Deux millions d’abonnés du site de TF1 piratés

Deux millions d’abonnés du site de TF1 piratés

Les données de deux millions d’abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

Deux millions d’internautes menacés. Les abonnés du site de TF1 regarderont à deux fois avant de s’inscrire sur des plates-formes numériques. Deux millions d’entre eux ont en effet vu leurs données personnelles (RIB, mais aussi toutes les informations qui ont trait à l’identité numérique) piratées par des hackers vendredi. L’information, rapportée par RTL, a été révélée par Damien Bancal, un spécialiste en cybercriminalité qui a découvert ce piratage.

Techniquement, les hackers sont parvenus à attaquer la partie abonnement presse du site de TF1, sur laquelle il est possible de s’abonner à différents journaux. Une plate-forme que la chaîne privée ne gère pas directement, c’est un prestataire commercial externe qui assure son fonctionnement.

Des usurpations d’identités numériques possibles
Selon Damien Bancal, le spécialiste en cyber-criminalité, ce piratage de grande ampleur pourrait permettre aux hackers d’usurper l’identité des personnes inscrites sur le site. Cela pourrait également déboucher sur « une utilisation de ces données pour lancer d’autres escroqueries, aujourd’hui ou plus tard ».
Autre possibilité, cette base de données pourrait être vendue plusieurs milliers ou millions d’euros à d’autres cybercriminels. Les administrateurs du site ont quant à eux déjà corrigé la faille technique dans laquelle se sont engouffrés les pirates.

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

Source : http://www.europe1.fr/medias/tf1-piratage-de-masse-des-donnees-d-abonnes-2333529

Surveillance des internautes

– La loi valse sous haute discrétion

	Surveillance des internautes – La loi valse sous haute discrétion

Le 24 décembre, Matignon a publié un décret sur une mesure très contestée permettant aux agents de l'État de surveiller le Net français. Habile !C'est un cadeau de Noël dont les internautes et les opérateurs français se seraient bien passés. Le gouvernement a publié mercredi 24 décembre, à la faveur des fêtes de Noël, le décret d'application du très contesté article 20 de la loi de programmation militaire (LPM). Ce texte prévoit un accès très vaste des services de l'État aux télécommunications (téléphone, SMS, Internet, etc.) des Français, et à toutes les informations qui transitent par les réseaux nationaux.
La mesure de surveillance, pudiquement nommée « accès administratif aux données de connexion », avait été votée fin 2013 et entrera en vigueur le 1er janvier 2015. Dénichées par notre excellent confrère Next INpact (http://www.nextinpact.com/news/91534-le-decret-l-article-20-lpm-publie-on-fait-point.htm), qui évoque « un décret qui sent le sapin », ce sont les modalités de sa mise en oeuvre, tout aussi importantes, qui ont été dévoilées pour Noël.
Comme dans de nombreuses démocraties, le spectre terroriste permet au gouvernement de faire passer des mesures très floues et de tirer pleinement parti des systèmes d'information de plus en plus performants afin de surveiller la population.

Qui chapeaute le système ?
Le décret du 24 décembre présente « le groupement interministériel de contrôle […], un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion ». Ce groupement est chargé de centraliser les demandes des agents et de les transmettre aux opérateurs concernés, en les épurant de toute information sensible.
En effet, si les services de l'État doivent justifier leurs requêtes auprès du Premier ministre (qui nomme une « personnalité qualifiée »), il est hors de question de transmettre ces explications aux opérateurs. Les fournisseurs d'accès ne sauront même pas de quel service ou ministère émane une demande, ni à quelle date elle a été formulée.

Quelles données sont concernées ?
Sans surprise, le décret se réfère à l'article 20 de la LPM, sans vraiment le préciser. Peuvent donc être interceptés les « informations ou documents traités ou conservés par les réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».
On notera l'utilisation de la formule « y compris », qui n'est aucunement exhaustive : difficile de faire plus vaste.

Un contrôle démocratique insignifiant
Face aux critiques sur l'intrusion dans la vie privée, le gouvernement invoque la Commission nationale de contrôle des interceptions de sécurité (CNCIS), un organe très joli sur le papier mais qui n'a jusqu'à présent pas été doté d'un réel pouvoir. Cette commission « dispose d'un accès permanent aux traitements automatisés », et « l'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la commission tous les éclaircissements que celle-ci sollicite », promet le décret, plein de bons sentiments.

