Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.

« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés ».« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon

Quelles sont les modalités de blocage des sites Internet ?

Quelles sont les modalités de #blocage des sites Internet ?

M. Lionel Tardy interroge M. le ministre de l'intérieur sur le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographiques.
Ce décret précise les modalités d'applications de l'article 6-1 de la loi pour la confiance dans l'économie numérique (LCEN). En complément, il souhaite savoir si, une fois la procédure appliquée, l'OCLCTIC sera également destinataire de données statistiques relatives aux tentatives de connexions aux sites bloqués, et le cas échéant, les modalités de ce recueil.

Texte de la réponse
La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a doté la France de nouveaux moyens face à la menace constante et croissante à laquelle elle est confrontée. Elle permet, notamment, de mieux combattre la propagande terroriste sur internet. Ses textes réglementaires d'application ont été rapidement publiés et toutes ses dispositions sont donc aujourd'hui applicables. Il en est ainsi des dispositions visant, suivant un dispositif gradué et équilibré garantissant le respect des libertés publiques, à renforcer les capacités de blocage des sites internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application a été publié dès le 5 février 2015 (décret no 2015-125 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique). S'agissant du nombre de connexions à un site dont l'accès est bloqué, il fait l'objet d'une comptabilisation assurée par la sous-direction de lutte contre la cybercriminalité de la direction centrale de la police judiciaire. Cette comptabilisation s'inscrit dans une démarche d'évaluation du dispositif mais vise aussi à mieux appréhender l'évolution du comportement des internautes. Lorsqu'un internaute tente de se connecter à un site dont l'accès est bloqué, il est immédiatement renvoyé sur une page d'information du ministère de l'intérieur, lui expliquant la nature du blocage et l'informant sur les voies de recours. L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste. Différents éléments peuvent expliquer cet écart. Dans la liste des sites dont l'accès est bloqué, ceux concernant la pédo-pornographie sont plus nombreux que ceux provoquant à des actes terroristes ou en faisant l'apologie (rapport de 3 pour 1). Par ailleurs, les connexions aux sites pédo-pornographiques ne sont pas toujours volontaires (liens publicitaires sur sites pornographiques légaux, « pourriels », etc.). Au-delà de ces dispositions nationales, le ministère de l'intérieur a engagé plusieurs actions à l'échelle européenne et internationale. En témoignent, notamment, les récentes rencontres du ministre de l'intérieur avec les grands acteurs américains de l'internet pour les amener à davantage participer à la régulation des contenus appelant à la commission d'actes terroristes ou en faisant l'apologie. Ces travaux ont notamment permis de décider la création d'une plate-forme de bonnes pratiques dans la lutte contre la propagande terroriste sur internet.

Réagissez à cet article

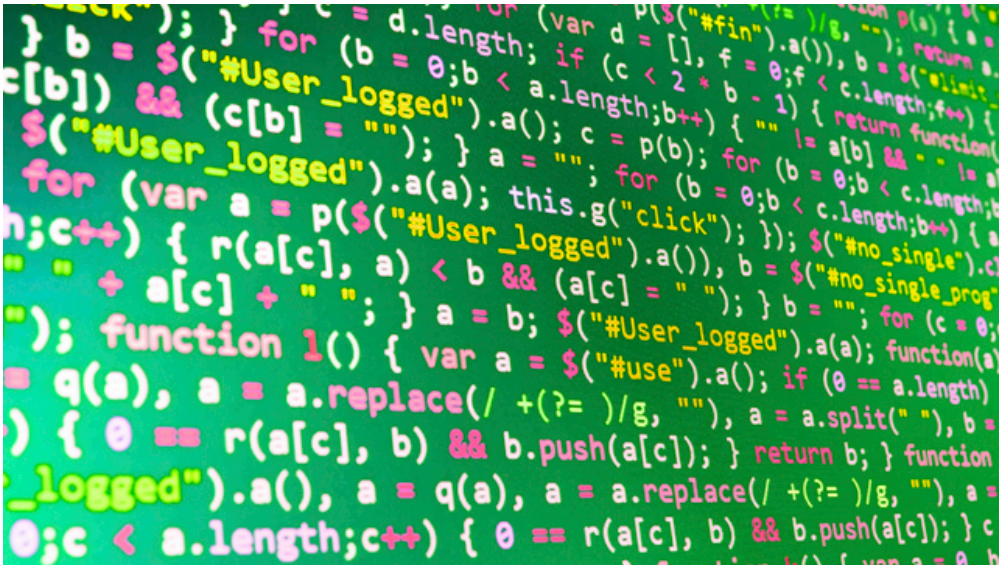
Source : *Question n°74166 – Assemblée nationale*

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

---

Les sites Web censurés sont désormais indiqués par un code « Error : 451 » de l'Internet Engineering Task Force.



