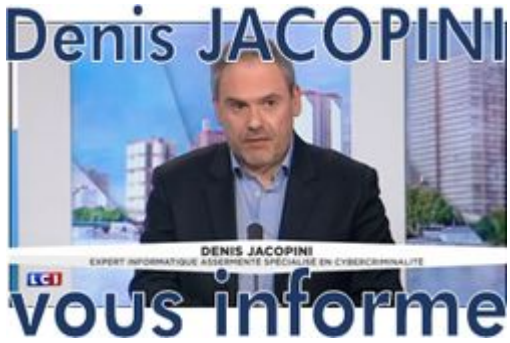
Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse



Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

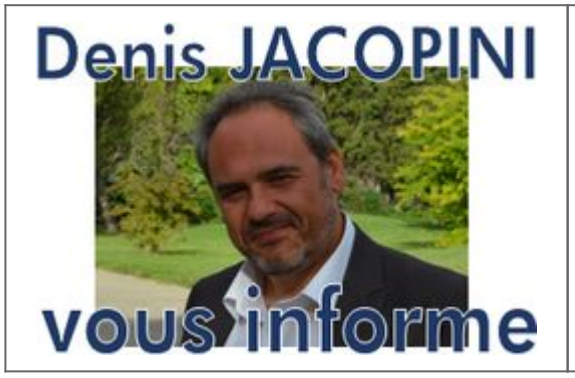
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

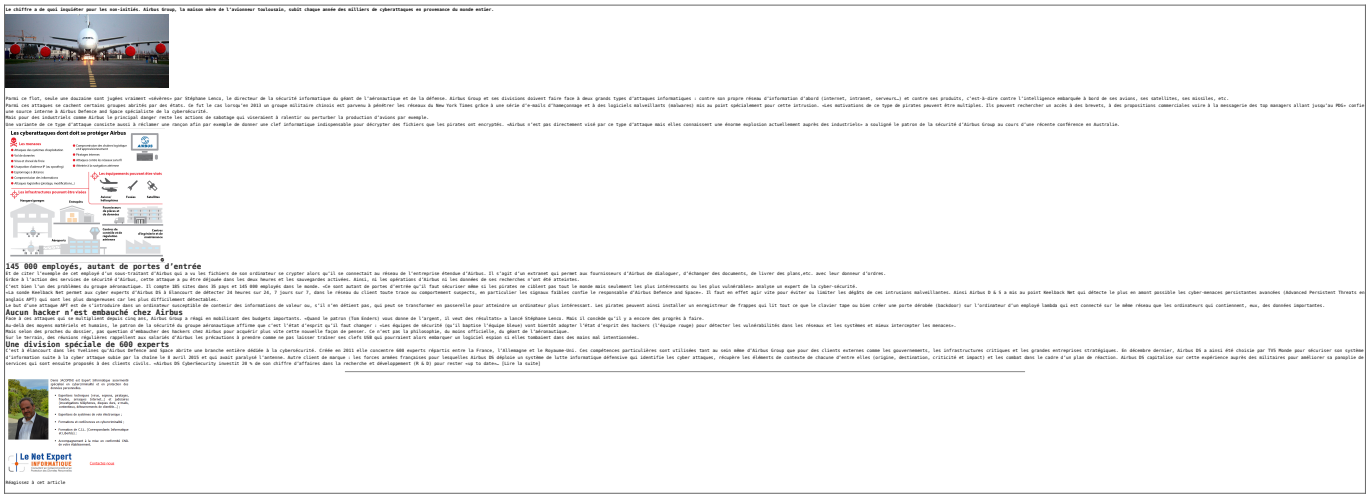
Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Airbus déjoue douze attaques informatiques majeures par an



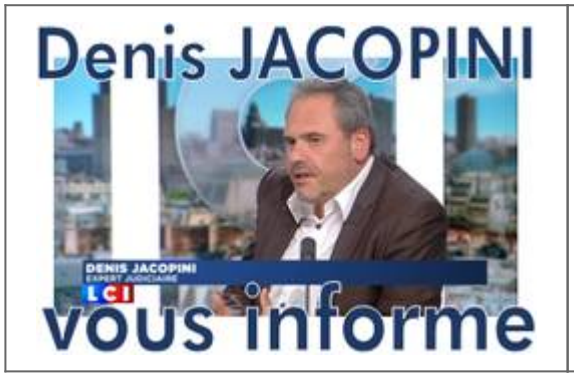
Airbus déjoue douze attaques informatiques majeures par an



Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an – 06/05/2016 – ladepeche.fr*

article de Gil Bousquet

Comment s’introduire dans le web invisible ?