Néanmoins, la CNCIS **n'a toujours pas le pouvoir de sanction et ne peut même pas alerter la justice en cas de manquement sur un dossier couvert par le secret de la défense nationale**. Habile…

Par ailleurs, le gouvernement se protège en supprimant ses archives en un temps record. Si l'on peut saluer la suppression des informations et des fichiers recueillis au bout de trois ans, on ne peut être que surpris par le fait que les registres mentionnant qui a autorisé telle ou telle surveillance soient eux aussi « automatiquement effacés » après trois ans. Le seul contrôle démocratique possible lorsqu'on jongle avec le secret défense, celui qui s'effectue a posteriori, est donc rendu impossible, pour la CNCIS comme pour la justice.

À quel prix ?
« Les coûts supportés par les opérateurs pour la transmission des informations ou des documents font l'objet d'un remboursement par l'État », précise le décret. Pas un mot sur la grille tarifaire qui sera appliquée, car ils seront définis par les ministères concernés.

Qui peut demander les informations ?
Trois ministères sont habilités à émettre des demandes. Le décret détaille le nombre impressionnant de services pour lesquels les vannes du Web français sont ouvertes :

– Au ministère de l'Intérieur : la Direction générale de la sécurité intérieure (DGSI), la Direction générale de la police nationale (unité de coordination de la lutte antiterroriste, Direction centrale de la police judiciaire, Direction centrale de la sécurité publique, Direction centrale de la police aux frontières), la Direction générale de la gendarmerie nationale (sous-direction de la police judiciaire ; sous-direction de l'anticipation opérationnelle ; service technique de recherches judiciaires et de documentation ; sections de recherches), la préfecture de police (Direction du renseignement ; direction régionale de la police judiciaire ; service transversal d'agglomération des événements ; cellule de suivi du plan de lutte contre les bandes ; sûreté régionale des transports ; sûretés territoriales).

– Au ministère de la Défense : la Direction générale de la sécurité extérieure (DGSE), la Direction de la protection et de la sécurité de la défense, la Direction du renseignement militaire.

– Au ministère des Finances et des Comptes publics : la Direction nationale du renseignement et des enquêtes douanières, le service de traitement du renseignement et d'action contre les circuits financiers clandestins.

Dans tous ces services, seuls les agents et officiers « dûment habilités » par leur directeur pourront réclamer des informations, assure le décret.

Des perspectives inquiétantes
La loi de programmation militaire a mis en place un outil de surveillance de la population française qui aurait fait pâlir d'envie les pires dictateurs de l'histoire. Si nous sommes très loin d'un régime totalitaire en France, il n'est pas exclu que des leaders extrémistes disent demain merci au gouvernement Valls pour leur avoir fourni un tel outil clé en main.

Pour info :
Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029958091&dateTexte&categorieLien=id

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

Source :
http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/le-cadeau-de-noel-du-gouvernement-aux-internautes-la-surveillance-26-12-2014-1892495_506.php
Par GUERRIC PONCET

La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'aprè

La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'après de récents documents

Newly published NSA documents show agency could grab all Skype traffic

A National Security Agency document published this week by the German news magazine Der Spiegel from the trove provided by former NSA contractor Edward Snowden shows that the agency had full access to voice, video, text messaging, and file sharing from targeted individuals over Microsoft's Skype service. The access, mandated by a Foreign Intelligence Surveillance Court warrant, was part of the NSA's PRISM program and allowed "sustained Skype collection" in real time from specific users identified by their Skype user names. The nature of the Skype data collection was spelled out in an NSA document dated August 2012 entitled "User's Guide for PRISM Skype Collection." The document details how to "task" the capture of voice communications from Skype by NSA's NUCLEON system, which allows for text searches against captured voice communications. It also discusses how to find text chat and other data sent between clients in NSA's PINWALE "digital network intelligence" database. The full capture of voice traffic began in February of 2011 for "Skype in" and "Skype out" calls—calls between a Skype user and a land line or cellphone through a gateway to the public switched telephone network (PSTN), captured through warranted taps into Microsoft's gateways. But in July of 2011, the NSA added the capability of capturing peer-to-peer Skype communications—meaning that the NSA gained the ability to capture peer-to-peer traffic and decrypt it using keys provided by Microsoft through the PRISM warrant request. The NSA was then able to "task" any Skype traffic that passed over networks it monitored or by exploitation of a targeted user's system. "NSA receives Skype collection via prism when one of the peers is a (FISA Amendments Act Section 702) tasked target," the Skype collection guide stated. Because Skype has no central servers, the guide explained, for multiparty calls, "Skype creates a mesh-network, where users are connected together through multiple peer-to-peer links. Instant Messages sent to this group of meshed participants can be routed through any participant." If any participant in a chat was monitored, the NSA could capture all of the IM traffic in the shared chat. Initially, NSA analysts had to piece together voice communications between peers because they were carried over separate streams, but a service added by August of 2012 by the NSA's Cryptanalysis and Exploitation Services (CES) automatically stitched both audio streams of a conversation together. As of 2012, however, analysts still had to search for associated video from a call session to match it up with audio in a tool called the Digital Network Intelligence Presenter (DNIP).
Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire… Source : http://arstechnica.com/tech-policy/2014/12/newly-published-nsa-documents-show-agency-could-grab-all-skype-traffic/