L'Internet Engineering Task Force – IETF – vient d'officialiser un nouveau code d'erreur pour indiquer qu'un site est bloqué ou censuré par un organisme gouvernemental. Suite à ce vote, les internautes du monde entier vont désormais savoir quand un gouvernement veut leur interdire d'accéder à un site Internet. Le code en question – Error 451 (en anglais) – devient synonyme de censure sur Internet. Le code HTTP Erreur 404 est bien connu des internautes, tout comme le code Erreur 500 dans une moindre mesure – qui indique un problème de serveur. Ne doutons pas que l'**Erreur 451** va rapidement devenir l'un des codes d'erreur stars de la toile.

L'organisme de standardisation du Web a décidé d'indiquer dans un souci de transparence qu'un site Internet est interdit, bloqué ou censuré dès qu'un utilisateur tente de s'y connecter. L'IETF prévoit notamment que le gouvernement à l'origine de cette censure pourra accompagner le message d'erreur d'une explication sur les causes du blocage d'accès. L'origine du nombre « 451 » est une référence dans la plus pure tradition des geeks, puisque l'erreur 451 renvoie à l'ouvrage de science-fiction de Ray Bradbury « **Fahrenheit 451** » publié en 1953 et dont le thème central est la dénonciation de la censure et de toute forme de propagande. Le message universel de libre accès l'information sur Internet existe encore.

Réagissez à cet article

Source : *Le code Erreur 451 synonyme de censure*

Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

	Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

A ce jour, il existe certains exemples de moyens, usités par les terroristes, permettant de contourner une mesure de blocage d'un site, notamment, l'utilisation d'un « Virtual Private Network » (Réseau Privé Virtuel).

Ce dernier établi un réseau fictif, reliant un ordinateur (celui du client VPN) à un serveur (le serveur VPN), afin de permettre une connexion à Internet de manière anonyme.

De cette façon, les échanges de données sont cryptés et sont protégés par des clés de chiffrement. De plus, ce système permet d'utiliser une adresse IP différente de celle réellement utilisée par un ordinateur, ce qui complique considérablement la localisation de cette machine. De même, le logiciel « Tor » permet de se connecter à Internet par le biais de serveurs répartis dans le monde dans l'anonymat. Il convient de noter que ces procédés cryptologiques sont parfaitement légaux, effectivement, l'article 30 de la loi LCEN du 21 juin 2004 érige en principe que « l'utilisation des moyens de cryptologie est libre ». Dès lors, peut-on envisager l'introduction d'un contrôle par l'autorité administrative, sous forme d'autorisation préalable, lorsque l'utilisation de tels procédés est faite à des fins de provocation au terrorisme ?

Enfin, ces mesures de blocage de sites peuvent sembler illusoires étant donné que celles-ci ne s'appliquent qu'à des FAI et hébergeurs situés sur le territoire français. D'autant que de telles mesures drastiques ne sont pas exemptes de risques de « surblocage ». En 2013, l'Australie a pu en faire les frais en bloquant par accident 250 000 sites sur sa toile.

En conséquence, loin d'être la panacée, cette nouvelle disposition, faussement pragmatique, semble foncièrement superfétatoire.

Sur la conformité de la loi par rapport au bloc de constitutionnalité ?
A titre liminaire, il importe de se poser la question de savoir si la loi du 20 novembre 2015 est susceptible d'être déclarée non conforme à la constitution compte tenu de l'absence de consécration constitutionnelle du statut de l'état d'urgence. A cette fin, il conviendra d'appliquer mutatis mutandis le raisonnement adopté par le Conseil Constitutionnel dans deux décisions : celle du 10 juin 2009 concernant la loi HADOPI et celle relative à la loi sur la pédopornographie du 10 mars 2011.

