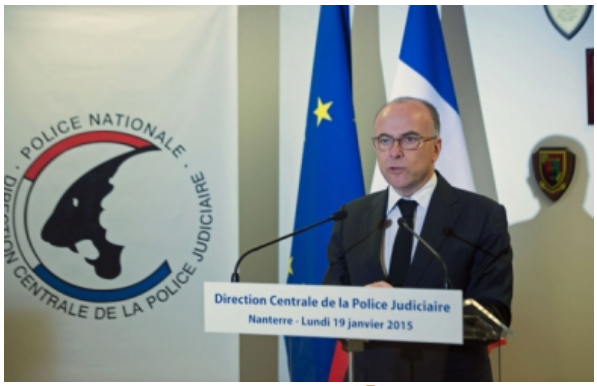
1.300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve



1,300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve

Lors d’une visite à la sous-direction de lutte contre la cybercriminalité de la police judiciaire (PJ) française à Nanterre (Hauts-de-Seine), Bernard Cazeneuve a annoncé lundi que « plus de 1.300 attaques ont été revendiquées par des équipes (de) hackers se revendiquant d’organisations islamistes » radicales. Le ministre de l’Intérieur a également indiqué que plus de 25.000 sites français avaient été piratés.

La plateforme gouvernementale nationale Pharos, où sont signalés en France les contenus illicites liés à Internet, « a traité plus de 25.000 signalements de contenus illicites sur le net », a en effet déclaré Bernard Cazeneuve, évoquant des « cyberattaques malveillantes » sur des sites institutionnels et privés. Des « contact privilégiés » ont été noués avec Facebook, Dailymotion ou Google et des « demandes de retraits en ligne » ont eu lieu par exemple de sites ou vidéos « liés aux attaques terroristes ».

Des propositions mercredi

« La puissance publique doit prendre des initiatives et affirmer sa puissance pour protéger les internautes » face aux « menaces », a réaffirmé le locataire de la place Beauvau, « dans le respect des libertés publiques ».

Mercredi, à l’issue du Conseil des ministres, des mesures antiterroristes seront présentées par le gouvernement dont certaines visant Internet, a réaffirmé Bernard Cazeneuve. La semaine dernière, Manuel Valls lui avait demandé des propositions « dans les huit jours » concernant le contrôle d’Internet. « Elles devront concerner (…) les réseaux sociaux, plus que jamais utilisés pour l’embrigadement, la mise en contact et l’acquisition de techniques permettant de passer à l’acte », précisait alors le Premier ministre.

D’ici là, Bernard Cazeneuve se rend mardi à Lille pour le Forum international « sur la cybersécurité » en compagnie de son homologue allemand, Thomas de Maizière.

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

Source : http://www.lejdd.fr/Medias/Internet/1-300-cyberattaques-au-nom-d-organisations-islamistes-radicales-annonce-Bernard-Cazeneuve-713734

Faut-il craindre une cyberguerre ?

Faut-il craindre une cyberguerre ?

Leurs PC sont leurs armes et leur guerre se mène en ligne. Après les attentats à Paris, des cyberattaques ont été menées contre des sites internet français, par des hackers affirmant agir au nom du groupe Etat islamique (EI). Dans le même temps, des « hacktivistes » se revendiquant d'Anonymous ont piraté des sites et comptes sur les réseaux sociaux des organisations islamistes et de leurs membres.

Mais c'est loin d'être terminé. Des comptes YouTube et Twitter appartenant au commandement militaire américain au Moyen-Orient (Centcom) ont également été visés, et une attaque d'envergure est annoncée pour jeudi 15 janvier. Sommes-nous à l'aube d'une cyberguerre ? Non, toujours pas, répond Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).

Francetv info : Peut-on parler de cyberguerre lorsque l'on évoque les attaques informatiques menées par des hackers qui se revendiquent du jihad ?
Gérôme Billois : Non, on n'y est pas du tout. Ce serait exagéré de parler de « guerre ». Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruption de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel.

Alors comment pourrait-on appeler cela ?
Il n'existe pas vraiment de mot pour déterminer ces actes. Après l'attaque contre la société Sony Pictures, qui a subi une destruction massive de son système d'information et le vol d'une importante quantité de données, Barack Obama parlé de cybervandalisme. Le terme semble assez juste. Ce qui se passe aujourd'hui, c'est comme si des activistes entraient dans des centaines de boutiques pour y coller leurs affiches et repartir. Les propriétaires de ces magasins n'avaient pas bien fermé la porte en partant et en revenant le lendemain matin, ils trouvent des affiches qui font la publicité de l'Etat islamique.

