'aime

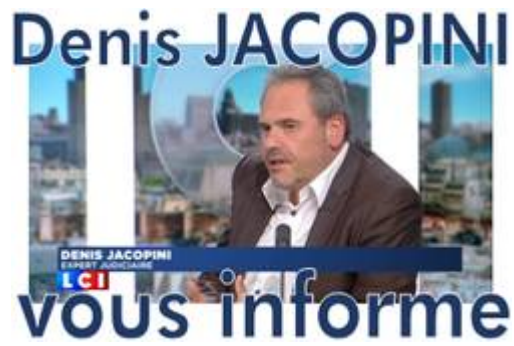
Rien à faire pour linstant du côté de lutilisateur

Dans tous les cas, la victime n'a pas besoin d'avoir l'option activée, et il n'y a donc rien qu'elle puisse faire de son côté. Tous les protocoles liés au VPN, comme OpenVPN et IPSec, sont également concernés. La seule solution est actuellement d'attendre, jusqu'à recevoir une notification de son fournisseur de solution VPN, si bien entendu ce dernier prend la peine de communiquer.

Réagissez à cet article

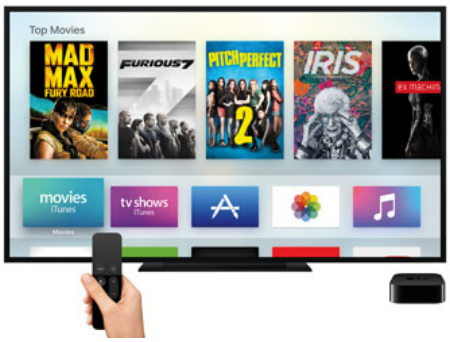
Source : http://www.nextinpact.com/news/97495-vpn-fail-solutions-vpn-touchees-par-faille-sur-redirection-ports.htm

Les Smart TV, prochaines cibles des pirates ?



Les Smart TV, prochaines cibles des pirates ?

Il est aisé d'installer un malware sur une Smart TV, et presque impossible de le retirer. Une cible de choix pour les ransomwares.

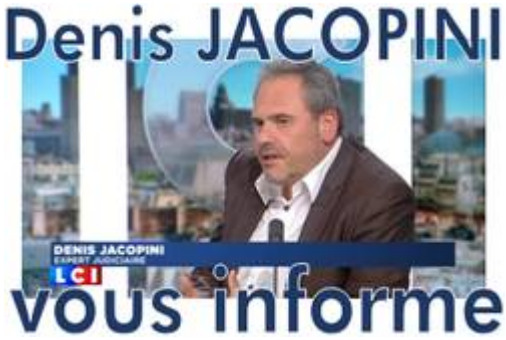


Softpedia rapporte que les malwares pourraient bientôt débarquer en force sur les téléviseurs connectés.
En cause, la montée en puissance de la plate-forme logicielle des Smart TV, qui leur permet de faire tourner des applications tierces, et donc des malwares.
Candid Wueest, de Symantec, a utilisé une technique de type man-in-the-middle pour infecter un terminal Android TV avec un malware.
Opération d'autant plus facile à réaliser que la liaison entre le téléviseur et les serveurs du constructeur se fait en clair. Il suffit donc d'attendre le lancement d'une mise à jour, ou le téléchargement d'une application, pour installer un logiciel indésirable. Un ransomware a ainsi pu être installé sur un téléviseur.
Et il s'est avéré très difficile (voire impossible) à enlever, la Smart TV ne proposant pas de moyen matériel pour réinitialiser ses paramètres et son OS à leur état initial, et les opérations via la télécommande étant entravées par le ransomware.

Les Smart TV, futurs fantassins des botnets ?
Les pirates vont donc se régaler avec ce moyen simple de bloquer un téléviseur à distance, puis de rançonner à volonté ses utilisateurs pour leur redonner la main sur leur Smart TV. D'autres usages sont évoqués par Symantec : fraude au clic ; vol de données personnelles ; vol de données d'authentification ; utilisation de la puissance des téléviseurs pour du mining de cryptomonnaie ; enrôlement des Smart TV dans des botnets, etc.

