Attentats : les attaques contre les sites Web français s’intensifient

	Attentats : les attaques contre les sites Web français s’intensifient

Si les attaques sont pour le moment limités à du 'défaçage', les experts en sécurité craignent que les hacktivistes islamistes changent de braquet ce jeudi. Mais pour le moment, les attaques sont nombreuses mais limitées.

L'escalade des attaques a bien eu lieu. Premiers à réagir, les Anonymous qui ont promis de venger les victimes de Charlie Hebdo avec l'opération #OpCharlieHebdo. Cette offensive des hactivistes a évidemment provoqué une réaction de hackers de l'autre bord, soutenant les islamistes radicaux.
Et ces derniers ont massivement attaqué de nombreux sites Web français de tout ordre (églises, municipalités, universités, hôpitaux…). « Plus d'un millier de sites ont été touchés au total, plus ou moins fortement. Ces sites sont majoritairement de petite taille », explique à l'AFP François Paget, expert chez McAfee. D'autres sources avancent un chiffre de 19.000 sites touchés.

Plus de 1000 sites français cybervandalisés
La plupart du temps, il s'agit de campagnes de «defacement», soit une modification de la page d'accueil des sites visés avec la publication de messages à caractère idéologique. «Il n'y a de Dieu qu'Allah», «Death to France» (Mort à la France) ou encore «Death to Charlie»… Il ne s'agit donc pas d'une cyberguerre (comme certains voudraient le faire croire) mais plutôt de cybervadalisme.
Ces attaques ne sont d'ailleurs pas bien compliquées à mener : « des CMS, des applications Drupal, Joomla, WordPress tout simplement non mis à jour. Des mots de passe un peu trop légers… », commente le spécialiste Zataz.
Mais ces attaques pourraient prendre une nouvelle dimension ce jeudi. « Les revendications initiales parlaient d'un point d'orgue le 15 janvier », indique Gérôme Billois, expert du Cercle européen de la sécurité informatique et consultant pour le cabinet Solucom.
« Ce ne sont bien sûr que des suppositions, mais on pourrait par exemple assister jeudi à l'attaque de sites plus visibles, à des attaques plus groupées, ou à un changement de technique », estime le spécialiste.
A titre préventif, l'Agence nationale de la Sécurité des Systèmes d'information (ANSSI) a envoyé un petit manuel pédagogique dans les ministères, afin de faire le point sur les mesures de sécurité à prendre en urgence tandis que le volet numérique du plan vigipirate aborde les questions de sécurité informatique pour les opérateurs d'importance vitale.
AnonGhost a ainsi revendiqué ce jeudi la publication de coordonnées personnelles d'une dizaine d'employés des ministères des Finances et de l'Intérieur et affirment posséder une base de plus de 10.000 noms. Le collectif MECA (Middle-East Cyber Army revendiquait de son côté trois attaques contre le syndicat Sud Michelin, et l'institut de mathématiques de Toulouse….
Bref, on est encore très loin de la cyberguerre mais « C'est la première fois qu'un pays est confronté à une vague aussi importante de cybercontestation », observe ainsi le vice-amiral Arnaud Coustillière, officier-général de la cyberdéfense.

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

Source : http://www.zdnet.fr/actualites/attentats-les-attaques-contre-les-sites-web-francais-s-intensifient-39812939.htm

---

Votre box pourrait bien être utilisée pour des piratages

d’envergure…

Votre box pourrait bien être utilisée pour des piratages d’envergure…

Le groupe LizardSquad, qui a notamment orchestré les attaques Ddos sur le PSN et Xbox Live à Noël, a dévoilé peu de temps après une offre payante offrant des attaques par déni de service à la demande. Un « service » qui repose essentiellement sur des routeurs privés mal sécurisés.

Le 25 décembre, le groupe LizardSquad lançait une attaque Ddos contre les services en ligne du Playstation Network et du Xbox Live. Dieu merci (ou pas) Kim Dotcom est venu à la rescousse des utilisateurs et tout est rapidement rentré dans l’ordre. Mais peu de temps après, LizardSquad lançait une offre de Ddos payante à la demande, expliquant que ses récentes attaques largement relayées dans la presse n’étaient en fait qu’une opération de communication visant à faire preuve de l’efficacité de leurs techniques.

Business is business, as usual

L’offre présentée par LizardSquad vous permet, contre espèces sonnantes et trébuchantes (mais ils acceptent aussi les bitcoins) de lancer une attaque Ddos sur la cible de votre choix. Le tout sans avoir à s’embarrasser des aspects techniques : le groupe de pirates se charge de tout, vous offrant ainsi un service clef en main pour mettre des bâtons dans les roues de vos concurrents, ennemis, amis, bref, à peu près tout ce qui est en mesure de proposer un service en ligne et qui vous dérange. Officiellement, l’outil LizardStresser est avant tout pensé pour les utilisateurs souhaitant tester la robustesse de leurs services face à une attaque Ddos.

