Effet Charlie : explosion des signalements d’apologie du terrorisme en ligne

Effet Charlie : explosion des signalements d’apologie du terrorisme en ligne

Après les attentats de Paris, la plateforme de la police Pharos a recueilli en un mois 40.000 signalements de contenus illicites en ligne. Même explosion auprès de la plateforme des fournisseurs d’accès et de services Internet, pourtant après une forte baisse en 2014.
La fusillade meurtrière ayant ciblé « Charlie Hebdo » le 7 janvier à Paris, suivi du meurtre de la policière à Montrouge et de la prise d’otages sanglante à l’Hyper Cacher de la porte de Vincennes, ont provoqué un sursaut mais aussi un déferlement de haine sur Internet. Les chiffres officiels sont impressionnants : la plateforme de la police Pharos, qui permet à tout internaute de signaler un contenu illicite en ligne (internet-signalement.gouv.fr), a enregistré une explosion des notifications dans la foulée des attentats, comme l’avait évoqué Bernard Cazeneuve, le ministre de l’Intérieur, courant janvier.
« En moyenne, nous traitons 400 signalements par jour. Les attentats se sont traduits par un afflux de signalements : dans la semaine de 7 au 17 janvier, nous avons recueilli 29.000 signalements pour l’essentiel d’apologie du terrorisme et d’incitation à la haine raciale » a expliqué mardi Valérie Maldonado, chef de l’office central de la lutte contre la cybercriminalité liée aux technologies de l’information et de la communication (OCLCTIC).

Twitter beaucoup plus utilisé que Facebook
La commissaire divisionnaire, qui est également sous-directeur adjoint de la lutte contre la cybercriminalité de la Direction centrale de la police judiciaire, a relevé que « les attentats dans la vie physique ont eu un prolongement sur Internet avec ces propos de soutien en ligne. Twitter a été extrêmement utilisé, la plateforme la plus utilisée dans ce cadre, beaucoup plus que Facebook »
Julien Gauthier, le chef de la plateforme Pharos, a précisé que le nombre de signalements reçus entre le 7 janvier et le 7 février avait même atteint 40.000 à comparer aux 140.000 recueillis sur l’ensemble de 2014 ! Soit plus du quart du volume annuel en un mois seulement.
Ils intervenaient dans le cadre d’une présentation d’un bilan de l’année 2014 sur la suppression des contenus illicites en ligne, organisée par le service « Point de contact » de l’Association des fournisseurs d’accès et de services Internet (AFA), dont Orange, SFR, Bouygues Telecom, Google, Microsoft et Facebook sont membres, mais pas Free ni Numericable. Ce service, créé en 1998, permet à tout internaute par un formulaire simple et anonyme tout contenu choquant rencontré sur Internet. « Point de contact » a également relevé une explosion du nombre de signalements de contenus de propagande terroriste ayant reçu «pour le seul mois de janvier le volume de l’année 2014 dans cette catégorie. » Pourtant, le nombre de contenus de ce type dénoncés par formulaire avait été divisé par deux en un an (36 en 2014 et seulement 6 qualifiés comme tels).

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

Source : http://www.latribune.fr/technos-medias/20150210trib83405d360/effet-charlie-explosion-des-signalements-d-apologies-du-terrorisme-en-ligne.html

---

Attaque informatique contre sony pictures : Les pirates

s’appuient sur la naïveté des consommateurs

Attaque informatique contre sony pictures : Les pirates s’appuient sur la naïveté des consommateurs

Sony Pictures Entertainment a été victime, le 24 novembre 2014, d’une cyber attaque de grande envergure. Après avoir pénétré les systèmes informatiques de la société, des pirates ont publié des données volées qui comprenaient notamment des films, des scénarios (dont celui du prochain James Bond), des dossiers médicaux de salariés ou encore des e-mails internes.

La théorie généralement avancée est que le groupe responsable, Guardians of Peace, serait lié à la République populaire démocratique de Corée du Nord et que tout ce scénario-catastrophe serait en rapport avec la sortie d’une comédie potache hollywoodienne intitulée L’interview qui tue, ayant pour thème l’assassinat du dirigeant nord-coréen Kim Jong-Un.
Dans un communiqué, Tanguy de Coatpont, de Kaspersky Lab avoue : «Les avis sont partagés quant à savoir qui porte la responsabilité de l’attaque et le débat paraît devoir se prolonger. Or, dans le cas d’attaques ciblées, il est très difficile d’en identifier les auteurs, car il existe de nombreux moyens pour eux de masquer leurs traces. Malgré tout, deux éléments ont particulièrement retenu mon attention.»
Le premier concerne la sécurité de l’entreprise. Il est clair que Sony n’a pas su tirer les leçons de l’attaque qui avait frappé son réseau PlayStation Network au printemps 2011. La seconde observation porte sur les menaces proférées par les pirates (ou ceux revendiquant la responsabilité de l’attaque contre Sony), à savoir le risque d’attentats terroristes contre les cinémas projetant le film L’interview qui tue.
Cette menace d’une attaque physique contre la sécurité du grand public a de quoi alarmer. Nous vivons dans un monde connecté et des aspects de plus en plus nombreux de notre quotidien sont dématérialisés. Aucune entreprise, grande ou petite, n’est à l’abri d’une cyber attaque, que celle-ci soit ciblée ou le résultat de dommages collatéraux.
Toutefois, il est important de faire la différence entre le «hacking» et le «defacing» d’un site web. Si le premier peut avoir de graves conséquences en entraînant par exemple des vols de données importants, le deuxième vise surtout à occuper le terrain médiatique et véhiculer des messages politiques. Les antivirus classiques, qui constituent encore la seule ligne de défense de nombreuses sociétés, sont depuis longtemps inefficaces face aux nouveaux types d’attaque. Mais les pirates s’appuient aussi et surtout sur la naïveté des consommateurs, souvent peu au fait des dangers.