Dans sa décision du 10 juin 2009, le Conseil en raison du caractère disproportionné du blocage et de sa contrariété avec l'article 11 de la DDHC censure la loi HADOPI soumise à son contrôle « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

En substance, les Sages expliquent que l'octroie par la loi à une autorité administrative du pouvoir de suspendre l'accès à internet est une entorse à la « la libre communication des pensées et des opinions ». L'autorité administrative n'ayant pas le statut de juridiction, elle ne peut se voir octroyer ce pouvoir exorbitant de bloquer un site illicite.

A rebours, dans sa décision du 10 mars 2011, les Sages valident l'article 4 de la loi Loppsi 2 permettant de procéder au blocage administratif de sites pédopornographiques « considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

Dans cette décision, la mesure de blocage est déclarée conforme à l'article 11 de la DDHC de 1789 au motif qu'il existe un recours au fond ou en référé des décisions de blocage et qu'il est consacré un objectif à valeur constitutionnelle de sauvegarde de l'ordre public (ici l'exploitation sexuelle des mineurs).
En ce qui concerne la conformité du nouveau dispositif, il est à noter que ce nouvel article 11 de la loi de 1955 énonce que « le ministre de l'Intérieur peut prendre toute mesure » de blocage de sites faisant l'apologie du terrorisme. La large marge d'appréciation laissée à l'exécutif amène à s'interroger sur le caractère proportionné de cette disposition. Ainsi, un parallèle peut être opéré avec l'article L. 336-2 du CPI prévoyant des mesure de blocage en cas de violation d'un droit d'auteur ou d'un droit voisin. Celui-ci met en évidence l'éventuel caractère excessif du nouveau dispositif. Si ce dernier rend possible « toutes mesures », l'article L. 336-2 du CPI autorise seulement « toutes mesures propres » en vue de bloquer un site.

La référence au principe de proportionnalité, tangible dans cet article du CPI, ne l'est pas en ce qui concerne cette nouvelle mesure. Dans le cadre d'un raisonnement analogue à celui employé dans la décision du 10 juin 2009, on peut appréhender une potentielle censure par les Sages. En effet, la loi du 20 novembre 2015, compte tenu de sa rédaction large et générale, peut habiliter le ministre de l'Intérieur à « restreindre ou à empêcher l'accès à Internet ». De ce fait, un accroc à l'article 11 de la DDHC peut être redouté. D'ailleurs, le rapporteur au Sénat énonçait que « la disposition proposée [la loi lopssi 2] présente une portée beaucoup plus restreinte [que la loi HADOPI] puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite ». Ainsi, le nouveau texte de 2015 risque de connaître le même sort que celui donné à la loi HADOPI, en ce que rien n'interdit au ministre de l'Intérieur de prendre des mesures bloquant l'accès à un site sans pour autant bloquer un site en particulier.
Par ailleurs, une autre incertitude juridique semble planer sur cette loi du 20 novembre 2015 au regard de la décision du 10 mars 2011. S'il est vrai que la suppression du délai de 24 heures ne semble pas impacter la conformité de ce texte, il en va autrement de l'éviction du rôle de contrôle de la CNIL. En effet, l'article 66 de la Constitution dispose que l'autorité judiciaire est « gardienne de la liberté individuelle ». Auparavant, la loi de 2014, chargeait la CNIL d'assurer ce rôle de gardien a posteriori, c'est-à-dire, en actionnant en aval les recours nécessaires devant la juridiction compétente. De même, la CNIL détenait la faculté de contrôler le bien fondé des demandes de retrait de l'autorité administrative. La nouvelle loi éludant cet encadrement exercé par la CNIL, peut laisser sceptique sur sa conformité au texte constitutionnel. D'autant que la loi ancienne (de 2014) n'a jamais fait l'objet d'un contrôle, que ce soit de manière a priori ou a posteriori, devant le Conseil Constitutionnel !

