Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

	Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Une initiative franco-allemande va tenter de convaincre les acteurs internationaux d'Internet et de l'informatique de la nécessité d'ouvrir leurs codes et leurs chiffrements pour lutter contre le terrorisme. Des voix s'élèvent au nom de la sécurité et des libertés.

Après le conseil restreint de Défense à l'Élysée le 4 août 2016, le ministre de l'Intérieur, Bernard Cazeneuve, a parlé chiffre. Avec son homologue allemand, Thomas de Maizière, il a proposé le 23 août une initiative européenne à vocation internationale pour « faire face au défi du chiffrement, une question centrale dans la lutte antiterroriste ». Le sujet est brûlant. Pas seulement depuis l'assassinat du père Hamel par des usagers de Telegram , d'ailleurs pas considéré comme la solution la plus hermétique d'un marché en plein essor.
Outre Telegram, les terroristes, des criminels et des gens très soucieux de l'intégrité de leurs communications utilisent pléthore de dispositifs de chiffrement comme ChatSecure, Conversations, Kontalk, Signal, Threema ou WhatsApp (même s'il appartient à Facebook depuis 2014), sans parler des anonymes Tor (réseau décentralisé) ou ToX (pair à pair). Là n'est d'ailleurs pas la question centrale. L'ennemi pourrait émigrer vers d'autres cieux numériques voire créer son propre outil chiffré…

Incapable de casser le code

Depuis l'audition à l'Assemblée le 10 mai de Patrick Calvar, le directeur général de la sécurité intérieure, la pression monte. Pour les attentats de Bruxelles, le DGSI avoue que « même une interception n'aurait pas permis de mettre au jour les projets envisagés puisque les communications étaient chiffrées sans que personne soit capable de casser le chiffrement ». Face au chiffrement aléatoire et autres complications futures, le DGSI a une réponse martiale : « Je crois que la seule façon de résoudre ce problème est de contraindre les opérateurs. » Nous y voilà. En février, le FBI s'est heurté au refus d'Apple de livrer les données de l'iPhone d'un des meurtriers de Daech qui a tué 14 personnes à San Bernardino le 2 décembre 2015. Avant que le FBI n'annonce avoir réussi à casser le chiffre de la pomme…
Bernard Cazeneuve ne dit pas autre chose. Il prend pour exemple sa négociation avec les majors d'Internet en février 2015 qui a permis d'élaborer une charte sur le retrait des contenus et le blocage des sites haineux. « Sur le chiffrement, il faut que nous ayons la même méthode, la même volonté, le sujet est crucial. »
Sauf qu'un courrier, publié par Libération, du directeur de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et lui-même cryptologue, Guillaume Poupard, affirme le contraire aux autorités : « Un affaiblissement généralisé serait attentatoire à la sécurité numérique et aux libertés de l'immense majorité des utilisateurs. » Permettre une intrusion des services de renseignement (par des « portes dérobées ») pourrait profiter à des gens ou des États (pas seulement islamiques) mal intentionnés. Quelle tendance va l'emporter ? En cette époque sécuritaire, de l'état d'urgence éternel et du désarroi politique…
Article original de Olivier Berger

Réagissez à cet article

Original de l'article mis en page : Lutte contre le terrorisme : Faut-il ouvrir la porte du chiffrement aux services de renseignement ? – La Voix du Nord

---

Pourquoi le Conseil d'État

autorise une exploitation de données saisies via l’état d’urgence ?

	Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.
En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « *si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace* » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.

Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.
Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « *alors même qu'aucune infraction n'est constatée* ».
L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.
Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».
Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence – Politique – Numerama

---

Cyberattaques terroristes déjouées au Maroc

Cyberattaques terroristes déjouées au Maroc

Des cyberattaques de sites étatiques planifiées par des individus soupçonnés d’avoir des penchants extrémistes et des relations avec Daech ont été déjouées dans le Royaume du Maroc grâce à une vaste opération antiterroriste qui a abouti à l’arrestation et la garde à vue de 52 personnes.

