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

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

---

Quel cadre pour l'État d'urgence et la copie des données informatiques ?

Quel cadre pour l'État d'urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
• N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle.

Jean-Jacques Urvoas, ministre de la Justice, au Sénat.

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE,…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « *données accessibles à partir du système initial ou disponibles pour le système initial* », qui a disparu.

« *Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les* ***données contenues dans tout système informatique ou équipement terminal présent sur les lieux*** *de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.*

La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui ***en indique les motifs*** *et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition.* ***À compter de la saisie, nul n'y a accès avant l'autorisation du juge****.*

L'autorité administrative ***demande au juge des référés du tribunal administratif d'autoriser en tout ou partie leur exploitation****. Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il* ***statue dans un délai de quarante-huit heures*** *à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative.* ***Sont exclus de l'autorisation les éléments dépourvus de tout lien avec la menace*** *que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics.* ***En cas de refus*** *du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa,* ***les données copiées sont détruites*** *et les supports saisis sont restitués à leur propriétaire.*

Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont ***restitués à leur propriétaire****, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent,* ***à l'issue d'un délai maximal de quinze jours*** *à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent.* ***À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée****,* ***les données copiées sont détruites à l'expiration d'un délai maximal de trois mois*** *à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.*

En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. ***Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables*** *en matière de procédure pénale.*

Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. ***Ses décisions sont susceptibles d'appel*** *devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article.* »

Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

La sécurité des Opérateurs d’Importance Vitale (OIV) continue à se renforcer

La sécurité des Opérateurs d’Importance Vitale continue à se renforcer

---

Les premiers arrêtés encadrant la sécurité des OIV illustrent la difficulté à mettre en place un dispositif encadrant la cybersécurité des entreprises. L'Anssi vante une démarche pionnière et reconnaît que les organisations concernées devront investir pour se conformer aux nouvelles règles.

Trois arrêtés sectoriels sur 18. L'entrée en vigueur, au 1er juillet, des premières mesures encadrant la sécurité des OIV (Opérateurs d'importance vitale), 249 organisations dont le bon fonctionnement est jugé essentiel au fonctionnement de la Nation, illustre bien la difficulté à poser un cadre réglementaire sur la cybersécurité des grandes entreprises. Découlant de l'article 22 de la Loi de programmation militaire (LPM), votée fin 2013, cet ensemble de règles, qui comprend notamment la notification des incidents de sécurité à l'Anssi (Agence nationale de sécurité des systèmes d'information), avait fait l'objet d'un décret en mars 2015. Restait à adapter ce décret à la réalité des différents secteurs d'activité. Ce qui, de toute évidence, a pris plus de temps que prévu. Rappelons qu'à l'origine, l'Anssi espérait voir les premiers arrêtés sectoriels sortir à l'automne 2015…

Mais Guillaume Poupard, le directeur général de l'Anssi, assume tant le choix de la France d'en passer par la loi (plutôt que par un simple référentiel de bonnes pratiques) que le décalage de calendrier, révélateur de la difficulté à traduire sur le terrain l'article 22 de la LPM. Lors d'une conférence de presse organisée à l'occasion de la sortie des premiers arrêtés, dédiés aux secteurs de l'eau, de l'alimentation et de la santé, il explique : « Je préfère avoir dès le départ annoncé un calendrier ambitieux et avoir aujourd'hui un dispositif en place. Avec l'Allemagne, la France fait partie des pays pionniers de ce type de démarche. Et si nous avons pu prendre quelques mois de retard sur le calendrier initial, nous restons très en avance sur nos alliés. » D'autres arrêtés sectoriels devraient sortir en octobre 2016 et janvier 2017. Une fois ces textes publiés, les OIV ont, pour les règles les plus complexes, jusqu'à 18 mois ou 2 ans pour les mettre en œuvre. « On a déjà vérifié que ces règles étaient efficaces et soutenables financièrement », assure Guillaume Poupard.

« Oui, cela coûte de l'argent »

La définition de ces règles, au sein de 12 groupes de travail sectoriels, n'a pourtant pas été simple. Tout simplement parce qu'elles se traduisent par des investissements contraints pour les entreprises concernées sur les systèmes d'information considérés d'importance vitale. Certaines se verront dans l'obligation de revoir leurs architectures réseau par exemple. « On va imposer des règles, des contrôles, des notifications d'incidents, la capacité pour l'Anssi à imposer sa réponse aux incidents en cas de crise. C'est assez violent. Mais, il faut garder à l'esprit que ces règles ont été élaborés au sein de groupes de travail associant les OIV », tranche Guillaume Poupard. Selon ce dernier, la sécurité devrait peser entre 5 et 10 % du budget de la DSI de tout OIV. « Nos mesures ne s'inscrivent pas dans l'épaisseur du trait budgétaire. Mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique », tranche-t-il. Et d'assurer qu'aucun groupe de travail ne connaît une situation de blocage empêchant d'avancer sur la rédaction des arrêtés.

Si le dispositif se met donc en place au forceps, tout n'est pas encore parfaitement défini. Illustration avec les incidents de sécurité que les OIV doivent notifier à l'Anssi. Cette dernière ne peut matériellement pas consolider l'ensemble des incidents des 249 OIV français. Dès lors quels événements devront être communiqués et lesquels devront rester cantonnés entre les murs de l'organisation visée ? « C'est un sujet complexe car les premiers indices d'une attaque sont souvent de la taille d'une tête d'épingle, reconnaît Guillaume Poupard. C'était par exemple le cas pour l'affaire TV5 Monde. » Selon le directeur général de l'Anssi, des expérimentations sont en cours pour placer le curseur au bon endroit.