Sur le risque de contrariété de la loi avec la Convention Européenne des Droits de l'Homme ?
Dans un récent arrêt CEDH du 1er décembre 2015, la Cour censure des mesures de blocage de sites pratiquées par le gouvernement turc. En l'espèce, les autorités turques avaient ordonné le blocage de Youtube en raison de dix vidéos accusées de faire outrage à la mémoire d'Atatürk, fondateur de la République laïque turque. Des mesures de blocage ont été ordonnées entre 2008 et 2010.
La Cour reconnait une ingérence de l'autorité publique dans l'exercice des droits garantis par l'article 10 de la convention portant sur la liberté d'expression. De la même façon, la loi de novembre 2015 n'excluant pas la possible coupure d'un site Internet, elle encourt le risque d'être déclarée disproportionnée au regard de l'intérêt légitime poursuivi, à savoir, la lutte contre l'apologie du terrorisme.
Toutefois, l'article 15 de la CEDH autorise dérogation aux obligations de cette convention dans une situation d'état d'urgence, excepté pour les principes non dérogeables, dont ne fait pas partie l'article 10 de la CEDH. Mais un prolongement durable de l'état d'urgence posera nécessairement une difficulté relative à sa compatibilité avec l'article 15 de la CEDH. A moins, (ce que le gouvernement envisage) d'établir un socle juridique solide de l'état d'urgence, au sein de la constitution. En conséquence, de lege lata, la conformité de ce nouveau dispositif semble loin d'être évidente au regard d'un certain nombre de droits fondamentaux garantis.
Somme toute, est-ce qu'« à force de sacrifier l'essentiel pour l'urgence, on finit par oublier l'urgence de l'essentiel » ? (Edgar Morin)

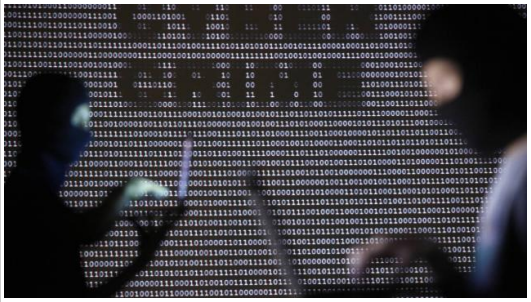
Réagissez à cet article

Source : *Utilité et conformité des mesures de blocage de sites Internet faisant l'apologie du terrorisme dans le cadre de l'état d'urgence. Par Dan Scemama.*

Crainte d'attentats pilotés à partir d'Internet en 2016

Crainte d'attentats pilotés à partir d'Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

La Turquie victime d’une grosse cyberattaque

La Turquie victime d’une grosse cyberattaque

Les serveurs internet turcs subissent depuis lundi une vaste cyberattaque qui a notamment considérablement ralenti les services bancaires, a-t-on annoncé vendredi de source proche du gouvernement turc.

L'organisation non-gouvernementale Nic.tr, chargée d'administrer les adresses des sites internet utilisant le nom de domaine «.tr» qui englobe les ministères, l'armée, les banques et de très nombreux sites commerciaux, a indiqué dans un communiqué sur son site internet que l'offensive émane de «sources organisées» en-dehors de Turquie.
Le ministre des Transports et des Communications Binali Yildirim, cité par les journaux, a évoqué une situation «préoccupante» et demandé que soient renforcées les mesures de sécurité, qui, selon lui, se sont avérées «insuffisantes».

Attaque russe?
Certains médias turcs pensent que cette attaque pourrait provenir de Russie, Moscou et Ankara traversant une grave crise diplomatique depuis qu'un bombardier russe a été abattu par la chasse turque à la frontière syrienne, le 24 novembre.
Selon la presse turque, le groupe de piratage informatique des Anonymous a de son côté déclenché une guerre numérique contre la Turquie et annoncé qu'il continuerait à perpétrer des attaques contre les systèmes informatiques en raison du «soutien de la Turquie au groupe de l'Etat islamique (EI)».

Dans un communiqué, le groupe de pirates informatiques a écrit : «La Turquie soutient Daech en lui achetant du pétrole et en soignant ses combattants (…) Si vous ne cessez pas votre soutien à Daech, nous continuerons à procéder à des cyber-attaques contre la Turquie».

Les experts ont cependant indiqué que pour le moment on ignorait l'origine de cette puissante attaque.

Réagissez à cet article

Source : *20 Minutes Online – La Turquie victime d une cyberattaque massive – Stories*

La SNCF va épier ses voyageurs

La SNCF va épier ses voyageurs

Plutôt que de surveiller ses millions de passagers de la même façon, la SNCF va tenter de les filtrer au moyen d'un logiciel qui prétend isoler les comportements présentant un risque.