Selon un communiqué du ministère de l’Intérieur cité par des médias locaux, dont le Matin.ma, ainsi que le quotidien ivoirien Fraternité Matin, cette opération antiterroriste a été menée sous la houlette du parquet général et visait 343 individus.

Outre des projets terroristes ciblant des centres de loisir, des festivals, des établissements sécuritaires du Royaume, des cyberattaques à un niveau de préparation bien avancée devaient être dirigées contre les institutions marocaines. Objectif? Bloquer le fonctionnement des structures étatiques et paralyser l’économie.

D’autres personnes arrêtées par les forces de police marocaine sont soupçonnées de recruter des combattants mineurs via les réseaux sociaux.

Article original de Alselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Terrorisme : des cyberattaques déjouées au Maroc | CIO MAG

Qui sont vraiment les Anonymous, ces justiciers du web ?

Qui sont vraiment les Anonymous, ces justiciers du web ?

Charlie Hebdo, ceux de Novembre 2015 et plus récemment attentats de Nice. A chaque tragédie, les Anonymous se manifestent au travers d'une vidéo dans laquelle ils menacent de faire régner la justice. Mais qui sont ces « hacktivistes » ? Véritables hackers ou grosse supercherie ? Nous avons étudié la question pour vous dire qui sont les Anonymous, ces justiciers du web.

Les Anonymous se sont faits connaître plus que jamais du grand public à la suite des attentats contre Charlie Hebdo. Dans une vidéo publiée quelques heures après le drame, ils promettaient aux terroristes une guerre sans merci. Le 18 Janvier 2015, ils attaquaient le site web de l'agence de l'informatique de l'Etat Sénégalais sur lequel on pouvait lire :
Vous avez voulu interdire la caricature de la Une de Charlie Hebdo ? Mauvais choix.
Plus tard, à la place de la page d'accueil du site institutionnel on pouvait voir la caricature du prophète Mahomet du journal ainsi qu'un hommage aux 17 victimes des attentats.
Cette action figure parmi beaucoup d'autres. Comptes Twitter révélés ou supprimés, sites islamistes bloqués, piratés ou rayés du web. Néanmoins, l'efficacité des Anonymous depuis maintenant plusieurs mois peut interroger. Certains ne prennent plus vraiment ces justiciers du web au sérieux, les accusant de n'être que des adolescents ayant quelques connaissances techniques. Pour en avoir le coeur net, nous avons mené l'enquête.

Origine des Anonymous

Aujourd'hui, les Anonymous font partie du paysage numérique à part entière. Mais sait-on vraiment d'où est né ce mouvement ? Les Anonymous sont-ils des hackers, des informaticiens, des révolutionnaires ou de simples passionnés ? Les mythes sont nombreux mais il convient de rétablir la vérité.
Au départ, le mouvement Anonymous n'a absolument rien à voir avec le hacking. A l'origine, le berceau d'Anonymous était un simple site d'images. En 2003, Christopher Poole, un new-yorkais de tout juste 15 ans ouvre un forum dédié aux mangas. Il s'inspire d'un site japonais baptisé 2chan et nomme son propre forum 4chan.

L'originalité de 4chan, c'est que les utilisateurs n'ont aucune limite dans les contenus qu'ils partagent. En effet, sur chaque fichier partagé avec la communauté, en lieu et place du nom de l'internaute, le serveur inscrit par défaut la signature « Anonymous ». 4chan connaissant un succès monstrueux, des milliers d'internautes ont alors été baptisés « Anonymous ». Le mouvement était né.

Qui sont vraiment les Anonymous ?