Le groupe de Cybercriminels Rex Mundi fait chanter les sociétés belges

Le groupe de Cybercriminels Rex Mundi fait chanter les sociétés belges

Rex Mundi, le “roi du monde” en latin , un groupe de cybercriminels, est passé à l’action à la nouvelle année en republiant sur le Net des informations, parfois privées, sur des milliers de Belges.

Ces informations proviennent de treize sociétés ou filiales belges piratées au cours des derniers mois, dont Numéricable, Mensura, Domino’s Pizza, Thomas Cook, Finalease Car Credit, Buy Way et d’autres sociétés spécialisées dans l’intérim comme Tobasco et Z-Staffing.
L’information a été publiée sur le blog d’un expert en piratage, Len Lavens, puis relayée par “De Tijd”. “Ce qui prouve ce que j’ai déjà dit à la télévision : une fois sur le Web, toujours sur le Web”, a commenté l’expert.
Le piratage de ces sociétés n’est pas un fait nouveau, mais la diffusion des informations est, dans, certains cas, nouvelle. Les données ont été publiées sur la plateforme Tor, haut lieu de l’échange anonyme de données (NdlR, voir article ci-contre).
“Pour nous, cette affaire date de janvier 2013”, souligne Alain De Deken, de la société de crédit Buy Way. “Ils ont eu accès à des gens qui avaient fait une demande de crédit personnel sur Internet. Il s’agissait de 545 demandes. On a repéré la fuite, et elle a été colmatée.”
Buy Way affirme que les données volées n’ont qu’une valeur commerciale. Rex Mundi, qui s’inspire par sa devise des Templiers, a tenté de faire chanter la société, contre 20 000 euros, en menaçant de publier les données sur le Net, “mais on n’a pas donné suite”.
Rex Mundi opère depuis 2012 et a déjà à son actif plusieurs sociétés belges dont Dexia et Voo. Dans ce dernier cas, le pirate affirmait avoir saisi des données de près d’un demi-million de clients du câblodistributeur. La société a déposé plainte et assuré que ses clients n’avaient subi aucun préjudice. Pressée de questions par la RTBF, elle n’a ni démenti ni confirmé qu’elle avait payé une rançon pour sortir d’affaire. “Des entreprises ont payé. Je crois que c’est une erreur. Car le maître chanteur peut revenir”, juge Olivier Bogaert, de la Computer Crime Unit de la police fédérale.
A l’égard de Domino’s Pizza, une rançon de 30 000 euros avait été réclamée. La société a refusé, et ses informations ont été publiées sur le Net.

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

Source : http://www.lalibre.be/economie/actualite/cybercriminalite-rex-mundi-fait-chanter-les-societes-belges-54a6e9b7357028b5e9d01b6d
Par Christophe Lamfalussy & P.V.C.

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs Directory Authorities dans le viseur

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs

Depuis les révélations d’Edward Snowden sur les pratiques d’espionnage de la NSA et du GHCQ, le réseau anonyme Tor a largement gagné en popularité, ce qui l’a rendu inévitablement le centre des convoitises des agences gouvernementales et la cible de plusieurs attaques.

