Le jour de la Cybersécurité maritime

	Le jour de la Cybersécurité maritime

---

Alors qu'était publié le 25 décembre 2011 mon premier article consacré à (l'absence de) la cybersécurité dans le secteur maritime, jamais je n'aurais imaginé y revenir avec une telle régularité chaque 25 décembre depuis [1].

De là à imaginer que ce jour pourrait devenir LE jour de l'année où l'on y penserait, il n'y a qu'un pas que j'ai eu envie de franchir ! J'appelle donc solennellement de mes vœux, et en toute simplicité, qu'une autorité nationale, européenne voire internationale décrète que chaque 25 décembre soit la journée de la cybersécurité du secteur maritime.
Si mon souhait se perd dans l'immensité intersidérale du cyberespace, vous pouvez compter sur moi pour cette amicale « piqûre de rappel » aussi longtemps qu'elle sera nécessaire. En souhaitant simplement que je cesse ce rappel avant 2020 sinon cela signifiera que le niveau d'inquiétude et, surtout, de risque aura grimpé en flèche. Mais puisque c'est actuellement la trêve des confiseurs et parce que l'année 2015 aura été particulièrement difficile en France [2], essayons de rêver quelques instants.
Saluons tout d'abord la tenue des « premières rencontres parlementaires cybersécurité et milieu maritime » le 12 février 2015 à Paris, brillamment organisées par le « Cybercercle » qu'il convient ici de saluer pour son rôle et son activisme passionné. A la suite de cette journée, une lettre autour de ces rencontres, que je recommande, a été publiée [3].
Fin octobre, le colloque Safer Seas [4] a réuni à Brest l'ensemble des acteurs du secteur. Une part modeste mais somme toute bien visible [5] a été laissée à la cybersécurité notamment sous l'angle de la cybercriminalité [6].
Si, sans doute, trop nombreux sont encore les décideurs du secteur maritime à découvrir que des ports aux navires en passant par la supply chain tout ce qui embarque de l'informatique doit être soumis à interrogation, ne boudons cependant pas notre plaisir. Oui la prise de conscience a lieu et, oui, enfin, tout le monde est en train de (ou va prochainement) se mettre autour de la table pour en discuter.
La prochaine étape va donc consister à passer de la prise de conscience aux paroles, que l'on espère fortes, puis à leur concrétisation : évaluation globale des risques informatiques, audits [7], développement et insertion de services et de produits qualifiés [8], processus d'homologation [9], éducation via de la sensibilisation à l'ensemble des salariés de la filière, bonnes pratiques, etc. L'ampleur de la tâche étant si vaste [10], il faut simplement souhaiter et agir rapidement pour que les prochaines étapes ne s'effectuent pas au rythme d'une annexe à rame mais bien plus sur celui d'un hydroglisseur commandé par un capitaine expérimenté et volontaire, entouré d'un équipage adroit et tenace y compris – et surtout – au cœur des tempêtes qui s'annoncent.

[1] ou presque : 2013 puis 2014
[2] tant par les attentats de janvier et de novembre que par l'inexorable montée du chômage et la paupérisation continue d'une part croissante de nos concitoyens
[3] http://fr.calameo.com/read/004370735c23949b43ff3
[4] http://www.saferseas-brest.org/
[5] http://presse.rivacom.fr/fr/newsletter/1494/la-cybersecurite-un-enjeu-majeur-pour-le-monde-maritime
[6] http://www.letelegramme.fr/bretagne/mer/cybercriminalite-bateaux-et-ports-pour-cibles-28-10-2015-10829564.php
[7] http://si-vis.blogspot.fr/2015/02/tester-son-niveau-de-cybersecurite.html
[8] http://www.ssi.gouv.fr/entreprise/qualifications/
[9] http://www.ssi.gouv.fr/actualite/pour-homologuer-votre-systeme-dinformation-suivez-le-guide/
[1 0]
http://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/

