Près de la moitié des Français confrontés à la cybercriminalité

Près de la moitié des Français confrontés à la cybercriminalité

Plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant.

Ransomware ou vol des données bancaires : près d'un Français sur deux (47%) a déjà été victime de cybercriminalité au cours de sa vie, selon l'étude annuelle Norton/Symantec révélée par Le Parisien / Aujourd'hui en France.
La cybercriminalité touche plus particulièrement les Français, puisque seulement quatre Européens sur dix sont confrontés à ce phénomène. En détail, plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant qui permet au cybercriminel de demander de l'argent aux utilisateurs en échange de la décontamination de leur ordinateur, alors que 20% des Français confient avoir été victimes du vol de leurs données bancaires.
Ce rapport montre que les Français sont particulièrement méfiants vis-à-vis de la cybercriminalité. Plus de la moitié des sondés (55%) ont aujourd'hui plus peur de se faire voler leurs données bancaires en ligne que de se faire subtiliser leur portefeuille. Plus de 17.000 consommateurs dans le monde ont été sondé cet automne pour les besoins de cette étude.

Réagissez à cet article
Source : http://www.lejdc.fr/france-monde/actualites/societe/techno/2015/11/30/pres-de-la-moitie-des-francais-confrontes-a-la-cybercriminalite_11685497.html

---

Une technologie parvient à

deviner qui est devant sa télévision

Une technologieparvient à deviner qui est devant sa télévision

En matière publicitaire, cette société américaine promet d'allier les atouts de ces deux médias. Marier le ciblage que permet l'Internet avec le confort de la télévision et sa propension à rendre la publicité presque agréable à « consommer ».

C'est la formule magique que promet aux câblo-opérateurs ou autres bouquets de chaînes, ainsi qu'aux annonceurs qui les choisissent pour communiquer, la société américaine Invidi.
Longtemps évoquée [la fondation d'Invidi remonte à 2000] , cette quadrature du cercle est en passe de se généraliser, Michael Kubin,vice-président exécutif de ce groupe, en est convaincu.
Concrètement, Invidi loge un logiciel à l'intérieur des décodeurs. En fonction des heures de la journée, des programmes vus et des comportements avec la télécommande, cet outil parvient à deviner qui est devant son poste par tranche d'âge et par sexe.
2 minutes de décrochages locaux pratiqués chaque heure Invidi croise ensuite ces données avec les renseignements proposés par des opérateurs de bases de données, ce qui lui permet d'affiner selon la géographie, les classes sociales, etc. Tout en respectant la confidentialité des données, promet-il.
Une fois ces informations recueillies, l'outil permet de pratiquer des décrochages publicitaires : différentes publicités sont passées en même temps à des publics différents.
Pour l'heure, explique Michael Kubin, Invidi permet aux distributeurs de télé américains de cibler leurs audiences de cette façon pendant les 2 minutes de décrochages locaux pratiqués chaque heure, ce qui représente environ 4 publicités.
Selon les experts du secteur, les publicités TV ciblées ne devraient pas être dominantes avant un moment. Mais leur place est appelée à croître.
Plus pertinent que Google Le ciblage fonctionne, assure Invidi. « Nous sommes quasiment à 100 % de fiabilité sur le genre et l'âge, explique Michael Kubin. Ensuite, les bases de données donnent des résultats très précis : nous considérons que notre mécanisme est plus pertinent que Google ». Invidi est embarqué dans les deux tiers des décodeurs aux Etats-Unis grâce à des accords avec DirecTV, Dish Network, Verizon, Comcast ou ATT. Le groupe vient de s'installer au Canada et discute avec Telenet, un FAI en Belgique.
L'an prochain, Invidi vise une entrée dans un ou deux pays en Asie et un ou deux autres en Europe. Il est en discussion avec un opérateur français. Invidi estime faire économiser de l'argent aux annonceurs, puisqu'il leur permet d'être plus précis.
Ensuite, la société se rémunère en ponctionnant une partie des revenus de publicité générés. Le groupe est avare de chiffres mais il assure que ses revenus vont doubler cette année, et encore l'an prochain.

Réagissez à cet article
Source : http://www.lesechos.fr/tech-medias/hightech/021521683400-invidi-la-technologie-qui-parvient-a-deviner-qui-est-devant-sa-television-1180389.php
Par Nicolas Madela

La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

La société Vtech, spécialisée dans les jeux ludo-éducatifs, a indiqué que la base de données de ses clients inscrits à son espace de téléchargement d'application, dont Explora Park en France, a été piratée.

