Les Etats-Unis victimes d’une nouvelle cyber-attaque | Le Net Expert Informatique

Les Etats-Unis victimes d’une nouvelle cyber-attaque

Des pirates chinois seraient à l’origine d’une nouvelle cyber-attaque visant les données de fonctionnaires américains © Reuters/Pichi Chuang

Les données de millions de fonctionnaires américains ont été piratées ces derniers mois, aux Etats-Unis. Des cyber-pirates chinois seraient à l’origine de l’attaque, ils ont réussi selon des officiels américains à s’introduire dans les serveurs de l’Office of Personal Management, qui stocke notamment les profils des employés fédéraux.
Une nouvelle cyber-attaque d’envergure aux Etats-Unis. Les données personnelles de fonctionnaires ont été piratées depuis décembre 2014. Des hackers, apparement chinois, ont réussi à s’introduire dans les serveurs de l’Office of Personal Management (OPM), une agence qui vérifie notamment les profils des employés fédéraux pour le compte de la sécurité nationale.

4 millions de victimes, peut-être plus

Pas moins de quatre millions d’agents fédéraux, en activité ou à la retraite, ont été victimes de cette cyber-attaque. Ils vont devoir s’assurer auprès de leur banque que leurs données privées n’ont pas été utilisés par les pirates. D’autres éléments, comme les numéros de sécurité sociale et autres identifiants personnels sont également tombées aux mains des hackers.
Dans son communiqué, l’OPM n’exclut pas que d’autres personnes aient pu être victimes de cette attaque en ligne, menée au moment même où l’agence se dotait d’un nouveau système de sécurité. Vol de données ou espionnage, l’objectif des pirates reste en revanche incertain.
Le FBI, qui enquête sur l’affaire, dit « prendre au sérieux toutes les attaques potentielles contre les systèmes du secteur public et privé ».

Vulnérabilité du réseau informatique américain

L’attaque a été découverte en avril, mais la pêche aux informations aurait débuté dès la fin 2014. Une affaire de plus qui confirme la vulnérabilité du réseau informatique de l’administration américaine, fragilité dénoncée par le Government Accountability Office (GAO), l’équivalent de la Cour des comptes française.
Il y a quelques jours encore, on apprenait qu’une cybermafia avait réussi à récupérer les déclarations fiscales de plus de 100.000 contribuables. L’an dernier, le Département d’Etat et la Maison Blanche faisaient les frais d’intrusions attribuées à des Russes. A l’époque les courriels du président Barack Obama avaient été compromis.

Source : http://www.franceinfo.fr/vie-quotidienne/high-tech/article/les-etats-unis-victimes-d-une-nouvelle-cyber-attaque-des-hackers-chinois-soupconnes-688588
par Arnaud Racapé

Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai | Le Net Expert Informatique

	Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai

Quand la réalité rejoint la fiction. Le projet de loi renseignement, qui va être défendu par le gouvernement dans l'hémicycle du Sénat à partir de ce mardi, va « légaliser » certaines pratiques déjà utilisées par les services de renseignement. Les données récupérées avec ces nouveaux outils vont pouvoir être versées au dossier judiciaire des suspects.

Loi «Renseignement»: Les séries TV savent ce… *par 20Minutes*

Si elle fait l'objet d'un large consensus parmi la majorité des parlementaires, cette loi est contestée par les sénateurs communistes qui ont déposé une série d'amendements de suppression et ont dénoncé un risque de « surveillance de masse ». La plupart des techniques sur le point d'être légalisées sont déjà utilisées. Et diffusées dans les séries TV. Florilège…

Poser un mouchard sous une voiture
Dans Breaking Bad (Episode 9, Saison 5), Walt accuse Hank qui travaille pour la DEA, la brigade des stupéfiants américaine, d'avoir posé un tracker GPS sous sa voiture. Le projet de loi prévoit l'emploi de balises « permettant de localiser en temps réel un véhicule ou un objet ».

Mettre un appartement sous vidéosurveillance

Dans la deuxième saison de Scandal, l'appartement de l'avocate Olivia Pope est placé sous vidéo-surveillance par Jake Ballard, le fidèle ami du président. Elle s'en rend compte dans le 18e épisode. Des caméras partout, ainsi que des micros quasiment indétectables sont utilisés. Le projet de loi permettra aux services de renseignement d'appliquer ce type d'écoutes. Les policiers passeront cependant à travers le filtre de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Les plus sceptiques regrettent le pouvoir amoindri de cet organe de contrôle.

Géolocaliser un téléphone portable

Dès le premier épisode de la saison 1 du Bureau des Légendes, Cyclone, un des clandestins du BDL, est arrêté à Alger alors qu'il est ivre au volant d'une voiture. Le Bureau des Légendes va s'inquiéter : Cyclone étant musulman pratiquant, il n'aurait pas dû être saoul. Sisteron décide alors de géolocaliser son téléphone portable. Le signal du mobile indique qu'il se trouve bien au commissariat.

Intercepter les métadonnées d'un téléphone
Dans la série américaine Those who kill, Catherine Jensen, experte en tueurs en série, fait appel à un détective de la brigade des stupéfiants pour mettre sur écoute un suspect. Ce dernier, à l'épisode 9 détaille comment les policiers parviennent à récupérer les données enregistrées sur un téléphone portable, en se faisant passer pour une antenne relais après avoir copié la carte sim. Dans la « vraie vie », les policiers utilisent des Imsi-Catchers qui peuvent intercepter dans un rayon donné toutes les données qui transitent via un téléphone. Cette technologie, rendue possible par la loi renseignement, fait pourtant polémique.