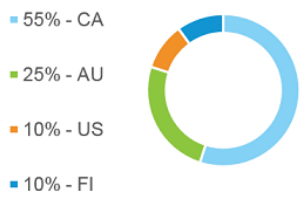
Réagissez à cet article

Source : *Si vis pacem para bellum: Cybersécurité maritime 2015*

Le cheval de Troie Ramnit refait surface

Le cheval de Troie Ramnit refait surface

Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle Une première pour un botnet bancaire selon IBM



En février dernier, suite à une opération menée par plusieurs États ainsi que des acteurs privés (parmi lesquels Microsoft, Symantec et AnubisNetworks) qui a été coordonnée par le centre de lutte contre la cybercriminalité d'Europol, un réseau de serveurs de contrôle du botnet Ramnit a été démantelé. Trois cents domaines internet exploités par les pirates ont également été redirigés.
Détecté pour la première fois en 2010, le cheval de Troie Ramnit permettrait de gagner un accès distant aux ordinateurs Windows infectés et de subtiliser par la suite des données sensibles, comme des informations bancaires. Wil van Gemert, le directeur des opérations d'Europol, a salué le succès de l'opération : « cette opération réussie illustre l'importance pour les forces de l'ordre internationales de travailler de concert avec l'industrie privée afin de lutter contre la menace globale du cybercrime ».
Seulement, les chercheurs d'IBM ont mis la main sur une variante du cheval de Troie qui se base sur une infrastructure C&C différente de son prédécesseur et emploie un fichier de configuration plus court ainsi qu'un schéma d'injection web différent pour infecter les victimes. Plus de la moitié des infections a été observée au Canada. En seconde position sur la liste des pays les plus affectés viennent l'Australie qui compte à elle seule une infection sur quatre, puis les États-Unis.
Selon les chercheurs de la X-Force d'IBM, il semblerait que ce soit la première fois qu'un botnet de fraude bancaire refasse surface, ce qui a aiguisé leur curiosité puisque, jusqu'à présent, c'étaient plutôt les botnets de spams qui étaient souvent ramenés en circulation, les cybercriminels derrière les botnets de fraude bancaire préférant se contenter de l'argent déjà collecté et du fait qu'ils n'aient pas été arrêtés.
Les experts expliquent que « le cheval de Troie arborait un fichier de configuration lourd avec des déclencheurs d'URL qui lui indiquaient vers quelle banque, quelle transaction et quels sites de réseau social se tourner pour collecter des informations d'identification ». La configuration de Ramnit est orientée pour tenir les victimes éloignées d'une liste exhaustive d'outils de scans en ligne, de sites web d'antivirus, des sites d'information sur le cybercrime, mais également des blogs de sécurité. « Dans son ancienne configuration, la seule utilisation des mots « cybercriminalité » ou « police » de la part des victimes suffisait à déclencher un effet de redirection ».
Une autre trace laissée par les anciennes configurations est la liste relativement importante de sites de recrutements récoltant les informations d'identification, afin de viser ceux qui sont à la recherche d'un emploi et de les recruter. « Pour les victimes, cela pouvait être une lame à double tranchant étant donné que les opérateurs Ramnit pouvaient également obtenir toutes les informations qu'elles ont mises sur leur CV professionnel ».
La X-Force Threat Intelligence d'IBM n'a pas eu vent du fait que le code source de Ramnit ait été vendu ouvertement, partagé avec d'autres groupes de cybercriminels ou sur les forums dans le marché noir. Aussi, ils pensent qu'il y a de fortes chances qu'il s'agisse là du même groupe d'individus qui a remis cette nouvelle version en activité.

Réagissez à cet article

Source : *Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle, une première pour un botnet bancaire selon IBM*

La cybercriminalité en nette hausse en fin d’année

La cybercriminalité en nette hausse en fin d’année

« La cybercriminalité en nette hausse au cours du 3e trimestre 2015 » , titre le site www.developpez.com qui ajoute que « ces problématiques de sécurité constituent un prélude à des événements majeurs dont l’impact sera, selon Trend Micro, particulièrement fort en 2016 ».