Un exemple des prix pratiqués par LizardSquad (Crédit original de l’image : The Register)

Le journaliste Brian Krebs, spécialisé dans la cybersecurité, s’est lancé dans une petite croisade contre ce groupe de pirate. Il avait dans un précédent article entrepris de révéler l’identité de certains d’entre eux et n’hésitent pas à les qualifier de « script kiddies », un terme péjoratif qui désigne les débutants sans connaissances réelles qui récupèrent et utilisent des programmes clef en main pour s’attaquer à des sites web ou des internautes. De part et d’autre, les insultes volent, LizardSquad n’hésitant pas à affirmer que leurs serveurs sont hébergés « quelque part sur le front de Brian Krebs »
Brian Krebs s’est penché sur les méthodes utilisées par le groupe pour mener à bien leurs attaques Ddos. En effet, plusieurs options sont disponibles pour parvenir un tel résultat : certain ont recours à des botnets, Anonymous de son coté s’était fait remarquer pour l’utilisation du soft LOIC qui transformait ses utilisateurs en « botnet consentant » et d’autres méthodes reposant sur l’exploitation de failles de sécurité sont également utilisées (On pense notamment à la technique de l’amplification DNS)
Routeurs domestique : l’ennemi intérieur ?
LizardSquad dispose lui aussi de son propre réseau Botnet pour mener à bien ses attaques, explique Brian Krebs, mais celui-ci est essentiellement constitué de routeurs domestiques. L’auteur explique être parvenu, avec l’aide de chercheurs non cités, à mettre la main sur le malware utilisé par LizardSquad. Celui-ci est une version modifiée d’un trojan signalé auparavant par la firme russe Dr.Web.

Krebs remarque que ce malware a pour fonctionnalité de scanner l’ensemble du réseau afin de trouver les routeurs ayant gardé leurs paramètres d’usine. En effet, la plupart des utilisateurs négligent la sécurité de leurs routeurs wifi, et si les mots de passe configurés en usine n’ont pas été changés, accéder à l’interface n’a rien de compliqué.

Le malware n’est pas spécifique aux routeurs domestiques, explique Krebs, il est conçu avant tout pour s’attaquer aux machines utilisant Linux. Le journaliste explique que les routeurs domestiques constituent la majeure partie du botnet de LizardSquad, mais que les routeurs de certaines universités et entreprises sont probablement infectés.

Si vous craignez que votre paisible routeur domestique ne soit en réalité un agent double à la solde de LizardSquad, Krebs détaille également dans la suite de son article les techniques de base permettant de sécuriser l’accès à son routeur. La plus simple et la plus efficace reste néanmoins la plus évidente : changer ses mots de passe.

L’article de Brian Krebs :
http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/#more-29431

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

Source :
http://www.zdnet.fr/actualites/lizardsquad-devoile-un-service-de-ddos-a-la-demande-qui-s-appuie-sur-les-routeurs-39812835.htm
Par Louis Adam

Alerte au phishing sur LinkedIn

Alerte au phishing sur LinkedIn

L'éditeur de sécurité Symantec a lancé une alerte à propos de mails de phishing ciblant les utilisateurs du réseau social LinkedIn. Ce mail frauduleux contient une pièce jointe à ne surtout pas ouvrir.

Satnam Narang, manager sécurité chez Symantec, a lancé une alerte sur la multiplication de mails de phishing visant les utilisateurs de LinkedIn. Dans un billet, ce dernier explique avoir observé un accroissement de mails prétendument envoyés par le service support du réseau social professionnel. En fait, il n'en est rien : il s'agit bien de mails frauduleux tentant de tromper les utilisateurs qui pourraient être tentés de suivre les recommandations indiquées dans ce message.

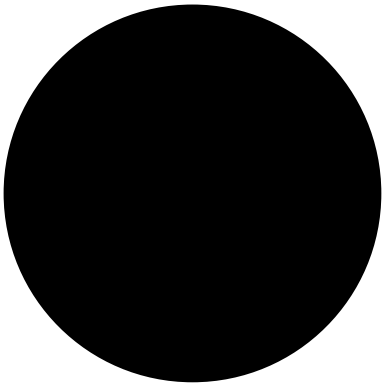
« En raison d'activités irrégulières, votre compte LinkedIn a fait l'objet d'une mise à jour de sécurité obligatoire. Parfois, LinkedIn rejette les identifiants dans les cas où nous pensons que le compte pourrait avoir été compromis. Pour ce faire, nous avons développé une nouvelle façon de garder votre compte sûr et attaché à ce mail un formulaire pour achever ce processus. Merci de le télécharger et de suivre les instructions sur votre écran » peut-on lire dans le mail de phishing.

Celui-ci est écrit de façon tout à fait correcte et peut donc piéger d'autant plus facilement l'utilisateur.
En cliquant sur le formulaire, une copie du véritable site, dont la source a été modifiée, s'affiche invitant l'utilisateur à se connecter avec ses identifiants. *« La méthode utilisée permet de contourner les listes noires du navigateur qui souvent détectent les sites web suspicieux pour prévenir les utilisateurs qu'ils sont victimes de phishing […] Les utilisateurs devraient envisager d'activer l'authentification à double facteur qui est la véritable mise à jour de sécurité […] »*, a prévenu Satnam Narang

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

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-au-phishing-sur-linkedin-59912.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Par Dominique Filippone

Le fichage des passagers heurte les libertés individuelles



Le fichage des passagers heurte les libertés individuelles – Politis

Ce procédé de récupération de données personnelles par le biais des compagnies aériennes était, jusqu'à présent, rejeté par le Parlement européen, pour incompatibilité avec la Charte européenne des droits fondamentaux.