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

Source : http://www.elwatan.com/hebdo/multimedia/l-attaque-informatique-contre-sony-pictures-les-eclairages-de-kaspersky-lab-08-02-2015-286984_157.php

Voitures connectées faciles à hacker

Voitures connectées faciles à hacker

Les promesses de la voiture connectée font rêver : sans conducteur, intelligente,… mais visiblement, elle est aussi facile à pirater. Un hackeur en prend ici le contrôle, faisant du véhicule un danger pour ses passagers. Dans son émission « 60 minutes », CBS News consacre un dossier aux voitures connectées et à leurs failles de sécurité. Kathleen Fisher, experte de la DARPA (Defense Advanced Research Projects Agency) présente la voiture connectée comme un « ordinateur sur roues », soulignant de fait la possibilité de hacker le véhicule.

Démonstration à l'appui : il est en effet possible de contrôler la voiture à distance, à l'aide d'un simple ordinateur portable. Si déclencher les essuie-glaces ou le klaxon peut sembler « inoffensif », quand le hackeur prend contrôle des freins, c'est tout de suite plus inquiétant. Ici, il ne s'agit que de plots en plastique, mais on imagine rapidement les dégâts si une voiture connectée perdait les pédales « dans la vraie vie ».

Plus tôt cette semaine, le sénateur américain Edward J. Markey a sorti un rapport sur les dangers des voitures connectées. Il y compile les données fournies par 16 constructeurs automobiles dont BMW, Fiat Chrysler, Ford, General Motors, Nissan, Mitsubishi ou Mercedes-Benz après qu'il leur ait adressé une lettre et un questionnaire en décembre 2013. Certains constructeurs dont Tesla ont cependant refusé de lui répondre… Selon ses résultats, aucune mesure ne serait mise en place pour détecter et empêcher les tentatives de piratage ou les vols de données. Par ailleurs, outre la sécurité, le rapport revient aussi sur les problèmes de confidentialité des données : les propriétaires de voitures connectés ne seraient pas au courant de tout ce qui est enregistré à leur propos… De quoi faire réfléchir avant d'investir dans la voiture du futur.

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

Source : http://www.ladn.eu/actualites/pop-insight,voitures-connectees-faciles-hacker,74,24953.html

Cybercriminalité : un milliard de données volées en 2014 !

Cybercriminalité : un milliard de données volées en 2014 !

Selon l'étude Breach Level Index publié par le leader mondial de la sécurité numérique plus de 1 500 failles de données ont été enregistrées en 2014, entraînant le vol d'un milliard d'enregistrements de données. Par rapport à 2013, ces chiffres représentent une augmentation de 49 % du nombre de failles de données et de 78 % des enregistrements de données volées ou perdues.

