Nouvelle chaîne de Ponzi sur le bitcoin, Marchés Financiers

Nouvelle chaîne de Ponzi sur le bitcoin, Marchés Financiers

Aux Etats-Unis, le gendarme des marchés engage des poursuites contre deux sociétés du secteur du bitcoin. Il suspecte une nouvelle chaîne de Ponzi.

Le gendarme des marchés financiers américains, la Securities and Exchange Commission (SEC), annonce des poursuites contre deux sociétés – GAW Miners et ZenMiner – en charge de la création du bitcoin, la célèbre devise digitale. La création de cette devise et la validation des transactions sont assurées par des sociétés qui doivent résoudre de complexes calculs informatiques. Une activité coûteuse (électricité) et dont la rentabilité dépend du cours du bitcoin, ces sociétés étant rémunérées dans cette devise.
Deux d'entre elles ont promis à 10.000 investisseurs de s'associer à la création de bitcoins et d'en partager les bénéfices. Or la SEC estime que GAW et Zen ont en fait opéré une chaîne de Ponzi : l'argent collecté chez les uns a servi à attirer d'autres investisseurs pour les convaincre qu'ils participaient à un investissement sûr et rentable. La chaîne de Ponzi a opéré entre août 2014 et début 2015. Seulement, durant cette période, le bitcoin a perdu plus de la moitié de sa valeur, ce qui a commencé à éveiller des suspicions sur la réalité des rendements vantés.

Une série de tromperies

Le 11 septembre 2014, les présumés escrocs avaient assuré que l'intégralité des bénéfices seraient reversés aux victimes du 11 septembre 2001, pour le 13e anniversaire des attaques terroristes. Une nouvelle tromperie. Le 23 juillet 2013, le gendarme des marchés américains avait mis au jour une autre chaîne de Ponzi, organisée cette fois par un particulier texan. Ce dernier assurait pouvoir générer un rendement de 7 % par semaine. La SEC avait alors été très explicite : « Ce n'est pas parce les fraudeurs ont recours au bitcoin qu'ils peuvent échapper aux sanctions et se croire à l'abri des lois. Tout investissement financier sur le sol américain, en devises traditionnelles ou monnaies virtuelles, est du ressort de la juridiction de la SEC. »
Autour de 360 dollars, le bitcoin s'est habitué à ces vicissitudes, la devise connaissant des chaînes de Ponzi, le plus souvent de petite taille (quelques millions de dollars) et autres arnaques de manière récurrente. Dans le secteur, on a tendance à dédramatiser ce type « d'incidents », jugés inévitables pour une devise jeune et décentralisée. Faire le ménage dans ce secteur est le meilleur moyen d'assurer l'avenir du bitcoin.

Réagissez à cet article
Source : http://www.lesechos.fr/finance-marches/marches-financiers/021527837471-nouvelle-chaine-de-ponzi-sur-le-bitcoin-1180949.php

---

Contrefaçon : Interpol s’attaque à un millier de sites vendant des produits interdits

Contrefaçon : Interpol s’attaque à un millier de sites vendant des produits interdits

Les services des douanes ont mené conjointement avec Interpol plusieurs mesures pour identifier et stopper l'activité de sites de vente de produits contrefaits.

Un millier d'entre eux ont été visés par les autorités.

Interpol annonce qu'un millier de sites proposant l'achat de produits contrefaits ou piratés ont été identifiés. Les autorités ont mené de nouvelles opérations conjointes des services policiers américains et européens.

« Les consommateurs du monde entier utilisent Internet pour acheter des biens de la vie de tous les jours et les criminels en profitent » pour vendre des produits « illégaux », estime le directeur de la branche crime organisé chez Interpol, Roraima Andriani.

Une vingtaine de pays ont pris part au 6e volet d'une opération baptisée « In our sites », dont la Belgique, la Bulgarie, la Colombie, la Croatie, le Danemark, la France, la Grèce, le Portugal, la Roumanie, l'Espagne ou le Royaume-Uni.

Ce type d'opération est désormais régulier. Chaque année, les autorités américaines et européennes dévoilent des listes de sites destinés à être fermés pour vente de produits contrefaits. Ces investigations surviennent lors de grandes occasions comme Noël, les soldes ou encore la Saint-Valentin.