Capter un écran d'ordinateur en direct grâce à un logiciel espion
Les experts de CSI : Cyber (saison 1, épisode 1), mettent au point ce qu'ils appellent un RAT (Remote Administration Tool), un outil d'administration à distance. En clair, un programme permettant la prise de contrôle total, à distance, d'un ordinateur depuis un autre ordinateur. Ils y ont introduit un logiciel espion qui permet, en fonction de mots-clés utilisés dans un mail, d'activer une alarme. Ils peuvent aussi capter en direct le mot-clé qui est tapé. Les défenseurs de la liberté numérique dénoncent à travers la loi Renseignement la surveillance massive des ordinateurs des internautes.

Source : http://www.20minutes.fr/societe/1621371-20150602-video-loi-renseignement-vu-series-tv-ca-pourra-passer-vrai
Par William Molinié

Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails | Le Net Expert Informatique

	Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails

Peut-on se passer de l'e mail dans le cadre de ses activités professionnelles ? Pratique et instantanée, la communication par e-mail s'est imposée au quotidien dans l'entreprise. Certaines études évaluent à plus de 100 milliards le nombre d'e-mails professionnels qui sont échangés chaque jour(1).

Nos e mails risquent-ils de laisser échapper des données sécurisées ?
Malgré ses nombreux atouts, l'e-mail présente également certains risques. Des récits de fuites de données sensibles font régulièrement la une des médias. Un des derniers incidents en date : la récente divulgation des numéros de passeport de 31 leaders mondiaux. En cause ? La fonctionnalité de saisie automatique à partir du carnet d'adresses d'Outlook. Cette fonctionnalité – aussi pratique soit-elle – ne fait qu'accentuer le risque de diffuser, par erreur, des données confidentielles.
Malgré l'augmentation du nombre d'erreurs d'aiguillage d'e-mails et l'évolution du contexte législatif – comme en atteste la récente loi australienne sur l'obligation de conserver des métadonnées et d'autres textes réglementant la transmission de données confidentielles (HIPAA, FIPPA et PCI) –, on peut s'étonner que les entreprises ne soient pas plus nombreuses à choisir de sécuriser le contenu de leurs e mails.
L'e mail est sans doute un peu trop pratique à en juger par la facilité avec laquelle des informations sensibles peuvent être envoyées, au risque de tomber dans les mauvaises mains.

Quelques chiffres :
• 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes (2).
• 21 % des employés déclarent envoyer des données sensibles sans les chiffrer(2). Les coûts liés à la perte de données s'envolent, sans parler des conséquences sur la réputation des entreprises et des éventuelles répercussions sur le plan juridique en cas de violation de la réglementation sur la transmission et le stockage de données confidentielles (notamment dans le cadre des lois HIPAA et FIPPA, et du standard PCI).
• 22 % des entreprises sont concernées chaque année par la perte de données via e-mail(3).
• 3,5 millions de dollars : coût moyen d'une violation de données pour une entreprise(4).

La solution
Il existe heureusement des solutions de sécurité des e-mails qui mettent les utilisateurs et leur entreprise à l'abri de ces menaces. La signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message et évitent que des données sensibles ne tombent dans de mauvaises mains. Le destinataire a également l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
Le chiffrement d'un e-mail revient à sceller son message puis à le déposer dans un dossier verrouillé dont seul le destinataire prévu possède la clé. Il est alors impossible pour une personne interceptant le message, pendant son transit ou à son emplacement de stockage sur le serveur, d'en voir le contenu. Sur le plan de la sécurité, le chiffrement des e mails présente les avantages suivants :
• Confidentialité : le processus de chiffrement requiert des informations de la part du destinataire prévu, qui est le seul à pouvoir consulter le contenu déchiffré.
• Intégrité du message : une partie du processus de déchiffrement consiste à vérifier que le contenu du message d'origine chiffré correspond au nouvel e-mail déchiffré. Le moindre changement apporté au message d'origine ferait échouer le processus de déchiffrement.
Avant de choisir une solution, il est important d'avoir en tête plusieurs choses. L'utilisateur est le mieux placé, car il connaît son entreprise mieux que personne. Phishing, perte de données… quels sont ses principaux sujets de préoccupation ? Quelle est l'infrastructure de messagerie en place dans l'entreprise ? Quel est le cadre réglementaire ? Les réponses propres à chaque entreprise orienteront les choix vers la solution la plus appropriée.

Sources :
(1) Email Statistics Report 2013-2017, The Radicati Group, Inc.
(2) SilverSky Email Security Habits Survey Report, SilverSky, 2013
(3) Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014
(4) Global Cost of Data Breach St'sudy, Ponemon Institute,

Source : http://www.globalsecuritymag.fr/Les-dernieres-fuites-de-donnees,20150601,53078.html
par GlobalSign

L’employé, la première faille de sécurité | Le Net Expert Informatique

	L’employé, la première faille de sécurité

Si les entreprises se concentrent toujours sur leur protection informatique vis-à-vis des intrusions externes, se méfient-elles assez de leurs propres employés ? Pas toujours à en croire certaines histoires de ces dernières années.