Dimanche 11 janvier, réunion de crise à Paris. Bernard Cazeneuve a réuni ses homologues européens pour évoquer les attentats qui ont frappé la capitale quelques jours auparavant. Le but : prendre des mesures pour renforcer la lutte contre le terrorisme. Très vite, le Passenger Name Record (PNR) se retrouve sur les lèvres des politiques et s'affirme comme étant une des réponses à apporter pour renforcer la lutte anti-terroriste.

L'idée est reprise officiellement mardi à la tribune de l'Assemblée nationale par Manuel Valls. Le Premier ministre, s'engage à la mettre en place en France rapidement et y « appelle, de manière solennelle, (…) le Parlement européen à prendre enfin, toute la mesure de ces enjeux et à adopter ce dispositif, comme nous le demandons depuis deux ans ». Ainsi, la France réclame que le Parlement européen « débloque » le PNR afin qu'il puisse entrer en vigueur sur tout le territoire européen.
Qu'est-ce que le PNR ? Il s'agit en fait des données personnelles concernant un passager d'une compagnie aérienne. Ces données regroupent, d'après le texte officiel, les dates du voyage, l'itinéraire, les informations figurant sur le billet, les coordonnées du passager, le nom de l'agent de voyage auprès duquel le vol a été réservé, le moyen de paiement utilisé, le numéro du siège et des données relatives aux bagages.

La récupération de ces données constitue un manquement certain à la protection de la vie privée et des données personnelles. La conservation des données, leurs potentielles transmission à d'autres organes que les départements de sécurité et enfin, l'incompatibilité globale du PNR avec la Charte européenne des droits fondamentaux ont amenés le Parlement européen à rejeter la plupart des textes de type PNR.

Car le débat n'est pas nouveau. A Strasbourg, plusieurs projets de PNR ont déjà été présentés depuis une dizaine d'année. En 2004, c'était avec les États-Unis qu'il était question de créer une base de données sur les passagers.
Le texte avait était rejeté par la Cour de justice de l'Union européenne, non parce qu'il constituait une violation de la législation européenne, mais pour vice de forme. Un projet de loi similaire est à nouveau présenté au Parlement en 2011. A ce moment, et contrairement à 2004, un avis positif du Parlement est impératif pour que ce texte soit voté. A la surprise générale, il est adopté. C'est la commission des libertés civiques qui rejette finalement la directive PNR en 2013. L'année suivante, en novembre 2014, le Parlement demande que le PNR avec le Canada soit examiné par la Cour de justice européenne.
Les PNR étaient donc rejetés…jusqu'à la semaine dernière, où devant les drames qui touchèrent la capitale française, les autorités réactivent le projet. Pourtant, d'après le G29, un groupe de travail représentants les autorités indépendantes de protection des données nationales, les USA, un pays qui pratique le PNR, « n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité ». En effet, selon Claudine Guerrier, enseignante-chercheuse en droit à l'institut des Mines Télécom, le PNR n'aurait réussi à faire intercepter que deux terroristes en dix ans.
Alors si le PNR est d'une efficacité relative, et si, comme le dit le contrôleur européen des données, Peter Hustinx, le PNR est contraire aux droits fondamentaux de l'UE, pourquoi les politiques insistent-ils aussi lourdement pour que le Parlement européen l'adopte ?
« Il faut qu'ils disent à l'opinion public qu'ils sont efficace », explique la députée européenne Front de gauche Marie-Christine Vergiat. « La question n'est pas d'être pour ou contre le terrorisme, la question est de ne pas se servir de ce prétexte pour mettre en place une surveillance généralisée. Ne pas agir au mépris des libertés publiques. »
Claudine Guerrier partage l'analyse : « C'est une mesure de facilité. Elle ne pose pas de problèmes de mise en place sur le plan juridique. Elle est quasiment prête, il n'y a qu'à prendre pour base les textes des précédents PNR qui n'ont pas aboutis. »
Mais si le Parlement européen tient bon depuis une dizaine d'années, cette fois, Marie-Christine Vergiat craint que « sous la pression de l'actualité et des Etats membres, certains eurodéputés ne changent d'avis à l'Assemblée ». Le PNR sera à l'ordre du jour du Conseil européen consacré en février à la lutte contre le terrorisme. Quoi qu'il arrive, Manuel Valls a de son côté annoncé que « la plate-forme de contrôle française sera opérationnelle dès septembre 2015 ».
Par Marie Roy

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

Source : http://www.politis.fr/PNR-Le-fichage-des-passagers,29704.html

---

FIC 2015 : Les cybergendarmes garants de la confiance

numérique

FIC 2015 : Les cybergendarmes garants de la confiance numériqueInformatique

5 jours avant l'ouverture du Forum International de la Cybersécurité, nous avons pu rencontrer les forces de gendarmerie à la pointe de la lutte contre la cybercriminalité.

Juste avant la septième édition du FIC (les 20 et 21 janvier 2015 au Grand Palais de Lille), nous avons pu rencontrer le jeudi 8 janvier les organisateurs du salon et les équipes de cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N).
L'occasion de faire un premier point sur les principaux enjeux de cette manifestation dédiée à la cybersécurité et les menaces les plus inquiétantes pour les entreprises comme les citoyens. Comme nous l'a expliqué le général (2s) Marc Watin-Augouard, fondateur du FIC, « cette 7e édition du FIC, lancé en 2007, attend plus de 4 000 personnes françaises et étrangères. 3 000 inscrits aujourd'hui, dont 800 utilisateurs dans les entreprises (RSSI, risques manager, directeurs juridiques…), 800 offreurs, 800 institutionnels, 300 personnes du monde académique, et 400 étrangers (britanniques, allemands…). […]
Si la dimension business du salon s'affirme, trois lignes de force sont attendues sur le salon :
• l'innovation dans les technologies de sécurité et de confiance numérique,
• les données
• la place de l'humain dans la cybersécurité ».
Comme tous les ans plusieurs ateliers seront bien sûr organisés avec notamment une démonstration technique de Thales sur une simulation de cyberattaques, et des challenges techniques avec l'Epita et Sogeti.