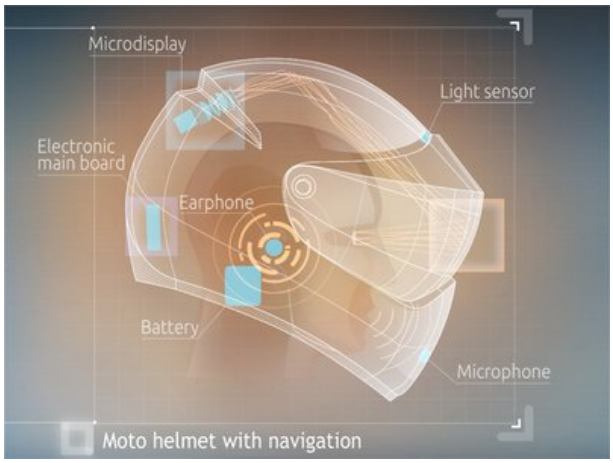
C’est dans ce contexte que le directeur du projet Tor – Roger Dingledine – a annoncé que le réseau anonyme serait sous la menace d’une attaque informatique ou d’une procédure judiciaire dans les prochains jours.
Dans son billet de blog, Dingledine a tenu à rassurer les utilisateurs que des dispositifs techniques ont été pris pour assurer l’anonymat des utilisateurs, alors qu’ils seront notifiés en cas d’attaques dans les plus brefs délais via le blog et le compte Twitter du projet. De plus, la redondance de l’infrastructure du réseau devrait permettre le fonctionnement de Tor même en cas d’attaque selon le même responsable.
Toutefois, des réserves peuvent être émises quant à la capacité de Tor à résister à cette menace, en effet ladite attaque/procédure cible principalement les serveurs DA (Directory Authorities) via une attaque de type DDoS ou encore par la saisie des serveurs physiques, hors ces derniers qui sont au nombre limité de 10, jouent un rôle crucial dans l’anonymat du réseau, en mettant à disposition des utilisateurs une liste de relais potentiels qui seront par la suite utilisés pour débuter toute communication.
Ainsi, la perturbation du bon fonctionnement des serveurs DA devrait impacter le réseau, pire encore ces serveurs sont aussi responsables de la validation de la liste des relais utilisables, validation qui se fait chaque heure par l’aval de la majorité (au moins 5 serveurs), dès lors le contrôle d’au moins 5 serveurs DA permettrait à l’attaquant de réorienter le trafic vers des relais non sécurisés et déjà sous son emprise, ce qui pourrait signer le coup d’arrêt temporaire de tout le réseau Tor.
À noter aussi que les serveurs DA sont les premiers à être contactés par les utilisateurs, de ce fait leurs adresses IP sont inscrites en dur dans le code du client, ce qui limite le champ d’action et de riposte des responsables du projet.
Quant à la cause d’une telle entreprise, les spéculations vont bon train, allant même à affirmer que cela est relatif au récent piratage de Sony, même si aucune information n’a filtrée lors de l’annonce officielle.
Finalement, le mystère reste entier et les risques sont accrus pour les utilisateurs, ce qui laisse place à la vigilance et à la prudence comme étant les seules consignes en vigueur.

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

Sources :
http://www.developpez.com/actu/79522/Tor-sous-la-menace-d-une-attaque-en-mesure-de-corrompre-l-anonymat-des-utilisateurs-les-serveurs-Directory-Authorities-dans-le-viseur/
https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network
par Arsene Newman

Un casque moto connecté à réalité augmentée prévu pour

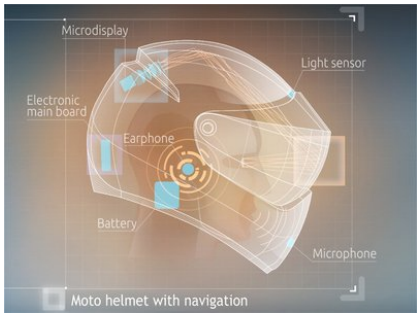
cet été



Un casque moto connecté à réalité augmentée, prévu pour cet été

La société russe Livemap annonce avoir levé 300 000 dollars pour commercialiser son produit phare. La sortie de son casque de moto affichant des éléments visuels sur la visière du conducteur est prévue pour cet été.

La société russe Livemap développe un produit très particulier pour les conducteurs de deux-roues. Il s'agit d'un casque intégrant plusieurs technologies comme la réalité augmentée ou encore, le contrôle de services grâce à la voix. Le dispositif peut se relier au GPS et afficher un itinéraire sur la visière du conducteur.