L'ennemi a beau souvent être à l'extérieur de l'entreprise, il n'en reste pas moins que les employés eux-mêmes peuvent devenir de véritables problèmes, à plus ou moins grande échelle. Bien entendu, les plus grands risques internes sont faits à l'insu du collaborateur, du fait de son manque de technique et/ou d'attention, mais parfois, l'acte malveillant est réellement sciemment.

L'affaire Coca Cola

Fin 2013, le géant Coca Cola, qui compte tout de même près de 130 000 employés, s'est par exemple rendu compte qu'elle avait été victime durant de longues années d'un voleur d'ordinateurs portables. L'employé en question a ainsi dérobé 55 ordinateurs sur plusieurs années, volant ainsi des données sur environ 74 000 personnes, la plupart étant des employés du géant américain ou des collaborateurs reliés à la firme.

Réalisé par un employé (au nom inconnu) ayant en charge les équipements informatiques, non seulement l'acte en lui-même a sonné comme une véritable claque pour la firme US, mais surtout, parmi toutes les données concernées, 18 000 concernaient les numéros de sécurité sociale, données particulièrement sensibles outre-Atlantique.

Pire encore, selon un mémo de Coca Cola envoyé aux employés et révélé par le Wall Street Journal, aucune des données volées n'était chiffrée. Nous apprenons aussi qu'afin d'éviter la panique, le spécialiste de la boisson gazeuse a tenté de résoudre le problème en secret durant plusieurs semaines. Les vols ont ainsi été remarqués en décembre 2013, mais la firme a attendu le 24 janvier pour en informer ses employés.

Plus que le côté technique, cette histoire nous montre donc que la sécurité est aussi (surtout ?) une question de processus. La « faille » de Coca Cola ainsi été humaine et organisationnelle plus qu'autre chose.

Boeing aussi

Coca n'est toutefois pas la seule très grande compagnie concernée par ce genre de problématique. En 2006, un employé de Boeing a par exemple été licencié non pas pour avoir dérobé du matériel et des données, mais du fait de sa responsabilité dans un vol d'ordinateur. Le collaborateur a ainsi enfreint les règles de l'entreprise en téléchargeant des informations confidentielles sur son PC portable sans même les chiffrer.

Problème, l'employé avait téléchargé des données personnelles de 380 000 employés actuels et passés de la compagnie, comme des numéros de sécurité sociale, des noms, des adresses, etc. Le tout fut ensuite volé en décembre 2006, entraînant le licenciement du collaborateur.

Cette faute grave n'était pas une première, puisque selon le porte-parole de Boeing, deux autres vols d'ordinateurs portables contenant des données sur les employés ont été dérobés entre 2005 et 2006. « Nous encourageons les gens à travailler hors du serveur, ce qui permettrait de garder l'information derrière le pare-feu. Si vous téléchargez des informations sur votre ordinateur portable, cela est censé être temporaire et l'information est censée être cryptée » a bien insisté Boeing à l'époque. Du simple bon sens a priori peu respecté par certains de ses employés.

Moralité de ces deux histoires : la sécurité est avant tout une affaire d'organisation, de processus et de règles. S'il est évident qu'il faut se prémunir des actions malintentionnées extérieures, « l'ennemi » peut aussi être à l'intérieur, que ce soit du fait d'actes réalisés délibérément ou non. BYOD ou non, les comportements des employés peuvent être cruciaux pour la sécurité de l'entreprise. Rédiger une politique stricte et mettre en place des systèmes de surveillances (ou au moins de vérification), notamment pour ceux manipulant des données sensibles, est ainsi indispensable si l'on veut éviter de lourdes déconvenues…

Source : http://www.zdnet.fr/actualites/l-employe-la-premiere-faille-de-securite-39819662.htm

Votre entreprise est-elle assurée contre les pirates informatiques ? | Le Net Expert Informatique

	Cyberattaques: votre entreprise est-elle assurée contre les pirates ?

Pertes de données, poursuites judiciaires, systèmes informatiques endommagés… les cyberattaques représentent une nouvelle gamme de risques auxquels les entreprises petites et grandes sont confrontées. Sentant la bonne affaire, certains assureurs offrent maintenant une protection contre ces écueils. En quoi consiste une telle assurance ? Est-elle devenue incontournable ?

Évaluer les risques

Inutile de parler d'assurance si on ne connaît pas d'abord le risque auquel on est exposé. Celui d'être victime d'une cyberattaque ne se mesure pas tant selon la taille de l'entreprise que par rapport au type d'information que l'on y traite. Ce n'est donc pas seulement le souci des grandes boîtes. L'étude «Internet Security Threat Report 2014» du concepteur d'antivirus Symantec révèle d'ailleurs que 61 % des hameçonnages ciblés ont visé des PME en 2013, comparativement à 50 % un an plus tôt.

Or, des études récentes de Cisco montrent qu'un peu plus de la moitié des entreprises canadiennes n'ont pas encore mis en place un plan en matière de sécurité informatique. «C'est primordial pour déterminer les types de renseignements à protéger, les moyens de les stocker, les personnes qui y ont accès, l'équipement, etc.», précise Maya Raic, présidente-directrice générale de la Chambre de l'assurance de dommages.

Stockez-vous sur vos serveurs une base de données contenant le numéro d'assurance sociale de médecins spécialistes ? Ou un simple catalogue de vos produits ? Les données ont un degré de sensibilité variable. Cela dit, plus vous traitez de l'information de tiers ou de la propriété intellectuelle, plus vous avez de risques de poursuites en cas de brèche de sécurité.