Pour vous, ces actions restent plutôt d'ordre symbolique ?
Extrêmement symbolique, puisqu'il s'agit d'une lutte entre deux idéologies. Avec d'un côté l'#opFrance (pour « Opération France », lancée par des cyberjihadistes), annoncée pour le 15 janvier, qui vise à tenir l'image de la France en attaquant un grand nombre de structures dans l'Hexagone, et de l'autre l'#opCharlieHebdo, qui vise à dénoncer et rendre indisponibles des sites jihadistes.

Qui se trouve derrière cette contre-attaque ? Certains revendiquent leur appartenance aux Anonymous…
On ne peut pas dire qu'il s'agit « des » Anonymous. Ce sont, en fait, des groupes très divers. Il faut d'ailleurs savoir que certains des groupes qui attaquent la France aujourd'hui ont pu participer à des opérations des Anonymous, ou s'en revendiquer. Il y a des acteurs en commun, qui œuvraient auparavant dans une même direction et se divisent aujourd'hui sur ce cas particulier. La logique de « l'hacktivisme » au sens large c'est : « Il se passe un événement, je me positionne par rapport à celui-ci et à chaque nouvel événement je redéfinis ma doctrine ».

Quelle est la force de frappe des cyberjihadistes aujourd'hui ?
Aujourd'hui, ils mènent des attaques de faible intensité. Sur une échelle de 1 à 10, ils atteignent 5, au maximum. Ces pirates utilisent des vulnérabilités connues depuis longtemps ainsi que des outils disponibles facilement sur internet. De plus, ils s'attaquent à des sites peu sécurisés et pas mis à jour. Il existe tout de même un risque à moyen terme. Ces groupes de pirates, petit à petit, vont apprendre, se développer, et augmenter ainsi leurs capacités d'attaque pour viser des services plus importants. On sait que l'EI dispose d'importants moyens financiers. Il n'aura, de toutes façons, pas de problème de matériel : avec un simple PC, vous pouvez lancer des attaques.

Qu'est-ce qui pourrait rendre ces groupes plus dangereux ?
Pour eux, il s'agit d'abord de gagner en expérience. Mais ils peuvent aussi acheter ce qu'on appelle des « vulnérabilités zero day », c'est-à-dire des connaissances sur une vulnérabilité qui n'est pas encore connue des éditeurs de sécurité. Quand vous possédez cet atout, vous pouvez attaquer un système, même s'il est mis à jour. Pour poursuivre l'analogie des boutiques vandalisées : imaginons que quelqu'un, comme un chercheur, découvre que pour la marque de serrure XYZ il existe un pass universel. Avec cette information, il peut faire deux choses : soit prévenir le fabricant de la serrure pour qu'il corrige son produit, soit vendre cette vulnérabilité à des criminels sur le marché noir.

Les pirates ont donc toujours un temps d'avance sur les systèmes de sécurité…
Oui et non. Une partie des pirates, les plus pointus, certains groupes de cybercriminels, peuvent aller jusqu'à dédier une partie de leurs moyens à faire de la recherche en attaques et trouver ces « vulnérabilités zero day ». Ces groupes-là, oui, peuvent avoir cette capacité. Il peut s'agir soit d'Etats un peu belliqueux, soit de cybercriminels pointus. Mais il n'y en a pas des milliers. Dans le cas qui nous intéresse, les pirates n'ont pas cette avance. Ils utilisent simplement des failles connues, dont certaines ont été rendues publiques depuis 2012. Or, nous sommes en 2015 et les systèmes qu'ils attaquent n'ont pas été corrigés. On parle de petites mairies, d'universités, de PME… Ces structures-là n'ont pas forcément l'expertise ni les moyens pour maintenir leurs systèmes à jour.

D'autres structures, susceptibles de devenir des cibles plus importantes comme les grandes banques françaises par exemple, sont-elles mieux protégées ?
Oui, les systèmes sensibles sont mieux protégés. Les grandes sociétés ont les capacités nécessaires pour investir dans la sécurité. Les banques en ligne, par exemple, réalisent quotidiennement, voire plus encore, des tests de vulnérabilité automatisés, qui mènent les mêmes actions que les pirates. Les résultats de ces tests remontent aux services de sécurité informatique qui peuvent très rapidement effectuer les mises à jour nécessaires. Ce qui n'empêche qu'un site d'une grande banque est tombé, pendant une des attaques. Mais il s'agissait d'un site satellite sur lequel il n'y avait aucune transaction financière.