Une technique d'injection de code SQL a été utilisée
On ne peut pas dire que Vtech ait été gâté pour Noël. Alors que les fêtes de fin d'année approchent à grands pas, la société spécialisée dans la vente de jouets et de jeux vidéo ludo-éducatifs a subi la plus grande cyberattaque de son histoire. Et le moins que l'on puisse dire, c'est que l'addition pourrait être salée avec près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants, tous inscrits à son service de téléchargement et de vente en ligne.

Près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants…
Connu en France sous le nom d'Explora Park, cet espace permet de télécharger jeux, applications et autres e-books pour différentes consoles et tablettes de la marque dont notamment Storio et Mobigo. «
Un accès non autorisé à la base de données clients de notre espace d'apprentissage a eu lieu le 14 novembre. Dès que nous en avons eu connaissance, nous avons lancé une enquête et pris des mesures pour nous défendre contre de futures attaques », a indiqué Vtech dans un communiqué. « Notre base de données clients contient des informations de profils incluant des noms, mails, adresses, mots de passes chiffrés, réponses aux questions secrètes, adresses IP, adresses mails et historique de téléchargement. » En revanche, la société a précisé que la base de données piratée ne contenait aucune donnée et information bancaire.

Une attaque par injection de code SQL. Les conséquences de ce piratage pourraient être lourdes.
Si Vtech n'a pas officiellement indiqué le nombre de clients impacté par ce vol de données, il pourrait s'élever à plus de 4,8 millions, selon nos confrères de Motherboard qui avaient prévenu la société après avoir été contacté à ce sujet par des pirates la semaine dernière.
D'après eux, le piratage a été perpétré par le biais d'une attaque par injection de codes SQL. Une technique classique permettant d'insérer des commandes malveillantes dans les formulaires d'un site web dans le but de collecter de façon détournée des informations sensibles et/ou confidentielles pour ensuite obtenir un accès root aux bases de données serveurs et permettre un accès complet à ces dernières.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-piratage-vtech-5-millions-de-donnees-clients-exposees-63117.html
Par Dominique Filippone

Edward Snowden a-t-il indirectement contribué aux

attentats de Paris ?

Edward Snowden a-t-il indirectement aux attentats de Paris vendredi 13 novembre ?

Des responsables politiques et des membres des services de renseignement internationaux accusent les systèmes de communication chiffrés des géants du web de profiter aux terroristes.

Crédit : DENIS CHARLET / AFP Un gendarme de la Brigade Départementale de Renseignements et d'Investigations Judiciaires (illustration)

Edward Snowden a-t-il indirectement contribué aux fusillades meurtrières qui ont balayé l'est de Paris vendredi 13 novembre ?

Certains acteurs de premier plan du renseignement américain ne sont pas loin de l'affirmer. Sans prononcer le nom de l'ancien analyste de la NSA (l'agence nationale de sécurité américaine), le directeur de la CIA John Brennan a clairement laissé entendre la semaine dernière lors d'une allocution à Washington que ses révélations sur les interceptions massives de communications téléphoniques par la NSA en 2013 avaient participé à faire émerger des failles dans la surveillances des réseaux d'extrémistes.

L'ancien directeur de la CIA James Woolsey ne s'embarrasse pas de ces précautions. Selon lui, Snowden a tout simplement « du sang sur les mains ».

À l'époque, ces révélations avaient poussé le Congrès américain à voter la fin du stockage des métadonnées des appels téléphoniques des citoyens américains par la NSA. Elles avaient surtout encouragé les géants du web à adopter des technologies de chiffrement violemment critiquées par la communauté du renseignement.

Depuis le scandale des pratiques d'écoutes de masse par les États-Unis, la protection des données personnelles est devenu un argument commercial pour les sociétés technologiques auprès d'utilisateurs de plus en plus méfiants des services proposés par les entreprises de la Silicon Valley.

Après le rachat de Whatsapp par Facebook, près de 5 millions d'utilisateurs se sont par exemple rabattus sur le service de messagerie sécurisé Telegram, également plébiscité par les terroristes de Daesh.

Apple a développé des systèmes de sécurité de plus en plus draconiens érigeant ses téléphones en véritables forteresses.