« 117 339: c'est le nombre de cyberattaques commises chaque jour dans le monde, d'après une récente enquête de PwC. Et ce ne sont là que celles dont les entreprises sont conscientes, puisque près des 3/4 des attaques ne sont pas décelées. »

Des polices sur mesure

«On compte actuellement une dizaine d'assureurs au Canada qui protègent les entreprises contre les cyberrisques», soutient Maya Raic.

Comme on n'en est qu'aux balbutiements de ce type d'assurance, les clauses varient d'un assureur à l'autre. «On traite encore les clients au cas par cas, donc ceux-ci peuvent négocier les termes», mentionne Jean-François De Rico, associé au cabinet d'avocats Langlois Kronström Desjardins.

Les polices peuvent couvrir la responsabilité liée aux pertes de données (les recours collectifs potentiels, les atteintes à la réputation commerciale ou les frais liés au redémarrage des systèmes), la gestion de crise, l'interruption des affaires, la cyberextorsion, etc.

Quant aux exclusions standards, ces polices n'en comportent pas vraiment, contrairement aux autres types d'assurance qui excluent d'emblée certains risques. Ce que vous pourriez voir toutefois, c'est une clause qui délimite le cadre de l'assurance. «Par exemple, la responsabilité civile des dirigeants et des administrateurs n'est pas couverte par la cyberassurance, puisque cette protection existe déjà dans une autre police d'assurance sans lien avec le cybercrime», illustre Alexis Héroux, courtier en assurance de dommages chez Marsh Canada.

« Installer les mises à jour dans les 48h où elles sont disponibles par les fournisseurs d'antivirus réduit les risques de cyberattaques de 85%. »

C'est combien ?

Les limites de couverture varient énormément selon les compagnies d'assurance et peuvent aller de 500 000 dollars à 20 millions de dollars. Si plusieurs assureurs se réunissent, la limite peut même atteindre 250 millions de dollars.

On devine que le coût des primes varie tout autant, selon la limite choisie et l'ensemble des facteurs qui peuvent influencer le risque : le type et la quantité de données utilisées et recueillies par l'entreprise, le système de gestion en place, etc. Les PME dont les besoins de protection sont moindres pourraient réussir à obtenir une prime annuelle minimale de 1 500 dollars, mais c'est en général beaucoup plus coûteux. Retenez surtout que tout se négocie, selon votre budget.

« 201$: c'est le prix que coûte en moyenne chaque donnée de tiers sensible et confidentielle qui a été volée. »

Cela dit, comme pour les autres types d'assurance, les cyberrisques ne reposent jamais entièrement sur les épaules des assureurs. L'entreprise a sa part de responsabilité. Aussi, plus on a une infrastructure de sécurité sophistiquée et bien gérée, plus on réduit le risque, et donc le coût de la prime (voire la nécessité d'une protection d'assurance).

Cependant, quand on sait que même des spécialistes comme Symantec ont déjà été victimes d'une cyberattaque, il vaut mieux, parfois, investir un certain montant en assurance pour couvrir ces nouveaux aléas.

Source : http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-votre-entreprise-est-elle-assuree-contre-les-pirates-/579164

Attaque à grande échelle de routeurs | Le Net Expert Informatique

Une attaque à grande échelle utilise les browsers pour détourner les routeurs

Des chercheurs ont découvert un outil d'attaque web qui permet à des pirates de détourner les serveurs DNS des routeurs et de les remplacer par des serveurs voyous.

Des cybercriminels ont développé un outil d'attaque web à grande échelle qui leur permet d'exploiter les vulnérabilités des routeurs et de détourner leurs paramètres DNS quand les utilisateurs visitent des sites web compromis ou sont dirigés vers des publicités malveillantes depuis leurs navigateurs. L'objectif de ces attaques est de remplacer les serveurs DNS configurés sur les routeurs par des serveurs voyous contrôlés par des attaquants. Ainsi, les pirates peuvent intercepter le trafic, le rediriger vers des sites frauduleux, détourner les requêtes de recherche, injecter des publicités malveillantes sur les pages web et plus encore.

L'adresse DNS, qui est comparable à un annuaire de l'Internet, a un rôle essentiel. Elle traduit les noms de domaine, plus faciles à mémoriser, en adresses IP indispensables pour faire communiquer les ordinateurs entre eux. La gestion des adresses DNS se fait en cascade. Quand un utilisateur tape le nom d'un site Web dans un navigateur, la requête est d'abord transmise au système d'exploitation. Et, pour diriger le navigateur vers l'adresse IP demandée, le système d'exploitation doit passer par le routeur local qui est lui-même chargé d'interroger les serveurs DNS généralement configurés et gérés par le fournisseur d'accès internet. La chaîne de commandes se poursuit jusqu'à ce que la demande parvienne au serveur ayant autorité pour le nom de domaine recherché ou jusqu'à ce qu'un serveur fournisse les informations de son cache. Or, si des attaquants d'immiscent dans une des étapes du processus, ils peuvent répondre à la requête en renvoyant une adresse IP frauduleuse. Ils peuvent ainsi tromper le navigateur et l'orienter vers le site d'un serveur différent. Typiquement, ce site pourrait, par exemple, héberger la réplique d'un site réel qui servirait aux pirates à dérober des informations de connexion d'un utilisateur.