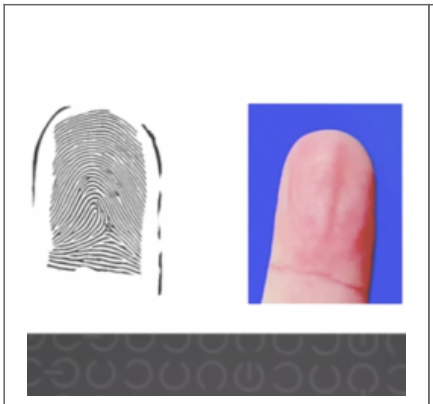


Après avoir développé de premiers concepts, la start-up indique que son produit est désormais prêt à être commercialisé. Elle précise au site américain Techcrunch avoir levé la somme de 300 000 dollars auprès du ministère des Sciences de Russie, afin de procéder à la mise sur le marché de son dispositif.
Grâce à ces fonds, Livemap indique s'être notamment concentrée sur le dispositif permettant de projeter des images sur la visière. Son dernier prototype devrait être présenté au printemps prochain, pour une commercialisation au trimestre suivant.

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

Source : http://pro.clubic.com/actualite-e-business/investissement/actualite-746953-casque-moto-realite-augmentee-levee-fonds.html
Par Olivier Robillart

Un hacker parvient à reproduire des empreintes digitales à partir de photos



Un hacker parvient à reproduire des empreintes digitales à partir de photos

Il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales.

On savait déjà quil était possible de récupérer les empreintes digitales d'une personne ayant touché une surface lisse, comme un verre ou un smartphone. Mais un hacker allemand a montré qu'il était possible de voler ces caractéristiques biométriques spécifiques à partir d'une simple photo.
Lors de la 31e convention annuelle (27-30 décembre, Hambourg, Allemagne) du Chaos Computer Club, la plus grande association de hackers européens, un hacker du nom de Jan Krissler, également connu sous le pseudonyme de « Starbug », a expliqué comment reproduire les empreintes digitales d'une personne à partir de simples photos.
Pour sa démonstration, il a copié l'empreinte de la ministre de la Défense allemande, Ursula Von der Leyen.
En effet, il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales. Étant donné que ces empreintes peuvent être utilisées pour l'authentification biométrique, « Starbug » estime que sa démonstration va vraisemblablement obliger « les politiciens à porter des gants lors de leurs apparitions publiques ».
Pour réussir son exploit, Jan Krissler a utilisé le logiciel VeriFinger disponible dans le commerce. Comme source, il est reparti d'un gros plan du pouce de la ministre, pris lors d'une conférence de presse donnée en octobre dernier, plus d'autres photos prises sous des angles différents pour restituer une image complète de l'empreinte digitale.

Si la méthode est aussi facile à réaliser que ce qu'a montré le hacker, elle pourrait remettre en question l'usage des empreintes digitales pour la sécurisation de certains accès. Et dans ce cas, il faut garder ces options de détournement en mémoire. Mais, même si la reproduction des empreintes digitales s'avère viable pour forcer l'accès d'un système, aussi bien un smartphone qu'un lieu très sécurisé, l'exploit accompli par le hacker au 31C3 ne signifie pas pour autant que leur usage est devenu brusquement obsolète.
Les systèmes de sécurité parfaits n'existent pas, et les empreintes digitales ont encore leur place dans la sécurisation des systèmes. Dans un grand nombre de situations, on peut renforcer la sécurité en ajoutant des codes PIN, et il est toujours temps de coupler les solutions biométriques existantes avec des codes ou d'autres protections par mots de passe pour multiplier les niveaux de sécurité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-hacker-parvient-a-reproduire-des-empreintes-digitales-a-partir-de-photos-59753.html
Par Jean Elyan

Les hackers iraniens montent en puissance

Les hackers iraniens montent en puissance

Les pirates informatiques iraniens montent en puissance et ont déjà dérobé des données « hautement sensibles » lors d'attaques contre des gouvernements et des entreprises aux Etats-Unis, en Chine ou en France, affirme aujourd'hui une société américaine de cyber-sécurité. « A mesure que les capacités de l'Iran en matière de cyber-attaque se transforment, la probabilité d'une attaque qui aurait un impact dans le monde réel, à un niveau national ou mondial, augmente très rapidement », met en garde Cylance.