Le site s’appuie sur une étude de Trend Micro intitulé « Hazards Ahead : Current Vulnerabilities Prelude Impending Attacks », qui revient longuement sur le bilan en forte progression des faits de délinquance informatique au 3e trimestre 2015, avant d’esquisser une perspective pour l’année 2016 qui sera aussi riche, selon l’étude, du fait notamment du développement des technologies mobiles et de l’internet des objets.
Pour un responsable de chez Trend Micro, interrogé par les auteurs de l’enquête de terrain, il est clair que « l’évolution des piratages commence à grever la rentabilité des entreprises et le quotidien de tout un chacun ».
L’intérêt de cette étude est qu’elle donne un aperçu sur les « dégâts » occasionnés par la délinquance informatique sur la vie privée de citoyens qui en sont victimes.
« Des cas de suicides ont d’ailleurs été recensés du fait des conséquences de cette attaque sur la vie privée des utilisateurs du site », relève le site qui évoque, en effet, une attaque massive, avec vol de données de quelque 30 millions d’utilisateurs contre Ashley Madison. Il s’agit, nous apprend l’encyclopédie en ligne Wikipedia d’un « site de rencontres en ligne et un réseau social canadien.
Le public visé est celui des internautes mariés, ou du moins vivant en couple, et souhaitant avoir une relation extraconjugale ».

Réagissez à cet article

Source : « *La cybercriminalité en nette hausse au cours… – Horizons*

Le site de la BBC victime d’une cyber-attaque

Le site de la BBC victime d’une cyber-attaque

Ce jeudi matin, tous les sites de la BBC étaient inaccessibles à cause d'une attaque par déni de service…

Une cyber-attaque de grande ampleur. Le fonctionnement du site Internet de la BBC a été perturbé jeudi matin par une attaque par déni de services, rendant la consultation des informations impossible, selon un article du groupe britannique d'audiovisuel public.

« Une attaque par déni de service »

« Tous les sites Internet de la BBC étaient inaccessibles jeudi matin en raison d'une importante cyber-attaque », a indiqué la chaîne dans un article publié dans la section technologie de son site Internet attaqué qui était consultable par intermittence dans la matinée.
« Des sources au sein de la BBC ont indiqué que les sites étaient inaccessibles à cause d'une attaque par déni de service », ajoute l'article qui précise que l'attaque a porté sur le site et des services associés comme le service iPlayer pour revoir les émissions et l'application iPlayer Radio.

La situation est revenue à la normale

« Le site de la BBC est maintenant de retour et fonctionne normalement. Nous nous excusons pour le désagrément », a indiqué peu après 12h GMT une porte-parole de la chaîne dans un communiqué.
Ce type d'attaques a pour but de rendre un service indisponible en inondant un réseau ou en perturbant les connexions à un serveur.

La BBC déjà victime d'une cyber-attaque

En juillet 2014, une précédente attaque avait paralysé le service iPlayer de la BBC pendant un week-end entier, précise le groupe britannique d'audiovisuel public.
En septembre dernier, c'était le site Internet de l'Agence britannique de lutte contre le crime (NCA) qui avait été perturbé en raison d'une attaque équivalente, dans ce qui s'apparentait à une riposte d'un groupe de pirates après une série d'arrestations.
Selon la police, quelque 30 % des entreprises britanniques ont signalé avoir subi des attaques par déni de service en 2014.