Détecter le routeur pour adapter l'attaque

Un chercheur en sécurité indépendant, connu en ligne sous le nom de Kafeine, a récemment observé des attaques dites « drive-by » lancées à partir de sites web compromis qui redirigeaient les utilisateurs vers un kit d'exploits inhabituel basé sur le web, spécifiquement conçu pour compromettre les routeurs. En général, les kits d'exploits vendus sur les forums illégaux et utilisés par les cybercriminels cherchent à exploiter des vulnérabilités dans les plug-ins pour navigateurs comme Flash Player, Java, Adobe Reader ou Silverlight. Leur but est d'installer des logiciels malveillants sur les ordinateurs qui n'auraient pas téléchargé les dernières versions de ces modules populaires. Le plus souvent la stratégie de ces attaques consiste à injecter un code malveillant dans des sites compromis ou de l'inclure dans des publicités malveillantes, code qui redirige automatiquement les navigateurs vers un serveur d'attaque chargé de déterminer l'OS, l'adresse IP, la localisation géographique, le type de navigateur utilisé, les plug-ins installés et d'autres détails techniques. En fonction de ces informations, le serveur d'attaque sélectionne dans son arsenal d'exploits ceux qui ont le plus de change de réussir.
Mais, les attaques observées par Kafeine fonctionnent différemment : cette fois, les utilisateurs de Google Chrome ont bien été redirigés vers un serveur malveillant, mais celui-ci a chargé un code destiné à déterminer le modèle de routeur utilisé afin de remplacer les serveurs DNS configurés sur l'appareil. « Beaucoup d'utilisateurs pensent que si leurs routeurs ne sont pas configurés pour la gestion à distance, les pirates ne peuvent pas exploiter les vulnérabilités de leurs interfaces d'administration web à partir d'Internet, parce que ces interfaces ne sont accessibles qu'à partir des réseaux locaux. Mais, cela est faux », a déclaré le chercheur. De telles attaques sont possibles grâce à une technique appelée Cross-Site Request Forgery (CSRF), laquelle permet à un site web malveillant de forcer le navigateur à exécuter des actions malveillantes sur un site Internet différent. Et le site cible peut justement être l'interface d'administration d'un routeur uniquement accessible via le réseau local. De nombreux sites web ont mis en place des défenses pour se protéger contre ces attaques CSRF, mais les routeurs ne bénéficient généralement pas de ce type de protection.

Les principaux routeurs vulnérables

Le nouveau kit d'exploits drive-by identifié par Kafeine a utilisé la technique du Cross-Site Request Forgery pour détecter plus de 40 modèles de routeur de divers fournisseurs dont Asustek Computer, Belkin, D-Link, Edimax Technology, Linksys, Medialink, Microsoft, Netgear, Shenzhen Tenda Technology, TP-Link Technologies, Netis Systems, Trendnet, ZyXEL Communications et HooToo. Selon le modèle, l'outil essaie de changer les paramètres DNS du routeur en exploitant des vulnérabilités connues par injection de commande ou en utilisant des identifiants d'administration courants. Dans ce cas aussi, il utilise la technique CSRF. Et en cas de succès de l'attaque, le serveur DNS primaire du routeur passe sous contrôle des attaquants et le serveur secondaire, utilisé comme relais en cas de panne, est paramétré en tant que serveur DNS public de Google. De sorte que, si le serveur malveillant est temporairement hors service, le routeur disposera toujours d'un serveur DNS parfaitement fonctionnel pour résoudre les requêtes, et le propriétaire ne pourra pas soupçonner une défaillance, ni être tenté de reconfigurer l'appareil.

Selon Kafeine, l'une des vulnérabilités exploitées par l'attaque affecte les routeurs de divers fournisseurs, et a été rendue publique en février. « Certains fournisseurs ont effectué des mises à jour de firmware sur leurs routeurs, mais le nombre de matériels mis à jour au cours des derniers mois reste probablement très faible », a déclaré le chercheur. Car la plupart des routeurs doivent être mis à jour manuellement et l'opération exige certaines compétences techniques. Voilà pourquoi un grand nombre de routeurs ne sont pas mis à jour. Et les attaquants le savent. En fait, d'autres vulnérabilités sont ciblées par ce kit d'exploits, dont l'une a été identifiée en 2008 et l'autre en 2013.

1 million de tentatives le 9 mai

Toujours selon le chercheur indépendant, il semble que l'attaque a été menée à grande échelle : au cours de la première semaine du mois de mai, le serveur d'attaque a comptabilisé environ 250 000 visites uniques par jour, avec un pic de près de 1 million de visites le 9 mai. Les pays les plus touchés étaient les États-Unis, la Russie, l'Australie, le Brésil et l'Inde, mais la répartition du trafic a été plus ou moins globale. Pour se protéger, les utilisateurs doivent vérifier régulièrement si de nouvelles mises à jour de firmware pour leurs routeurs sont disponibles sur les sites Web des fabricants et ils doivent les installer, surtout si ces mises à jour concernent des correctifs de sécurité. Si le routeur le permet, les utilisateurs devraient également limiter l'accès à l'interface d'administration à une adresse IP à laquelle aucun terminal n'a normalement accès, mais qu'ils peuvent affecter manuellement à leur ordinateur en cas de besoin de façon à pouvoir modifier les paramètres de leur routeur.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-attaque-a-grande-echelle-utilise-les-browsers-pour-detourner-les-routeurs-61265.html
Par Jean Elyan

« Vol » de documents via Google, la condamnation de Bluetouff confirmée | Le Net Expert Informatique

	« Vol » de documents via Google, la condamnation de Bluetouff confirmée

Olivier Laurelli, relaxé en première instance, avait accédé sans piratage à un extranet accessible par le moteur de recherche. Condamné en appel, son pourvoi en cassation a été rejeté.