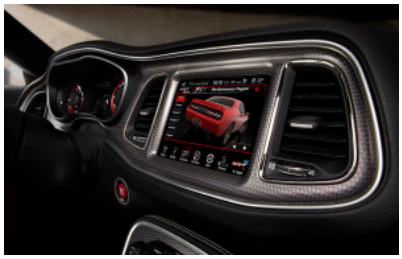
Réagissez à cet article
Source : http://www.silicon.fr/les-smart-tv-prochaines-cibles-des-pirates-132446.html

Objets connectés : une moyenne de 5 failles par objet



Objets connectés : une moyenne de 5 failles par objet

9271 vulnérabilités majeures découvertes dans le firmware de 185 « objets de l'internet », principalement des routeurs, modems DSL/câble, téléphone IP, caméras de surveillance sous IP etc.

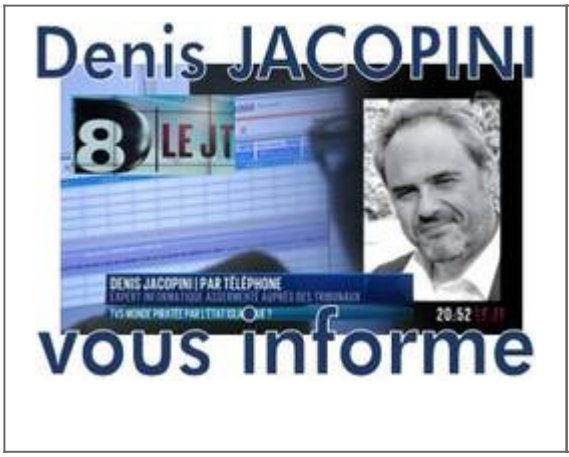


C'est le résultat brut de l'étude signée Andrei Costin et Aurélien Francillon d'Eurecom avec le concours d'Apostolis Zarras de l'Université de Bochum.
Réduire l'étude de ces trois chercheurs en quelques chiffres ne rend pas justice au travail effectué. En fait, son aspect le plus intéressant porte surtout sur l'automatisation et le travail à grande échelle de cette chasse au bug, grâce à la mise en place d'un environnement d'émulation.
La machine virtuelle est adaptée aux principaux systèmes et matériel du commerce, et les firmware chargés puis épluchés de manière dynamique les uns après les autres. Une sorte de « VM de torture » reproduisant au mieux l'environnement d'exécution.
Autre point important, cette recherche s'est limitée (sic) aux simples interfaces Web d'administration et de paramétrage qui sont en général intégrées dans le moindre des objets IoT. Et qui, pourrait-on ajouter, constituent le ventre mou de ces systèmes embarqués depuis des lustres. En d'autres mots, il n'est pas question ici des failles matériel, des trous Wifi/bluetooth/DECT, bref, de ce qui sort du volet « httpd » de ce travail. Il y a fort à parier que si l'analyse avait pu s'étendre à ces aspects, le nombre de défauts recensés aurait été probablement doublé.
Mais ce genre de tests est nettement moins susceptible de pouvoir être automatisé. Les armes de chasse sont classiques : Arachni, Zed Attack Proxy, w3af, ce qui n'interdit pas à tout chercheur souhaitant continuer ce travail d'y ajouter Metasploit ou Nessus.
L'environnement lui-même, Qemu, a été retenu en raison du nombre important de processeurs supportés : Arm, Mips, Mipsel, Axis Cris, bFLT, PowerPC, X86 et même Nios II d'Altera.
Certains cœurs échappent à ce crible, tels les processeurs spécifiques de Dlink ou un Risc 32 bits peu répandu, le Arctangent A5.
Plus de la moitié des objets utilisant un ARM ont été vulnérables à un Chroot et une attaque Web, entre 17 et 21 % pour les systèmes à base de MIPS, et un peu moins de 30 % pour les IoT avec moteur Mipsel.
Les vulnérabilités les plus fréquemment rencontrées sont : XSS (5000 sur les 9271 recensées), manipulation de fichiers (1129), exécution de commandes arbitraires (938), ajout de fichiers (513), divulgation de fichiers (461), injection SQL (442)…

La confiance dans l'IoT, ça se mérite. Toutefois, précisent les trois chercheurs, il est des domaines où la sécurité est prise nettement plus au sérieux.
C'est notamment le cas de boîtier de télévision payante, par câble ou satellite. Probablement en raison des conséquences de pertes économiques directes qu'un défaut de sécurité provoquerait immédiatement, certainement aussi conséquemment aux multiples hacks qui, depuis plus de 20 ans, ont conduit ces intégrateurs à s'engager dans une course au blindage antipirates.
Comme quoi, c'est pas la sécurité qui manque, dans le domaine de l'Internet des Objets, c'est la menace financière.