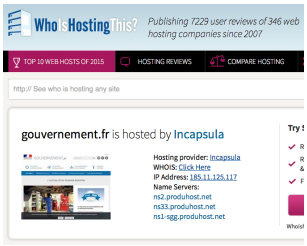
Réagissez à cet article

Source : http://pro.clubic.com/actualite-e-business/actualite-788224-contrefacon-internet.html

Le site web du gouvernement français utilise un CDN « made in USA »

Le site web du gouvernement français utilise un CDN « made in USA »

Le site web du gouvernement français est hébergé en France, mais utilise le CDN d'un opérateur états-unien. Étrange, car plusieurs opérateurs français ont des offres en la matière. Et savez-vous qui héberge le site web du Noël de la French Tech ?



Le site web du gouvernement français est en partie « made in USA » Vendredi dernier, le gouvernement subissait quelques sarcasmes pour avoir lancé, depuis son site web www.gouvernement.fr, un « concours de selfies tricolores » à l'occasion de l'hommage national aux victimes des attentats djihadistes du 13 novembre à Paris. Je suis allé sur le site web de notre exécutif pour voir ce qu'il en était de cet appel et il m'a semblé que les temps de réponse n'étaient pas excellents. J'ai alors utilisé la commande traceroute, qui m'a donné ce résultat :

```
> traceroute www.gouvernement.fr
traceroute: Warning: www.gouvernement.fr has multiple addresses; using 8.253.93.126
traceroute to cdn2.cdn-tech.com.c.footprint.net (8.253.93.126), 64 hops max, 52 byte packets
1  10.60.1.254 (10.60.1.254)  1.542 ms  0.814 ms  0.711 ms
2  reverse.completel.net (46.218.145.105)  2.448 ms  5.900 ms  3.290 ms
3  * * *
4  172.19.130.117 (172.19.130.117)  29.751 ms  30.536 ms  28.127 ms
5  te0-5-0-13.ccr21.par04.atlas.cogentco.com (149.6.164.101)  28.094 ms  26.642 ms  27.093 ms
6  level3.par04.atlas.cogentco.com (130.117.14.94)  27.026 ms  27.511 ms  20.037 ms
7  * * ae-3-80.ear2.paris1.level3.net (4.69.168.140)  21.277 ms
8  * * *
```

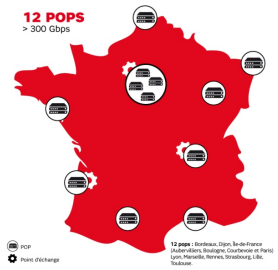
J'ai exécuté à nouveau cette commande, quelques minutes plus tard :

```
> traceroute www.gouvernement.fr
traceroute: Warning: www.gouvernement.fr has multiple addresses; using 204.160.107.126
traceroute to cdn2.cdn-tech.com.c.footprint.net (204.160.107.126), 64 hops max, 52 byte packets
1 10.60.1.254 (10.60.1.254) 1.431 ms 0.691 ms 0.694 ms
2 reverse.completel.net (46.218.145.105) 4.667 ms 2.219 ms 5.282 ms
3 * * *
4 172.19.130.113 (172.19.130.113) 16.804 ms 17.153 ms 15.894 ms
5 te0-0-0-3.rcr11.b015531-1.par05.atlas.cogentco.com (149.6.166.45) 26.342 ms 54.703 ms 30.250 ms
6 be2337.rcr21.par05.atlas.cogentco.com (130.117.1.1) 20.723 ms 29.652 ms 29.864 ms
7 be2424.ccr41.par01.atlas.cogentco.com (130.117.2.237) 30.037 ms
be2425.ccr42.par01.atlas.cogentco.com (130.117.3.205) 53.502 ms
be2424.ccr41.par01.atlas.cogentco.com (130.117.2.237) 33.899 ms
8 be12308.ccr21.par04.atlas.cogentco.com (130.117.49.42) 19.653 ms
be12309.ccr21.par04.atlas.cogentco.com (154.54.39.66) 22.496 ms
be12308.ccr21.par04.atlas.cogentco.com (130.117.49.42) 29.791 ms
9 level3.par04.atlas.cogentco.com (130.117.14.94) 28.197 ms 54.186 ms 30.102 ms
10 ae-32-80.car2.paris1.level3.net (4.69.168.131) 29.984 ms
11 ae-12-60.car2.paris1.level3.net (4.69.168.3) 16.255 ms 12 ae-42-90.car2.paris1.level3.net (4.69.168.195) 20.175 ms
13 * * *
```