Là, nous parlons de sites internet. Qu'en est-il des systèmes informatiques internes ?
Ces systèmes-là disposent d'un niveau de sécurité, a priori, plus fort. Ne peuvent y rentrer que des employés ou des collaborateurs connus. Soit parce qu'il existe une protection physique : il faut entrer dans le bâtiment de la société. Soit parce qu'il y a des mots de passe ou des cartes à puce pour accéder à distance aux données. On n'est pas pour autant à l'abri d'une attaque visant le système d'information interne. C'est ce qui est arrivé chez Sony. Le FBI l'a dit : 90% des sociétés américaines seraient tombées si elles avaient été confrontées à la même méthode de piratage. C'est énorme.

Donc la menace existe…
Oui. La vraie question est de savoir si les jihadistes passeraient à ce type d'actions. Leur logique, pour l'instant, est plutôt de faire du bruit, de multiplier les cibles, de casser des milliers de sites, pour pouvoir dire mille fois qu'ils l'ont fait. Une attaque plus poussée, qui ferait plus de mal, aurait peut-être moins de résonance médiatique.

C'est tout de même une menace prise au sérieux, sur laquelle l'Otan se penche sérieusement. Est-ce à cause des menaces de ces jihadistes ?
Pas seulement. On distingue trois grandes « familles d'attaquants » : les « hacktivistes », qui attaquent par idéologie comme les cyberjihadistes, les cybercriminels, qui volent des données pour les monnayer, et enfin les Etats, qui développent des capacités défensives et offensives. Mais on peut craindre des regroupements entre ces groupes. Dans l'exemple de Sony, l'attaque est attribuée à la Corée du Nord, mais on sait qu'elle aurait été appuyée par des groupes d' »hacktivistes ».

Comment les Etats se préparent-ils face à cette menace ?
La cyberdéfense ne se résume pas à créer des murs en attendant que des pirates tentent de les casser. Cela inclut aussi des techniques de contre-attaque, pour pouvoir neutraliser les attaquants. Tous les Etats s'y préparent. Pour ce qui est de mener des attaques, on peut estimer que tous les pays industrialisés ont déjà des moyens et les renforcent au quotidien.

Concrètement, en quoi consiste la contre-attaque face à des cyberjihadistes ?
Les moyens de contre-attaque sont quasiment les mêmes que les moyens d'attaque. On peut imaginer attaquer leurs systèmes, les rendre inopérants, capturer les données pour bien comprendre qui ils sont. On peut aussi « boucher leurs tuyaux » pour éviter que les attaques ne passent.
Mais la difficulté, dans ce domaine, est de bien savoir qui se trouve en face de nous. Dans le cas Sony, on lit que l'attaque serait partie d'un hôtel en Thaïlande. A mon avis, elle est passée par là, mais ce n'est pas son point de départ. J'ai déjà vu des attaques menées contre certains de mes clients provenir de serveurs d'écoles maternelles au Vietnam. On se doute bien que ce n'est pas un écolier vietnamien qui l'a lancée, qu'il s'agit simplement de brouiller les pistes. Dans des scénarios plus vicieux, il peut s'agir de faire croire que l'attaque vient d'un endroit en particulier, pour provoquer une contre-attaque sur cette cible. Si l'on n'attribue pas l'attaque au bon responsable, on risque d'infliger des sanctions à un leurre.

Quand vous parlez de « boucher les tuyaux », s'agit-il d'attaques par déni de service, méthode qu'utilisent justement certains hackers ?
Cette méthode-là n'est efficace que temporairement, pour freiner une attaque. Mais les Etats ont la possibilité, à distance, de faire tomber les réseaux, de les couper, plutôt que de les boucher. Je parle bien des Etats, car les entreprises privées n'ont pas le droit de contre-attaquer. La légitime défense n'existe pas dans le cyberespace. En France, le seul cadre légal aujourd'hui, c'est la loi de programmation militaire, qui donne cette capacité à l'Agence nationale de sécurité des systèmes d'information (Anssi) ou, en tout cas, aux services rattachés au Premier ministre.