Le colonel Mathieu Frustié, commandant la section de recherches (SR) de Paris avec 2 de ses experts en cybercriminalité, le capitaine Gwénaël Rouillec et le major Etienne Neff.
Et comme tous les ans les politiques seront de la partie avec Bernard Cazeneuve (le ministre de l'Intérieur), Thomas de Mezière (le ministre allemand de l'Intérieur), Jean-Yves Le Drian (le ministre de la Défense) et Axelle Lemaire (secrétaire d'Etat chargé du Numérique). Rappelons enfin que le FIC est organisé par la Gendarmerie Nationale, Euratechnologies et le CEIS avec le soutien financé de la Région Nord-Pas de Calais.
Au C3N, la Gendarmerie est bien entrée dans le 21 siècle. Cette journée porte ouverte à la cybergendarmerie a également été l'occasion de parler de l'affaire Charlie Hebdo, et notamment des outils employés pour analyser les forums Internet et les réseaux sociaux. L'équipe du colonel Eric Freyssinet, responsable du C3N, utilise l'outil OsincLab développé avec Thales pour détecter et suivre des communautés et des utilisateurs afin de dresser une véritable cartographie de leurs relations (amis sur les réseaux sociaux, gens parlant de la même chose…). Suite à l'attentat contre Charlie Hebdo, de nombreux tweets manifestaient par exemple leur satisfaction #bienfaitpourcharlie. Le travail de la brigade consiste avant tout à comprendre ce qui se passe et traquer toutes les expressions d'incitation à la haine raciale. Les auteurs pouvant éventuellement être poursuivis si la Justice se saisit de l'affaire. Une équipe place Beauvau, le SRTI, effectue également une surveillance des groupuscules et identitaires sur Internet, tout comme la DGSI (Direction générale de la sécurité intérieure) qui possède des équipes spécifiques pour suivre les activistes sur les réseaux publics ou souterrains.

Le colonel Eric Freyssinet, responsable du C3N de Rosny sous Bois qui déménagera à Pontoise en juin prochain.

Nous reviendrons la semaine prochaine sur le travail de ces supergendarmes numériques qui réalisent un travail éprouvant pour anticiper les menaces, sensibiliser les entreprises et les collectivités et très souvent assurer la répression dans les affaires d'extorsion, de vols et de pédophilie. 1800 gendarmes N-Tech, c'est à dire formés aux techniques d'investigation numériques, couvrent le territoire français et collaborent avec les services de police judiciaire et de gendarmerie. A Rosny sous Bois par exemple, deux drones saisis dans le cadre d'une retentissante affaire de survols sont actuellement analysés par le laboratoire technique afin de déterminer leurs plans de vol. Nous ne pouvons pas en dire plus…


Les drones saisis dans une affaire de survol sont étudiés par les experts du C3N.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-fic-2015-les-cybergendarmes-garants-de-la-confiance-numerique-59858.html
Par Serge Leblal

La traque de la gendarmerie sur Internet

	La traque de la gendarmerie sur Internet

Au lendemain de l'attaque de Charlie Hebdo, la presse informatique spécialisée était invitée par la gendarmerie pour mieux faire connaître ses outils et ses équipes dédiées à la lutte anticriminelle dans le Cyber espace.

Programmée de longue date, la visite des services de gendarmerie, et la rencontre avec les équipes en charge de la traque informatique, le 8 janvier, préparait le grand rendez-vous annuel de la cyber criminalité des 20 et 21 janvier, le FIC, qui s'ouvrira en effet à Lille.
La gendarmerie française en est l'un des promoteurs avec Euratechnologies et la compagnie européenne d'intelligence stratégique (CEIS), l'organisation ayant le soutien économique de la Région Nord-Pas de Calais.
Le Général Marc Watin-Augouard, l'un des créateurs du FIC (Forum International de la Cybercriminalité) se réjouissait d'ailleurs de la venue de spécialistes étrangers de nombreuses polices et de plusieurs membres des différentes cellules de recherches du cyber espace parmi les 4000 visiteurs attendus. Pour sa 7eme édition, ce sont 40 ateliers durant les deux journées du FIC qui permettront de mesurer les dernières évolutions de la lutte contre la criminalité informatique. Outre Bernard Cazeneuve, notre ministre de l'Intérieur, celui de l'Allemagne Thomas de Mezière et Jean-Yves Le Drian, notre ministre de la Défense, devraient détailler les ambitions d'un « Shengen du numérique ». Axelle Lemaire, la secrétaire d'Etat chargée du Numérique devrait relancer une fois de plus la filière française sécurité qui progresse doucement. Le premier Ministre, Manuel Walls, non confirmé, pourrait venir appuyer ses ministres dans cette période de crise.
Le Lieutenant-colonel Freyssinet, chef de la division cybercriminalité de la gendarmerie, précisait ce jeudi-là, les différentes opérations menées pour réduire les risques liés aux attentats: « Dés hier après midi, nous nous sommes mis en mode de surveillance pour identifier les réactions favorables aux attentats et créer une base réduite d'individus à priori dangereux. C'est exactement ce que l'on fait dans la rue pour identifier les gens qui auraient un comportement inquiétant. On fait une nette différence entre une simple réaction épidermique et des appels à la violence.
L'équipe se sert d'un outil d'analyse statistique OsincLab développé avec Thales pour détecter et identifier des groupes de personnes parlant du même sujet. Interrogé sur les possibilités d'empêcher l'accès à des sites en langue française incitant au terrorisme, le Lieutenant-colonel Freyssinet nous a précisé : «Les sites dangereux sont protégés par des sites écrans et des sites relais. Ils sont abrités dans des pays qui n'ont pas les mêmes législations que nous. On ne peut se rendre sur certains sites à l'étranger, il faut des commissions rogatoires. On le pratique parfois dans le cadre de la recherche pédopornographique mais cela reste exceptionnel. La Convention de Budapest sur la cybercriminalité a permis d'avancer mais il n'existe pas encore pas de Schengen numérique ».