Ces éléments techniques ne laissent aucun doute : le site officiel du gouvernement français est accessible via plusieurs IP différentes, il utilise très probablement un Content Delivery Network – ou CDN – et en l'occurrence il semble bien s'agir du CDN de l'opérateur états-unien Level3 Communications, un des plus importants opérateurs Internet au monde.
Surpris, j'effectue alors une autre recherche via le site WhoIsHostingThis : selon cette source d'information technique, le site serait « hébergé par » Incapsula.

En creusant un peu, il apparaît que Incapsula propose du CDN. Serait-il basé sur le réseau de Level3 ? On peut le penser puisque, selon cette page, « *Incapsula's CDN runs on top of major Tier 1 provider networks* »
Je pense que l'on peut légitimement se poser des questions sur les risques d'atteinte à l'intégrité du contenu diffusé à partir du site du gouvernement français. En effet, il est avéré que le gouvernement des USA ne se prive pas d'espionner tous les gouvernements étrangers, y compris en Europe, et même des entreprises privées. **Soyons un peu paranoïaques, et imaginons que des agences gouvernementales des USA souhaitent manipuler l'opinion publique française** : il ne serait pas très difficile de « faire mentir le CDN » et de lui faire remplacer des portions de contenu issus d'un site web par d'autres. Le CDN, situé entre le site web de notre gouvernement et les citoyens de notre République, pourrait substituer à dessein une photo truquée à une photo authentique, remplacer un texte, par exemple un discours officiel, par un autre, etc.

Vous imaginez le pouvoir d'influence sur l'opinion publique française que cela procurerait ?
J'ai contacté Romain Pigenel, directeur adjoint en charge du numérique au Service d'Information du Gouvernement. Il m'a assuré que le site web du gouvernement était bien hébergé en France, sur des serveurs situés à l'intérieur du territoire national. Et d'ailleurs la page de mentions légalesdu site indique explicitement « *Hébergement Alter Way Hosting*» .
Rappelons que cela fait plus de 3 ans que de grands opérateurs français ont lancé des offres de CDN : si l'offre CDN d'Orange a été construite en partenariat avec Akamai, encore un acteur venu des États-Unis, en revanche l'offre CDN de SFR a été conçue par des équipes françaises. Ce CDN repose sur des infrastructures de proximité, déployées en 12 points du territoire national et tirant profit des points de peering régionaux disponibles à Paris, Lyon et Bordeaux :

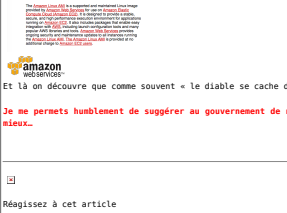


Le Noël de la French Tech hébergé… chez Amazon !

Autre épisode un peu malheureux, avec l'annonce hier matin par Axelle Lemaire de l'opération « **Noël de la French Tech** » :

Il s'agit d'une excellente initiative qui fait découvrir de nombreux produits, issus de startups françaises, susceptibles d'être offerts lors des fêtes de fin d'année. Je trouve tout à fait positif de mettre un coup de projecteur sur des entreprises françaises et de contribuer, fût-ce de façon marginale, à améliorer la balance de notre commerce extérieur, qui souffre du fait que les produits électroniques, informatiques et technologiques sont très majoritairement importés.
Mais malheureusement un afflux de connexions sur le site promu par la secrétaire d'État chargée du numérique a quelque peu perturbé son fonctionnement :

Du coup, en tapant www.noeldelafrenchtech.fr, je suis arrivé sur cette page :



Et là on découvre que comme souvent « le diable se cache dans les détails » : ce site web est hébergé dans le cloud d'Amazon… alors que les offres d'hébergement made in France ne manquent pas.

