Le site de l’Afnic visé par une attaque informatique DDoS

Le site de l’Afnic visé par une attaque informatique DDoS

Le site de l’Afnic était indisponible plusieurs heures dans la journée d’hier. Une maintenance préventive, alors que l’association chargée de la gestion du .fr subissait une attaque Ddos un peu plus sérieuse que d’habitude.

Le Ddos est la nouvelle tendance de ce début d’année 2015. Enfin, le défacage de sites fait également un retour en force mais depuis le début de l’année, les attaques de déni de service se succèdent et se ressemblent un peu. L’Afnic n’y a pas échappé : hier à la mi-journée, le site web de l’association Française pour le nommage Internet en coopération était inaccessible.
Une maintenance provoquée par une attaque Ddos comme l’explique l’Afnic sur son site : plusieurs services ont été interrompus brièvement, il était par exemple devenu impossible d’enregistrer des noms de domaines en .fr sur le site de l’Afnic dans le courant de l’après midi et les services tels que le whois étaient inaccessibles. La résolution DNS en revanche n’a pas été affectée, ce qui limite fortement la visibilité de l’attaque au grand public. Les perturbations sur les autres services du site se sont poursuivies tout au long de la journée avant un retour à la normale dans la soirée.
Interrogé par nos confrères de Next Inpact, Pierre Bonis directeur adjoint de l’Afnic est revenu sur l’attaque « Nous avons régulièrement des attaques DdoS, mais celle-ci nous est parue plus importante. Elle a fait tomber un de nos pares-feu » explique-t-il dans leurs colonnes. Face à l’ampleur de l’attaque, le directeur adjoint explique que l’Afnic a préféré mettre son site web en maintenance afin de protéger le reste des services.
L’attaque n’a pour l’instant pas été revendiquée et les investigations et analyses sont encore en cours, l’Afnic ayant fait part de son souhait de porter plainte suite à cette attaque. Dans le contexte actuel, on serait tenté de faire le lien entre cette attaque et la récente vague d’attaques subie par les sites web français à la suite des attaques terroristes de début janvier mais pour l’instant aucun élément concret ne vient étayer cette hypothèse.

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

Source : http://www.zdnet.fr/actualites/ddos-le-site-de-l-afnic-vise-par-une-attaque-39813445.htm
Par Louis Adam

Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

	Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

S**ur demande du FBI, Microsoft a livré en un temps record des informations liées à des comptes de messagerie de suspects impliqués dans l'attentat de Charlie Hebdo. Une attitude qui remet sur le devant de la scène l'éternel débat entre protection des données personnelles et enjeux de sécurité.**

45 minutes. Tel a été le temps de réaction éclair de Microsoft pour transmettre au FBI des données liées à l'attentat qui a frappé Charlie Hebdo le 7 janvier dernier. Le journal économique Bloomberg explique ainsi que la firme de Redmond a répondu de façon hyper réactive à une requête du FBI réalisée dans le cadre de cette terrible affaire.

Brad Smith, avocat général de Microsoft, aimerait bien que sa société n'ait pas à jouer sur les deux tableaux en matière de vie privée et de sécurité. (crédit : D.R.)

« Il y a juste deux semaines, en pleine chasse aux suspects impliqués dans l'attaque de Charlie Hebdo, le gouvernement français a demandé à obtenir le contenu de mails de deux comptes clients détenus par Microsoft », a indiqué dans un discours à Bruxelles Brad Smith, l'avocat général de l'éditeur dont Bloomberg s'est fait écho. La firme de Redmond s'est ainsi montrée particulièrement coopérative en répondant à la demande du FBI de faire remonter le contenu des e-mails en question en tout juste 45 minutes.
Une réactivité dont n'a justement pas toujours fait preuve le même Microsoft pour fournir des informations, également liées à des mails et comptes de messagerie, à la justice américaine dans le cadre d'autres affaires comme celle, récente, relative à un trafic de drogue. La firme de Redmond ayant alors à l'époque tenu un discours qui tranche avec la réactivité dont elle a fait preuve pour répondre à la requête du FBI dans l'affaire Charlie Hebdo : « En vertu du 4e amendement de la constitution américaine, les utilisateurs ont le droit de garder leurs communications par courriel privées. Nous avons besoin que notre gouvernement respecte les protections constitutionnelles de vie privée et respecte les règles en matière de vie privée établies par la loi ».