Comment passe-t-on de site d'image à une communauté de hackers ? Pour bien comprendre, il faut oublier toute idée reçue. **La plupart des Anonymous ne sont pas des hackers.**
Dans les débuts de 4chan, les « Anons » sont avant tout des adeptes du troll, des amateurs de blagues un peu débiles. C'est ce que l'on appelle le mouvement « Lulz » (pluriel déformé de « LOL ») qui consiste à tourner en dérision un peu tout et n'importe quoi. Parfois, les intervenants n'hésitent pas à y glisser une pointe de méchanceté.
C'est **en 2007 que les Anonymous commencent à s'attaquer à des institutions**. L'un des membres de la communauté tombe sur une vidéo de Tom Cruise faisant l'apologie de la scientologie. Toujours dans l'esprit « Lulz » ils la diffusent sur le web.
Les scientologues, piqués au vif précisent que la vidéo est soumise à des copyrights, et que toute personne l'exploitant serait traînée en justice. Mal leur en a pris. Les « Anons » ont alors vu dans cette censure comme une atteinte à leur liberté. Ils décident de lancer une opération baptisée « Opération Chanology ». Il s'agira de la toute première opération des « Anons ».
Cette première tentative repose sur un procédé que l'on verra se répéter par la suite. « Opération Chanology » consistait à pirater les sites de l'Eglise scientologue en y publiant des affiches et des vidéos parodiques. En parallèle, les Anons ont organisé des manifestations sur le web. Ils se mettent alors en scène dans des vidéos devenues désormais célèbres.

Pour conserver leur anonymat, **ils portent le masque de Guy Fawkes**. Cet anglais avait tenté en 1605 de faire sauter le Parlement de Londres. Dans le Blockbuster hollywoodien « V pour Vendetta », le justicier porte également ce masque. De plus, pour camoufler leurs voix, ils utilisent un logiciel de synthèse vocale qui énonce un texte écrit avec une voix robotique.
Jusqu'en 2011, les Anonymous poursuivent leur lutte en gardant le **même esprit de liberté, de partage du savoir**, des connaissances, des logiciels, des contenus. La seule condition est de ne pas les utiliser à des fins pécuniaires. N'importe qui peut devenir Anonymous, une simple recherche sur le web suffit. Tous les accès aux sites sont libres.
A l'époque, la plupart des « Anons » ne sont absolument pas des experts du hacking. Il s'agit simplement de geeks. Ils communiquent sur les forums, sur Facebook, Twitter et autres réseaux sociaux. Les contenus partagés sont des images et des vidéos dont on connaît maintenant la teneur. L'objectif des Anonymous à cette période est de **créer une mouvance conduisant à la révolte du peuple** face à des pratiques considérées comme liberticides. Leur devise officielle, un tantinet pompeuse, est la suivante :
Nous sommes Anonymous. Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Préparez-vous à notre arrivée.
En 2011, le mouvement prend une toute autre ampleur. Des experts en hacking rejoignent les équipes des Anonymous. Mais ces derniers radicalisent le mouvement suite aux propos de HB Gary, un site expert en sécurité, qui affirme avoir identifié une trentaine de membres des Anonymous et qu'il va les dénoncer au FBI. Il ajoute par ailleurs qu'il existe une hiérarchie au sein du mouvement.
C'est cette ultime accusation qui a provoqué la colère des membres. Car les « Anons » tiennent à leur modèle de fonctionnement reposant sur le « Hive Mind » (Esprit de ruche). Comme le font les abeilles, les Anonymous **sauraient chacun instinctivement quel rôle ils ont à jouer dans une opération.**
Il n'y a aucune leader, aucune hiérarchie même si certains membres sont plus actifs, plus créatifs ou plus techniques que d'autres. L'image de hacker qui colle à la peau des Anonymous est totalement erronée. La **plupart sont des geeks experts en graphisme, en montage vidéo ou en réseaux sociaux**. D'autres n'ont même aucune expertise mais contribuent comme ils le peuvent au mouvement.

Il y a bien des hackers, mais ils ne sont pas majoritaires. Il s'agit pour la plupart d'entre eux de programmeurs de génie, de chercheurs en sécurité ou encore d'administrateurs système. Le problème aujourd'hui c'est que le mouvement a une telle notoriété que certains petits malins s'en prennent à certains sites sans aucune raison en s'auto-proclamant Anonymous.

Comment les Anonymous opèrent-ils ?