Depuis la fin 2014, les emails, SMS et photos de l'iPhone sont chiffrés et personne, pas même Apple, ne peut y avoir accès.

Selon un expert en cybersécurité cité par Les Échos, « la seule manière d'essayer de les récupérer est de décaper le composant avec de l'acide pour ensuite le passer au microscope ». Une opération qui peut coûter plusieurs millions d'euros.

Dans le même temps, Google, Facebook, WhatsApp, Skype ou Twitter n'ont pas ménagé leurs efforts pour sécuriser les données de leurs abonnés. Si bien qu'il est impossible pour les autorités de lire et d'écouter les conversations sur ces services en dehors de réquisitions judiciaires ou d'un accord avec ces entreprises.

Une loi à l'étude au Royaume-Uni

Les autorités et la communauté du renseignement montent régulièrement au créneau pour réclamer un changement de politique des entreprises technologiques.

Le procureur de Manhattan, Cyrus Vance, a répété à plusieurs reprises qu'il a dû abandonner cette année une centaine d'affaires impliquant des meurtriers, faute d'avoir pu accéder aux données de leurs téléphones.

Le directeur du FBI dénonçait en juillet le chiffrement pratiqué par Whatsapp et les entreprises privées, qui permet, selon lui, à des criminels de se mettre à l'abri de la loi.

Au premier rang de leurs revendications figure la création de clés de chiffrement ou de portes dérobées qui leur donneraient accès aux données des utilisateurs quand la situation l'exigerait.

Le débat est également d'actualité de l'autre côté de l'Atlantique. Après les attentats de janvier à Paris, le premier ministre britannique, David Cameron, s'était publiquement interrogé sur les risques de l'existence de données cryptées auxquelles la police ne peut pas accéder. Il souhaite désormais faire figurer dans l'Investigatory Powers Bill, sorte d'équivalent de la loi renseignement française, l'interdiction des méthodes de chiffrement qui n'incluraient pas de porte dérobée permettant aux autorités munies d'un mandat de justice d'accéder aux informations chiffrées. Une nouvelle législation que le locataire du 10, Downing Street justifie par la nécessité de « ne pas créer une situation dans laquelle les terroristes, les criminels et les ravisseurs d'enfants auraient un espace libre pour communiquer ».

Les géants du web rappellent leur attachement au chiffrement

Les géants du net sont fermement opposés à ce type de mesure. Selon eux, leur mise en place reviendrait à introduire une faille dans leurs programmes. Apple, Microsoft, Google, Samsung, Twitter, Facebook et une cinquantaine d'entreprises technologiques regroupées au sein de l'Information Technology Council ont rappelé dans une lettre ouverte que le chiffrement est un outil de sécurité indispensable pour leurs utilisateurs. « Affaiblir le chiffrement quand on a pour but de l'améliorer n'a aucun sens, estiment-ils. Le chiffrement est un outil de sécurité utilisé tous les jours pour empêcher des criminels de vider nos comptes en banque, pour protéger nos voitures et avions des piratages et pour préserver notre sécurité. (…) Affaiblir le chiffrement ou créer des portes dérobées (…) créerait des vulnérabilités qui pourraient être exploitées par les méchants, ce qui causerait certainement des problèmes physiques et financiers sérieux dans notre société et notre économie ».

La France n'a pas encore pris de position claire sur la question. Mi-août, le procureur de la République de Paris, François Molins, a cosigné une tribune du New York Times avec plusieurs responsables internationaux de la lutte antiterroriste pour appeler les géants du web à changer leur politique de chiffrement pour ne pas affaiblir les capacités d'investigation de la justice contre le terrorisme. Adoptée en juin, la loi Renseignement portée par le gouvernement après les attentats de janvier n'évoque pas précisément la cryptologie. Selon Médiapart, le gouvernement avait l'intention de légiférer mais y a finalement renoncé. C'était avant les attentats de Paris. François Hollande a depuis affirmé devant le Parlement réuni à Versailles qu'il souhaitait adapter l'état d'urgence aux évolutions technologiques, sans donner plus de détails.