Microsoft en aucun cas prêt à se substituer au législateur
Mais depuis les attentats qui ont marqué la France et leurs répercussions partout dans le monde, des voix politiques se sont élevées pour fendre l'armure de la vie privée au nom des enjeux de sécurité. Notamment celle du Premier Ministre de la Grande-Bretagne, David Cameron, qui a prôné pour un renforcement des pouvoirs des services de sécurité pour s'assurer que les terroristes n'utilisent pas Internet pour communiquer secrètement entre eux.
« Si les membres du gouvernement veulent déplacer le curseur entre sécurité et vie privée, la façon appropriée de le faire est de modifier la loi plutôt que de demander aux acteurs privés comme nous de le déplacer nous-mêmes », a déclaré Brad Smith. Une saillie qui ne va à coup sûr pas manquer de raviver l'éternel débat – et les polémiques – entre ardents défenseurs de la vie privée et militants d'une sécurité sans faille. Car si tout le monde est d'accord pour détecter et empêcher les terroristes d'agir, l'étendue et la puissance des moyens à mettre en oeuvre pour y parvenir est loin de faire l'unanimité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-microsoft-a-fourni-en-45mn-des-donnees-au-fbi-59995.html
par Dominique Filippone

Les services DDoS à la demande des pirates de Sony,

Lizard Squad, piratés

Les services DDoS à la demande des pirates de Sony, Lizard Squad, piratés

L’adage veut que les cordonniers soient toujours les plus mal chaussés. Le piratage de LizardStresser, le service de DDoS à la demande de Lizard Squad, tend à confirmer cette règle : le fichier contenant les identifiants et mots de passe des membres n’était même pas chiffré.

Petit retour en arrière. Nous sommes fin décembre, à quelques heures de Noël, et le groupe de pirates connu sous le nom de Lizard Squad se rappelle au bon souvenir de tout le monde en mettant le PlayStation Network et le Xbox Live hors ligne. Les conséquences s’étendent sur plusieurs jours et le collectif peut se réjouir : il a livré une démonstration très visible de la force de frappe de son réseau basé sur des routeurs piratés. Son service LizardStresser, qui propose de lancer des attaques DDoS à la demande, enregistre alors de nombreuses inscriptions.
Mais cette période faste n’a été que de courte durée. En effet, outre plusieurs arrestations, notamment outre-Manche, un autre pirate ou groupe de pirates s’en est pris au site hébergeant le service LizardStresser. Le service en lui-même est a priori intact, mais sa base de données incluant notamment les pseudonymes et mots de passe des membres est maintenant dans la nature. Or, de manière assez curieuse, Lizard Squad n’a pas jugé nécessaire de se protéger contre le piratage : ses fichiers sont stockés en clair.

Ceux-ci ayant rapidement été publiés, tout le monde a pu voir que les affaires marchaient plutôt bien. Au moment du piratage, LizardStresser comptait la bagatelle de 14 241 membres. Beaucoup, toutefois, n’étaient que des curieux. Comme le pointe KrebsonSecurity, ils n’étaient « que » quelques centaines à avoir alimenté leur compte dans le but de financer une attaque. En tout, Lizard Squad aurait perçu un peu plus de 11 000 $, versés en bitcoins.
Bien sûr, le collectif de pirates n’a que modérément apprécié de voir de ses précieuses données étalées sur la toile. Une copie des documents, en particulier, était disponible sur Mega. Le groupe ne s’est donc pas démonté et a formulé une requête au titre de la loi DMCA, qui protège le droit d’auteur en imposant aux hébergeurs de retirer les contenus publiés illégalement. Comble de l’absurde, celle-ci a été acceptée. De nombreuses copies, néanmoins, demeurent disponibles sur d’autres sites.

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

Source : http://www.lesnumeriques.com/lizard-squad-service-ddos-a-demande-pirate-n38817.html

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From: EU Counter-Terrorism Coordinator
To: Delegations
Subject: EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

La montée en puissance du terrorisme en Europe relance le débat sur le chiffrement des communications et la création de backdoors réservés aux forces de l’ordre européenne. Le coordinateur antiterrorisme de l’UE, Gilles de Kerchove, demande sans détour un accès aux clefs de chiffrement des géants de l’Internet.