Réagissez à cet article
Source : http://www.cnis-mag.com/iot-une-moyenne-de-5-failles-par-objet.html

Les pirates du régime iranien ont ciblé les comptes Facebook des fonctionnaires du Département d'Etat américain



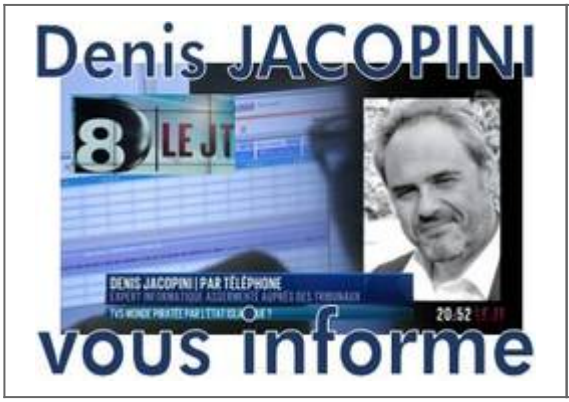
Les pirates du régime iranien ont ciblé les comptes Facebook des fonctionnaires du Département d'Etat américain

Des pirates liés au régime iranien ont augmenté leur cyber-attaques contre des cibles au sein du Département d'État aux États-Unis au cours du mois dernier, ont déclaré des officiels américains et des entreprises de sécurité privés.

Selon des responsables diplomatiques et policières proches de l'enquête, au cours du mois dernier, les pirates iraniens ont identifié les fonctionnaires du Département d'Etat qui travaillent sur l'Iran et le Moyen-Orient et ont fait des intrusions dans leurs messageries et dans leur compte Facebook, a rapporté mardi le journal New York Times.
Facebook a dit aux victimes que des « acteurs étatiques » avait fait des intrusions dans leurs comptes. C'est seulement après ce signalement de Facebook que le Département d'Etat a pris connaissance de cette affaire.
« L'intrusion a été faite de façon très subtile et ils ont identifié les fonctionnaires américains qui travaillent sur les questions relatives à l'Iran », a déclaré un officiel américain de haut-rang qui supervise l'enquête et qui a demandé l'anonymat pour permettre l'avancement de l'enquête.
L'attaque contre le Département d'Etat a été réalisée en utilisant les comptes Facebook de jeunes employés du gouvernement pour accéder aux comptes de leurs amis au sein de l'administration.
Après la signature de l'accord nucléaire, les responsables des services de renseignement aux Etats-Unis avaient dit aux hauts fonctionnaires du gouvernement qu'ils soupçonnent le régime iranien de procéder à des actions de cyber-espionnage.
Le mois dernier, l'équipe de sécurité Facebook avait envoyé des alertes à plusieurs officiels américains pour leur signaler que des pirates avaient fait des intrusions dans leur compte Facebook.
Le message d'alerte de l'équipe de sécurité de Facebook leur disait :
« Nous croyons que votre compte Facebook et vos autres comptes en ligne peuvent être la cible d'attaques de la part des acteurs étatiques. »

Réagissez à cet article
Source
: http://www.ncr-iran.org/fr/actualites/iran-a-monde/16906-les-pirates-du-regime-iranien-ont-cible-les-comptes-facebook-des-fonctionnaires-du-departement-d-etat-americain.htm

La menace du phishing plane sur les PME : trois étapes pour éviter le pire



La menace du phishing plane sur les PME : trois étapes pour éviter le pire

Les attaques informatiques ciblant de grands groupes, comme TV5monde, font régulièrement la une des journaux. Selon le rapport 2014 PwC sur la sécurité de l'information, 117 339 attaques se produisent chaque jour au niveau mondial.