Selon les données recensées dans l'indice BLI initialement réalisé par SafeNet pour l'année 2014, les cybercriminels sont principalement intéressés par le vol d'identité, 54 % des failles y étant rattachées, soit davantage que toute autre catégorie de failles y compris l'accès aux données financières. De plus, les infractions concernant les vols d'identité représentent également un tiers des failles de données les plus graves selon la notation du BLI (« catastrophique » pour une note comprise entre 9,0 et 10, ou « sévère » pour une note comprise entre 7,0 à 8,9). Les failles sécurisées, c'est-à-dire les failles de sécurité périmétrique où les données sont totalement ou partiellement cryptées, ont progressé de 1 % à 4 %.
« Nous assistons sans l'ombre d'un doute à un tournant dans la tactique abordée par les cybercriminels, le vol d'identité à long terme se substituant de plus en plus à l'immédiateté qui caractérise le vol des numéros de cartes de crédit », affirme Tsion Gonen, Vice-président en charge de la stratégie, Identity & Data Protection, Gemalto. « Le vol d'identité peut entraîner l'ouverture de nouveaux comptes de crédit frauduleux, la création de fausses identités à des fins criminelles, ainsi que d'autres activités d'une grande gravité. Les failles de données sont de plus en plus personnalisées, et il apparaît que pour l'utilisateur lambda, l'exposition aux risques est de plus en plus forte ».
Outre cette évolution vers le vol d'identité, les failles ont également augmenté en gravité en 2014, deux tiers des 50 failles les plus importantes selon leur score BLI ayant eu lieu l'année dernière. De plus, le nombre de failles de données impliquant plus de 100 millions d'enregistrements de données a doublé par rapport à 2013.
« Non seulement le volume des failles de données est en hausse, mais leur gravité est également de plus en plus importante. La question n'est plus de savoir « si » vous allez être victime d'un vol de données, mais « quand ». ajoute Tsion Gonen. La prévention des failles et la surveillance des menaces s'arrêtent là et ne sont pas toujours suffisantes pour repousser les cybercriminels. Les entreprises doivent adopter une vision des menaces numériques « centrée sur les données » en commençant par la mise en œuvre de meilleures techniques de gestion des identités et de contrôle d'accès, telles que l'authentification multi-facteurs, le chiffrement ou la gestion des clés pour sécuriser les données sensibles. Ces outils rendent les données subtilisées par les voleurs parfaitement inutilisables », précice-t-il.
En ce qui concerne les secteurs touchés, les services financiers et la grande distribution ont connu en 2014 les évolutions les plus significatives par rapport à d'autres segments industriels. La grande distribution est en légère augmentation par rapport à l'an dernier, avec 11 % de l'ensemble des failles de données enregistrées en 2014. Cependant, par le nombre d'enregistrements de données touchées, ce secteur est passé de 29 % en 2013 à 55 % en 2014 et ce, en raison de l'augmentation du nombre d'attaques visant les terminaux point de vente (TPV). Pour le secteur des services financiers, si le nombre de failles de données est resté relativement stable d'une année sur l'autre, le nombre moyen de dossiers perdus par faille a été multiplié par dix, passant de 112 000 en 2013 à 1,1 million en 2014.

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

Source : http://afriqueinside.com/cybercriminalite-milliard-donnees-volees-en-2014-12022015/

Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

	Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

Capgemini lance sa nouvelle ligne de services mondiale dédiée à la cybersécurité. Celle-ci repose sur l'expertise de 2 500 professionnels de la cybersécurité, notamment des consultants, des auditeurs, des architectes, des spécialistes de la Recherche & Développement et des hackers éthiques , ainsi qu'un réseau mondial de 5 Centres Opérationnels de Sécurité (SOC, Security Operations Centers) et un large écosystème de partenaires technologiques. Capgemini prévoit une croissance élevée à deux chiffres de sa nouvelle ligne de services au cours des douze prochains mois. Elle doit permettre aux entreprises de mettre en œuvre un programme de transformation digitale en toute sécurité et de tirer parti des technologies du « SMACT » (Social, Mobile, Analytics, Cloud and Internet of Things) en toute confiance.

L'évolution rapide de la cybercriminalité a placé la sécurité au cœur des préoccupations des dirigeants. En effet, **entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120%** dans le monde et **le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an**, soit une augmentation de 10%. En outre, les hackers ont considérablement accru leurs connaissances des systèmes ciblés. De ce fait, les conséquences de leurs attaques sont de plus en plus importantes. Pour les entreprises du secteur de l'industrie, ces conséquences ne sont pas seulement financières ou réputationnelles mais peuvent également être matérielles ou humaines.
La nouvelle ligne de services mondiale dédiée à la cybersécurité de Capgemini répond aux problématiques de sécurité des systèmes IT, des systèmes industriels (OT), ainsi que des objets connectés (IoT- Internet Of Things). Selon la récente étude menée par Capgemini Consulting auprès de fournisseurs de technologies d'objets connectés, **les entreprises doivent être mieux préparées à faire face aux menaces qui pèsent sur la sécurité et sur la confidentialité des données** : seules 33% d'entre elles pensent que leurs objets connectés sont « très résistants » aux futures menaces de cybersécurité et 70% considèrent que « les questions de sécurité influencent les décisions d'achat des clients relatives aux objets connectés » .
La nouvelle ligne de services développera des services packagés et industrialisés qui peuvent être répliqués dans tous les pays. Ces offres de services packagés répondent aux besoins de sécurité de l'IT de nouvelle génération tels que la sécurité des infrastructures Hadoop, la sécurité des SDDC (Software-Defined Data Centers), ainsi que la sécurité des Clouds hybrides privés et publics. De nouvelles offres seront également lancées, telles que des tests de sécurité des applications « as-a-service » et des solutions de gestion des identités et des accès « as-a-service », pour permettre aux entreprises de tirer parti de l'approche Cloud et faciliter le déploiement de solutions de sécurité.
Selon Forrester Research , « L'importance de la protection de la vie privée, la recrudescence des cyberattaques et l'éclatement du périmètre de l'entreprise digitale ont obligé les professionnels de la sécurité et de la gestion des risques à renforcer la protection des données elles-mêmes. Dans la bataille pour recruter, servir et fidéliser ses clients, la protection de la vie privée et la sécurité des données sont devenues des avantages concurrentiels, et de ce fait une priorité business et technologique. »

La ligne de services mondiale dédiée à la cybersécurité de Capgemini permettra aux entreprises d'adopter une approche globale et pragmatique de leur stratégie de sécurité. Elle consolide l'expertise de Capgemini en tant qu'intégrateur de systèmes et fournisseur de services. Elle repose également sur sa connaissance approfondie de la cybersécurité, acquise dans le cadre des nombreuses missions réalisées auprès de ses clients au cours des dix dernières années dont celles menées pour le ministère du Travail et des Retraites (DWP) au Royaume-Uni, l'Agence spatiale française (CNES), Alstom Transport et Foyer (le plus important groupe d'assurance au Luxembourg).