Comment s’introduire dans le web invisible ?

La façon la plus répandue et la plus simple de s'introduire dans cette partie immergée du web est le serveur Tor, acronyme pour The Onion Router. Pourquoi oignon ? Parce que le logiciel assure plusieurs couches de protection, qui permettent entre autres de conserver l'anonymat de l'internaute.

Tous les sites qui ont cours sur ce moteur de recherche se terminent par .onion. L'étudiant en informatique qui a accepté de faire une démonstration à L'Express affirme qu'à toutes les fois qu'une personne brassant des affaires sur le «*deep web*» fait une requête, elle ne passe jamais par le même chemin afin de brouiller les pistes.
«Tout le monde se connecte sur un même serveur et une fois que tu es connecté sur ce serveur, tu passes par un réseau de connections international, explique-t-il. Tu as un serveur d'entrée et un serveur de sortie. Ce qui se passe entre, on ne le sait pas. Ton adresse IP se perd. »

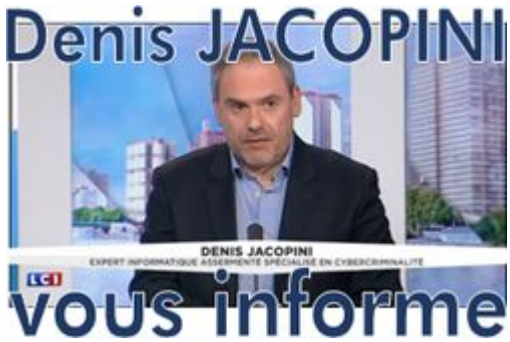
Un enseignant en informatique au Cégep de Drummondville, Louis Marchand, abonde également en ce sens : «Si la personne est excessivement prudente dans ses démarches, la seule chose qui pourrait être retracée serait sa connexion au réseau Tor. Toutes les actions, légales ou pas, que cette personne a pu effectuer à l'intérieur du serveur sont pratiquement introuvables.» Pratique lorsqu'on veut publier des anecdotes sur un blogue en évitant la censure… ou pour publier une offre d'achat de cocaïne.
Ce moteur de recherche, développé par la marine américaine, se télécharge aussi facilement que Google Chrome et est associé avec le moteur Firefox. Comme quoi Tor n'est pas illégal du tout : «c'est l'utilisation qu'on en fait qui peut être négative», complète l'étudiant.

Les bitcoins, la monnaie virtuelle anonyme
La monnaie ayant cours sur le web invisible est le *bitcoin*, une forme d'argent virtuelle cryptée. Elle n'est soumise à aucun taux de change ni à aucune banque, donc aucun intermédiaire n'existe entre l'acheteur et la marchandise. Cependant, son atout majeur pour les consommateurs de produits illicites est qu'elle peut être utilisée de façon anonyme.
Louis Marchand décrit le bitcoin comme n'étant rien d'autre qu'un fichier. «Il faut faire attention à ça : toutes les transactions sont enregistrées, même si le bitcoin en tant que tel n'est pas identifié. C'est beaucoup plus difficile de retracer de l'argent liquide, puisque absolument rien ne lie un 20 $ à son propriétaire», spécifie-t-il.

Selon l'enseignant, le bitcoin fonctionne exactement comme l'or ou le diamant. «Ce qui diffère, c'est que quelque chose de virtuel change beaucoup plus rapidement que n'importe quelle ressource physique. Demain, un bitcoin peut valoir 2 $ et le lendemain, plus de 2000 $. C'est un coup de dé.»
Cette monnaie est cependant extrêmement difficile à générer et est très coûteuse en électricité, d'après Louis Marchand : elle nécessite beaucoup de ressources et de temps, puisqu'elle doit correspondre à des critères mathématiques très précis. C'est notamment ce qui expliquerait la valeur toujours montante des bitcoins. Au moment de la vérification de L'Express, un de ces fichiers valait 550 $.
Selon les dires de l'étudiant en informatique qui a préféré conserver l'anonymat, lorsqu'il s'est lui-même procuré huit bitcoins il y a quelques années, ça ne lui avait pas coûté plus d'une centaine de dollars. «Si je me souviens bien, ça a déjà monté à 1400 $. C'est hallucinant», s'étonne-t-il.
Il faut dire que le marché du web invisible, dans lequel évoluent les bitcoins, est aussi extrêmement lucratif. La Sureté du Québec, les deux compères ayant testé les drogues du «*deep web*» et l'informaticien s'accordent tous sur un point : la rémunération est la motivation principale de n'importe quel trafiquant de marchandises illégales sur Internet, selon eux.
«Moins c'est légal, plus c'est payant. Personne n'ira vendre un foie sur Internet, à part pour l'argent que ça rapporte. Il faut oublier le côté humain et ne penser qu'au montant final», croit Louis Marchand… [Lire la suite]