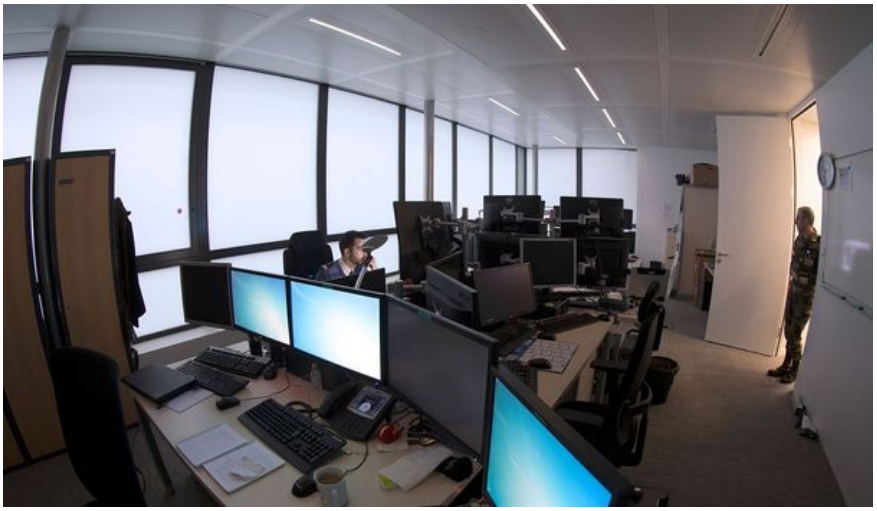
Manuel Valls va annoncer une série de mesures, dont certaines concernent internet. Où placer le curseur, entre la neutralité de net, le verrouillage pour empêcher les cyberjihadistes de nuire et la protection de la vie privée ?
C'est une question idéologique fondamentale, mais on n'y trouvera pas de réponse parfaite. Ce qui est certain, c'est qu'il y a une menace, qui, il faut le préciser, représente une très faible portion des usages d'internet. L'énorme majorité des usages sont très bénéfiques, pour l'économie, la culture, notre quotidien. Le plus important, selon moi, c'est le contrôle des moyens qu'on se donne. Il faut, certes, pouvoir être très réactif, car les attaques peuvent être menées très vite, mais il faut se contrôler pour éviter de tomber dans la surveillance généralisée. Ce contrôle peut être exercé par la justice ou des autorités indépendantes.

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

Source : http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyberguerre_796909.html

---

Cyberdéfense: la guerre de demain a déjà commencé



Cyberdéfense: la guerre de demain a déjà commencé

Paris – A l'heure des cyberattaques en série, notamment après les dernières caricatures du prophète Mahomet, le Calid, « gendarme » des systèmes informatiques de l'armée française, est sur le pied de guerre, derrière la façade discrète d'un immeuble parisien.

Installé devant un rideau d'écrans, un cybersoldat en treillis scrute attentivement les informations qui défilent. Soudain une mention « SUSPICIOUS » (suspect) se détache en rouge sur l'un des ordinateurs.
« J'ai relevé une alerte sur un site, un utilisateur qui essaie d'aller sur un serveur cloud », lâche le sous-officier qui, avec une trentaine d'autres militaires, surveille 24 heures sur 24 les réseaux du ministère de la Défense, à l'affût du moindre intrus mal ou très mal intentionné.
« Ce qu'on cherche à détecter, c'est un pic de réseau anormal, un trafic important de messagerie. On dispose pour cela de +capteurs+ sur les entrées vers nos réseaux, les postes de travail », explique le cybersoldat, qui préfère garder l'anonymat.
Et les ennemis invisibles ne manquent pas. Le 6 janvier, le site du ministère a été piraté par le groupe Anonymous. Ces derniers jours, l'armée a été la cible d'une dizaine de cyberattaques visant notamment des régiments. Le 12 janvier encore, des pirates se réclamant de l'organisation Etat islamique (EI) prenaient brièvement le contrôle des comptes Twitter et Youtube du commandement militaire américain au Moyen-Orient (Centcom).
« Les gens de Daech (acronyme de l'EI en arabe) ont de l'argent, recrutent des informaticiens. Ils manquent peut-être de réseaux de renseignement sur les cibles mais sont capables assez rapidement de bloquer des sites », relève le vice-amiral Arnaud Coustillière, responsable Cyberdéfense à l'état-major des armées.
« C'est de la gesticulation. Mais dans la guerre de l'image, ce peut être très intéressant », ajoute ce spécialiste. Les jihadistes n'ont pas en revanche les moyens, selon lui, de mener des attaques d'envergure.
Le Calid (Centre d'analyse de lutte informatique défensive) surveille aussi les cyberattaques qui peuvent paralyser des systèmes d'armes ou détourner de l'information sur les moyens et les cibles des forces. Il envoie pour cela des équipes au coeur des théâtres d'opération.
Car plus que les attaques de sites internet, voilà bien le véritable cauchemar des états-majors: que des missiles soient stoppés net dans leur course, des drones, piratés, des frégates, détournées à distance au beau milieu d'une intervention militaire.