Depuis 2009, les incidents détectés ont progressé de 66%.
Cependant, ce type d'attaques, très répandue, cible en grande partie les PME. Selon un rapport de l'ANSSI, 77% des cyber-attaques ciblent des petites entreprises.
Les conséquences peuvent être désastreuses pour ces structures à taille humaine, n'ayant pas forcément la trésorerie suffisante pour assurer leur activité en attendant le remboursement de leur assurance. Le coût d'une attaque peut s'avérer très élevé et la crédibilité de l'entreprise visée peut également en pâtir.
Suite à une attaque informatique du type « fraude au président », la PME française BRM Mobilier a ainsi perdu cet été 1,6 M€ et se trouve aujourd'hui en redressement judiciaire.
En mai dernier, le PMU a effectué un test grandeur nature en envoyant un faux email, proposant de gagner un cadeau, avec une pièce jointe piégée. Résultat : 22% des salariés ont téléchargé la pièce jointe et 6% ont cliqué sur le lien contenu dans l'email et renseigné leurs données personnelles.

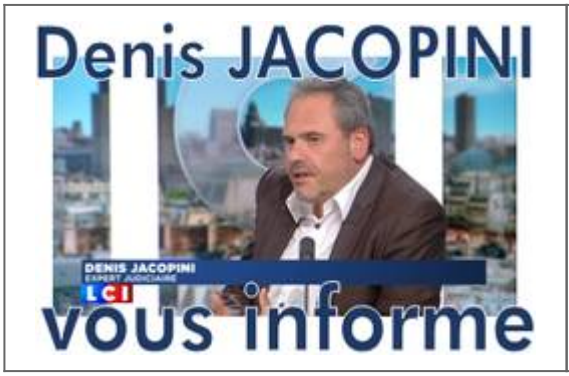
Comment éviter que ce type de scénario ne vire à la catastrophe ?
1 – Connaitre le déroulé d'une attaque Le phishing, également appelé hameçonnage, est une technique employée par les hackers pour obtenir des données personnelles, comme des identifiants ou des données bancaires.
Le déroulement est simple : le hacker envoie un email en usurpant l'identité d'un tiers de confiance, comme un partenaire, un organisme bancaire, un réseau social ou encore un site reconnu.
L'email contient une pièce jointe piégée ou un lien vers une fausse interface web, voire les deux.
Si le subterfuge fonctionne, la victime se connecte via le lien, et toutes les informations renseignées via la fausse interface web sont transmises directement au cybercriminel.
Autre possibilité : la pièce jointe est téléchargée et permet ainsi à un malware d'infester le réseau de l'entreprise.

2 – Comprendre la dangerosité d'une attaque pour l'entreprise
Pour les entreprises, le phishing peut s'avérer très coûteux. Il est bien évidemment possible que le hacker récupère les données bancaires pour effectuer des virements frauduleux.
Puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites, les informations recueillies sont parfois réutilisées pour pirater d'autres comptes, comme une messagerie, un site bancaire, ou autre.Mais – puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites – il est aussi possible que le hacker réutilise les informations recueillies pour pirater une boite mail, ou un compte cloud.
Le cybercriminel peut ainsi consulter l'ensemble de la boîte mail, ou des comptes de sauvegarde cloud, et mettre la main sur des documents confidentiels, comme des plans ou des brevets, pouvant nuire à l'entreprise.
Enfin, les hackers profitent du piratage des boîtes mails pour envoyer à tous les contacts un nouvel email de phishing. La crédibilité de l'entreprise peut ainsi être touchée et ses clients pourraient subir à leur tour des pertes.