Un thème repris par le ministre de l'intérieur, dimanche, ce qui veut dire qu'il devrait y avoir à terme une homogénéisation des procédures. Bien que la recherche des tueurs des membres de Charlie Hebdo le mercredi 7 janvier, ait été confiée à la préfecture de police, la gendarmerie via le GIGN et le BRI étaient en première ligne. Tous ses services étaient, depuis la mise en place du plan Vigipirate, en alerte maximale. Le paroxysme a été atteint, le dimanche 11 janvier, avec la surveillance des différentes manifestations de soutien aux victimes du terrorisme.

Gérer les différentes crises du moment sans perdre de vue l'essentiel
Mais cette crise exceptionnelle n'a pas remis en cause les activités régulières et le travail de fond des services du centre de lutte contre les criminalités numériques surnommé le C3N. La surveillance, la lutte contre la vente de produits illicites (drogues, médicaments frauduleux, produits de contrefaçons) et l'espionnage industriel qui minent l'économie française constituant leur travail quotidien. Ce sont les sujets qui seront traités au FIC la semaine prochaine.
the-world-of-cybercrime-is-becoming-increasingly-dominated-by_16001213_800941061_0_0_14082810_300 La défense des sites d'entreprise et la lutte contre les attaques à leurs présidents, qui ont connu une croissance exceptionnelle, sont le principal souci actuel. Identifiées par un travail d'ingénierie sociale incroyable les cibles des voleurs montrent que leur savoir faire ne fait que s'accroître. Les 1800 gendarmes N-Tech, dont plus de 250 à Paris, c'est à dire formés aux techniques d'investigation numériques, sont encore en nombre insuffisant pour couvrir tout le territoire français. Le N-tech est un enquêteur spécialisé dans le domaine des nouvelles technologies et de la cybercriminalité. Ils collaborent avec les services de police judiciaire et de gendarmerie. Le BRI comprend par exemple 253 spécialistes Ntech, 1540 correspondants et 37 Antech, des spécialistes ultra pointus

Des équipements récents
Parmi les nombreux équipements présentés lors de la visite des locaux de la gendarmerie, les UFED (Universal Forensics Extraction Device) sont des outils d'intervention rapides. Ces extracteurs de données (photo)UFED2 sont destinés à « faire parler » les téléphones mobiles, découverts sur des sites de crimes ou sur des personnes soupçonnées de malversations. Ils permettent de lire tous les éléments contenus dans de stockage : les contacts, l'historique des appels, les données de réseaux sociaux, les vidéos, les textes, les photos, etc. Des dizaines d'interfaces pour différents types (Android, Windows phone, IOS, et bien d'autres) et des centaines d'autres interfaces sont utilisées pour des connections modèles d'appareils mobiles.
Le même type d'appareil existe pour extraire les données des PC ou tablettes sans jamais modifier les contenus, un impératif pour le bon fonctionnement de la justice.
Pour les appareils endommagés, l'INL, le département informatique et électronique est capable d'extraire les données de n'importe quel support de stockage. Qu'il s'agisse de puces de circuits abimés au cours d'incendies ou d'immersions prolongées. Les analyses permettent, par exemple, de connaître grâce aux informations issues des GPS, la trajectoire des personnes et des véhicules mis en cause.

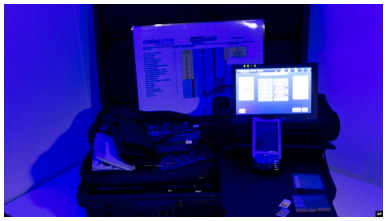
Au centre national d'analyse des images de pédopornographie
Le service d'analyse qui fonctionne en continu 24/24 avec trois officiers suit les activités sur le net de plusieurs centaines de personnes et tente, dés que c'est possible d'identifier les victimes et contrevenants. Interrogé sur place l'un des trois officiers qui tenait a rester anonyme nous confiait : « L'essentiel des images et des vidéos qui sont saisies proviennent de pays étrangers. Mais il reste une petite production en France. C'est en particulier favorisé par la multiplication de caméras et des smartphones. Au-delà des personnes, on cherche souvent à localiser les lieux et les dates de prises de vues, ce qui permet d'identifier par exemple les lieux privilégiés du tourisme sexuel. C'est possible grâce à de nombreux outils d'analyses utilisés par l'ensemble des services liés à Interpol qui maintient un fichier des personnes inculpées. On est parfois face à des situations difficiles où par exemple dans une vidéo un père est en train de prendre son bain avec ses enfants qui jouent et ce document est utilisé dans le cadre d'une procédure de divorce pour prouver que le père a des attitudes incestueuses. »
Confrontés à des images parfois intolérables, ces gendarmes sont accompagnés psychologiquement. « On peut changer de services si l'on n'en peut plus. Pour moi, cela fait plus de 5 ans et l'on se soutient. C'est important d'être au sein d'une équipe qui vous écoute.»
Une réflexion qui montre que le travail des forces comme celles des médecins urgentistes d'ailleurs est difficile. L'accumulation des tragédies quotidiennes éprouve, même s'ils s'en défendent, les nerfs des personnes qui vont au secours des autres.