Trop fouiller dans Google peut être cause de sanction judiciaire. Olivier Lorelli, alias Bluetouff, blogueur reconnu dans le domaine de la sécurité informatique, cofondateur du site Reflets.info, en fait l'amère expérience. Le spécialiste voit en effet sa condamnation pour « maintien frauduleux » dans le système et « vol » de documents confirmée par la Cour de cassation, révèle Le Parisien.
Rappel des faits. En 2012 Bluetouff avait trouvé par hasard « le serveur extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses), utilisé par les chercheurs pour stocker et échanger leurs documents de travail. Au lieu d'être protégées par un identifiant et un mot de passe, comme elles auraient dû l'être, ces données, indexées sur Google, étaient accessibles sans le moindre piratage. »
Le blogueur télécharge alors 8.000 de ces documents internes, sur des données de santé publique. Il publie plus tard un article sur les nanoparticules qui utilise une infime partie de ces documents, ce qui alerte l'Anses, laquelle lance la police sur l'affaire. La DCRI identifie le blogueur, et s'ensuivent une perquisition à son domicile, la saisie de son matériel informatique et une garde à vue de 30 heures. Rien que ça.

« Gogleu ? Lojin ? »
Olivier Laurelli est presque logiquement relaxé en première instance. En avril 2013, les juges considèrent qu'il n'y a pas eu de piratage pour accéder aux documents (récit par l'intéressé) : « Il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier Laurelli a pu récupérer l'ensemble des documents sans aucun procédé de type « hacking » », écrivaient-ils.
L'Anses ne fait d'ailleurs pas appel, contrairement au Parquet qui ne digère pas cette relaxe. Mauvaise pioche pour Bluetouff, le second procès, en décembre dernier, a opposé le pseudo-pirate à des juges visiblement très loin de maîtriser le sujet.
Un journaliste de Médiapart rapporte que « la magistrate chargée de rappeler les faits semblait même ne pas connaître Google, prononcé à la française « gogleu », ni savoir ce que signifie un « login », prononcé « lojin ». Difficile, dans ces conditions, d'expliquer qu'il est effectivement possible de tomber sur des documents de travail par une simple recherche… […] « Vous ne vous souciez pas de savoir si vous alliez tuer toute la planète? » s'indigne ainsi une magistrate alors que l'accusé vient de lui expliquer que ces documents n'étaient, visiblement, pas confidentiels. »
Si les juges relaxent le blogueur du chef d'« accès frauduleux », il le condamne néanmoins à une amende de 3.000 euros pour « maintien frauduleux dans un système de traitement automatisé de données » et « vol » de documents. De plus, cette peine sera inscrite à son casier judiciaire.
Olivier Laurelli et son avocat, Olivier Iteanu, décident alors de se pourvoir en cassation, pourvoi donc rejeté : la condamnation est donc confirmée. Dénonçant un « vrai scandale », l'avocat du blogueur, a annoncé à nos confrères son intention de saisir la Cour européenne des droits de l'Homme. Selon lui, on « fait payer » à son client des écrits « mettant en cause des entreprises et des services français ».
Le fait qu'aucun piratage n'ait été effectué n'a pas ému la cour qui rappelons-le ne juge que la forme, pas le fond de la procédure. Reste que cette condamnation confirmée constitue une très mauvaise nouvelle pour les lanceurs d'alerte.

Source : http://www.zdnet.fr/actualites/vol-de-documents-via-google-la-condamnation-de-bluetouff-confirmee-39819710.htm

Alerte : Des millions de routeurs domestiques peuvent être attaqués à distance | Le Net Expert Informatique

Une faille dans le driver NetUSB permet à un pirate de prendre le contrôle total de l'équipement et d'y installer, par exemple, des malwares. Pour l'instant, seul TP-Link a fourni un correctif.

Netgear, TP-Link, Trendnet, Zyxel… Si vous possédez un routeur domestique de l'une de ces marques, il est probable que vous ayez un problème de sécurité. La plupart de ces routeurs disposent en effet d'une fonctionnalité théoriquement assez pratique, à savoir le partage en réseau d'une connexion USB. Concrètement, vous connectez un équipement en USB sur votre routeur – un disque dur par exemple – et celui-ci devient alors accessible à distance au travers du réseau. Beaucoup de ces routeurs s'appuient pour cela sur un module logiciel nommé « NetUSB », développé par le fournisseur taiwanais KCodes.
Le problème, c'est qu'il existe dans ce module une faille qui permet à une personne mal intentionnée de faire crasher le routeur ou d'y exécuter n'importe quel code. Et donc d'en prendre possession pour, par exemple, y installer des malwares. Cette vulnérabilité a été découverte par les chercheurs en sécurité de la société autrichienne SEC Consult. Elle repose sur une erreur de codage : quand le nom de l'ordinateur qui souhaite se connecter à distance est supérieur à 64 caractères, le module NetUSB génère un dépassement de mémoire tampon et le fait planter. Pire : comme ce module est exécuté au niveau du noyau Linux du routeur, cette faille permet d'accéder au plus haut niveau de privilège. Plutôt pratique pour un pirate.

Exemple de routeur vulnérable.