Source : *Le logiciel Tor, la porte d'entrée du web invisible – Actualités – L'Express – Drummondville*

Darknet: qu’est ce qu’on y trouve et comment y accéder ?



Darknet:, qu’est ce qu’on y trouve et comment y accéder ?

Au fil de nos CyberBalades, notre souris s’est arrêtée sur un article très intéressant sur le DarkNet. Pour votre plus grand plaisir, veuillez trouver ci-dessous un extrait et le lien permettant de le consulter en entier.

Qu’est-ce qu’on trouve dans le Darknet ?

Ce qui frappe en premier c’est la **quantité de contenus illégaux**. On compte environ un tiers de porno (dont une bonne partie de pédopornographie et d’autres trucs louches), un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables… [Lire la suite]

Liste des URL intéressantes pour explorer le darknet

• **Moteur de recherche** : http://hss3uro2hsxfogfq.onion
• **Hidden wiki**: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
• **Annuaire des liens** : http://torlinkbgs6aabns.onion
• **Facebook pour Tor**: https://facebookcorewwwi.onion
• **Moteur de recherche Darknet**: http://grams7enufi7jmdl.onion
• **Vente des mobiles débloqués:** http://mobil7rab6nuf7vx.onion
• **Location des services d’un hacker**: http://2ogmrlfzdthnwkez.onion
• **Moteur de recherche DuckDuckGo**: http://3g2upl4pq6kufc4m.onion
[Lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Darknet: qu'est ce qu'on y trouve et comment y accéder ?*

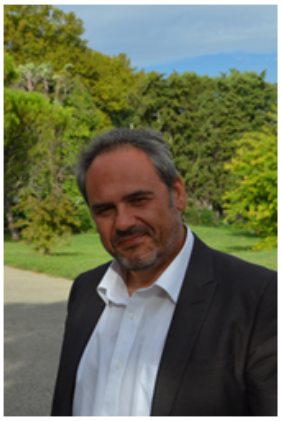
Auteur : Ahmed EL JAOUARI

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Les passagers d'un vol interne australien ont eu une petite frayeur à cause d'un réseau WiFi.

Le réseau WiFi en question a été repéré par un des passagers qui, inquiet de ce nom étrange, en a tout de suite informé le personnel de bord. Ce dernier a alors remonté l'information jusqu'au commandant de bord, qui a décidé de garder l'avion au sol tant que l'appareil émetteur de ce réseau n'a pas été repéré. Une annonce retentit dans les hauts parleurs de l'avion afin de prévenir les passagers, mais après une demi-heure de recherche, la source n'est toujours pas localisée.
« Un réseau WiFi peut avoir une bonne portée, donc cela aurait pu venir d'une personne dans le terminal », explique un des passagers. Des recherches sont menées dans et autour de l'avion, sans résultat. Finalement, après trois heures d'attente sur le tarmac, l'avion se met finalement en route pour sa destination, Perth, en Australie, où il atterrit sans encombre 80 minutes plus tard... [Lire la suite]