Les géants de l’Internet vont-ils bientôt être obligés de partager leurs clés de chiffrement avec la police et les agences de renseignement européennes pour les aider à lutter contre le terrorisme ? C’est en tout cas une recommandation ferme de Gilles de Kerchove, le coordinateur antiterrorisme de l’Union Européenne. C’est une suggestion étonnante quand on se souvient que les entreprises comme Google ou Facebook ont commencé à chiffrer leurs communications pour lutter contre la curiosité des agences de renseignement chinoises mais aussi américaines, anglaises, allemandes, hollandaises et françaises comme l’ont indiqué les documents révélés par Edward Snowden.

L’association de protection des droits civils Statewatch
a divulgué un document rédigé par le coordinateur
antiterroriste Gilles de Kerchove.

Gilles de Kerchove suggère que la Commission européenne « devrait revoir ses règles pour obliger les entreprises de l’Internet et des télécommunications opérant dans l’UE à fournir … aux autorités nationales compétentes un accès à leurs communications [c’est à dire leurs clefs de chiffrement] », selon un document divulgué par l’association de protection des droits civils Statewatch. Dans ce document, M. de Kerchove expose ses vues sur les mesures anti-terrorisme à prendre dans l’UE en vue d’une réunion des ministres de la Justice et de l’Intérieur de l’UE à Riga, la semaine prochaine.

Des keyloggers pour suivre les échanges

Cette proposition est controversée parce que, comme le note le coordinateur, la généralisation du chiffrement pour les échanges sur Internet rend très difficile, voire impossible, les interceptions légales par les autorités nationales compétentes. Nous avons discuté de ces questions avec les cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N). Sans coopération des fournisseurs de services (Whatsapp, Skype ou encore iMessage), il est très difficile de lire les messages échangés. La solution la plus facile – pour les forces de l’ordre – est aujourd’hui l’installation d’un cheval de Troie ou keylogger (un enregistreur de frappes) sur les terminaux des suspects, smartphones, tablettes ou PC. Une opération toujours délicate puisqu’elle doit être effectuée à l’insu des utilisateurs.
« Whatsapp ou Viber commencent à être très utilisés par les criminels avec des mobiles jetables », nous avait confié le major Etienne Neff de la section de Paris. « Les criminels sont aujourd’hui plus sophistiqués et utilisent également des solutions payantes ». Les forces de l’ordre peuvent toujours accéder aux métadonnées fournies par les opérateurs mais il faut séparer le flux et le reconditionner pour le traiter.

Les entreprises également sous surveillance

L’appel à plus de surveillance des échanges sur Internet est revenu sur le devant de la scène en Europe suite aux assassinats perpétués dans les bureaux du magazine satirique Charlie Hebdo et à l’épicerie HyperCacher à Paris. Après les deux attentats, les ministres de la Justice et de l’Intérieur de l’UE avaient publié une déclaration commune dans laquelle ils soulignaient qu’il est essentiel « d’entretenir une étroite collaboration avec les FAI pour endiguer la propagande terroriste en ligne ».
Si la Commission a refusé de commenter les plans anti-chiffrement de M. de Kerchove, le document fuité contient des détails supplémentaires comme le contrôle du « chiffrement décentralisé » des entreprises. Cela pourrait être une référence au chiffrement de bout-en-bout utilisé par certaines entreprises sensibles pour verrouiller leurs communications.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-l-ue-doit-elle-obliger-les-geants-de-l-internet-a-ceder-leurs-cles-de-chiffrement-59993.html
Par Serge Leblal

Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteursNicolas Messayaz / Sipa Olivier Aballain

	Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteurs

Denis JACOPINI, expert judiciaire en informatique diplômé en Cybercriminalité, était présent ce mardi au 7eme Forum International de lutte contre la Cybercriminalité.