Face à la menace terroriste, la SNCF teste la réponse technologique. Dans quelques gares, la compagnie ferroviaire s'est déjà équipée d'un logiciel d'analyse du comportement des voyageurs au travers des caméras de vidéosurveillance existantes. À défaut de filtrer tous les passagers avec des portiques de sécurité tels que proposés par la ministre de l'Écologie, la société publique va essayer de détecter les attitudes suspectes.

Stéphane Volant, le secrétaire général de l'entreprise publique, a expliqué dans les grandes lignes à l'AFP le fonctionnement de ce logiciel, dont l'analyse se base sur « le changement de température corporelle, le haussement de la voix ou le caractère saccadé de gestes qui peuvent montrer une certaine anxiété ». Une vidéosurveillance qui se veut donc intelligente, mais qui risque de générer énormément de faux positifs.

Vers un nouveau cap dans la surveillance

Avec cette expérimentation – qui s'étendra aux colis abandonnés -, la SNCF veut aussi mesurer le niveau d'acceptabilité des voyageurs pour ce genre de technologie. Mais au quotidien, personne ne verrait jamais ces logiciels, puisque les caméras elles-mêmes ne différeront pas. Le seul changement perceptible pour le public sera peut-être le nombre d'interpellations préventives de gens à l'attitude jugée suspecte…

Vidéosurveillance gare

Alors que ces tests auraient vocation à durer et que ce logiciel – dont le nom n'a pas été révélé – pourrait être étendu aux 40 000 caméras de la SNCF, se pose la question de la protection de la vie privée. Sur ce point, la compagnie ferroviaire a déjà répondu que ces expérimentations sont menées sous le contrôle de la Cnil.

Dans sa boîte à outils sécuritaire, la société lancera au printemps prochain une application mobile pour les voyageurs afin qu'ils signalent un danger. La SNCF imagine aussi équiper ses agents de caméras. Quant aux portiques, ils seront adoptés pour l'accès aux trains Thalys, en réponse à l'attentat déjoué au mois d'août. Gageons que les trains qui arrivent en retard ne génèrent pas trop de hausse de température corporelle.

Réagissez à cet article

Source : *Surveillance : la SNCF va épier ses voyageurs*

Les opérateurs satellitaires européens nient leur rôle dans la fourniture d'Internet à Daesh

Outil central dans la machine de propagande de Daesh, Internet permet de recruter au-delà des frontières. Pour se connecter, les terroristes utiliseraient les capacités de satellites européens.

Dans une enquête publiée le week-end dernier, le journal allemand Spiegel Online pointe du doigt plusieurs acteurs de l'Internet satellitaire européens (SES, Avanti et le français Eutelsat) pour leur rôle supposé dans la fourniture d'une connexion au Web à Daesh. Alors que les géants du Net Google, Facebook ou Twitter sont appelés à contenir la propagande de l'organisation terroriste, se pose ici la question de son accès au réseau.

Et cette question est centrale dans la lutte contre le terrorisme, car Internet est l'un des vecteurs principaux utilisés par Daesh pour embrigader ses futures recrues. L'organisation diffuse sur les réseaux sociaux grand public ses messages de propagande, qu'elle adapte dans les langues locales, afin de toucher le plus de gens.

Des paraboles turques

Selon le Spiegel, l'organisation terroriste contourne le mauvais état des infrastructures Internet des zones qu'elle contrôle – en Syrie et en Irak – en se connectant par satellite, au moyen de paraboles achetées dans des pays frontaliers, dont la Turquie. En tant que prestataires techniques situés en amont de la chaîne, les opérateurs satellitaires se sont défendus de connaître les clients finaux, voire d'avoir pris des précautions.

C'est le cas d'Eutelsat, seul à avoir réagi publiquement

Le français, contrôlé à 26 % par l'État via la Caisse des dépôts, apporte dans un communiqué deux « clarifications ». Premièrement, il « n'a pas de contact avec des utilisateurs finaux », deuxièmement, « son réseau de distribution n'inclut aucun fournisseur de services en Syrie ». Eutelsat souligne qu'en 2013, il a interdit aux distributeurs de fournir des services Internet en Syrie.