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

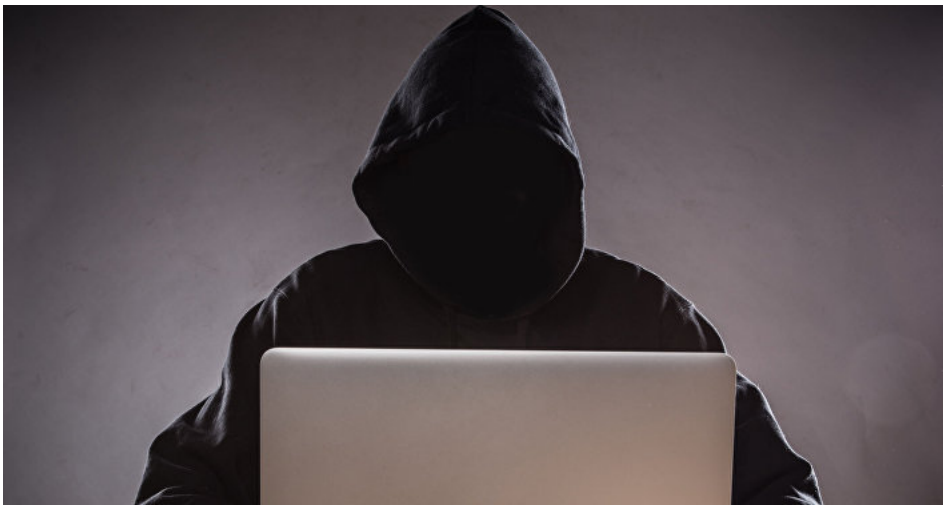
Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Une alerte à la bombe dans un avion causée par un réseau Wi-Fi*

Des hackers proches de Daech menacent les New-Yorkais

	Des hackers proches de Daech menacent les New-Yorkais

Un groupe de hackers liés à Daech a dévoilé sur Internet une liste contenant les données personnelles de milliers de new-yorkais et a exhorté les adeptes du groupe à les cibler.

Les hackers ont mis en ligne non seulement les noms des New-Yorkais, mais aussi les lieux de résidence et leurs adresses électroniques, rapporte le Reuters, qui précise qu'une grande partie des données sont désuètes. En outre, la liste inclut les données personnelles d'un grand nombre de fonctionnaires du département d'Etat américain ainsi que de citoyens sans relations avec les services publics.
Des agents fédéraux et des policiers de New York ont contacté les personnes figurant sur la liste pour les informer, mais les forces de l'ordre ne considèrent pas cette menace comme crédible, indique la source.
« Bien que notre pratique courante consiste à refuser de commenter les questions opérationnelles et les enquêtes spécifiques, le FBI avertit régulièrement les individus et les organisations sur l'information recueillie au cours d'une enquête qui peut être perçue comme une menace potentielle », stipule la déclaration du FBI.
Précédemment, le groupe de pirates informatiques de Daech connu comme « Cyber-califat uni » a annoncé qu'il avait obtenu les informations personnelles de 50 employés du département d'Etat américain, y compris leurs noms et numéros de téléphones. Pour le prouver, les pirates ont publié des captures d'écran et ont menacé d' »écraser » les Etats-Unis, de tuer ces employés et de détruire le système de sécurité nationale. De son côté, le département d'Etat américain n'a fourni aucun commentaire.

Croyant attaquer Google, les hackers de Daech manquent leur cible
Auparavant, les Etats-Unis avaient ouvert une nouvelle ligne de combat contre l'Etat islamique, comprenant des attaques contre des réseaux informatiques de Daech. Des cyberattaques seront réalisées contre l'Etat islamique parallèlement à l'usage des armes traditionnelles.
Depuis 2013, les autorités américaines ont arrêté plus de 70 personnes pour collaboration avec l'Etat islamique… [Lire la suite]

Réagissez à cet article

Source : *Des hackers proches de Daech menacent les New-Yorkais*

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L’iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

Daech prend le contrôle d’une centrale nucléaire – Futuriste ?

	**Daech prend le contrôle d’une centrale nucléaire. Futuriste ?**

Le coordinateur de l'UE pour la lutte contre le terrorisme estime que les djihadistes seront bientôt capables de cyberattaques contre des sites sensibles.

La prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité « avant cinq ans », a admis samedi le coordinateur de l'Union européenne pour la lutte contre le terrorisme alors que la sécurité des sites nucléaires belges est pointée du doigt.
« Je ne serais pas étonné qu'avant cinq ans il y ait des tentatives d'utiliser l'Internet pour commettre des attentats », notamment en prenant le contrôle du « centre de gestion d'une centrale nucléaire, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer », estime Gilles de Kerchove dans une interview au quotidien La Libre Belgique.
« À un moment donné, il y aura bien un gars » au sein de l'organisation djihadiste État islamique « avec un doctorat en technologie de l'information qui sera capable d'entrer dans un système », a-t-il estimé.