3 – Se préparer et éduquer avant qu'il ne soit trop tard
Les emails de phishing ont bien souvent une notion « d'urgence », qu'il s'agisse d'une demande pressante de la part d'un organisme ou d'un partenaire, ou d'une participation à un jeu concours « express ». Le but étant bien évidemment de ne pas laisser le temps à la victime de prendre du recul.
Comprendre le procédé d'une attaque est la première étape pour organiser sa défense. Il faut donc éduquer les salariés et leur donner quelques astuces pour ne pas tomber dans le piège :
• faire attention aux fautes d'orthographe : bien que les emails de phishing soient de mieux en mieux conçus, on y retrouve régulièrement des erreurs de syntaxe ou d'orthographe.
• regarder l'adresse mail ou le lien URL : même lorsqu'un email ou une interface web est une parfaite copie de l'original, l'adresse de l'expéditeur ou l'URL n'est pas la bonne puisqu'elle ne provient pas du même nom de domaine.
Des salariés éduqués et conscients du danger sont le meilleur atout contre les cyber-attaques, en particulier contre le phishing.
Mais, cela n'est pas suffisant, notamment sur les terminaux mobiles où nous avons tous tendance à être plus spontanés et donc, à adopter des comportement à risques.
Il est donc important de mettre en place un filtre anti-phishing aussi bien sur les postes fixes que sur les terminaux mobiles. Ces filtres scannent automatiquement les expéditeurs et les contenus afin de bloquer les emails suspects.
Pour les PME, il est donc important d'éduquer l'ensemble du personnel, mais aussi de mettre en place des solutions de filtrage email et de sécurité complètes. Par ailleurs, garder une proximité avec son équipe informatique, ou ses fournisseurs de services, peut également jouer un rôle primordial pour limiter les dommages si un employé est tombé dans le piège.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-menace-du-phishing-plane-sur,20151123,57740.htm

Droit à l'oubli : Google dévoile les domaines les plus affectés



Droit à l'oubli : Google dévoile les domaines les plus affectés

---

Google a publié un nouveau rapport concernant ses travaux dans le cadre du droit à l'oubli. Celui-ci met en évidence les noms de domaine principalement concernés.

En mai 2014, la Cour de justice de l'Union européenne avait ordonné aux moteurs de recherche en Europe de publier un formulaire de droit à l'oubli.
Ce dernier permet à un individu, ou une entreprise, de gérer sa réputation sur Internet en demandant au moteur de retirer des liens pointant vers certaines pages désuètes, ou qui affectent son image ou sa vie privée.
Au total, Google explique avoir reçu 348 085 requêtes de la part des internautes, lesquelles portent au total sur 1 234 092 liens. Le géant de la recherche affirme avoir accepté 42% de ces demandes.

En France, 73 399 formulaires ont été remplis portant sur 246 158 URL.

Google en a profité pour partager les noms de domaine qui reviennent le plus souvent au travers du formulaire de droit à l'oubli :
www.facebook.com (10220 liens supprimés)
profilengine.com (7986 liens supprimés)
groups.google.com (6764 liens supprimés)
www.youtube.com (5364 liens supprimés)
www.badoo.com (4428 liens supprimés)
plus.google.com (4134 liens supprimés)
annuaire.118712.fr (3930 liens supprimés)
www.twitter.com (3879 liens supprimés)
www.wherevent.com (3465 liens supprimés)
www.192.com (3083 liens supprimés)

Ces noms de domaine compteraient pour 9% de l'ensemble des requêtes reçues par Google.

Réagissez à cet article
Source : http://pro.clubic.com/entreprises/google/actualite-787400-droit-oublie-google-domaines-affectes.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1262345739##pid=22889469

Les nouveaux moyens de communication des terroristes

Les nouveaux moyens de communication des terroristes

La cybercriminalité traque en permanence les terroristes et tente par tous les moyens de trouver comment ils communiquent entre eux. Playstation, réseaux sociaux et même, sites de rencontre, tout est envisageable.

« Tout système de communication par messagerie peut potentiellement être utilisé par les terroriste… » s'exprimait Eric Freyssinet, chef de la division de lutte contre la cybercriminalité.
L'appli Telegram utilisée par les djihadistes Cette appli permet aux messages d'être cryptés. C'est par ce biais que Daech communiquerait, une appli qui, contrairement à Viber ou Whatsapp qui gardent tous les messages, permettrait plus de discrétion.
De plus, la plupart du temps ils s'expriment en arabe et en langage codé ce qui complique la tâche des enquêteurs.