Le repérage et la traque des réseaux jihadistes sur internet sont au programme de Bernard Cazeneuve ce mardi: le ministre de l'Intérieur a ouvert à Lille le 7e Forum international de lutte contre la Cybercriminalité (FIC).
Le rendez-vous tombe à pic, puisque Manuel Valls lui-même a rappelé le 19 janvier sur i-Télé que «ce n'est pas dans les mosquées que ces recrutements [de djihadistes] s'organisent, c'est le plus souvent sur internet».
Après une rencontre avec le ministre de l'Intérieur allemand, Bernard Cazeneuve a prononcé un discours vers 10h au cours duquel il a annoncé le déblocage de 108 millions d'euros sur 3 ans pour développer les moyens des services de l'État pour l'enquête en matière de criminalité sur internet

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

Source : http://www.20minutes.fr/lille/1521015-20150120-direct-bernard-cazeneuve-forum-international-cybercriminalite
Par Olivier Abalain

Le Forum International de la Cybersécurité FIC 2015 en vidéo

Le Forum International de la Cybersécurité FIC 2015 en vidéo

« Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité »

Le ministre de l'Intérieur Bernard Cazeneuve a inauguré mardi matin le Forum international de cybersécurité à Lille. Le général Marc Watin-Augouard, fondateur du Forum FIC et directeur du CREOGN, a expliqué que « nous sommes tous les vecteurs de cyberattaques, soit directes, soit par rebonds. »

Source vidéo : « Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité

La cybersécurité au Grand Palais

Orange, cybersécurité et cyberdéfense

Le plateau TV pendant le Forum International de la Cybersécurité 2015 – FIC 2015
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://videos.tf1.fr/infos/2015/nous-sommes-tous-les-vecteurs-de-cyberattaques-pour-le-fondateur-8549855.html

---

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.

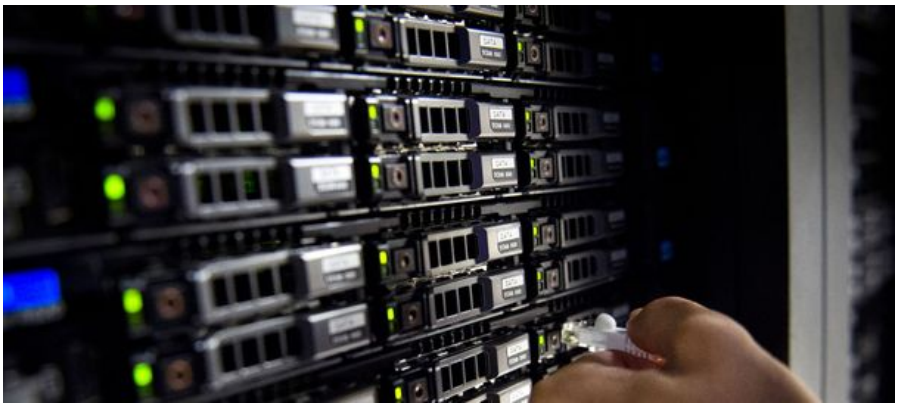
D'ici là, Bernard Cazeneuve se rend mardi à Lille pour le Forum international « sur la cybersécurité » en compagnie de son homologue allemand, Thomas de Maizière.

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

Trois contrats pour assurer

son informatique



Trois contrats pour assurer son informatique

En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel.

Qu'elle soit de production ou de gestion, l'informatique est présente dans chaque entreprise. Il est nécessaire de couvrir non seulement le matériel, mais également les données qu'elle contient. En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel : trois fois plus qu'en 2010 (2,2 milliards d'euros). En 2014, le coût par donnée piratée se chiffrerait à 351 euros contre 98 euros en 2010, selon les estimations de la société de sécurité informatique Symantec.
Aux traditionnels risques de dommages du matériel informatique et de responsabilité civile, s'ajoute depuis peu, la cybercriminalité. Le point sur les trois catégories de contrat que peut souscrire l'entreprise.
A noter : les contrats multirisques de matériels de bureaux peuvent couvrir les dommages informatiques. En revanche, la responsabilité civile comme la criminalité informatique font l'objet de contrats spécifiques, à souscrire séparément.

1. Dommages informatiques
Existant sur le marché français depuis une quinzaine d'années, l'assurance de dommages couvre le matériel informatique en cas d'incendie et de vol. L'assureur garantit essentiellement les frais de reconstitution des données et les coûts supplémentaires d'exploitation, en versant un capital à l'entreprise ayant subi un dommage. Traditionnellement, cette garantie faisait l'objet d'un contrat d'assurance « Tous Risques Informatiques ». Mais la tendance consiste à l'inclure dans le contrat « Multirisques Bureaux ».