La miniaturisation des explosifs mais également la connaissance accrue des combattants de l'État islamique dans les biotechnologies constituent de réelles menaces pour l'avenir, selon lui. « Que se passera-t-il quand on en sera à comment élaborer un virus dans la cuisine de sa mère ? » s'est-il demandé.
En revanche, M. de Kerchove a estimé que le département belge de la Défense était « assez bon » en matière de cybersécurité. « Ils n'ont, bien sûr, pas les capacités de représailles des Français, des Anglais ou des Américains, mais en cas d'attaque, je pense que notre département de la Défense est assez bon », a-t-il dit, précisant cependant qu'il ne savait pas « si le gouvernement » belge était « capable d'anticiper et de résoudre de grosses attaques ».

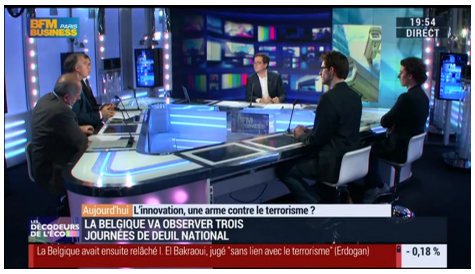
Sécurité renforcée
Des médias belges et internationaux ont rapporté vendredi que la cellule terroriste bruxelloise responsable des attentats de mardi avait prévu une attaque à l'arme de guerre dans les rues de Bruxelles, type 13 novembre à Paris, et la fabrication d'une « bombe sale » radioactive après une surveillance vidéo par deux des kamikazes, les frères El Bakraoui, d'un « expert nucléaire » belge.
À la suite des attaques survenues mardi à Bruxelles qui ont fait 31 morts, la sécurité avait été renforcée autour des deux centrales nucléaires de Belgique.
C'est dans ce contexte de suspicion sur la sécurité des sites nucléaires qu'un agent de sécurité dans le nucléaire a été abattu et son badge volé jeudi soir dans la région de Charleroi, dans le sud de la Belgique, selon le journal La Dernière Heure. Samedi, la piste terroriste a été écartée, par la justice belge. La piste terroriste est formellement démentie, rapporte l'agence de presse Belga, citant le parquet de Charleroi, dans le sud du pays. Le juge d'instruction spécialisé dans les matières terroristes n'a pas été saisi. Les raisons de la mort de la victime, abattue, tout comme son chien, de plusieurs balles à son domicile, ne sont pas encore connues mais les enquêteurs pensent à un cambriolage qui aurait mal tourné ou à un crime pour des raisons privées.
Le parquet de Charleroi a démenti le vol de son badge d'accès de centrale nucléaire… [Lire la suite]

-

Réagissez à cet article

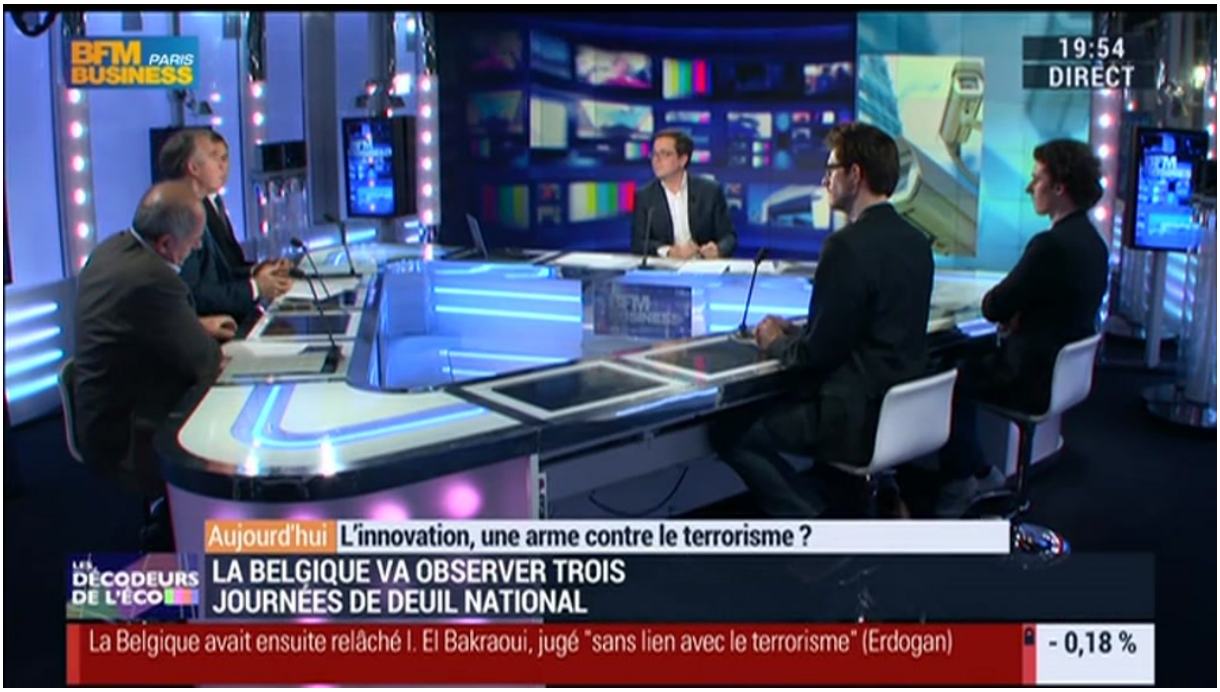
Source : *Quand Daech prendra le contrôle d'une centrale nucléaire – Le Point*