Malgré tout, après 2011 les opérations se multiplient en utilisant toujours la même technique : des attaques DDoS combinées à une communication sur le web efficace. L'organisation est extrêmement simple.
Les Anons lancent une discussion sur un forum sur une opération à venir. Le jour J, les Anonymous du monde entier se retrouvent sur ce même forum pour programmer une saturation des serveurs d'un site ciblé. Pour faire simple, grâce à un logiciel spécifique, tous les membres envoient un nombre de données plus important que le serveur ne peut en supporter. Il « explose », offrant la possibilité aux hackers de prendre la main sur la page d'accueil du site.
Entre le 14 et le 18 janvier 2015, à la suite des attentats contre Charlie Hebdo, ce sont **20 000 sites web faisant l'apologie du terrorisme** qui ont fait l'objet du même type d'attaque. Le but est de bloquer les moyens de communication des terroristes.

Ainsi, les Anons ont élargi leur champ de travail aux réseaux sociaux qui sont désormais majoritairement utilisés par les terroristes. Ils ont dévoilé par exemple des milliers de comptes appartenant à des djihadistes. Le problème, c'est que ces comptes sont créés plus vite qu'ils ne sont supprimés.

Article original de Romain Vitt

Réagissez à cet article

Original de l'article mis en page : Anonymous : qui sont vraiment ces justiciers du web ?

L'application Telegram a aussi sa faille

L'application Telegram a aussi sa faille

Un chercheur a trouvé une faille de sécurité sur la version Mac de Telegram. L'éditeur minimise l'importance de cette vulnérabilité.

Une grave affaire prise à la légère ou, au contraire, beaucoup de bruit pour rien ? Les avis sont partagés à propos de la faille de sécurité découverte sur **Telegram** par le dénommé Kirill Firsov.
Ce chercheur russe s'est aperçu que la version Mac du service sécurisé de messagerie enregistrait, dans les journaux système (*syslog*), chaque message collé dans le champ de discussion depuis le presse-papiers. Le 23 juillet, il avait, sur Twitter, interpellé Pavel Durov, cofondateur du service avec son frère Nikolai.
S'est ensuivi un échange de tweets à l'issue duquel le bug a été résolu… sans qu'on puisse mesurer quelle était sa réelle ampleur. L'explication entre les deux hommes s'est effectivement terminée sur un « Imagine que la police saisisse ton ordinateur portable et qu'elle retrouve trace de tes messages 'secrets' dans syslog » lancé par Kirill Firsov.

La sandbox pour limiter les dégâts

Pour Pavel Durov, la vulnérabilité, repérée sur les versions 2.16 et 2.17 de Telegram, n'est pas aussi importante qu'elle en a l'air : n'est concerné que le texte collé depuis le presse-papiers… auquel toutes les autres applications Mac ont accès.
Sans nier cet état de fait, Kirill Firsov avait pointé du doigt le fait que les messages font l'objet d'une journalisation. Ce à quoi Pavel Durov avait répondu qu'avec le mécanisme dit de « bac à sable » (*sandbox*), les applications téléchargées sur l'App Store d'OS X – à l'image de Telegram – ne peuvent qu'écrire dans *syslog* ; pas y accéder en lecture (voir, à ce propos, la documentation d'Apple).
Bilan pour celui qui a financé Telegram via son fonds Digital Fortress, corriger la faille revient juste à éliminer une redondance : le fait que toutes les applications peuvent accéder au contenu du presse-papiers.