De l'efficacité de ce dispositif dépendra la réalisation d'un des objectifs de l'Anssi, la capacité à organiser la défense collective. L'Agence se voit en effet comme un tiers anonymisateur permettant d'assurer le partage d'informations sur les menaces à l'intérieur d'un secteur ou à l'échelle de l'ensemble des OIV. Une mise en commun que rechignent à effectuer les entreprises – même si des secteurs comme la banque se sont organisés en ce sens – pour des raisons concurrentielles.

L'Anssi veut les codes sources

En parallèle, pour compléter ce dispositif, l'Anssi s'est lancée dans un travail de qualification des prestataires et fournisseurs à même d'implémenter les règles édictées dans les arrêtés. Un processus plus lourd qu'une simple certification. Aujourd'hui, une vingtaine de prestataires d'audit ont ainsi été qualifiés. L'agence doit également publier des listes de prestataires de détection d'incidents, de réactions aux incidents ainsi que des sondes de détection. Si Guillaume Poupard écarte toute volonté de protectionnisme économique déguisé, il reconnaît que cette démarche de qualification – qui va jusqu'à l'évaluation des experts eux-mêmes ou l'audit du code source pour les logiciels – introduit un biais, favorisant les entreprises hexagonales. « L'accès au code source est par exemple accepté par certains industriels américains, mais refusé par d'autres », reconnaît-il.

Si, malgré les réticences de certains OIV, la France a décidé de presser le pas, c'est que les signaux d'alerte se multiplient. « Nous craignons notamment la diffusion des savoirs aux groupes terroristes, via le mercenariat. Nous avons des informations des services de renseignement nous indiquant que ces groupes ont la volonté de recruter des compétences cyber », assure Louis Gautier, le secrétaire général de la défense et de la sécurité nationale. Un pirate informatique kosovar, arrêté en Malaisie en octobre 2015, a ainsi reconnu avoir vendu ses services à Daesh. Connu sous le pseudonyme Th3Dir3ctorY, il vient de plaider coupable devant la justice américaine et risque 20 ans de prison.

De son côté, Guillaume Poupard s'inquiète du comportement de certains assaillants qui semblent mener des missions d'exploration sur les réseaux des entreprises françaises. « Comme s'ils voulaient préparer l'avenir. Que cherchent-ils à faire exactement ? Nous ne le savons pas, mais ces opérations de préparation sont particulièrement inquiétantes », dit le directeur général de l'Anssi, qui précise que les alliés de la France observent le même phénomène.

Article original de Reynald Fleychaux

Réagissez à cet article

Original de l'article mis en page : La sécurité des OIV mise au pas par l'Etat… petit à petit

---

Inquiétantes intrusions dans les réseaux d'entreprises

Inquiétantes intrusions dans les réseaux d'entreprises

Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et labsence de vols de données laisse craindre des tentatives de sabotages ou dattaques terroristes, a déclaré lundi le directeur général de lAgence nationale de la sécurité des systèmes dinformation (Anssi).

Le Secrétariat général de la défense et la sécurité nationale (SGDSN) et l'Anssi, deux services rattachés à Matignon, ont présenté lundi les trois premiers arrêtés liés à la protection des opérateurs d'importance vitale dans la santé, la gestion de l'eau et l'alimentation, qui entreront en vigueur le 1er juillet.

« Il y a de plus en plus d'attaquants, ce sont des agents dormants qui préparent les choses », a expliqué Guillaume Poupard à des journalistes. « Il y a eu beaucoup de cas à traiter ces derniers mois ».

Ces intrusions, par exemple par le biais d'emails piégés envoyés dans les entreprises, permettent aux attaquants de cartographier un réseau en toute discrétion et, en passant d'un réseau à l'autre, de pénétrer dans des zones inattendues.

« Ils prennent pied progressivement (..) et on les retrouve très profond au sein des réseaux d'entreprises, à des endroits où il n'y a même plus d'informations secrètes à voler, par exemple sur les systèmes de production de contrôle qualité », a ajouté Guillaume Poupard.

Ce nouveau type d'intrusion est d'autant plus inquiétant qu'il est presque plus facile d'entrer dans un réseau pour en modifier le fonctionnement ou en prendre le contrôle que pour voler des données, a-t-il souligné.

Au contraire de la banque, de l'aérospatiale et de l'automobile, habitués à surveiller de près leurs réseaux, l'industrie est encore mal préparée, étant moins sujette aux vols de données, a noté Guillaume Poupard.

« L'idée que des gens qui depuis l'autre bout du monde puissent chercher à détruire leur système de production c'est un nouveau scénario qui n'a pas vraiment d'équivalent dans le monde réel », a-t-il souligné.

Pour mieux défendre les PME, « un des maillons faibles », cible rêvée d'un attaquant, il prône le recours aux solutions de « cloud computing » des spécialistes de la sécurité numérique et à l'intégration de systèmes de protection dans les machines outils et les automates industriels dès leur conception. (Cyril Altmeyer, édité par Jean-Michel Bélot)

Réagissez à cet article

Original de l’article mis en page : SAFRAN : France : Inquiétantes intrusions dans les réseaux dentreprises

Appli alerte attentats : «Il faut que la France respecte les standards internationaux»

	Application Alerte Attentats : «Il faut que la France respecte les standards internationaux»

Original de l’article mis en page : Appli alerte attentats : «Il faut que la France respecte les standards internationaux» – Libération

---

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*

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

	**Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue**

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*