Les terroristes n'ont pas attendu Snowden

En attendant, il n'a pas été établi à ce stade de l'enquête que les commandos des attentats de Paris ont utilisé un système de communication crypté pour organiser leurs attaques. Le site d'investigation britannique The Intercept a rappelé récemment que les terroristes et les criminels n'ont pas attendu les révélations de Snowden pour se méfier des voies de communication traditionnelles. Les attentats de New York (2001), Bali (2002), Madrid (2004), Londres (2005), Mumbai (2008) et Boston (2013) peuvent malheureusement en témoigner. Le commanditaire des attentats du 11 septembre, Oussama Ben Laden, s'appuyait par exemple uniquement sur un système de messagers humains par crainte d'être pisté par les services de renseignement, notait le Washington Post. Un système qui lui a permis de naviguer en dehors des radars antiterroristes pendant près d'une décennie.

Réagissez à cet article

Source : http://www.rtl.fr/culture/web-high-tech/apple-google-et-les-geants-du-web-entravent-ils-la-lutte-contre-le-terrorisme-7780616618

PAR BENJAMIN HUE

e-Réputation : un internaute condamné pour un faux commentaire malveillant

e-Réputation : un internaute condamné pour un faux commentaire malveillant

Un internaute a été condamné par le Tribunal de grande instance de Dijon pour avoir publié sur PagesJaunes.fr un faux avis malveillant concernant un restaurant qui n'avait pas encore ouvert.

Un internaute, connu sous le pseudonyme de Le Clarifieur, a été condamné le 6 octobre dernier à une amende de 2 500 euros et 5 000 euros de frais par le Tribunal de grande instance de Dijon pour avoir publié sur le site Web PagesJaunes.fr un commentaire faux et malveillant concernant le restaurant Loiseau des Ducs de Dijon, appartenant au groupe Bernard-Loiseau.
Cet internaute avait en effet publié, le 11 juillet 2013, ligne sur le site Internet des Pages Jaunes un commentaire bien peu élogieux concernant le nouvel établissement Loiseau des Ducs (1 étoile au Guide Michelin) : « très surfait, tout en apparat et très peu de chose dans l'assiette. L'assiette la mieux garnie est celle de l'addition ».
Petit souci : à la date de publication de cet avis, le restaurant en question n'avait même pas encore ouvert ses portes. Aucun client n'avait donc pu y déguster un repas…

Ahlame Buisard, gérante du restaurant et directrice générale du groupe Bernard-Loiseau, avait alors fait constater par voir d'huissier la publication de ce commentaire et avait ensuite porté plainte. « On a voulu mener l'affaire jusqu'au bout et donner une leçon à ces personnes qui font des commentaires pour détruire », a souligné Ahlame Buisrad, rapporte le quotidien Le Bien Public, après la condamnation de l'internaute fautif.
Selon le Tribunal de grande instance de Dijon, « ces commentaires fautifs (…) du fait même de leur diffusion sur Internet sur un site largement consulté par les internautes à la recherche des coordonnées d'établissements, visaient à dissuader de potentiels futurs clients de se rendre dans le restaurant critiqué ».
Une condamnation qui met en avant la difficulté pour les commerçants et prestataires des services de gérer et modérer la parution sur le Web de commentaires, bons ou mauvais, de la part de vrais ou faux clients et ainsi de garder la main sur leur e-réputation.
« Aujourd'hui des dizaines de plateformes, spécialisées ou non permettent aux consommateurs de partager leurs avis sur un magasin, un restaurant, un hôtel ou n'importe quel autre produit ou service. C'est même un métier à temps plein pour certaines sociétés et il faut ajouter à cela les réseaux sociaux où s'échangent des milliers d'avis chaque jour », souligne Aurelien Dubot, Senior Product Manager chez Bazaarvoice, fournisseur américain de solutions d'avis de consommateurs.
« Les sites tiers n'assurent pas toujours une modération exemplaire ni même un filtrage sommaire des commentaires publiés ».
Bazaarvoice recommande ainsi aux entreprises soucieuses de leur réputation en ligne de prendre les devants, en mettant à disposition de leurs clients une plate-forme dédiée leur permettant de partager leur retour sur un service ou un produit.
Il s'agit également de vérifier l'authenticité des avis publiés, via notamment une norme AFNOR visant à fiabiliser les avis en ligne. Sans oublier qu'il convient d'accepter le fait de voir publier des commentaires négatifs, gage d'authenticité et d'honnêteté vis-à-vis des clients.
Crédit image : PathDoc – Shutterstock.com

Réagissez à cet article
Source : http://www.itespresso.fr/#e-reputation-internaute-condamne-faux-commentaire-malveillant-113258.html

Cyber-terrorisme : un recrutement en 4 phases

Cyber-terrorisme : un recrutement en 4 phases