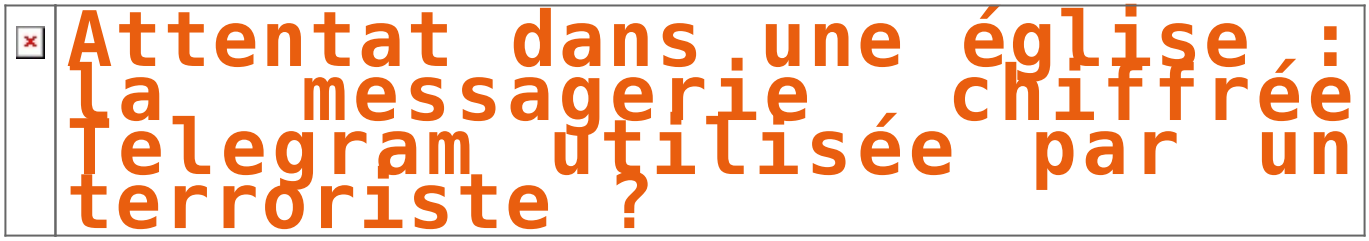
Le service qui monte

L'histoire de Telegram est particulière. Ses fondateurs s'étaient installés à Berlin après avoir, sur fond de lutte d'influence politique avec l'entourage de Vladimir Poutine, perdu le contrôle du réseau social vKontakte, qu'ils avaient créé en Russie.
Utilisé à l'origine par les seules équipes de vKontakte, Telegram avait basculé, en 2013, dans une exploitation ouverte au grand public.
En insistant sur la dimension de confidentialité des échanges, le service a dépassé, fin février, les 100 millions d'utilisateurs actifs par mois, souligne ITespresso.
Une ascension qui n'a pas laissé la concurrence indifférente. Illustration chez WhatsApp, qui avait décidé, fin 2015, de bloquer, sur Android, les liens vers l'application Telegram diffusés par ses utilisateurs.
Le service, qui exploite un protocole de chiffrement maison (MTProto), a aussi été mis en lumière pour des considérations plus sombres : selon Trend Micro, 34 % des organisations terroristes l'utilisent comme point de contact.
Article original de Silicon

Réagissez à cet article

Original de l'article mis en page : Sécurité : Telegram, une vulnérabilité qui prête à discussion

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama



Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama

---

Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

Op hashtag – La police fédérale Brésilienne aurait infiltré le WhatsApp et Telegram utilisaient par des terroristes locaux. Plusieurs groupes échangeaient des informations sur des tactiques de guerre. Des attentats prévus lors des Jeux Olympiques de Rio ?

Un nouveau cheval de bataille pour la justice brésilienne qui tente de contrôler les réseaux sociaux au Brésil. J'apprends dans le journal brésilien blasting news que La police fédérale brésilienne aurait infiltré le WhatsApp et Telegram de terroristes locaux lors d'une opération baptisée Op Hashtag. Plusieurs personnes s'échangeaient des informations sur des tactiques de guerre. Dans ce nouveau cas, la police fédérale parle clairement de « djihadiste » qui fomentaient des attaques à l'occasion des Jeux Olympique de Rio.

Opération HashTag

L'opération « Hashtag » a été lancée dans la matinée du jeudi 21 juillet. Cette action policière démontre comment la police fédérale aurait réussi à avoir accès aux messages de plusieurs groupes de « terroristes ». Des commanditaires d'attaques en Europe, qui souhaiteraient agir au Brésil.
Alexandre Moraes, le ministre de la Justice, a expliqué que la police tentait de surveiller les conversations WhatsApp. Action difficile puisque tous les messages sont chiffrés « ce qui rend impossible pour quiconque d'avoir accès, y compris à la justice« . Cependant, l'infiltration avec la création de faux comptes d'internautes aurait porté ses fruits. Le ministre a refusé de donner des détails sur la façon dont l'enquête a été menée, mais comme il est impossible de surveiller les messages échangés dans l'application, il est certain que les agents de police se sont présentés comme des candidats brésiliens aux actes assassins réclamaient par Daesh, Al Qaeda …
La Cour fédérale du Paraná a lancé 12 mandats d'arrêt grâce aux enregistrements téléphoniques d'internautes qui se seraient déclarés prêts à orchestrer des attaques lors des JO de Rio. Des internautes qui s'échangeaient aussi des modes d'emploi de tactiques militaires. Le ministre de la Justice a également révélé que certains des brésiliens arrêtés lors de l'Opération Hashtag avaient prêtés serment d'allégeance à l'État islamique.