Selon son rapport, l'opération « Cleaver » menée depuis deux ans par des hackers basés à Téhéran leur a déjà permis de conduire une « importante campagne d'infiltration et de surveillance » dans une longue liste de pays qui compte également Israël, l'Arabie Saoudite, l'Allemagne ou l'Inde. Leurs attaques ont ciblé les gouvernements mais également les entreprises du secteur militaire ou pétrolier ainsi que des infrastructures stratégiques (aéroports, hôpitaux…), énumère la société qui affirme avoir des « preuves » que la sécurité aérienne a été par exemple particulièrement « compromise » en Corée du Sud et au Pakistan.

« Les capacités techniques de l'opération Cleaver évoluent plus vite que toutes les précédentes tentatives iraniennes », assure Cylance, selon qui cette offensive répond aux cyber-attaques subies par Téhéran en provenance d'Israël ou des Etats-Unis et visant son programme nucléaire controversé. L'attaque du virus informatique « Stuxnet », qui avait frappé l'Iran vers 2010-2011, aurait ainsi « ouvert les yeux » des autorités de Téhéran en révélant leur vulnérabilité et les a conduits à « contre-attaquer » en lançant l'opération « Cleaver », explique le rapport, selon qui le soutien du régime à cette offensive ne fait aucun doute.

Plusieurs grandes entreprises américaines, dont Apple ou la banque JPMorgan ont récemment été victimes de cyber-attaques dont l'origine n'a pas été formellement identifiée, suscitant des mises en garde croissantes des autorités.

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

Source : http://www.lefigaro.fr/flash-actu/2014/12/03/97001-20141203FILWWW00452-les-hackers-iraniens-montent-en-puissance.php
Par Gilbert Kallenborn

Accès administratif aux données de connexion: rassuré avec le décret ?

Accès administratif aux données de connexion: rassuré avec le décret ?

Le décret sur l'accès administratif aux données de connexion, en lien avec l'article 20 de la LPM, a été publié le 24 décembre. La cyber-surveillance tend à se généraliser malgré la vigilance de la CNIL.

C'est un grand classique quel que soit le gouvernement : la tentation de faire passer des décrets juste avant Noël pour éviter de faire trop de bruit. Mais le tour de passe-passe n'a pas échappé à des médias vigilants sur la protection de la vie privée comme NextInpact.

Dans le JORF en date du 26 décembre, on découvre le décret 2014-1576 « relatif à l'accès administratif aux données de connexion » (qui avait été approuvé le 24 décembre).
Une belle tentative de mettre en œuvre en catimini d'ici le premier janvier 2015 ce qui avait provoqué une polémique sur la protection des droits civils à l'ère numérique dans le cadre de l'examen du projet de loi sur la programmation militaire (LPM).
Adopté en décembre 2013, le texte dense intègre un article 20 au contour flou qui a des répercussions sur la vie civile : l'accès par les autorités – sans décision judiciaire – aux données de connexion des internautes.
Une approche qui suscitait des craintes sur l'encadrement de l'accès aux données à caractère personnel. Gare à la dérive cyber-sécuritaire, estimait des associations professionnelles du secteur IT comme Renaissance Numérique ou l'ASIC à l'époque.
Ainsi, la loi prévoit initialement l'accès par l'administration aux « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques ». Le champ des données surveillées n'était pas limité aux seules données de connexion, mais pouvait concerner l'ensemble des données stockées par l'utilisateur : documents sur le cloud, mails, échanges sur les réseaux sociaux, pseudos, mots de passé, etc.

L'élargissement de la cyber-surveillance reste d'actualité avec la publication du décret associé à l'article 20 de la LPM. Le régime d'exception de l'accès administratif aux données de connexion – jusqu'ici associé principalement à la lutte antiterroriste – est généralisé : « Les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses et sont accessibles à un nombre de plus en plus important d'organismes. »
Et ce, pour des finalités très différentes » au nom de divers intérêts nationaux : « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

Le spectre du Big Brother serait écarté partiellement avec les nouveaux éléments fournis dans le décret du 24 décembre sur « l'accès administratif aux données de connexion ». Celui-ci limite la collecte d'information aux données de connexion (identité de la personne, date et heure de communication, etc.) mais il reste néanmoins à préciser l'exact périmètre des données recueillies.