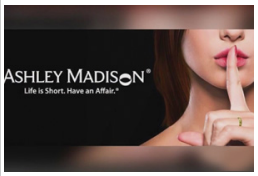
Je me permets humblement de suggérer au gouvernement de redoubler d'efforts pour mettre ses actes en accord avec sa communication : promouvoir les entreprises technologiques françaises c'est bien, utiliser leurs services en toute occasion où c'est possible c'est encore mieux…

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/trange-le-site-web-du-gouvernement-francais-utilise-un-cdn-made-in-usa-39829142.htm
Par Pierre Col

L’individu cible des cyber attaques

L’individu cible des cyber attaques

Si les cyberattaques les plus marquantes ont visé des grands comptes ou des acteurs industriels majeurs, les PME se voient de plus en plus menacées. Reste à faire comprendre à un dirigeant, qu'au-delà de la taille de son entreprise, ce sont les individus – lui compris – qui sont visés.



En août 2015, les données (32 millions de comptes) du site de rencontres extraconjugales, Ashley Madison, ont été piratées.
Tavish Vaidya, doctorant de l'université de Georgetown à Washington, documente depuis quelques années le nombre et l'importance des cyberattaques du XXIe siècle. Il livrait récemment dans la MIT Technology Review, son top 20 où l'on retrouve l'assaut du ver Stuxnet sur des centrifugeuses iraniennes en 2010 ou l'infection en décembre 2013 par des hackers chinois des ordinateurs de membres européens du G20 lors de la réunion de l'organisation internationale à Saint-Pétersbourg.

La faille est toujours humaine

Mais la nature de ces cyberattaques très médiatisées, qui ont touché de grandes organisations, ne joue pas forcément à l'avantage de ceux qui veulent provoquer une prise de conscience chez les dirigeants.
« Longtemps, la cybersécurité n'a concerné que les grands comptes. Et, chez la majorité de nos interlocuteurs en entreprise, la réponse reste encore : "ces sociétés sont très connues. Ce n'est pas comme nous, qui sommes beaucoup plus petits… Et ceci, même si la donne a changé" », explique Sergio Loureiro, président et cofondateur de SecludIT, une start-up créée en 2011 qui propose de réaliser en continu des scans automatiques de vulnérabilité sur les infrastructures des entreprises.
« Nous constatons que les grands groupes ont progressivement élevé leur niveau de sécurité, compliquant et rendant moins intéressant le fait d'attaquer directement leurs systèmes. Par contre, cela a encouragé les assaillants à s'en prendre aux PME… qui sont souvent leurs prestataires », détaille PierreYves Popihn, directeur technique de NTT Com Security (ex-Integralis), la filiale cybersécurité du groupe de télécommunications japonais.
Les entreprises, de plus en plus ouvertes sur leur écosystème, risquent alors de se compromettre les unes les autres… Malgré ses impacts résolument business, la cybersécurité traîne une étiquette trop « technique » auprès des directions générales, qui s'en défaussent sur le responsable de la sécurité des systèmes d'information (RSSI) ou le responsable informatique. Or, le message martelé par les experts est tout autre : dans la majorité des cas, la faille est humaine.
« 100 % des entreprises que nous testons ont au moins une faille critique dans leur système d'information, et nous sommes toujours arrivés à accéder à des informations confidentielles sur les collaborateurs ou les clients… Mais une fois qu'un attaquant a mis le pied dans l'entreprise, il va viser des individus en particulier, pour obtenir davantage, fait valoir Sergio Loureiro. Dans ces conditions, le PDG peut tout aussi bien être le maillon faible que la standardiste. »
Un exemple récent illustre justement le rôle important de « l'ingénierie sociale » pour exploiter les failles de sécurité.