Contrôler les réseaux sociaux

Le Brésil est précurseur sur de nombreux points concernant le contrôle des réseaux sociaux. Ce pays, qui est un immense vivier de pirates informatiques, tente aussi de cyber surveiller les propos et les internautes passant par ses Internet. Souvenez-vous, en juin 2014, lors de la coupe du monde football, les cyber manifestations lancées par Anonymous. Plus proche de nous, décembre 2015, avec le blocage de WhatsApp durant 48 heures. Un troisième blocage interviendra en mai 2016. Sans oublier l'arrestation d'un dirigeant de Facebook.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes – ZATAZ

Détecter les futurs

terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

	Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

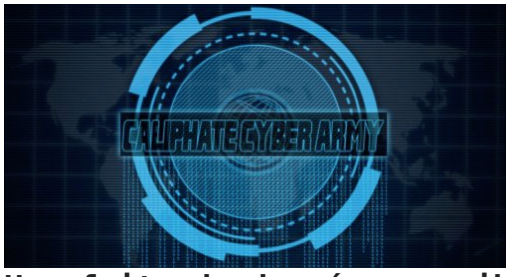
Original de l'article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

La France visée par une nouvelle cyberattaque de l'EI

La France visée par une nouvelle cyberattaque de l'EI

Les équipes CybelAngel ont repéré lundi 16 mai une base de coordonnées de citoyens français et américains publiée sur le site justepaste.it. L'utilisateur à l'origine de la publication se revendique de la Caliphate Cyber Army (#CCA).



Une fuite de données sensibles mais accessibles depuis 6 mois

Le message commence par une représentation de la basmala, un verset leitmotiv du Coran à la gloire de Dieu. Des mots-dièse "CCA #CyberCaliphate #UCC" et un logo de la Caliphate Cyber Army viennent compléter la revendication introductive.

Vient ensuite une liste de 77 emails, mots de passe, numéros de téléphone, adresses, comptes Paypal et soldes de compte Paypal. La liste concerne 38 adresses françaises, 31 américaines, 6 australiennes, 1 philippine et 1 néerlandaise. Les coordonnées semblent être uniquement personnelles et non professionnelles.

Après analyse, il semblerait que les données exposées ici étaient déjà présentes sur le Dark Web avant cette publication. En effet, un message publié le 12 janvier dernier sur le site pastebin.com reprenait 35 paires d'emails/mots de passe correspondant exactement à ceux publiés le 16 mai par la Cyber Caliphate Army. A l'aune de cette troublante similarité entre le 12 janvier et le 16 mai, la CCA reprendrait à son compte des adresses en libre accès sur le Dark Web ; ce qui ne serait pas la première fois.

Une Cyber Armée aux attaques peu techniques mais à fort impact médiatique

La Cyber Caliphate Army est issue de la volonté de l'Etat Islamique de projeter son action dans l'espace virtuel en 2014. Elle est dans un premier temps dirigée, et probablement entièrement constituée par Junaid Hussain, un hacker anglais.

De son lancement pendant l'été 2014 jusqu'à l'assassinat de Hussain par un drône américain en août 2015, la CCA a revendiqué une série de cyberattaques peu sophistiquées mais très médiatiques : plusieurs défacements de comptes Twitter du Commandement Central des Armées américaines (CENTCOM), de Newsweek, de chaînes de télévisions américaines, l'arrêt des retransmissions des 11 chaînes de TV5 Monde (action dont la parenté est mise en doute par de nombreux experts).

Cette nouvelle fuite souligne les faiblesses de la Cyber Armée du Califat

Depuis la mort de Husain, la CCA a mené des actions nettement moins symboliques : des défacements indiscriminés de milliers de sites et des actions à la parenté douteuse dont des fermetures de systèmes informatiques revendiquées ex-post et des diffusions de données en réalité déjà en ligne, comme celle détectée ce 16 mai par CybelAngel.

Face à ce potentiel de nuisance visiblement réduit, 4 groupuscules d'hacktivistes islamistes dont la Cyber Caliphate Army ont proclamé leur union en un United Cyber Caliphate en avril ainsi que nous vous le rapportions la semaine dernière. Quelques semaines plus tard, le groupuscule Cyber Caliphate Army revendique pourtant en son nom propre une action et ne mentionne le United Cyber Caliphate qu'en un hashtag UCC. Il semblerait que l'intégration des différents groupes hacktivistes islamistes prenne plus de temps que prévu.

Article de CybelAngel Analyst Team

Réagissez à cet article

Source : *La France visée par une nouvelle cyberattaque de l’EI*

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]

Réagissez à cet article

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