Internet qui est au coeur de la crise actuelle favorise-t-il les crimes en tous genres ?
Que dire des télévisions qui à longueur d'années progamment des films policiers et des reportages sur de crimes violents. La TV, Internet, les jeux vidéos ultra réalistes en banalisant « l'ultra violence « sont devenus une véritable école du crime. Les jeunes désoeuvrés, souvent à la recherche d'une identité valorisante, peuvent facilement endosser les costumes de « rebelles vengeurs ».
Les évènements récents mettent en lumière la prise de conscience collective et les nouvelles mesures qui seront prises pour limiter les impacts de la « jungle » du net devraient simplifier au moins le travail des enquêteurs. Mais si l'on peut réduire les effets du mal, l'analyse des causes des différentes ruptures de notre société doit rester le sujet principal du travail des politiques.

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

Source : http://www.informatiquenews.fr/cybercriminalite-traque-gendarmerie-internet-28190

Les particuliers, pierre angulaire de la lutte contre la cybercriminalité



Les particuliers, pierre angulaire de la lutte contre la cybercriminalité

En fin de compte, constate Mary Galligan des services de cybersécurité de la société Deloitte, c'est aux particuliers d'assumer leurs responsabilités.

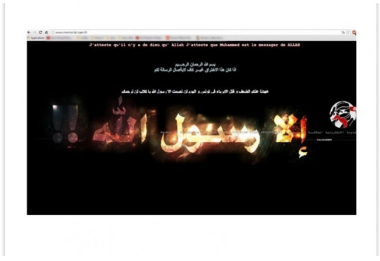
La cybercriminalité est partout, ont constaté les participants. Même le Pentagone en fait les frais puisque lundi, les comptes Twiter et YouTube du Commandement Central (CENTCOM) ont été piratés. Comment mieux se protéger ? Souvent, fait valoir l'expert Austin Berglas, qui travaille pour le FBI, un employé tout à fait innocent prend une décision fatale.
« Peu importe combien d'argent une organisation consacre à la cyber-sécurité ; c'est encore et toujours un employé, ou le dernier utilisateur de l'ordinateur, qui clique sur un lien malveillant » explique Austin Berglas.
Malheureusement, il n'en faut pas beaucoup pour sombrer dans la cybercriminalité : un serveur, qu'on peut louer, un code malicieux, qu'on distribue par e-mail – et voilà, le cybercriminel prend le contrôle de votre ordinateur.
En fin de compte, constate Mary Galligan des services de cybersécurité de Deloitte, c'est aux particuliers d'assumer leurs responsabilités.
« Nous devons commencer à réfléchir à ce que faisons-nous pour protéger nos informations. Nous nous attendons à ce que les milieux d'affaire fassent le nécessaire pour nous, mais nous ne sommes pas disposés à prendre les mesures de sécurité les plus simples », constate Mme Galligan. Pour commencer, il faut que les usagers comprennent que rien n'est secret sur le web, et qu'ils prennent des mesures en conséquence.

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

Source : http://www.lavoixdelamerique.com/content/les-particuliers-pierre-angulaire-de-la-lutte-contre-la-cybercriminalite/2596924.html

---

Charlie Hebdo : Des cyberpirates musulmans répondent aux Anonymous



Charlie Hebdo : Des cyberpirates musulmans répondent aux AnonymousInformatique

Quelques jours après le tragique attentat de Charlie Hebdo et celui qui a frappé la supérette casher de la porte de Vincennes, les Anonymous ont débuté un combat contre les sites d'entreprises et d'organisations en lien avec ces attaques terroristes. Des cyberpirates musulmans, regroupés sous l'étendard de la Middle East Cyber Army, ont quant à eux entrepris des actions pour montrer que l'Islam n'est pas synonyme de terrorisme, tout en envisageant une attaque massive le 15 janvier…