2. Responsabilité civile
A ce stade, il faut distinguer la responsabilité civile d'exploitation, de la responsabilité professionnelle.
La responsabilité civile d'exploitation joue par exemple lorsqu'une entreprise transmet un virus informatique à un client.
La responsabilité civile professionnelle pour les mises en cause de l'entreprise au titre de ses prestations : conseils ou services. « Couvrant les dommages immatériels causés au cours d'une mission, la responsabilité civile professionnelle intéresse surtout les sociétés d'informatique », précise Benoît Salembier, à la tête du cabinet de courtage Add Value Assurances.

3. Criminalité informatique
Les compagnies d'assurance anglo-saxonnes ont une longueur d'avance sur leurs homologues européens. Les quelques acteurs en pointe sur les nouvelles technologies – Ace Europe, Hiscox, Beazley, Chartis, CNA – proposent un contrat ou garantie réduisant les risques de piratage et d'intrusion dans les systèmes d'information d'une entreprise.
Le contrat « Cybercriminalité » proposé par le courtier Add Value permet à l'entreprise de couvrir sa responsabilité et les dommages subis suite à une attaque informatique. « Les frais de restauration des données perdues constituent un vrai sujet. Les pertes de revenus ou d'exploitation consécutives à cette attaque sont également à prendre en compte. Quand on est une marque importante, il arrive que les hackers demandent une rançon à l'entreprise attaquée pour lui restituer les données », détaille Benoit Salembier.
Deux critères jouent sur le risque de criminalité. D'une part la taille de la base de données d'une entreprise : plus elle est grande, plus elle est exposée aux risques de piratage. D'autre part, la nature des données. Plus elles sont sensibles, plus elles sont exposées à la cybercriminalité. Ainsi par exemple les cabinets d'avocats, les experts comptables et même les journalistes seraient particulièrement visés.

Cybercriminalité : deux exemples de sinistres garantis
Avec le concours d'Add Value Assurances, voici deux cas de criminalité informatique réels avec les garanties que vous pouvez demander à votre assureur.
Exemple n°1. Piratage d'un site internet
Une société X crée un site e-commerce afin de vendre ses produits au grand public. Son succès attise la convoitise de ses concurrents. Des hackers réussissent à pirater son site et à le mettre hors service, ce qui signifie l'arrêt quasi complet de l'activité. En effet cette société commercialise ses produits à 75% sur internet.
L'assureur peut prendre en charge les frais engagés par les consultants mandatés pour identifier la faille de sécurité, et remettre le site web en état, à hauteur du plafond de garantie défini dans le contrat. De même, il indemnise l'entreprise de la perte de chiffre d'affaires sur la période d'arrêt du site internet, à hauteur du plafond de garantie défini dans le contrat.

Exemple n°2. Extorsion de données clients
Des hackers ont détourné une base de données clients d'une agence de voyage comprenant notamment leurs coordonnées bancaires. Ils demandent une rançon de quelques centaines de milliers d'euros euros à la direction pour la récupérer. Après deux semaines de négociation et le paiement de la rançon, l'entreprise piratée récupère sa base de données.
La base de données était assurée. L'assureur mandate ses consultants spécialisés pour accompagner l'assuré et mener à bien les négociations. Il indemnise l'entreprise assurée pour le paiement des honoraires des consultants et de la rançon, dans la limite des plafonds définis dans le contrat.
A noter. Avant de souscrire un contrat informatique, mieux vaut s'adresser à un expert qui déterminera votre exposition aux risques. En fonction de cela, votre intermédiaire d'assurance – courtier ou agent – évaluera le capital à assurer. Bien sûr, il faut être vigilant aux exclusions, c'est-à-dire les cas où l'assurance ne joue pas. Exemple : les dommages dus à une erreur de programmation sont généralement exclus. Et bien examiner les plafonds de garantie et les franchises

En savoir plus sur
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html

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

Source :
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html
Par Martine Denoune

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

L’équipe de la PLCC a épinglé récemment Dames Wamien Ahou Chantal et Oulobo Ahou Véronique, toutes deux caissières d’une maison de transfert d’argent de la place.
L’interpellation fait suite à l’exploitation d’une information anonyme selon laquelle ces dames se sont rendues complices d’un cybercriminel au fait de recevoir de ce dernier par SMS, des codes de transaction. Et ce, en vue de retirer des fonds. La contrepartie de ce concours frauduleux serait qu’elles prendraient 10% et expédieraient le reliquat au cybercriminel via orange money.