– 'Dans la peau de l'attaquant' –
En Afrique, l'opération antijihadiste française Barkhane a ainsi été la cible d'une tentative d'attaque cyber, confie-t-on au ministère de la Défense. « Cela peut se faire à partir d'un ordinateur et d'un téléphone ».
Depuis longtemps déjà, James Bond fait des émules. Lors du raid israélien contre de présumées installations nucléaires syriennes en 2007, une attaque numérique a ainsi trompé les défenses adverses en renvoyant une image radar tronquée.
Dans l'affaire Stuxnet, un ver informatique, espionnant et reprogrammant des automates industriels, s'est attaqué aux centrifugeuses iraniennes soupçonnées de faire de l'enrichissement d'uranium à des fins militaires.
Les systèmes sont d'autant plus vulnérables qu'ils sont de plus en plus interconnectés. Sur un navire, navigation, propulsion, combat et communications sont intégrés. Faute de sécurisation, il sera bientôt possible de bloquer le bateau en pleine mer ou de l'empêcher de combattre.
Derrière le Calid, des dizaines de chercheurs de la Direction générale de l'armement (DGA) s'emploient à anticiper cette cyberguerre de demain.
« On se met dans la peau de l'attaquant et on voit quelles attaques on peut mener sur nos propres systèmes d'armes pour voir quelles menaces sont crédibles », raconte Frédéric Valette, chef du pôle sécurité des systèmes d'information à la DGA.
Face à une menace de plus en plus pressante, la France s'est dotée d'un budget cyberdéfense d'un milliard d'euros sur la durée de la loi de programmation militaire (2014-2019). Le Calid doit doubler de taille dans les cinq ans à venir et 400 spécialistes être recrutés.
La France reste loin derrière les Etats-Unis, la Chine et Israël, à un niveau comparable avec la Grande-Bretagne ou la Russie, selon le ministère de la Défense.
« L'idée c'est d'arriver à un niveau de sécurité suffisant. Il n'y a pas de sécurité absolue. Il faut savoir anticiper, mettre en place des niveaux de protection adaptés et être capables de réagir en cas d'attaque », résume M. Valette.

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

Source : http://www.lexpress.fr/actualites/1/societe/cyberdefense-la-guerre-de-demain-a-deja-commence_1642214.html

Thierry Mandon veut entamer la transformation numérique de l’Etat

Thierry Mandon veut entamer la transformation numérique de l’Etat

Le secrétaire d'État à la Réforme de l'État et à la Simplification, annonce un vaste plan pour accélérer la transformation digitale de l'Etat. Elle passe par plus d'open data, la mise en place de plusieurs projets numériques ou encore la création de « correspondants digitaux » dans les administrations.

2015 sera probablement l'année de grands changements en terme de « numérisation » de l'Etat. Déjà l'année dernière, le gouvernement avait annoncé plusieurs projets concernant le numérique. Nous pensons par exemple à la réorganisation des infrastructures, à la création d'un service interministériel créé par la DISIC ou encore au programme « Dites-le nous une seule fois ». Rappelons également qu'en décembre dernier, Axelle Lemaire avait quant à elle confirmé le lancement « début 2015 » de l'Agence Française du Numérique. Plus globalement, le rapport Lemoine rendu en novembre 2014 donnait lui aussi de nombreuses pistes de réflexion « pour adapter l'économie française à la transformation numérique ».
Les pistes sont donc nombreuses mais le secrétaire d'État à la Réforme de l'État et à la Simplification Thierry Mandon a donné plus de détails sur les chantiers à venir cette année. Le premier « paquet » concerne l'open data avec 4 mesures concrètes :
• L'ouverture des données en « open data » deviendra la « règle générale »
• L'utilisation sera gratuite
• L'utilisation de ces données sera également « conforme aux règles européennes pour certaines redevances »
• De nouveau pouvoirs seront données à l'administrateur général des données pour notamment régler les éventuels « conflits entre administrations »

Transformation numérique et correspondants digitaux
Thierry Mandon veut surtout accélérer la transformation numérique de l'Etat ; un thème qui concerne également les entreprises privés. « Il y a une nécessité de révolutionner le management du changement dans l'Etat », explique-t-il. Car selon lui, la « culture digitale est insuffisamment partagée et comprise dans les administrations » et cela doit entraîner un « programme massif de diffusion de la culture digitale » dans l'Etat.


Thierry Mandon, lors du débat d'orientation pour la stratégie numérique de la France

S'il faut attendre la concrétisation de tous ces projets, il faut d'abord saluer la prise de conscience du secrétaire d'État, qui est déjà en soi une première étape importante à franchir. D'ailleurs, il se livre à une analyse intéressante : « La révolution numérique implique de grands changements pour les grandes entreprises et les grandes administrations. Elles sont encore organisées de manière hiérarchique, autoritaire, quand le numérique impose une vraie démocratisation et des mises en place de politiques publiques, déhiérarchisées. Les grandes organisations ont et auront à piloter cette transformation qui sera longue ».
Pour diffuser cette « culture digitale », Thierry Mandon annonce également la création d'un nouveau statut, celui des « correspondants digitaux ». Ils auront la responsabilité de définir « la mise en œuvre des politiques numériques et de faire l'interface avec les usagers ».