La France vit en ce moment des heures très sombres mais elle se relève. Après le tragique attentat de mercredi dernier à Charlie Hebdo qui a coûté la vie à 12 personnes, mais également celui qui a frappé une supérette casher porte de Vincennes, les Français ont défilé en masse dimanche pour défendre la liberté avec plus de 3 millions de personnes dans les rues. Depuis mercredi dernier, on a toutefois vu se multiplier des actions de piratage, émanant de groupes islamistes – ou se revendiquant comme tels – mais également des Anonymous et de cyber-hackers musulmans.
Des centaines de sites d'organisations publiques et privées (des sites de l'Université Paris Sud, Memorial de Caen, Palais des papes, plus de 200 médiathèques, la Fondation Jacques Chirac, les communes de Goussainville, Ézanville, Jouy-le-Moutier…) ont par exemple été piratés. Sur le site du Memorial de Caen, la page d'accueil a été altérée par la « Fallaga Team », affichant un message en arabe, traduit par France 3 Basse-Normandie, sur fond noir.
Face à ces opérations, le collectif des Anonymous, regroupé pour l'occasion sous le hashtag #OpCharlieHebdo, s'est élevé et a publié une vidéo en ligne dans laquelle il expose un message très clair : « Le 7 janvier 2015, la liberté d'expression a été meurtrie […] Il est de notre devoir de réagir. Charlie-Hebdo, une figure historique du journalisme satirique a été pris pour cible par des lâches. Anonymous a toujours combattu pour la liberté d'expression et la liberté de la presse. Nous ne renoncerons pas. Attaquer la liberté d'expression, c'est attaquer Anonymous. Nous ne le permettrons pas. Toutes entreprises et organisations en lien avec ces attaques terroristes doivent s'attendre à une réaction massive d'Anonymous. Nous vous traquerons. Nous vous trouverons et nous ne lâcherons rien. »

Des sites de Carrefour et de BNP Paribas piratés
Les Anonymous ont ainsi commencé leur riposte samedi 10 janvier avec l'altération de plusieurs sites radicaux dont celui du djihadiste français Ansar-alhaqq.net qui pointe toujours ce lundi après-midi vers le moteur de recherche DuckDuckGo. Mais les Anonymous ne comptent pas en rester là. Au-delà de leurs opérations classiques d'altération de sites ou d'attaques DDoS pour saturer les sites, le collectif prévoit aussi d'en extraire des bases de données d'adresses et de contacts pour les transmettre aux forces de l'ordre.
Depuis hier, on a par ailleurs vu fleurir des attaques de sites revendiquées par différents pirates (AnaCoNdA, kh.mar.404, RebelGhost DX, Scream4.0.4, Silent Killer, Hamooda El Bess…) regroupés derrière le groupe MECA pour Middle East Cyber Army. Objectif, selon son porte-parole interrogé par nos confrères de Zataz, « prouver au monde que l'Islam n'est pas synonyme de terrorisme. Un musulman n'est pas un terroriste. C'est exactement l'inverse de l'Islam. Notre religion est paisible, toute personne qui a lu le Coran comprend cela. » Un postulat qui n'empêche pas cependant ce groupe de mener des actions sur les sites de la filiale géorgienne de Carrefour, de Terraillon, du Centre National de Ressources Biologiques Marines et de plusieurs filiales étrangères de Peugeot mais également de l'espace Cash Management de BNP Paribas, pour lequel ce groupe indique être en possession de « toute la base de données ».
Le 15 janvier, MECA ainsi que plusieurs autres groupes annoncent une attaque massive : « Nous avons déjà piraté des milliers de sites, mais ce qui va venir le 15 janvier sera beaucoup, beaucoup plus important ».

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

Source : http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-des-cyberpirates-musulmans-repondent-aux-anonymous-59874.html
Par Dominique Filippone

Comme les États-Unis en 2001, ira-t-on vers un « Patriot Act » ?

Comme les États-Unis en 2001, ira-t-on vers un « Patriot Act » ?

Les communications téléphoniques et sur Internet sont des vecteurs parfois utilisés par les terroristes. Après l'attentat de la semaine dernière, la France pose la question du renforcement de la surveillance.

Sous l'émotion des attentats du 11 septembre 2001 aux États-Unis, l'administration Bush avait adopté, sept semaines plus tard, une loi d'exception. Elle renforçait les pouvoirs du FBI, de la CIA et de la fameuse NSA, afin de lutter plus efficacement contre le terrorisme. Prévue, initialement, pour une durée de quatre ans, elle fut reconduite plusieurs fois. En 2015, le « Patriot Act » existe encore, et pourrait faire un émule en France.
Après l'attentat du 7 janvier contre Charlie Hebdo et les assassinats qui ont suivi, la classe politique française commence à formuler des propositions en ce sens. L'une des personnalités les plus unanimes sur le sujet est sans doute Valérie Pécresse, ministre UMP de l'Enseignement supérieur de 2007 à 2011. Sur Twitter, elle écrit ce lundi : « Il faudra bien entendu un Patriot Act à la française. Il faut une réponse ferme et globale ».

« Des mesures à prendre sur le Net »
En matière de renseignement, la surveillance des communications joue un rôle central. Alors que le suivi des frères Kouachi, suspectés d'avoir perpétré la tuerie à Charlie Hebdo, aurait connu un arrêt durant l'année 2014, le Premier ministre, Manuel Valls, considère qu'il y a une « faille » et appelle à « travailler à de nouveaux dispositifs pour être encore plus efficace ». Il suppose que des mesures seront prises pour combattre la diffusion de messages de « haine » sur Internet. « Il y a des mesures à prendre en plus sur le Net, car cela a un effet de contamination, de mimétisme », ajoute le ministre des Affaires étrangères, Laurent Fabius.

Des prises de position rejointes par l'opposition
L'ancien chef de l'Etat, Nicolas Sarkozy, s'exprimant au sujet d'Internet, a demandé à « surveiller ce qu'il s'y passe ». « Ce n'est pas parce que c'est virtuel que l'on peut s'exonérer des règles que l'on a mis plusieurs siècles à établir », a-t-il poursuivi. Si les débats ont commencé cette semaine au niveau politique, ces pistes sécuritaires ont suscité des réactions sur les réseaux sociaux.