Coordonnées GPS

Pourtant, lorsque les équipements fournis par les FAI se connectent aux satellites, ces derniers reçoivent des coordonnées GPS. Des informations censées permettre, en théorie, de pouvoir remonter la piste. Ainsi selon le Spiegel, de telles connexions sont bel et bien réalisées depuis le territoire de Daesh, dont Raqqa, la capitale autoproclamée, ou encore la ville de Mossoul, en Irak. Mais du côté des opérateurs satellitaires, aucun signal.

L'opérateur luxembourgeois SES a déclaré ne « pas (avoir) connaissance que ses satellites sont utilisés par l'EI ou dans des zones syriennes contrôlées par l'EI » et que si tel était le cas, il mettrait « tout en œuvre pour y mettre fin ». Eutelsat, lui, dit « n'avoir aucune connaissance d'utilisation de ses ressources par Daesh ». Si l'Internet satellitaire était coupé, il enrayerait la propagande, mais aussi les efforts de résistance des civils.

Réagissez à cet article

Source : http://pro.clubic.com/actualite-e-business/actualite-789264-eutelsat-daesh.html

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html

Edward Snowden a-t-il indirectement contribué aux attentats de Paris ?

Edward Snowden a-t-il indirectement aux attentats de Paris vendredi 13 novembre ?

Des responsables politiques et des membres des services de renseignement internationaux accusent les systèmes de communication chiffrés des géants du web de profiter aux terroristes.

Crédit : DENIS CHARLET / AFP Un gendarme de la Brigade Départementale de Renseignements et d'Investigations Judiciaires (illustration)

Edward Snowden a-t-il indirectement contribué aux fusillades meurtrières qui ont balayé l'est de Paris vendredi 13 novembre ?

Certains acteurs de premier plan du renseignement américain ne sont pas loin de l'affirmer. Sans prononcer le nom de l'ancien analyste de la NSA (l'agence nationale de sécurité américaine), le directeur de la CIA John Brennan a clairement laissé entendre la semaine dernière lors d'une allocution à Washington que ses révélations sur les interceptions massives de communications téléphoniques par la NSA en 2013 avaient participé à faire émerger des failles dans la surveillances des réseaux d'extrémistes.

L'ancien directeur de la CIA James Woolsey ne s'embarrasse pas de ces précautions. Selon lui, Snowden a tout simplement « du sang sur les mains ».

À l'époque, ces révélations avaient poussé le Congrès américain à voter la fin du stockage des métadonnées des appels téléphoniques des citoyens américains par la NSA. Elles avaient surtout encouragé les géants du web à adopter des technologies de chiffrement violemment critiquées par la communauté du renseignement.

Depuis le scandale des pratiques d'écoutes de masse par les États-Unis, la protection des données personnelles est devenu un argument commercial pour les sociétés technologiques auprès d'utilisateurs de plus en plus méfiants des services proposés par les entreprises de la Silicon Valley.

Après le rachat de Whatsapp par Facebook, près de 5 millions d'utilisateurs se sont par exemple rabattus sur le service de messagerie sécurisé Telegram, également plébiscité par les terroristes de Daesh.

Apple a développé des systèmes de sécurité de plus en plus draconiens érigeant ses téléphones en véritables forteresses.

Depuis la fin 2014, les emails, SMS et photos de l'iPhone sont chiffrés et personne, pas même Apple, ne peut y avoir accès.

Selon un expert en cybersécurité cité par Les Échos, « la seule manière d'essayer de les récupérer est de décaper le composant avec de l'acide pour ensuite le passer au microscope ». Une opération qui peut coûter plusieurs millions d'euros.

Dans le même temps, Google, Facebook, WhatsApp, Skype ou Twitter n'ont pas ménagé leurs efforts pour sécuriser les données de leurs abonnés. Si bien qu'il est impossible pour les autorités de lire et d'écouter les conversations sur ces services en dehors de réquisitions judiciaires ou d'un accord avec ces entreprises.

Une loi à l'étude au Royaume-Uni

Les autorités et la communauté du renseignement montent régulièrement au créneau pour réclamer un changement de politique des entreprises technologiques.