Capgemini a conçu une gamme de services de cybersécurité assurant la protection des utilisateurs (identité numérique et contrôle d'accès), des applications, des terminaux (les terminaux de bureau, smartphones, tablettes, capteurs et autres objets connectés), des infrastructures (stockage, réseaux, serveurs, virtualisation et orchestration) et des données.

Les services proposés sont les suivants :

• Le conseil en sécurité et l'audit de sécurité
o Cela inclut l'évaluation des systèmes de sécurité, la définition de feuilles de route, les conseils opérationnels de sécurité et les audits de sécurité, tels que les tests d'intrusion et les investigations numériques.
o En janvier 2015, lors du Forum international de la cybersécurité (FIC), le prix « Label France Cybersecurity » a été décerné à Sogeti France, filiale du groupe Capgemini, par Axelle Lemaire, Secrétaire d'Etat chargée du numérique pour ses services d'audit de sécurité.
o Capgemini a aussi récemment conduit plusieurs missions de conseil comme pour Alstom Transport, incluant une analyse de risques, l'identification des cibles de sécurité et des recommandations d'architecture afin d'assurer la cybersécurité des trains et du système de signalisation.

• La conception et le développement de solutions pour protéger les systèmes informatiques, les systèmes industriels et les systèmes intelligents (objets connectés) :
o Grâce à l'acquisition d'Euriware, société française de services informatiques, Capgemini propose des services pour sécuriser les systèmes SCADA (systèmes de contrôle et d'acquisition de données). En outre, Sogeti High Tech offre des services qui permettent d'intégrer la sécurité dans le processus de développement des objets connectés.
o En outre, en partenariat avec Pivotal, Capgemini a récemment lancé une offre de Détection de Comportements Anormaux (Anomalous Behavior Detection) pour permettre aux entreprises d'identifier et de répondre aux menaces informatiques internes et externes les plus sophistiquées.

• Surveillance de la sécurité 24h/24 et 7j/7 :
o Aujourd'hui, Capgemini exploite cinq Centres Opérationnels de Sécurité (SOC, Security Operation Centers) mutualisés, qui sont les yeux et les oreilles permettant de détecter et de réagir aux cyberattaques. Ils sont situés en France, au Royaume-Uni, au Luxembourg et en Inde – où il y en a deux. Ces centres bénéficient de l'aide d'équipes de Recherche & Développement spécialisées en identification de vulnérabilités et en investigations numériques. Capgemini construit actuellement un sixième SOC en Belgique. Il conçoit et met également en place des SOC ad hoc pour ses clients.

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

Source : http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
Par Marc Jacob

En 2015, vous serez la première cible visée par la cybercriminalité

13

En 2015, vous serez 13la première cible visée par la cybercriminalité

ESET®, pionnier globale en protection proactive depuis plus de deux décennies, vient de publier un rapport très complet sur les principales tendances pour 2015 en cybercriminalité. Ce rapport est gratuit et peut être télécharger sur in the white paper section on WeLiveSecurity.com.

Alors que l'an dernier tout se concentrait autour de la protection de la vie privée sur Internet et le malware sur Android, de nouveaux secteurs de risques en sécurité informatique émergent en 2015. Le rapport gratuit Trends for 2015, est axé sur les cinq principaux domaines sur lesquelles les entreprises doivent se concentrer pour combattre les attaques. Il explique pourquoi les entreprises doivent être sur leurs gardes, commente l'évolution des menaces et leur donne des conseils pour protéger au mieux leurs actifs.
"Alors que les organisations améliorent continuellement leurs connexions digitales, de nouvelles pistes s'ouvrent aux cybercrime, " explique Marc Mutelet, CEO de MGK Technologies, distributeur exclusif des produits ESET sur la Belgique et le Luxembourg. L'astuce est de faire en sorte que vos défenses soient plus impénétrables que celles des entreprises qui vous entourent. En comprenant mieux le paysage des menaces vous êtes bien mieux préparé pour contrer les choses indésirables qui se cachent autour de vous. "

Le rapport est axé sur les principaux risques :
1. L'évolution of des APTs
2. Malware au point de vente
3. Fuite de l'information
4. Vulnérabilités
5. Internet des objets …. ou Internet des menaces?

"Nous pouvons tous imaginer combien il est frustrant pour les entreprises de devoir continuellement protéger leurs actifs contre les pirates et les criminels, c'est pour cela que nous avons voulu leur fournir de l'aide avec ce rapport, " commente Marc Mutelet. "Nous avons demandé à nos experts en sécurité de nous fournir une analyse détaillée de ce qu'ils pensent être des menaces émergeantes. Ce rapport est destiné à fournir des informations supplémentaires aux organisations, à les aider à revoir leurs technologies et processus de sécurité et à mettre en place les ressources nécessaires aux endroits stratégiques. "

Le rapport détaillé peut être téléchargé sur :
http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf.