En phase avec le président du Syntec Numérique


Interrogé récemment par nos soins, le président du Syntec Numérique Guy Mamou-Mani saluait « l'excellente orientation prise par Thierry Mandon ». Toutefois, il est aussi amer et critique sur l'usage qui est fait des outils numériques. « L'application de paiement des impôts en ligne est superbe, mais utilisée par 1/3 des foyers fiscaux français. Tout comme MonServicePublic est un outil génial mais sous utilisé. Pourquoi ? », s'interrogeait-il, rappelant que la France est « un pays extraordinaire » en la matière. En 2015, il attend le déploiement de tous ces projets et surtout « un Etat plus léger, moins cher et plus efficace ».

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

Source : http://www.linformaticien.com/actualites/id/35431/thierry-mandon-veut-entamer-la-transformation-numerique-de-l-etat.aspx
par Emilien Ercolani

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

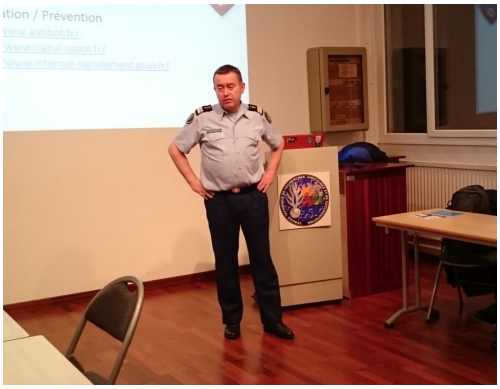
FIC 2015 : Les cybergendarmes garants de la confiance numérique

	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.

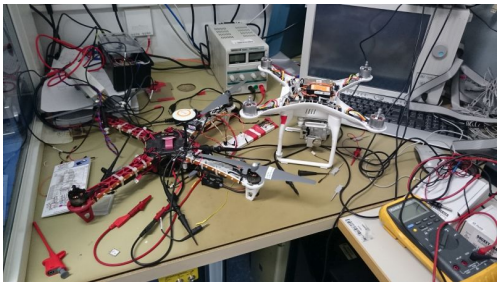
Juste avant la septième édition du FIC (les 20 et 21 janvier 2015 au Grand Palais de Lille), nous avons pu rencontrer le jeudi 8 janvier les organisateurs du salon et les équipes de cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N).
L'occasion 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.

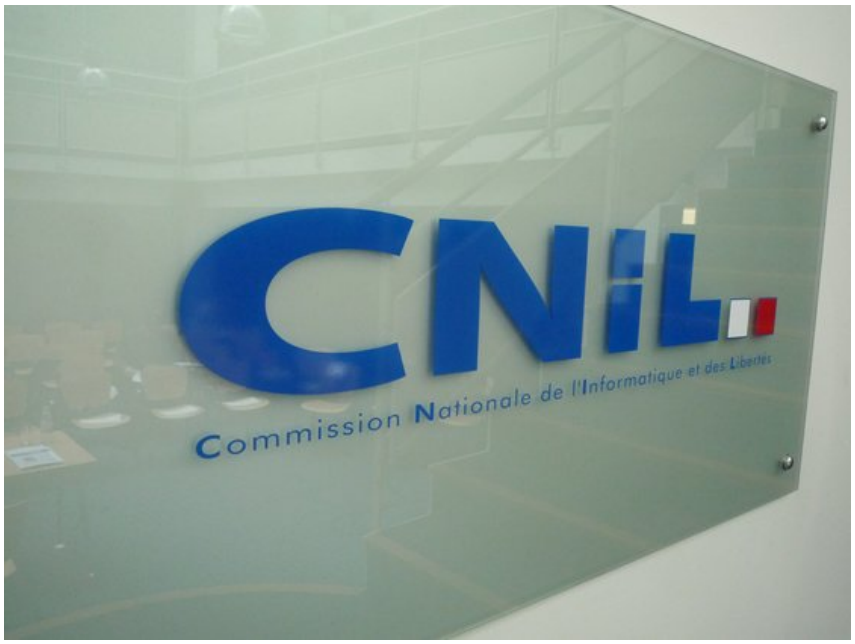
Nous reviendrons la semaine prochaine sur le travail de ces supergendarmes numériques qui réalisent un travail éprouvant pour anticiper les menaces, sensibiliser les entreprises et les collectivités et très souvent assurer la répression dans les affaires d'extorsion, de vols et de pédophilie. 1800 gendarmes 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 Cnil lance un nouveau label sur la gestion des données



La Cnil lance un nouveau label sur la gestion des données

Face à la prolifération des données qu'une entreprise a à gérer et à la complexité réglementaire qui l'accompagne, la Cnil lance un nouveau label visant à prouver la conformité de sa gouvernance.