Attaque par Internet
Certains d'entre vous se diront que ce n'est pas si grave que cela, car il faut déjà pouvoir rentrer dans le réseau domestique pour réaliser cette attaque. Mais cela n'est pas toujours vrai. Les chercheurs de SEC Consult ont trouvé que pour un certain nombre de routeurs, les connexions NetUSB étaient accessibles par Internet, peut-être en raison d'une mauvaise configuration. Par ailleurs, il s'avère que la procédure d'authentification utilisée pour initier une connexion avec NetUSB est totalement inutile : « les clés AES sont statiques et peuvent être trouvées dans le driver », expliquent les chercheurs. En d'autres termes, lorsque le routeur expose sa fonctionnalité NetUSB sur le web, un pirate pourra s'y introduire sans problème.
Une rapide recherche a montré qu'au moins 26 fabricants de routeurs utilisent le logiciel de KCodes dans au moins 92 produits. Ce qui représente certainement plusieurs millions de clients dans le monde. Contacté par les SEC Consult, KCodes n'a fait aucun commentaire. Que faut-il faire pour se protéger ? Seul TP-Link a développé, à ce jour, un correctif qu'il diffusera progressivement dans ses différents modèles. Dans certains équipements, il est possible, par ailleurs, de désactiver le partage de connexion USB. Les clients de Netgear, en revanche, ne pourront rien faire. Le fabricant a indiqué d'emblée ne pas pouvoir produire de patch, et qu'il était impossible de désactiver la fonction de partage. Il ne reste alors qu'une seule solution : la prière.

Source : http://www.01net.com/editorial/655187/des-millions-de-routeurs-domestiques-peuvent-etre-attaques-a-distance/

Denis JACOPINI questionné par un journaliste de l’Express | Le Net Expert Informatique

	Denis JACOPINI questionné par un journaliste de l’Express

Le site d'actualité de jeux vidéo Nintendojo.fr a faussement annoncé mercredi 1er avril avoir été bloqué par le ministère de l'Intérieur. Une blague douteuse qui, par l'absurde, révèle néanmoins certains écueils de la loi Cazeneuve. Explications.

Voici l'écran qui s'affiche ce mercredi lorsque l'on tente de se connecter au site Nintendojo.fr

Ministère de l'Intérieur

Enfin, les détracteurs de la loi Cazeneuve tiennent leur martyr! Jugez donc: Nintendojo.fr, un simple site consacré à l'actualité des jeux Nintendo, est inaccessible ce mercredi. Il renvoie vers une page du ministère de l'Intérieur qui explique que le contenu a été bloqué. Une mesure qui est autorisée depuis le vote de la loi Cazeneuve fin 2014, avec de premiers cas en mars dernier, mais en principe réservée aux sites terroristes ou pédophiles.

Rassurez-vous tout de suite. « Il s'agit d'une blague de mauvais goût et ça nous a bien fait rigoler », explique à L'Express Mortal, l'administrateur du site. Il ne faut donc pas voir la main du ministère de l'Intérieur derrière ce faux blocage, mais un poisson d'avril qui aura trompé des dizaines d'internautes et quelques sites d'information.

Pourquoi ce gag?

« Ce n'est pas un geste politique, mais nous estimons quand même que la loi qui permet le blocage de certains sites internet est mauvaise, justifie Mortal, qui se revendique de la Quadrature du Net, association de défense des libertés sur internet hostile au dispositif. On avait envie de piquer les gens pour que ça éveille un peu les consciences sur le sujet. Cela pourrait arriver pour de vrai à d'autres demain, c'est ça le problème », tranche-t-il.

De la difficulté de distinguer « vrai » et « faux » blocage

Qu'on le juge drôle ou pas, le poisson d'avril de Nintendojo.fr pose de sérieuses questions sur le principe même de bloquer certains sites Internet. Est-il possible pour un internaute face à une page qui affiche le fameux message du ministère de l'Intérieur de savoir avec certitude que le site a été bloqué? « La réponse est simple: c'est non », estime **Denis Jacopini**, consultant en cybersécurité. Point de vue partagé par plusieurs observateurs interrogés ce mercredi.

« **Rien est impossible, poursuit l'analyste. Cela peut être un vrai message, bien sûr. Mais cela peut aussi être une blague de l'administrateur du site, ou l'oeuvre d'un hacker qui a modifié le site**« , avance-t-il.

Qu'en pense l'Intérieur? Contactés par L'Express, les services du ministère n'ont pas donné suite à nos sollicitations. A ce jour, les services de la Place Beauvau n'ont pas mis en place de dispositif pour informer sur de telles situations. Il ne serait pas étonnant, dans ce contexte, de voir fleurir les farces voire de réelles arnaques du même tonneau dans les semaines qui viennent.

Attention, arnaques à prévoir…

Dans le cas de Nintendojo.fr, l'artifice était plutôt élaboré. Le message affiché sur la page d'accueil du site reprenait, aussi bien graphiquement qu'au niveau du contenu, celui affiché en cas de blocage. Ce n'est pas tout. Un utilisateur de Twitter a comparé le code HTML de la page vers laquelle redirigeait Nintendojo.fr avec celui d'une page affichée via un site réellement bloqué par l'Intérieur, et ils étaient bien identiques.

Mais Nintendojo.fr est allé encore plus loin. « Nous avons vraiment procédé à un blocage DNS » (domain name system, nom de domaine) explique Mortal. Ce qui a pu donner l'illusion a certains que le site avait bel et bien été « bloqué ». « Techniquement, le dispositif de censure fait appel à un résolveur DNS menteur, c'est-à-dire qu'il ne renvoie pas le résultat correct, mais un mensonge tel que demandé par le gouvernement », explique nextinpact.com.