Vous êtes un chef d'entreprise, un élu, vous souhaitez sensibiliser votre personnel au risque informatique et le sensibiliser aux bonnes pratiques, n'hésitez pas à nous contacter.

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

Source :
http://www.informaticien.be/articles_item-17148-En_2015__les_entreprises_sont_la_premiere_cible_visee_par_la_cybercriminali.html

---

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater ?

Près de la moitié des cartes bancaires sont désormais équipées de la technologie de paiement sans contact. Un développement à marche forcée qui alimente les craintes de fraude chez les consommateurs.

Une envolée… en toute discrétion. En un an, le nombre de cartes de paiement sans contact en circulation en France a bondi de 50%, pout atteindre 30,3 millions en octobre 2014, selon les derniers chiffres de l'Observatoire du NFC et du sans contact. Elles représentent désormais 47,4% de l'ensemble des cartes bancaires, contre 31% douze mois plus tôt.
Pour savoir si votre carte est dotée de cette technologie, c'est très simple : elle comporte alors un petit logo représentant des ondes se propageant. Si vous ne le saviez pas, rien d'étonnant : les banques ont en effet assez peu communiqué sur le sujet, équipant le plus souvent leurs clients lors d'un renouvellement de carte sans forcément les en informer.

La généralisation de ce nouvel outil de paiement est-elle pour autant synonyme de risque pour consommateurs ? Plusieurs experts en sécurité informatique ont déjà pointé du doigt les potentielles failles de ce système. « Les informations contenues sur cette carte ne sont pas cryptées et peuvent être récupérées très facilement grâce à un smartphone », prévient Thomas Livet, de la société Sifaris.
Nous l'avons testé, le procédé est en effet d'une simplicité enfantine : il suffit de télécharger l'une des multiples applications dédiées disponibles sur la plate-forme d'Android avec un smartphone compatible avec la technologie « NFC », puis de diriger ce téléphone vers une carte bancaire pour obtenir en quelques secondes les 16 numéros inscrits au recto, la date d'expiration et le nom de la banque (voir la capture plus bas). Inquiétant.
Reste que certaines données essentielles ne peuvent pas être aspirées : en particulier le cryptogramme, c'est-à-dire les 3 chiffres inscrits au dos de la carte faisant office de code de sécurité lors d'un paiement en ligne, ainsi que le nom de l'utilisateur. Ce qui complique de fait la tâche des escrocs, puisque la plupart des grands sites de e-commerce français et étrangers demandent ces informations pour valider un paiement. « Evidemment on pourrait concevoir un logiciel pour générer les 999 combinaisons possibles de cryptogramme, mais cela paraît bien compliqué pour ce genre de petites escroqueries », relativise Maxime Chipoy, de l'association de défense des consommateurs, UFC Que Choisir.

Même si la possibilité de se faire escroquer par ce biais n'est pas nulle, le risque de fraude paraît donc limité. Aucune arnaque liée au système de paiement sans contact n'est d'ailleurs pour le moment remontée aux oreilles de l'UFC. Même son de cloche chez CLCV : « Nous avons eu des plaintes relatives au paiement sans contact, mais uniquement concernant le manque de communication des banques sur le sujet, et non en raison d'escroqueries », explique Olivier Gayraud, de l'association.
Certes, la technologie sans contact facilite aussi la tâche des fraudeurs qui arrivent à subtiliser une de ces cartes : ils peuvent en effet l'utiliser sans avoir à taper le code pin, dans n'importe quel magasin équipé de la technologie sans contact. Mais le montant de chaque transaction est limité à 20 euros, et vous devez retaper le code pin une fois dépassé un certain plafond, défini généralement entre 80 et 100 euros selon les banques.
Si vous craignez tout de même de vous faire hacker votre carte, vous avez le droit de demander à votre banque la désactivation de la fonctionnalité de paiement sans contact, voire une nouvelle carte bancaire non équipée de cette technologie. Même si les établissements sont parfois réticents à le faire, n'hésitez pas à insister : « Si votre conseiller s'y oppose, exigez un refus par écrit. Cela devrait suffire à débloquer la situation », conseille Olivier Gayraud. Certaines banques peuvent aussi fournir gratuitement des étuis de protection, faisant office de « cage de Faraday », permettant d'isoler complètement la carte bancaire des ondes extérieures. Il est aussi possible d'acheter ces étuis dans le commerce pour quelques euros, voire des portefeuilles « anti-NFC » moyennant entre 10 et 30 euros.

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

Source : http://www.capital.fr/finances-perso/actualites/paiement-sans-contact-votre-carte-bancaire-risque-t-elle-de-se-faire-pirater-1010288
Par Thomas Le Bars

La DGA-MI et le pôle d'excellence Cyber veillent

sur la Toile

La DGA-MI et le pôle d'excellence Cyber veillent sur la Toile

La Bretagne est au cœur du dispositif national de cyberdéfense. À Bruz, la DGA-MI et le pôle d'excellence Cyber veillent sur la Toile. Les entreprises doivent se prémunir.