L’innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016



L’innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016

Deuil national en Belgique au lendemain des attaques qui ont fait 31 morts et 270 blessés tandis que l'enquête s'accélère.
Deux frères kamikazes, auteurs des tueries à l'aéroport et dans le métro, ont été identifiés grâce à leurs empreintes digitales. Alors, comment prévenir un nouvel attentat comme celui de Bruxelles ?



La lutte contre le terrorisme passe par le renseignement et la surveillance sur le terrain. Mais les effectifs semblent insuffisants et épuisés. Reconnaissance faciale, logiciels d'analyse comportementale… l'une des armes efficaces contre le terrorisme ne serait-il pas l'innovation ? — Avec: Gérôme Billois, membre et administrateur du CLUSIF. Frédéric Simottel, éditorialiste high-tech BFM Business. Matthieu Marquenet, COO de Smart Me Up. Jean-Baptiste Huet, BFM Business. Et Jean-Louis Missika, adjoint à la mairie de Paris en charge de l'innovation. — Les Décodeurs de l'éco, du mercredi 23 mars 2016, présenté par Fabrice Lundy, sur BFM Business.

Réagissez à cet article

Source : *L'innovation, une arme contre le terrorisme ? — 23/03*

Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

Les hackeurs Anonymous déclarent la « guerre totale » à Daesh

Les Anonymous ont publié une nouvelle vidéo dans laquelle ils entendent renforcer leurs offensives contre l'Etat islamique suite aux attentats ayant touché Bruxelles cette semaine.

Daesh a revendiqué les deux attentats survenus en Belgique dans la ville de Bruxelles. Face à cette menace terroriste, le groupe de hackeurs Anonymous a diffusé une nouvelle vidéo sur YouTube dans laquelle ils affirment vouloir renforcer leurs offensives contre les sites et infrastructures de l'Etat islamique.

Anonymous rappelle les actions précédemment menées après les attaques survenues à Paris en novembre dernier. Le groupe a ainsi fait fermer des milliers de comptes Twitter liés à des sympathisants de l'El. Ils ont hacké plusieurs sites de propagande et récupéré l'argent obtenu des Bitcoin.

« *Cependant, tant qu'il y aura des attaques à travers le monde, nous ne nous arrêterons pas (…) nous défendrons le droit à la liberté (…)*

Sympathisants de Daesh, nous vous traquerons, nous vous trouverons, nous sommes partout et nous sommes bien plus nombreux que ce que vous pouvez imaginer », affirme Anonymous dans cette nouvelle vidéo. Chacun est invité à rejoindre les efforts de ce groupe de hackeurs.

En novembre, 22 000 comptes Twitter liés à Daesh avaient été listés par Anonymous et un site de l'Etat islamique avait subi les foudres des hackeurs.

Un peu plus tôt ce mois-ci, Anonymous avait déclaré une guerre totale au candidat à la présidence des Etats-UnisDonald Trump pour ses diverses déclarations choc au sujet des femmes, des étrangers ou des handicapés…. [Lire la suite]

Réagissez à cet article

Source : *Terrorisme : les Anonymous déclarent la « guerre totale » à Daesh*