La PS4 au centre des attentions

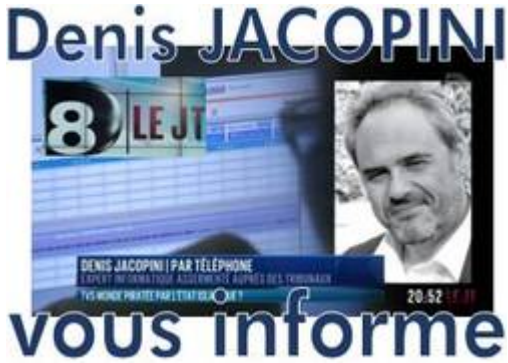
La raison ? Elle aurait été utilisée pour planifier les attentats du vendredi 13 novembre selon le site américain Forbes. Et si vous vous demandez comment, vous pouvez par exemple, avec le jeu Call Of Duty, écrire des mots sur un mur via l'impact des balles, traces qui finiront par définitivement s'effacer, sans laisser de preuves.
« J'ai entendu que le mode de communication entre terroristes le plus difficile à surveiller, c'est la PS4. C'est très, très difficile pour nos services » s'exprimait il y a quelques jours le ministre des Affaires étrangères belge. Sa déclaration n'a pas mis longtemps a agité les internautes…

Réagissez à cet article
Source : http://nextplz.fr/actualite/content/2151616-les-nouveaux-moyens-de-communication-des-terroristes

---

Beijing (Pékin) renforce son

niveau de sécurité



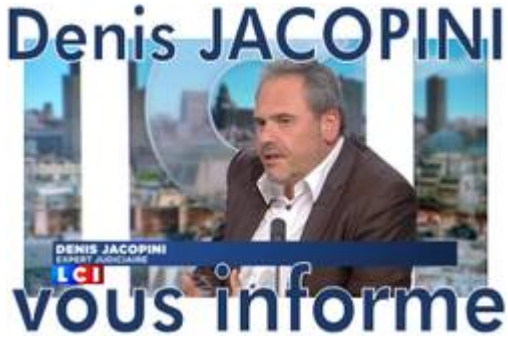
Beijing (Pékin) renforce son niveau de sécurité

L’Agence de presse Xinhua a annoncé que la police de Beijing a déclaré samedi avoir renforcé la sécurité de la capitale dans le cadre d’un effort de lutte contre le terrorisme qui a vu une augmentation des forces de police et des contrôles plus stricts des colis.

Le Bureau municipal de la Sécurité Publique de Beijing (PSB) a relevé le niveau de sécurité pour la capitale le 15 novembre, deux jours après les attentats de Paris.
Davantage de policiers ont été mobilisés, et des contrôles plus stricts sur les services de messagerie, les grands événements et les transports publics ont été imposés.
Le PSB a mobilisé à la fois la police armée et les policiers réguliers, demandant « à la police de la circulation d’arrêter les voitures, aux hommes et femmes affectés aux patrouilles d’inspecter et d’enregistrer toutes les activités, à la police armée de faire une démonstration de force, et à la police auxiliaire de coopérer », a rapporté dimanche le Beijing Youth Daily.
Les forces de police collaborent pour effectuer des contrôles 24 heures sur 24 sur les gens, les voitures et les objets à chaque entrée de la municipalité de Beijing.
Selon le Beijing Youth Daily, depuis novembre, Beijing a inspecté plus d’1 million de voitures et plus d’1,6 million de personnes, et a arrêté plus de 100 suspects sur diverses charges.
De son côté, le Beijing Times a rapporté les propos de Wang Xiaohong, chef du PSB, qui avait dit en avril que la sécurité du transport par métro était la plus grande priorité pour les efforts de lutte contre le terrorisme. Ni Lexiong, un expert anti-terrorisme, a pour sa part dit dimanche que la prévention du terrorisme est non seulement une responsabilité de la police, mais aussi de la société dans son ensemble.
« Les entreprises et les organisations manquent actuellement de sensibilisation à la lutte contre le terrorisme. Si elles étaient attaquées par des terroristes, les résultats seraient inimaginables », a-t-il expliqué.
M. Ni a noté que dans Beijing, les endroits faisant face aux plus grands risques d’être attaqués par des terroristes comprennent les pôles de transport majeurs, les écoles, les hôtels et les lieux de réunion. Il a conseillé qu’une attention particulière soit également être accordée aux festivals chinois, en particulier le Nouvel An chinois. Xinhua a de son côté rapporté que la police de Beijing a également lancé des exercices anti-terroristes en mai et en octobre 2014.
« Malgré les efforts de la police, les écoles, les hôtels, les entreprises et les organisations devraient consacrer plus de personnel et d’argent à l’organisation d’exercices anti-terroristes et devraient proposer leurs propres plans pour faire face aux situations d’urgence », a souligné M. Ni.
Selon lui, la capitale a la capacité de surveiller les nouveaux canaux de communication, y compris la console de jeux vidéo PlayStation 4, si les terroristes l’utilisaient pour communiquer.
Li Wei, expert anti-terrorisme à l’Instituts des relations internationales contemporaines de Chine, estime pour sa part que la Chine est confrontée à des menaces plus terroristes et que le gouvernement devrait prendre davantage de mesures, y compris des actions contre le cyber-terrorisme, pour empêcher les attaques et protéger la vie et la propriété des gens.
Xinhua a également rapporté qu’au cours de la conférence sur la sécurité en cas d’urgence tenue le 15 novembre, Guo Shengkun, le patron de la police chinoise, a souligné la nécessité de renforcer la sensibilisation et le renforcement des mesures préventives anti-terrorisme.
Enfin, le Beijing Youth Daily a rappelé qu’en mars 2014, Beijing a aussi adopté de nouveaux règlements qui stipulent que les citoyens qui rapportent des informations liés à la violence et au terrorisme seront récompensés.