Garantir à ses clients que l'on est conforme aux bonnes pratiques de la Cnil en matière de gestion des données personnelles, c'est l'objet de ce nouveau label « Gouvernance Informatique et Libertés » dévoilé par la Commission. Après les labels « formation », « procédure d'audit » et « coffre-fort numérique », la Cnil veut maintenant donner au Correspondant Informatique et Libertés (Cil) un autre moyen d'améliorer la gestion.
Pour rappel, le Cil est depuis 2005 la personne intermédiaire entre une entreprise et la Cnil. Du coup, ce nouveau référentiel s'adressera forcément aux organisations possédant un tel référent (plus de 10 000 à ce jour). La création de ce nouveau label est partie du constat du régulateur que les entreprises et organismes publics avaient de plus en plus besoin « d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles ». Pour y prétendre, 25 exigences (.rtf) ont été définies par la Cnil.
Celles-ci sont organisées en trois thématiques : l'organisation interne liée à la protection des données, la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et la gestion des réclamations et incidents. Pour le régulateur, ce label témoignera « de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable » et constituera donc un atour pour ses clients.

Tous les organismes, publics ou privés ayant désigné un correspondant informatique et libertés peuvent prétendre à ce label.
Téléchargez le dossier de candidature
Une fois complété, envoyez le dossier
soit par le biais du formulaire de dépôt en ligne
soit par courrier postal (CNIL, 8 rue Vivienne, CS30223, 75083 paris Cedex 02)

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

Source : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-749887-cnil-gestion-donnees-personnelles-entreprise.html

L’attaque DDoS sur PSN et Xbox Live s’est appuyée sur… des routeurs domestiques

L’attaque DDoS sur PSN et Xbox Live s’est appuyée sur… des routeurs domestiques

Pour réaliser leurs attaques, les pirates de Lizard Squad ont créé un botnet qui s’appuie en majorité sur des modem-routeurs hackés. Leur malware a exploité une faille dans la configuration du système d’exploitation Linux.

Fin décembre dernier, les pirates de Lizard Squad ont mis en ligne un service DDoS payant appelé « Lizard Stresser ». Disponible à partir de 5,99 dollars/mois, cet « outil » avait fait ses preuves quelques jours auparavant, en mettant à genoux les réseaux de Playstation Network et Xbox Live. Mais où ces pirates ont-ils trouvé leur puissance de feu ? Principalement dans les petits routeurs domestiques, révèle ainsi KrebsOnSecurity.com.
Avec l’aide de quelques chercheurs en sécurité, le site spécialisé a réussi à mettre la main sur le malware qui a permis de construire le botnet de « Lizard Stresser ». Le logiciel malveillant exploite ainsi une faille de sécurité dans Linux pour prendre le contrôle d’objets connectés, et se diffuse de proche en proche comme un ver.
Après analyse, il s’avère que les routeurs domestiques sont très largement surreprésentés dans ce botnet, sans doute en raison de leur nombre et de leur faible niveau de protection. En effet, l’un des vecteurs d’infection du malware est d’utiliser les identifiants par défauts de ces équipements grand public, tels que « admin/admin » ou « root/12345 » !

Lizard Squad a également piraté le cloud de Google

Cette découverte montre – une fois de plus – qu’il est important de bien configurer et protéger tous ses équipements informatiques, et pas uniquement ses ordinateurs. Selon une récente analyse de l’éditeur Avast, plus de la moitié des modem-routeurs en France ont conservé leur configuration d’origine, et sont donc potentiellement vulnérables. D’ailleurs, se retrouver avec un modem-routeur zombie fait encore partie des choses les moins désagréables. D’autres pirates utilisent des équipements pour réaliser des attaques par détournement DNS, ce qui permet de quantité de données sensibles : mots de passe, informations bancaires, etc.
Mais Lizard Squad ne s’attaque pas seulement aux pauvres particuliers, mais visent également les géants du web. Selon KrebsOnSecurity, les pirates reptiliens ont utilisés des numéros de carte bancaire volés pour créer, fin décembre dernier, des milliers de serveurs virtuels sur le cloud de Google (« Google Compute Engine »). Cette fois, en revanche, le but n’était pas de faire des attaques DDoS, mais de créer des relais Tor. Ce qui a beaucoup énervé les développeurs de ce service d’anonymisation, car cet ajout massif avait pour effet de le fragiliser. Heureusement, Google a rapidement remarqué le subterfuge.