Enjeu de notre siècle, la cybersécurité se joue en grande partie en Bretagne. À Bruz (35), la DGA – Maîtrise de l'Information est un site référence en France et même l'un des principaux en Europe. Les attaques récentes dont ont été victimes des sites web dont de nombreux portails bretons ne montrent qu'une partie immergée et, paradoxalement plutôt rassurante, de l'iceberg.

Vol, déni de service…

Pour Paul-André Pincemin, ingénieur en chef de l'armement et chef de projet de ce pôle Cyber, l'une des préoccupations est d'identifier les trous dans la Toile. « Mais ce n'est pas ce que l'on voit qui est inquiétant… Imaginez le pire et c'est encore loin de la réalité, confie-t-il. Se faire voler des données et s'en rendre compte plus tard est beaucoup plus grave. » L'exemple récent de Sony l'atteste. Tout comme les attaques par « déni de service » qui peuvent s'avérer préjudiciables pour un site d'e-commerce par exemple, du fait d'une rupture de service.

30 M€ investis à Bruz

Aux portes de Rennes, on traque la menace. Le ministre de la Défense Jean-Yves Le Drian a fait de ce site militaire un pilier ouvert sur le privé via le Pôle d'excellence Cyber. On parle de « quatrième armée » pour ce nouvel espace à protéger. En octobre, il posait la première pierre d'un futur bâtiment de 10.000 m² de très haute sécurité. Un investissement de 30 M€ dans le cadre du Pacte Cyber lancé il y a un an.

50.000 cyber emplois bretons

Ce nouveau QG, qui sera livré au printemps 2016, doit accueillir 250 nouveaux salariés : cryptologues, codeurs… De quoi porter à plus de 1.450 le nombre de personnes (deux tiers d'ingénieurs) qui travaillent sur ce site réalisant 60 millions d'euros d'achats par an. En Bretagne, Jean-Yves Le Drian a dénombré 50.000 emplois (civils et militaires) positionnés sur la cybersécurité. On parle de « Cyber-valley ». Mais ce n'est pas nouveau, avec une présence historique à Bruz depuis 1968 et une filière transversale qui touche tous les secteurs (numérique, agro, santé…) et va monter en puissance, précise Loïg Chesnais-Girard, vice-président du conseil régional à l'économie qui l'a soutenue à près d'1 M€ en 2014. « Nous sommes l'une des régions européennes les plus en pointe. Il y a un enjeu énorme de se défendre et de concevoir des produits de demain. » Une centaine de PME ont été identifiées sur cette « filière d'avenir », inscrite dans la Glaz économie bretonne. Certaines étaient d'ailleurs au FIC 2015, à Lille en janvier. « Nous sommes dans une logique collaborative et d'ouverture », appuie Paul-André Pincemin dont la principale mission est de fédérer tous les acteurs autour de la même table, bien au-delà de la Bretagne. De ces échanges, par exemple, des clubs thématiques se constituent – un club d'entreprises va être créé – et de nouvelles formations émergent pour préparer les talents de demain. « Nous travaillons à ce que la disponibilité des compétences ne soit pas un frein au développement de la filière. » Cet essor est en effet souvent limité par la ressource humaine.

Tous concernés !

Et pour se prémunir d'une éventuelle attaque, les chefs d'entreprise sont de plus en plus sensibilisés via des conférences (lire ci-dessous), des formations animées par des ingénieurs en sécurité informatique… L'Institut des hautes études de la défense nationale (IHEDN, 150 membres dans le Grand Ouest), fait partie des maillons de cette chaîne. « La sécurité est l'affaire de tous, y compris la sécurité informatique ! Il y a des enjeux commerciaux derrière, insiste Jean-Marc Hainigue, son président. Les chefs d'entreprise sont des utilisateurs, pas des spécialistes. Ce sont d'abord eux qu'il faut sensibiliser. Ils doivent s'engager à sécuriser leurs données. Aujourd'hui, internet est un outil admirable mais nous avons le pire et le meilleur. »

Souvent du bon sens

Et cette prévention relève souvent du bon sens. À commencer par ne pas étaler tous ses faits et gestes sur le réseau. Les boîtes mail des stagiaires sont aussi une belle porte d'entrée. « J'ai rencontré une PME de 50 salariés qui avait 400 adresses mail ! », témoigne Jean-Luc Poulain, ancien communicant rennais, auditeur à l'IHEDN. Paul-André Pincemin conclut : « Il y a une opportunité de business ; protégez-vous avec des produits sûrs ! »

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

Source : http://www.lejournaldesentreprises.com/editions/35/actualite/conjoncture/cybersecurite-pas-ce-que-l-on-voit-le-plus-inquietant-06-02-2015-246633.php
Par Géry Bertrande www.ssi.gouv.fr

Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Victimes de «femmes fatales» sur les réseaux, ils se sont fait dérober des informations militaires ou personnelles.
La recette est vieille comme l'espionnage, mais elle fonctionne toujours à l'ère numérique : pour soutirer des informations à la rébellion syrienne, un groupe de pirates informatiques encore non identifié a utilisé de faux profils féminins sur les réseaux Skype et Facebook. C'est ce qu'a découvert une équipe de chercheurs travaillant pour la société américaine de sécurité informatique FireEye, dont le rapport, intitulé «Derrière les lignes de front numérique du conflit syrien», a été publié ce 2 février.