Réagissez à cet article

Source : *Le site de la BBC victime d'une cyber-attaque*

---

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Année après année, c'est le même constat : quels que soient leur taille et leur secteur d'activité, les entreprises ne protègent pas assez efficacement leurs réseaux et les données personnelles ou sensibles qu'elles hébergent. Dans la majorité des cas, les attaques informatiques ont été facilitées par le non-respect de règles essentielles : mises à jour des logiciels, mots de passe faible, données sensibles pas chiffrées…

Janvier : 20 000 sites français piratés
Des mairies, des universités, des conseils généraux, des églises ou des PME… Après l'attentat contre Charlie Hebdo, de nombreux sites ont été victimes de pirates se réclamant du groupe État islamique. Dans la majorité des cas, ce piratage s'est limité à du « défacement » (modification de la page d'accueil notamment en remplaçant du texte par des revendications et/ou des images). Ce nombre élevé peut surprendre. En réalité, très peu de sites appliquent des règles élémentaires de sécurité.

Février, le « casse » du siècle
Selon l'éditeur russe d'antivirus Kaspersky, une centaine d'établissements bancaires d'une trentaine de pays auraient perdu entre 260 à 800 millions d'euros. Cette attaque massive aurait été organisée par des équipes russes et ukrainiennes.

Avril : mauvais vol chez Ryanair
Environ 4,5 millions d'euros ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert

Juillet : des états civils plus privés
Des informations confidentielles sur la vie et l'état civil de près de 7% des Américains ont été volées dans les serveurs de l'Office of Personnel Management, une agence du gouvernement fédéral des États-Unis qui gère notamment les demandes d'emploi dans la fonction publique. 22, 5 millions de personnes sont concernées par ce vol de données personnelles. Ce n'est pas la première fois que des administrations américaines sont victimes d'intrusion.

Juillet : des hackers au volant
Ne plus se pas se véhicules seront connectés d'ici quelques années. Les constructeurs devront renforcer la sécurité de leurs modèles sous peine de sortie de route ! Dans le Missouri, deux hackers ont en effet démontré qu'il était possible de prendre le contrôle à distance d'une Jeep Cherokee commercialisée par le groupe Fiat Chrysler. Situés à une quinzaine de kilomètres du véhicule, Charlie Miller et Chris Valasek (deux experts en sécurité, le premier étant connu notamment pour avoir révélé plusieurs failles dans l'iOS d'Apple) ont coupé le moteur pendant que la voiture roulait sur une autoroute. Ils ont également pris le contrôle des freins et du volant.

Août : des rencontres adultères… publiques
13 millions de comptes utilisateurs (dont des Français avec des adresses du ministère de l'Intérieur, de la Culture ou de plusieurs mairies) d'Ashley Madison ont été récupérés par un pirate. La base de données de cet important site de rencontres adultères comprend des informations très sensibles, comme les préférences sexuelles ou le numéro de téléphone. Pire, aux États-Unis, plus de 15 000 adresses email utilisées pour la création du compte provenaient de l'administration américaine ou de l'armée. De quoi lancer des opérations d'usurpation d'identité ou du chantage. Des sanctions disciplinaires et des peines de prison sont annoncées. Les conséquences sont parfois dramatiques. La police canadienne enquête sur deux suicides potentiellement liés au piratage de ce site géré par Avid Life Media, une société canadienne de Toronto.

Novembre : jouets en panne
Le fabricant de jouets VTech a été victime du piratage d'une de ses bases de données. Des clients français, canadiens, ainsi que des ressortissants d'autres pays étaient enregistrés dans ce fichier d'environ 6 millions de données. Un internaute britannique de 21 ans a été arrêté le 17 décembre. Il ne serait pas le seul pirate à avoir pénétré ce serveur…