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

Source : http://www.01net.com/editorial/640591/l-attaque-ddos-sur-psn-et-xbox-live-s-est-appuyee-sur-des-routeurs-domestiques/
Par Gilbert Kallenborn

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

Les entreprises françaises sont de plus en plus victimes de hackers et d’espions industriels

Les entreprises françaises sont de plus en plus victimes de hackers et d’espions industriels

Devant un environnement économique de plus en plus concurrentiel et incertain, les formations spécialisées en sécurité des entreprises tardent à se développer en France.

Les entreprises françaises sont de plus en plus victimes de hackers et d'espions industriels. Le nombre d'entreprises concerné par ces piratages s'élève à 360. 300 millions d'euros c'est ce qu'ont coûté ces attaques par les gangs internationaux sur les trois dernières années. Face à ces menaces, la Direction Centrale de la Police Judiciaire (DCPJ) et le Medef vont sceller un accord pour résorber le phénomène, mercredi 14 janvier 2015. L'Office central pour la répression de la grande délinquance financière (OCRGDF) a quant à lui officialisé un accord signé avec l'Ecole des ingénieurs de numérique pour lutter contre « le fléau des escroqueries aux faux virements ».
L'Epita (l'école des ingénieurs du numérique) est aujourd'hui, un des rares établissements français à proposer un enseignement qui se focalise sur la sécurité des entreprises. « Aujourd'hui, il manque une vraie filière qui aille du niveau bac +1 à bac +5 » d'après Olivier Hassid interrogé par Le Figaro, dirigeant du Club des Directeurs de Sécurité et de Sureté des Entreprises (CDSE). D'après ses dires, la pluralité des matières permet de créer une filière avec des acquis enseignés en licence. La France montre un réel retard concernant les formations sur la sécurité des entreprises.

Les grandes écoles intéressées par ce domaine de sécurité
Deux raisons à ce retard, d'une part le manque de prise en compte des enjeux qui est dû à l'insuffisance de la recherche, et d'autre part le manque de besoin exprimé par les entreprises. « Les problématiques de sécurité ont réellement vu le jour dans années 2006/2007. C'est à ce moment là qu'un certain nombre de grands groupe ont créé des directions en sûreté et sécurité », explique Olivier Hassid.
« Les balbutiements de la formation en sécurité datent des années 90 avec la création de l'IHESI, aujourd'hui devenu l'Institut national des hautes études de la sécurité et de la justice (INHESJ) » raconte le dirigeant du Club. L'INHESJ est la véritable première formation française en matière de sécurité. En plus des formations de l'INHESJ, on retrouve aujourd'hui en France un Master en Gestion globale des risques et des crises à l'université Paris 1, une licence en sécurité à l'université Paris Descartes et, depuis quelques temps, un certificat du management de la sécurité et de la sûreté informatique, avec l'école Epita qui valide la qualité de la formation.
Mais selon Oliver Hassid, le développement des formations spécialisées en sécurité des entreprises doit être impératif pour peut-être un jour arriver à un cursus complet. Il indique que « Les instituts d'études politiques s'intéressent à ces problématiques, tout comme les écoles de commerces. Il y a une vraie tendance avec l'effet Snowden et les inquiétudes concernant le cyberespace. »

Vers un rapprochement de la sécurité et l'intelligence économique
Au vu du développement de l'enjeu sécuritaire, la notion d'intelligence économique s'est développée en France. Le concept a émergé dans la seconde partie des années 90, immédiatement, contrairement à la sécurité des entreprises, des formations ont été créées. Christian Harbulot crée en 1997 l'école de guerre économique (EGE), et d'autres également à cette période comme l'Ecole Européenne d'Intelligence Economique (EEIE). Aujourd'hui ce genre de formations est aussi retrouvé dans les grandes écoles de commerce et d'ingénieurs mais aussi à l'université.
Selon Christian Harbulot, le directeur de l'EGE, et Olivier Hassid, on se dirige vers le rapprochement de ces deux pôles stratégiques des entreprises car leur rapport à l'information est similaire. Ainsi, les futures formations devraient joindre les deux domaines à l'avenir.
Il y a bon nombre d'enjeux et les fraudes sont de plus en plus sophistiquées. La criminalité via les réseaux est en expansion, les risques géopolitiques et la sécurité des entreprises à l'international peuvent augmenter dans un contexte encore plus instable.

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

Source : http://www.digischool.fr/enseignement/securite-entreprise-vraie-filiere-peine-mettre-place-france-25849.php
Par Manare BARCHI