Une lutte d'ego

La société BRM Mobilier, PME des Deux-Sèvres spécialisée dans l'aménagement de médiathèques et bibliothèques, a été placée en redressement judiciaire début septembre 2015, après que des malfaiteurs se sont fait passer tour à tour, par e-mail et téléphone, pour le président de cette entreprise de 44 salariés, et pour ses avocats. Les juges ont prononcé le redressement judiciaire avec poursuite des activités jusqu'au 11 mars 2016, le temps de retrouver un repreneur éventuel. Cette « arnaque au président » a permis de détourner 1,6 million d'euros par l'intermédiaire de la responsable administrative et financière de la société. *« Contrairement à une attaque à base de code malicieux, où un collaborateur ouvre une fausse pièce jointe d'e-mail, par exemple une facture, l'arnaque au président ne fait pas appel à un malware, il s'agit avant tout d'une escroquerie »*, note Charles Rami, expert cybersécurité chez Proofpoint, une entreprise américaine qui se spécialise notamment sur la protection des e-mails.
« Dans le cas de BRM, l'arnaque n'a sans doute pas été montée au hasard. Elle s'est déroulée juste après une importante entrée d'argent. Il est possible que l'entreprise ait été préalablement infectée par un cheval de Troie étudiant l'environnement financier et bancaire de l'entreprise. L'usurpation de l'identité en e-mail, elle, est très simple techniquement », décrit-il plus précisément. Un avis partagé par Pierre-Yves Popihn, qui estime que 15 % des cyberattaques en France servent avant tout à faire de la reconnaissance pour se voir ensuite presque littéralement « ouvrir la porte » de l'entreprise par un de ses salariés ou le dirigeant lui-même.

Cette usurpation d'identité peut-elle provoquer un déclic chez les dirigeants ?

« Tout le monde est concerné, mais deux populations sont très sensibles. Les personnes du service IT qui testent des usages et des technologies dans l'entreprise comme ils le feraient à leur domicile ; et les membres du top management, qui souhaitent connecter au SI leurs propres outils, leur smartphone personnel par exemple, même si cela peut entraîner des complications en termes de sécurité. Ces acteurs disposent souvent de comptes à privilège, c'est-à-dire des "clés" du système d'information, même quand cela n'est pas nécessaire au quotidien », témoigne Sandro Lancrin, architecte Sécurité SI et RSSI de Radio France.
Il souligne d'ailleurs, que cette problématique des individus revient trop régulièrement à une lutte d'ego, un directeur s'offusquant que l'un de ses subalternes dispose de droits informatiques et pas lui…

> **"Toutes les entreprises que nous testons ont au moins une faille critique dans leur SI"**
> Sergio Loureiro
> *président et cofondateur de SecludIT*

Malgré tout, la « conscience cyber » fait petit à petit son chemin en entreprise. Les affaires grand public, comme le vol de données du site d'adultère Ashley Madison l'été dernier, contribuent à attirer l'attention. *« C'est à double tranchant,* note Mounir Chaabane, conférencier Eucles pour l'Institut national des hautes études de la sécurité et de la justice, une émanation de la délégation interministérielle à l'Intelligence économique, *en donnant tant de visibilité à des affaires comme l'arnaque au président de BRM ou Ashley Madison, on se focalise sur des cas presque anecdotiques vu la diversité des formes que peut prendre une attaque. Ce vers quoi il faudrait tendre, c'est une culture qui mette les individus en face de leurs responsabilités, qu'ils soient PDG, trésorier, agent des ressources humaines ou administrateur système. »* Une culture bien plus présente dans d'autres pays, de la Finlande aux Etats-Unis, où des dirigeants ont déjà été tenus responsables des conséquences de cyberattaques menées contre leurs entreprises, et mis à la porte. Ainsi, le PDG et fondateur d'Ashley Madison n'a pas tardé à quitter son poste : l'an dernier, dans un entretien télévisé, il avait décrit les serveurs du site comme étant « impénétrables »…

A lire également

Suite à l'affaire BRM de Bressuire, la chambre de commerce et d'industrie des Deux-Sèvres a publié un guide « Spécial Arnaque », destiné aux chefs d'entreprise face aux nouvelles formes d'escroquerie, notamment la cybercriminalité. Pour le consulter : http://bit.ly/1ijoKRH.
Lire aussi les 22 fiches thématiques sur « La sécurité économique au quotidien », publiées par la Direction interministérielle à l'intelligence économique, http://bit.ly/1iOEGow

---

Réagissez à cet article
Source : http://www.alliancy.fr/a-laffiche/securite/2015/11/30/cybersecurite-lindividu-pour-cible

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