0
Réagissez à cet article

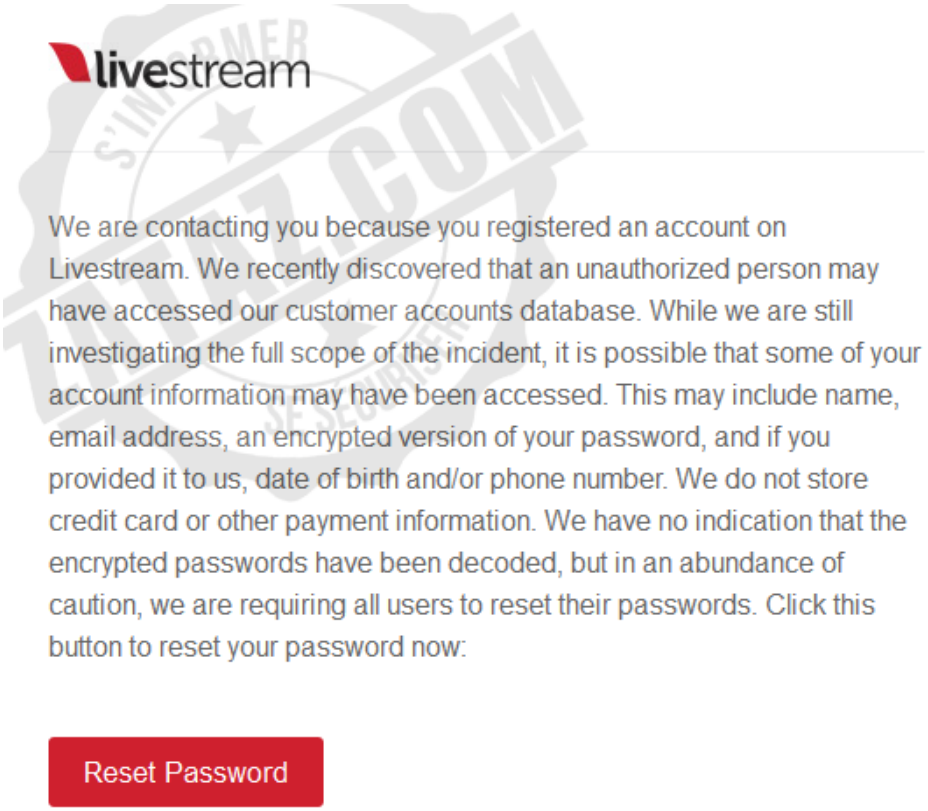
Source : *Les plus gros piratages de 2015 | Techniques de l'ingénieur*

Alerte : livestream.com victime d'un vol de données

Alerte : livestream.com victime d'un vol de données

Le site Internet dédié aux concerts en live sur Internet, livestream.com, visé par un piratage informatique.

C'est via un courrier électronique laconique, envoyé après le réveillon de Noël, que le site Internet dédié aux concerts en live sur Internet, livestream.com, indique avoir été visé par un piratage informatique. « ***Nous vous contactons parce que vous avez enregistré un compte sur Livestream,*** explique la missive. ***Nous avons récemment découvert qu'une personne non autorisée a pu avoir accès à nos comptes clients.***«


livestream

We are contacting you because you registered an account on Livestream. We recently discovered that an unauthorized person may have accessed our customer accounts database. While we are still investigating the full scope of the incident, it is possible that some of your account information may have been accessed. This may include name, email address, an encrypted version of your password, and if you provided it to us, date of birth and/or phone number. We do not store credit card or other payment information. We have no indication that the encrypted passwords have been decoded, but in an abundance of caution, we are requiring all users to reset their passwords. Click this button to reset your password now:

Reset Password

Bilan, une faille qui a donné accès à la base de données et aux informations des utilisateurs. « ***Cela peut inclure le nom, l'adresse électronique, une version chiffrée de votre mot de passe.*** » Bref, toutes les informations que les clients ont pu sauvegarder. Aucunes données de carte de crédit ou autres informations de paiement ont pu être lues par le pirate, la base de données impactées ne concernées par ce secteur numérique de livestream.com. « ***Dans un souci de prudence, nous conseillons aux utilisateurs de réinitialiser leur mot de passe***« .

Réagissez à cet article

Source : *ZATAZ Magazine » Piratage de données pour livestream.com*

Augmentation de la cybercriminalité encore prévu pour 2016

Augmentation de la cybercriminalité encore prévu pour 2016

Le nombre de piratages informatiques a substantiellement augmenté en 2015, une tendance qui devrait encore s'affirmer en 2016. Chefs d'Etat, groupes industriels, médias, banques, petites entreprises ou particuliers, personne n'est à l'abri de la menace.