Bonne nouvelle : le décret semble écarter les risques de droit de regard sur les contenus.
De même, la DGSE, la DGSI ou tout autre service de police judiciaire ne pourront pas directement installer des logiciels d'espionnage (« mouchards ») de manière intensive sur les réseaux des opérateurs.
Selon l'avis de la CNIL rendu le 4 décembre (sur ce qui était à l'époque un projet de décret) mais qui vient juste d'être publié dans le prolongement de la promulgation du décret, il en résulte que « cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes ».
L'autorité française en charge de la protection des données personnelles reste vigilante. « Elle appelle l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques. »
L'année 2015 va mal démarrer alors que le gouvernement prépare une loi sur le numérique. L'occasion d'éclaircir le débat ? Dans le cadre de la consultation gouvernementale ouverte au grand public pour élaborer cette loi, on espère un peu plus de transparence à propos de cette extension de la cyber-surveillance.

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

Source : http://www.itespresso.fr/acces-administratif-donnees-connexion-rassure-publication-decret-85710.html

Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

	Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

Ils sont de plus en plus jeunes et stupides puisque incapables d'évaluer les risques liés à l'objet de leurs forfaits. Avec la création de la cellule de lutte contre la cybercriminalité, nombre d'entre eux apprennent désormais à leurs dépens que certains actes ne restent jamais impunis.

Les faits remontent au lundi 15 septembre 2014 dans la zone ACI, une cité résidentielle censée pourtant être sous surveillance accrue au regard de ses occupants, pour la plupart, des ressortissants étrangers (missions diplomatiques, organisations internationales, etc.). Mais qu'importe pour les malfrats désormais regaillardis par les nombreuses failles du dispositif sécuritaire dans la capitale et surtout, par des décisions pour le moins controversées des plus hautes autorités de la République.
C'est donc en plein jour, aux environs de 14 heures dans la zone indiquée que trois individus armés ont envahi un magasin de vente de téléphones portables de grandes valeurs et autres accessoirs electroniques dont des clés USB, des chargeurs, des puces, cartes mémoires, etc.
Les deux premiers tinrent la gérante en joue pendant que le troisième dévalisait litteralement la boutique. Ils purent ainsi emporter des appareils d'une valeur marchande de plusieurs dizaines de milliers de nos francs ainsi que la somme de 35.000 F CFA en espèces. Et ils repartirent sans être inquietés. Mission accomplie? Loin s'en fallait !

La victime décida de porter plainte contre X au niveau de la Brigade d'Investigation judiciaire (BIJ) et, naturellement, la nature des objets volés aidant, l'affaire fut confiée à la Cellule de lutte contre la Cybercriminalité dirigée par l'Inspecteur divisionnaire Papa Mambi Keïta surnommé « l'Epervier du Mandé». Commença alors la cyber-traque !

Nous ne cesserons jamais de le dire: les objets électroniques sont de véritables traîtres. Ils sont susceptibles de tout révéler sur leurs propres utilisateurs. Et le saviez-vous ? Il est même possible d'ouvrir le micro de certains téléphones à distances. Quant aux puces, cartes mémoires ou clés USB, elles peuvent être également activées de loin. A ce stade, certains commentateurs comparent déjà notre époque à celle décrite par l'auteur de roman de science fiction, Georges Orwell dans «1984» avec le fameux « Big Brother » désormais présent dans la légende contemporainne*.
Naturellement, ces méthodes de surveillance necessitent des équipements adéquats, une collboration accrue des services techniques et surtout, une bonne dose d'intelligence; un aspect de la question qui ne fait nullement défaut au niveau de la cellule de lutte contre la cybercriminalité.

Mettant ainsi toutes ces aptitudes à contribtion, les enquêteurs parvinrent à identifier un nommé Souleymane Doumbia comme utilisateur d'un des objets volés. Il fut interpellé dans les heures qui suivront et sa victime l'identifia formellement comme étant un de ses agresseurs. Il était inutile de nier les faits. Mais comment diantre les enquêteurs sont-ils parvenus jusqu'à lui ? C'est bien la question qu'il se pose encore à l'heure actuelle. Difficile de trouver réponse à cette intérrogation. Et pour cause, « Big Brother » est passé par là. Ses complices, quant eux, attendent à leur tour d'être arrêtés. Une question de jours.

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

Source : http://maliactu.net/mali-arrestation-de-braqueurs-dans-la-zone-aci-big-brother-est-passe-par-la/