Le procureur de Manhattan, Cyrus Vance, a répété à plusieurs reprises qu'il a dû abandonner cette année une centaine d'affaires impliquant des meurtriers, faute d'avoir pu accéder aux données de leurs téléphones.

Le directeur du FBI dénonçait en juillet le chiffrement pratiqué par Whatsapp et les entreprises privées, qui permet, selon lui, à des criminels de se mettre à l'abri de la loi.

Au premier rang de leurs revendications figure la création de clés de chiffrement ou de portes dérobées qui leur donneraient accès aux données des utilisateurs quand la situation l'exigerait.

Le débat est également d'actualité de l'autre côté de l'Atlantique. Après les attentats de janvier à Paris, le premier ministre britannique, David Cameron, s'était publiquement interrogé sur les risques de l'existence de données cryptées auxquelles la police ne peut pas accéder. Il souhaite désormais faire figurer dans l'Investigatory Powers Bill, sorte d'équivalent de la loi renseignement française, l'interdiction des méthodes de chiffrement qui n'incluraient pas de porte dérobée permettant aux autorités munies d'un mandat de justice d'accéder aux informations chiffrées. Une nouvelle législation que le locataire du 10, Downing Street justifie par la nécessité de « ne pas créer une situation dans laquelle les terroristes, les criminels et les ravisseurs d'enfants auraient un espace libre pour communiquer ».

Les géants du web rappellent leur attachement au chiffrement

Les géants du net sont fermement opposés à ce type de mesure. Selon eux, leur mise en place reviendrait à introduire une faille dans leurs programmes. Apple, Microsoft, Google, Samsung, Twitter, Facebook et une cinquantaine d'entreprises technologiques regroupées au sein de l'Information Technology Council ont rappelé dans une lettre ouverte que le chiffrement est un outil de sécurité indispensable pour leurs utilisateurs. « Affaiblir le chiffrement quand on a pour but de l'améliorer n'a aucun sens, estiment-ils. Le chiffrement est un outil de sécurité utilisé tous les jours pour empêcher des criminels de vider nos comptes en banque, pour protéger nos voitures et avions des piratages et pour préserver notre sécurité. (…) Affaiblir le chiffrement ou créer des portes dérobées (…) créerait des vulnérabilités qui pourraient être exploitées par les méchants, ce qui causerait certainement des problèmes physiques et financiers sérieux dans notre société et notre économie ».

La France n'a pas encore pris de position claire sur la question. Mi-août, le procureur de la République de Paris, François Molins, a cosigné une tribune du New York Times avec plusieurs responsables internationaux de la lutte antiterroriste pour appeler les géants du web à changer leur politique de chiffrement pour ne pas affaiblir les capacités d'investigation de la justice contre le terrorisme. Adoptée en juin, la loi Renseignement portée par le gouvernement après les attentats de janvier n'évoque pas précisément la cryptologie. Selon Médiapart, le gouvernement avait l'intention de légiférer mais y a finalement renoncé. C'était avant les attentats de Paris. François Hollande a depuis affirmé devant le Parlement réuni à Versailles qu'il souhaitait adapter l'état d'urgence aux évolutions technologiques, sans donner plus de détails.

Les terroristes n'ont pas attendu Snowden

En attendant, il n'a pas été établi à ce stade de l'enquête que les commandos des attentats de Paris ont utilisé un système de communication crypté pour organiser leurs attaques. Le site d'investigation britannique The Intercept a rappelé récemment que les terroristes et les criminels n'ont pas attendu les révélations de Snowden pour se méfier des voies de communication traditionnelles. Les attentats de New York (2001), Bali (2002), Madrid (2004), Londres (2005), Mumbai (2008) et Boston (2013) peuvent malheureusement en témoigner. Le commanditaire des attentats du 11 septembre, Oussama Ben Laden, s'appuyait par exemple uniquement sur un système de messagers humains par crainte d'être pisté par les services de renseignement, notait le Washington Post. Un système qui lui a permis de naviguer en dehors des radars antiterroristes pendant près d'une décennie.

Réagissez à cet article

Source : http://www.rtl.fr/culture/web-high-tech/apple-google-et-les-geants-du-web-entravent-ils-la-lutte-contre-le-terrorisme-7780616618

PAR BENJAMIN HUE