Concrètement, le gouvernement n'efface pas les sites bloqués: l'internaute qui essaye de s'y connecter est simplement redirigé vers la fameuse page ministérielle. Un mécanisme que Nintendojo.fr a plutôt bien singé ce mercredi.

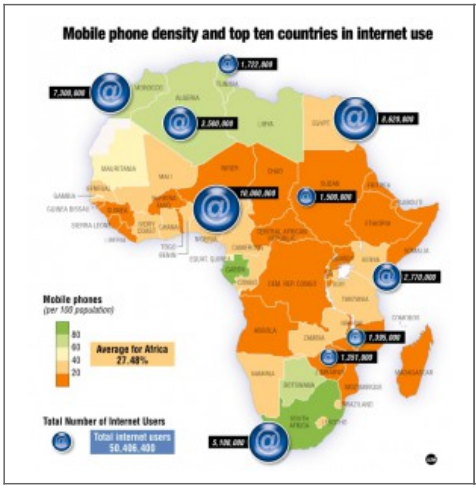
« On aurait pu faire encore plus sophistiqué »

Les bons connaisseurs, eux, ont néanmoins pu déjouer la supercherie en testant d'autres DNS. Ils ont alors observé que tous renvoyaient vers la page du ministère de l'Intérieur, ce qui n'aurait pas été le cas pour un « vrai » blocage gouvernemental. En situation réelle, les fournisseurs d'accès à Internet (FAI) bloquent le site concerné au fur et à mesure, ce qui prend du temps. De plus, il existe des DNS publics, gérés par d'autres acteurs du Web (par exemple, Google), qui peuvent ne pas faire l'objet de blocage. Changer de résolveur DNS est d'ailleurs précisément l'une des solutions pour ceux qui souhaitent contourner la censure.

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

Source : http://lexpansion.lexpress.fr/high-tech/les-vraies-questions-que-pose-le-faux-blocage-de-nintendojo-par-le-gouvernement_1667195.html

En Afrique la communication digitale s’impose en entreprise Le Net Expert Informatique



En Afrique la communication digitale s’impose en entreprise

Décidément, la communication digitale rivalise avec les outils du marketing classique, et grignote désormais une part importante du « budget communication » des entreprises, associations, organisations et institutions gouvernementales.

Au fur et à mesure de l'accroissement de l'utilisation d'Internet en Afrique, les différentes formes d'entreprises et institutions se tournent de plus en plus vers des experts en communication digitale pour renforcer leur présence sur le web.
« le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions » Indique l'UIT

Quelques chiffres clés sur le digitale en Afrique
Selon le rapport annuel publié par l'UIT (Union Internationale des Télécommunications), en fin de l'année 2014, seulement 42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010, une croissance considérée relativement importante en une période de 4 ans. Selon la même source, le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions.

Pénétration Internet et Mobiles dans les pays d'Afrique
La même année Google a également réalisé une étude statistique portant sur le comportement des internautes dans le monde notamment les Africains qui sont de plus en plus présents sur Internet dans l'objectif d'acheter quelque chose ou simplement consulter des produits sur le web. Cette étude chiffrée indique que l'augmentation des achats en ligne est de 33% au Kenya, 37% en Afrique du Sud et 49% au Nigeria.
Ces chiffres illustrent en partie l'évolution du comportement des Africains vis-à-vis du réseau internet.
Ces estimations indiquent également un avenir prometteur pour la communication digitale sur ce continent. Les pays les plus matures en matière de marketing digital sont certainement ceux ayant les taux de pénétration d'Internet les plus élevés, à citer le Nigeria, l'Afrique du Sud, l'Égypte, le Maroc et la Tunisie.

Rôle des agences de communication digitale ou webmarketing
Une présence proactive sur Internet permet non seulement de maîtriser l'e-réputation mais aussi de booster les ventes et conquérir de nouveaux marchés. Les agences de communication digitale utilisent aujourd'hui des techniques très avancées pour cibler efficacement les internautes et aussi suivre l'audience des sites web.
En exemple, l'Inbound marketing (ou marketing entrant), par opposition au marketing classique, consiste à faire venir le client vers l'entreprise. Cette forme de webmarketing, mettant en œuvre divers leviers du marketing digital, prouve depuis quelques temps son pourvoir et son mérite d'être un moyen de communication pertinent. Chaque site internet devient donc son propre média en diffusant en ligne des contenus attractifs, de bonne lisibilité et visibilité.

Le marketing digital ou webmarketing, est assez vaste qu'il devient difficile à cerner
Ce nouveau mode de communication touche divers domaines, de la création des sites internet au management de l'e-réputation en passant par le référencement, la gestion des contenus web et la diffusion d'informations via les réseaux sociaux, sans oublier les bannières, outil de publicité classique sur Internet.

L'un des avantages du marketing digital est qu'il permet de communiquer directement avec les clients et de suivre efficacement leur comportement, contrairement au marketing traditionnel. Cette forme de marketing permet également un certain degré de précision pour le ciblage des internautes par centres d'intérêt, âge, sexe ou encore par zones géographiques.

Source : http://www.info-afrique.com/5336-en-afrique-communication-digitale/
Par Thierry Barbaut avec l'Agence 360