Après interrogatoire, les nommées WAMIEN AHOU CHANTAL ET OULOBO AHOU AHOU VERONIQUE ont reconnu sans ambage avoir rencontré un certain nommé GYPY ainsi que les faits qui leur sont reprochés.
De l’acte délictueux, elles ont avoué avoir retiré quatre (04) mandats Western-Union d’un montant total de 1 225 207 FCFA. De cette somme, elles ont également fait l’aveu d’avoir pris 106 000 FCFA et expédié le reste au cybercriminel par orange money.

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

Source : http://www.connectionivoirienne.net/106570/cote-divoire-cybercriminalite-deux-caissieres-dune-agence-western-union-epinglee

Sites d’info bloqués: La thèse de la cyberattaque écartée

Sites d’info bloqués: La thèse de la cyberattaque écartée

Ce n’est sans doute pas la grosse attaque promise par les hackers islamistes qui s’en prennent depuis une semaine au Web français, mais le timing interroge. De nombreux sites d’information, dont 20minutes.fr, ont été bloqués une heure et demie ce vendredi matin en raison d’un incident technique chez leur hébergeur Oxalide d’une ampleur a priori inédite.

France Inter, Le Parisien, Slate… et Sushi Shop

Les sites de 20 Minutes, L’Express, Mediapart, France Info, France Inter, Le Parisien, Slate, ZDNet ou encore Marianne, tous hébergés par Oxalide, sont devenus inaccessibles vers 10h. Des sites d’e-commerce, comme Sushi Shop, ont eux aussi été perturbés. Vers 11h30 certains sont redevenus accessibles. «Le niveau actuel d’information ne permet ni d’affirmer que la responsabilité d’Oxalide soit engagée, ni qu’il s’agisse d’un acte malveillant lié à l’actualité», affirmait l’hébergeur un peu avant 13h. Un peu plus tard, il tweetait: «Les premiers éléments en notre possession nous permettent d’écarter l’hypothèse d’une attaque externe de type DDoS.»

Même s’il semble dès lors écarté, le scénario d’une cyberattaque était considéré comme plausible en fin de matinée par les experts en sécurité informatique. «Toutes les caractéristiques techniques d’une attaque par déni de service (DDoS, lorsqu’un site est noyé sous les requêtes de connexion)» étaient réunies, selon Thierry Karsenti, directeur technique Europe de l’entreprise de sécurité informatique Checkpoint. «Il s’agit probablement d’une attaque DDoS», estimait auprès de 20 Minutes Olivier Hassid, directeur général du Club des directeurs de sécurité des entreprises. «Vu les cibles, on peut penser à une attaque virtuelle venant d’islamistes», renchérissait Eric Filiol, expert à l’École supérieure d’informatique, électronique, automatique.

Mercenaires en ligne

Pour Gérôme Billois, expert du cabinet Solucom, «si une attaque par déni de service menée dans le but de nuire à la liberté d’expression était confirmée, on ne serait plus sur du menu fretin.» Car jusqu’ici, les très nombreuses cibles touchées par les hackers tendance islamistes souffraient de failles faciles à identifier souvent causées par un simple défaut de mise à jour logicielle. S’en prendre à l’hébergeur de nombreux sites de presse dénoterait une montée en puissance, peut-être rendue possible grâce à l’achat des services de cybercriminels dotés de véritables moyens.

Car comme le rappellent Gérôme Billois et Eric Filiol, la cybercriminalité est un business en pleine expansion et les hackers s’achètent comme des mercenaires. «Il existe une grille tarifaire», explique Gérôme Billois. «Pour 200 dollars, des sites hébergés en Europe centrale proposent de louer à l’heure 1.000 machines infestées permettant de lancer une attaque DDoS», illustre Eric Filiol. Qu’elle ait lieu aujourd’hui ou plus tard, une attaque contre la presse française serait peut-être moins la preuve d’une montée en puissance des «cyberdjihadistes» que de leur volonté de mettre la main au portefeuille.

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

Source : http://www.20minutes.fr/high-tech/1518695-20150116-sites-info-bloques-incident-technique-attaque-informatique
Par Nicolas Bégasse et Romain Lescurieux