Réagissez à cet article
Source : http://french.china.org.cn/china/txt/2015-11/23/content_37138481.htm

Blocage administratif des sites faisant l’apologie du terrorisme, nouvelle étude du projet de loi



Blocage administratif des sites faisant l’apologie du terrorisme, nouvelle étude du projet de loi

Après l'Assemblée, le Sénat s'est penché vendredi 20 novembre 2015 sur le projet de loi portant sur la prorogation de l'état d'urgence. Parmi les mesures adoptées : le blocage administratif des « services de communication en ligne » faisant l'apologie du terrorisme.

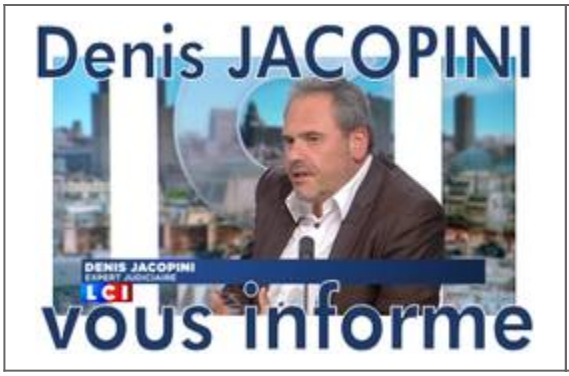
François Hollande avait promis une remise au goût du jour de la loi de 1955 encadrant l'état d'urgence « un toilettage » selon ses mots, afin de l'adapter aux évolutions technologiques du monde contemporain.
Le parlement se penche actuellement sur le texte du projet de loi et l'Assemblée a approuvé hier le texte en première lecture. Parmi les mesures évoquées, l'une d'entre elles porte sur le blocage de « services de communication en ligne » faisant l'apologie du terrorisme et permet au ministre de l'Intérieur de prendre « toutes les mesures » pour interrompre les services visés.
Une mesure qui avait un goût de déjà vu pour tous ceux ayant suivi les débats liés à la loi antiterroriste : de nombreux débats autour de la mesure prévoyant le blocage administratif des sites faisant l'apologie du terrorisme avaient eu lieu et la mesure avait finalement été approuvée par le parlement.