«MATA HARI NUMÉRIQUES»
La récolte est considérable. En remontant le fil de documents PDF contenant des logiciels malveillants (ou malwares), les chercheurs ont découvert un ensemble de 7,7 GB de données «révélant la stratégie de l'opposition syrienne, des plans de bataille, des besoins d'approvisionnement, et une foule d'informations personnelles et de sessions de messagerie instantanée appartenant aux hommes qui combattent les forces du président syrien Bachar al-Assad». Le piratage, qui se serait déroulé a minima de novembre 2013 à janvier 2014, a visé aussi bien des rebelles liés à l'Armée syrienne libre que des membres de groupes islamistes armés et des personnes sans affiliation précise. Parmi la soixantaine de cibles directes identifiées – un chiffre minimal, qui correspond au nombre de comptes Skype compromis –, l'équipe a notamment repéré un chef d'unité combattante, un ex-officier de haut rang ayant déserté les services de sécurité d'Assad, un coordinateur local d'une ONG turque, ou encore un membre d'un centre de presse basé en Syrie.
Lors de leurs échanges avec les «femmes fatales», les opposants au régime syrien se voyaient demander s'ils utilisaient Skype «sur un ordinateur ou sur [leur] téléphone», avant de recevoir une photo abritant le malware adéquat, grâce auquel les attaquants pouvaient ensuite accéder à l'ordinateur de leur cible. Les profils Facebook correspondants étaient, eux, truffés de liens malveillants, cachés derrière des discours favorables à l'opposition et des invitations à utiliser des outils de sécurisation des communications, tels que des réseaux privés virtuels ou le réseau d'anonymisation Tor.
Une stratégie de «Mata Hari numérique», comme l'a noté Martin Gropp, journaliste à la Frankfurter Allgemeine Zeitung :

DES OUTILS «SUR MESURE»
L'utilisation de faux profils féminins sur les réseaux sociaux à des fins d'espionnage n'est pas une nouveauté. Nicolas Arpagian, directeur scientifique à l'Institut national des hautes études de la sécurité et de la justice, fait notamment état d'une opération du même genre attribuée au Hezbollah : d'après un article du Spiegel paru en mai 2010, un faux profil Facebook aurait permis de soutirer des informations à quelque 200 soldats ou réservistes de l'armée israélienne. Il y a deux ans, une étude du département de la Défense australien a accusé les talibans d'user de la même méthode pour espionner ses soldats.

Dans le cadre du conflit syrien, en revanche, le déploiement à cette échelle de la méthode est inédit. «C'est la première fois que nous constatons un tel degré de sophistication dans l'utilisation de faux profils, et dans cet objectif», explique John Scott-Railton, chercheur associé au Citizen Lab de l'université de Toronto et l'un des auteurs du rapport de FireEye. Le mode opératoire – qui repose en grande partie sur «l'ingénierie sociale», autrement dit l'exploitation des failles humaines – n'est pas la seule différence avec ce qu'il a pu examiner jusqu'à présent (1). «Ces acteurs ont utilisé une boîte à outils plus diversifiée que ce que nous avions observé de la part de hackers pro-gouvernement ou dans l'attaque liée à l'EI, poursuit Scott-Railton. Ils ont des outils « sur mesure ». Et ils ont clairement ciblé des informations de nature militaire.» Au final, souligne le rapport, la moisson d'informations récoltées avait de quoi offrir «un avantage immédiat sur le champ de bataille».
L'attaque reste néanmoins assez peu technique, estime Raphaël Vinot, chercheur en sécurité au CERT (2) national du Luxembourg. La plupart des logiciels utilisés reprennent du code qui circulait déjà sur Internet. Le logiciel de prise de contrôle des ordinateurs à distance, dénommé «Darkcomet», existe depuis 2008 – son créateur, un programmeur français, a même cessé de le développer face aux utilisations malveillantes qui en étaient faites. «C'est un outil lourd, vraiment pas discret, estime le Luxembourgeois. Mais les antivirus ne le détectent pas, donc cela fonctionne dans la majorité des cas.»

Pour lui, l'outil le plus évolué pourrait être le malware ciblant le système d'exploitation pour smartphones Android. Ce qui est également, selon les chercheurs de FireEye, une nouveauté dans le contexte syrien. Or les smartphones sont une mine d'informations, en particulier dans une zone où, explique le rapport, «les pannes de courant régulières peuvent pousser les gens à se fier encore plus aux mobiles pour communiquer».