Si les cyber-attaques (attaques informatiques, ndlr) ont augmenté durant l'année 2015 en France et dans le monde, la tendance ne semble pas près de s'atténuer en 2016. C'est la mise en garde prononcée par de nombreux organismes, dont le Cercle européen de la sécurité et des systèmes d'information. Cet organe, qui fédère les professionnels du secteur de la sécurité informatique, redoute un cyber-sabotage de grande ampleur en 2016.
Difficile cependant de cerner le danger car il vient de partout, emploie des formes diverses et peut toucher tout le monde, directement ou pas. A grande échelle, une attaque déclenchée à distance peut viser des objectifs affectant des bassins entiers de population : réseau électrique, distribution de l'eau, contrôle de la circulation, trafic aérien. Ou encore s'en prendre à des organismes gouvernementaux avec les conséquences que cela implique.

Des attaques en forte hausse

L'Allemagne a eu affaire à ces deux types d'attaques ces douze derniers mois: la mise hors service par deux fois d'un haut-fourneau dans la Sarre et le piratage de l'ordinateur personnel d'Angela Merkel. En France, l'exemple le plus spectaculaire remonte au printemps dernier quand la chaîne francophone TV5Monde (257 millions de foyers à travers le monde) a carrément cessé d'émettre durant plusieurs heures après une attaque perpétrée par Daech.

TV5 Monde avait été ouvertement ciblée par Daech. REUTERS/Benoit Tessier

A moyenne échelle, les malfaiteurs peuvent s'en prendre à une entreprise pour lui voler des données ou gripper son système informatique. Le cabinet PricewaterhouseCoopers révélait en octobre dernier que les cyber-attaques contre les entreprises avaient progressé de 38 % en un an dans le monde et de 51 % en France alors que les pertes financières s'élevaient à 3,7 millions d'euros par entreprise victime d'attaque en moyenne. Il faut noter que plus d'un tiers des sources d'incident provient d'employés de la compagnie attaquée.
A plus petite échelle, les particuliers sont touchés par des escroqueries en tout genre, à la carte de crédit par exemple. Ainsi, un rapport récent de Norton/Symantec révélait qu'un Français sur cinq s'était fait dérober ses données bancaires après un achat en ligne. Le phénomène est tellement répandu que les banques ont peut-être trouvé la parade, du moins provisoirement : le cryptogramme dynamique qui change toutes les 20 minutes, un identifiant qui va commencer à figurer au dos des cartes de crédit en 2016.

De plus en plus sophistiqués

Les hackers, remarquent les professionnels, utilisent des méthodes de plus en plus sophistiquées pour fracturer les systèmes informatiques de leurs cibles. Dans un rapport récent, l'entreprise de sécurité informatique roumaine Bitdefender identifiait des évolutions notables pour 2016. La première touchait aux systèmes de monétisation publicitaires et en particulier les systèmes de blocage de publicité qui pourraient être utilisés par les pirates informatiques pour développer de nouvelles souches de logiciels malveillants.
D'après Bitdefender, le monde de l'entreprise va être encore plus touché en 2016 à travers des attaques ciblées visant essentiellement le vol d'informations. Mais les individus aussi seront plus vulnérables, en partie du fait de la multiplication des objets connectés qui recèlent de nombreuses failles de sécurité exploitables par les cybercriminels. Même des systèmes d'exploitation réputés plus sûrs, comme le Mac OS X d'Apple, ne seraient plus à l'abri d'être percés par les malfaiteurs en ligne, selon Bitdefender.

Réagissez à cet article

Source : *La cybercriminalité devrait encore augmenter en 2016 – France – RFI*

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.

Ainsi, il convient de prendre les précautions suivantes :

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
LA PRESIDENTE

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*