Les mains libre pour le ministre de l'intérieur
Il s'agit en réalité d'une version bien plus musclée que celle initialement prévue par la loi antiterroriste : sous le régime habituel, plusieurs garde-fous viennent limiter l'exercice de ce blocage par voie administrative.
Ainsi, les autorités sont tout d'abord tenues de contacter les hébergeurs du site en question afin de demander le retrait du contenu. En cas d'absence de réponse de sa part 24h après la demande initiale, les autorités peuvent alors se tourner vers les FAI pour mettre en place un blocage administratif du site redirigeant les utilisateurs qui tentent de se connecter vers une page d'avertissement.
De plus, la CNIL peut exercer un contrôle a posteriori des sites visés par de telles mesures afin de prévenir les risques de blocage abusif. Dans le contexte du nouvel état d'urgence proposé par le gouvernement, ces gardes fous sautent : le ministre de l'Intérieur a les mains libres pour bloquer l'accès à un site faisant l'apologie du terrorisme, sans avoir à notifier préalablement les éditeurs ou hébergeurs du site en question.
Le texte a été approuvé à la quasi unanimité par l'Assemblée, seuls 6 députés se sont prononcés en sa défaveur.
Le Sénat doit encore approuver le texte avant que celui-ci n'entre en vigueur : outre les mesures concernant le blocage administratif, les députés ont également validé les mesures précisant les conditions de perquisitions et étendant leur portée aux appareils numériques trouvés dans le lieu visé, ainsi que l'extension de l'état d'urgence pour trois mois.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/blocage-administratif-des-sites-le-gouvernement-en-remet-une-couche-39828440.htm

---

Anonymous découvre un portefeuille électronique de l'EI de 3 M USD



#Anonymous découvre un portefeuille électronique de l'EI de 3 M USD

Le groupe hacktiviste Anonymous déclare avoir découvert un portefeuille électronique du groupe terroriste Etat islamique dans le système Bitcoin.

Le groupe de hackers Anonymous tient ses promesses. Suite aux attentats de Paris, les hackivistes ont déclaré une « guerre sans merci » à l'Etat islamique (EI). Bien que tournés en ridicule par des gens qui affirmaient que leurs actions n'avaient aucun de poids comparé au sang réel qui était versé par les terroristes, ils sont rapidement passés à l'action. Ayant annoncé avoir piraté plus de 5.000 comptes de propagande liés à l'État islamique sur Twitter, ils déclarent maintenant avoir découvert un portefeuille électronique de l'EI de 3 millions de dollars en bitcoins, un système de paiement sur Internet.

Les Anonymous piratent plus de 5.000 profils de l'EI sur Twitter

« L'Etat islamique utilise de la crypto-monnaie pour financer ses opérations en cours et nous avons réussi à découvrir plusieurs adresses Bitcoin qu'il utilise », ont déclaré les Anonymous dans un commentaire pour NewsBTC. L'une des plus importantes fonctions de la monnaie cryptographique est qu'elle ne peut être censurée à la demande d'un tiers. On ne sait jamais ce qui sera ensuite à l'ordre du jour. Les activistes pour les droits des animaux, les défenseurs de l'environnement ou d'autres groupes dont les comptes peuvent être bloqués optent tous pour le Bitcoin, car il s'agit d'un service libre. Ainsi, le Bitcoin encourage à la fois des objectifs objectivement honorables mais peut aussi servir des intérêts qui le sont un peu moins, comme ceux de l'EI par exemple.
C'est pourquoi il constitue l'un des leviers numériques privilégiés par l'EI pour aider « ses amis » de Syrie, d'Irak, du Liban et de partout dans le monde.

Anonymous déclare (pour de bon) la guerre à l'EI

Pourtant, l'espoir n'est pas perdu. Le groupe hacktiviste Anonymous assure avoir réussi à bloquer la plupart des comptes de l'EI en Bitcoin qui avaient été dissimulés sur un type de bases de données appelé « deep Web ». Plus tôt, les hacktivistes s'étaient fixés pour mission d'anéantir la propagande terroriste ainsi que les réseaux de recrutement de l'EI sur Internet. Dans une vidéo publiée sur YouTube, un porte-parole de l'organisation virtuelle s'était engagé à « lancer la plus grande opération de tous les temps » contre l'EI.

Réagissez à cet article

Source : http://fr.sputniknews.com/international/20151121/1019708957/anonymous-portfeuilles-ei-hachtivistes-hackers.html