LA PISTE LIBANAISE
Quant à savoir qui se cache derrière cette opération, mystère. Les auteurs de l'étude avancent prudemment avoir «des indications selon lesquelles le groupe pourrait être financé et/ou situé en dehors de la Syrie». Ils font néanmoins état de multiples références au Liban, que ce soit dans les faux profils ou sur le site web mis en ligne par le même groupe, présenté comme émanant de l'opposition syrienne et lui aussi truffé de logiciels malveillants. Par ailleurs, deux versions de test des malwares utilisés ont été mises en ligne depuis le Liban. Vraie ou fausse piste ? «Avec Internet, tout est possible, rappelle John Scott-Railton. Mais si ce groupe a fait preuve d'une certaine sophistication dans l'attaque, peut-être qu'en matière de sécurité opérationnelle, il n'était pas en capacité de mettre en place une énorme « fausse bannière ».»

«C'est à juste titre que le rapport reste prudent, juge Eva Galperin, analyste à l'Electronic Frontier Foundation, qui a travaillé sur une précédente étude de cyberattaques en Syrie. Attribuer une attaque informatique est très difficile, et je ne vois rien, pour l'instant, qui indique de manière définitive un acteur originaire du Liban.» A ce stade donc, difficile d'aller plus loin que les conjectures. D'autant qu'à la différence de l'Armée électronique syrienne, qui s'illustre depuis près de trois ans par des coups d'éclat prioritairement orientés vers les médias – et dont Le Monde a été la plus récente victime –, ce groupe-ci a agi dans la plus grande discrétion.

Avant de rendre public leur rapport, les chercheurs ont contacté quelques-unes des victimes du piratage. Lesquelles ont eu une réaction assez fataliste : «Les groupes syriens ont tellement l'habitude que leurs communications soient espionnées, conclut Scott-Railton, qu'ils ne sont pas vraiment surpris d'avoir été piratés. En général, ils estiment qu'ils ont d'autres problèmes plus urgents.» Non seulement le cyberespionnage se démocratise très manifestement, mais il a en prime de beaux jours devant lui.

(1) Voir notamment les deux précédentes études auxquelles il a participé : l'une sur les attaques menées par des pirates informatiques pro-gouvernement («Quantum of Surveillance», rapport conjoint du Citizen Lab et de l'Electronic Frontier Foundation), l'autre consacrée à une attaque par malwareliée à l'État islamique.

(2) Computer Emergency Response Team, le centre d'alerte et de réaction aux attaques informatiques.

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

Source : http://www.liberation.fr/monde/2015/02/04/des-rebelles-syriens-pirates-grace-a-de-faux-profils-skype-et-facebook_1194718

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Ce n'est pas la première fois qu'une reforme du statut des hébergeurs est évoquée et ça ne sera surement pas la dernière : le coup vient cette fois de la ministre de la Culture Fleur Pellerin qui appelle dans une interview du journal Les Echos à une réévaluation du statut juridique de l'hébergeur. « Ces statuts datent de la loi de confiance dans l'économie numérique, de 2004, qui transpose elle-même une directive européenne de 2000. Internet a évolué depuis ! ».

L'objectif affiché par Fleur Pellerin est ici de permettre une meilleure lutte contre la contrefaçon en ligne d'œuvre de l'esprit. Si la ministre exclut la possibilité de rendre ces « plateformes » entièrement responsables du délit, elle appelle à la mise en place d'un statut « hybride » afin de garantir une meilleure défense du droit d'auteur et une plus grande réactivité face à ces contenus illégaux.
Des propositions qui s'inspirent librement des recommandations émises par le conseil d'état comme le souligne Nextinpact, qui avait dans son rapport annuel 2014 consacré au numérique évoqué la mise en place d'un principe de « loyauté des plateformes » qui se traduirait par une série d'obligations et de contraintes venant limiter la marge de manœuvre des éditeurs vis-à-vis des contenus qu'ils diffusent via leurs services.

L'Afdel craint les effets de rebonds

La reforme du statut des hébergeurs est un thème qui revient régulièrement dans les projets législatifs et autres rapports du gouvernement. Mais celui-ci ne manque pas de faire réagir l'Afdel, qui a publié par voie de communiqué une longue tribune mettant en garde le gouvernement à l'égard de ces mesures. Si l'Association des éditeurs de logiciels ne parait pas opposée sur le principe à de nouvelles mesures visant à protéger plus efficacement les œuvres de l'esprit, elle s'inquiète des éventuels ricochets que pourrait provoquer une reforme du statut de l'hébergeur.
L'association souligne ainsi que « le statut juridique de l'hébergeur ne fait pas la différence entre différents types d'hébergeurs (B2C, B2B…) » Un point à clarifier pour l'Afdel, qui s'inquiète d'un impact possible de ce nouveau statut sur les entreprises proposant des services en mode Saas ou « qui stockent des données à la demande du destinataire du service ».
Le gouvernement reste pour l'instant évasif sur les prochaines mesures concrètes visant à matérialiser cette volonté affichée. Mais la grande loi sur le numérique promise par Axelle Lemaire pour 2015 est encore dans les cartons et sera peut être l'occasion pour le gouvernement de détailler leurs intentions.

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

Source : http://www.zdnet.fr/actualites/statut-de-l-hebergeur-nouvelles-passes-d-armes-en-prevision-39814102.htm
Par Louis Adam