Un Patriot Act « serait un comble »
« Après 4 millions de Français dans la rue aux cris de « liberté ! », on parle de PATRIOT Act à la française », dénonce par exemple « Maitre Eolas » sur Twitter. « Se réjouir de l'émergence d'un « Patriot Act à la française », c'est avaliser une altération programmée de la démocratie », estime pour sa part l'entrepreneur Gilles Babinet. Le blogueur Olivier Laurelli de rappeler que le Patriot Act tel que conçu aux Etats-Unis ne se limite pas à la surveillance des communications et qu'« on va pouvoir avoir un Guantanamo à la française ».
Interrogé par Petit Web, Benoit Thieulin, le président du Conseil national du numérique, estime que « ce serait un comble, après s'être opposé à la guerre en Irak et les révélations d'Edward Snowden » et souligne qu'Amedy Coulibaly, un des tueurs présumés, « ne disposait plus de smartphone depuis quelques temps déjà, afin d'éviter d'être tracé ». Mais au-delà de l'écoute des télécommunications, se pose enfin la question des prises de parole publiques sur les réseaux sociaux, telles que celle du polémiste Dieudonné ce lundi.
Sur sa page Facebook, il a affirmé se sentir « Charlie Coulibaly », détournant le slogan « Je suis Charlie » et l'associant au nom du tueur présumé. « Il ne faut pas confondre la liberté d'opinion avec l'antisémitisme, le racisme, le négationnisme », a aussitôt répliqué Manuel Valls à Dieudonné, au sujet duquel une enquête a été ouverte pour apologie d'actes de terrorisme. Bref, le débat sur le rôle d'Internet est loin d'être terminé.

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

Source : http://pro.clubic.com/legislation-loi-internet/actualite-749325-patriot-act-france.html
Par Thomas Pontiroli

Antiterrorisme : les Fournisseurs d’Accès à Internet devraient travailler plus étroitement avec le gouvernement

	Antiterrorisme : les Fournisseurs d’Accès à Internet devraient travailler plus étroitement avec le gouvernement

Les attentats perpétrés en France, la semaine dernière contre Charlie Hebdo, et à Montrouge, pourraient poser quelques questions sur le niveau de sécurité dans l'Union européenne, ainsi que sur les moyens des services de renseignement. Les FAI pourraient prochainement devoir se rapprocher davantage des gouvernements.

« Je suis fermement convaincu que le moment est venu pour l'UE de s'unir dans une action commune et cohérente contre le terrorisme ». Tels sont les propos de Rihards Kozlovskis, ministre letton de l'Intérieur, qui a représenté la présidence du Conseil de l'Union européenne à la réunion ministérielle internationale qui s'est tenue hier.

Les ministres d'Intérieur de la France, de l'Allemagne, de l'Autriche, de la Belgique, de l'Italie, des Pays-Bas, de la Pologne, du Royaume-Uni, de la Suède, de l'Espagne et du Danemark ont publié une déclaration (PDF) conjointe condamnant les actions terroristes contre le journal français Charlie Hedbo et les assassinats commis à Montrouge et Vincennes. Ensemble, ils souhaitent également affermir leur lutte globale contre la radicalisation.

Internet jouant un rôle majeur dans le déploiement de la propagande terroriste, il s'agira de l'une des pistes de réflexion privilégiée pour renforcer les mesures de sécurité. Les ministres expliquent ainsi :

« Préoccupés par l'utilisation d'Internet à des fins de haine et de violence, nous sommes déterminés à ce que cet espace ne soit pas perverti à ces fins, tout en garantissant qu'il reste, dans le strict respect des libertés fondamentales, un lieu de libre expression, respectant pleinement la loi ».

Pour ce faire, les gouvernements entendent accroître leurs travaux avec les fournisseurs d'accès à Internet pour renforcer leurs dispositifs de surveillance :

« Dans cette perspective, le partenariat avec les grands opérateurs de l'Internet est indispensable pour créer les conditions d'un signalement rapide des contenus incitant à la haine et à la terreur, ainsi que de leur retrait, lorsque cela est approprié et/ou possible. »

Depuis des années, les grandes sociétés de la Toile française ont été sensibilisées à la lutte contre l'antisémitisme. L'on se souvient notamment que l'Amicale des déportés d'Auschwitz et des camps de Haute-Silésie, le Consistoire israélite de France, et le MRAP (Mouvement contre le racisme et pour l'amitié entre les peuples) avaient déposé une plainte contre Yahoo! en 2000 pour avoir permis la vente d'objets nazis sur ses pages Internet.

Le contenu de cette déclaration commune commence à créer une certaine polémique : plusieurs internautes sur Twitter (via le hashtag #CharlieDoesSurf) soulignent le caractère contradictoire des marches républicaines pour la liberté d'expression avec des mesures de surveillance accrues pour un meilleur contrôle du Web qui se profilent à l'horizon.

Reste à connaître la nature de ces mesures qui seront décidées entre les États membres de l'Union européenne pour renforcer la vigilance des FAI, mais également des autres acteurs majeurs de la Toile.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://pro.clubic.com/technologie-et-politique/actualite-749239-terrorisme-fai-devront-renforcer-vigilence-collaborer-gouvernement.html
Par Guillaume Belfiore