Michelin victime de « l'arnaque au président », Banque – Assurances

Michelin victime de « l'arnaque au président »

Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros au moyen de l'arnaque dite « du président ».

L'arnaque est désormais bien rodée, et Michelin en est la dernière victime. Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros via une escroquerie reposant sur de faux ordres de virement, a-t-il indiqué lundi à l'AFP, confirmant une information du journal « Le Parisien ». La méthode employée est celle de « l'arnaque au président », qui sévit de plus en plus dans les entreprises.

Modus operandi

Un individu se fait généralement passer pour le président ou l'un des directeurs d'une société ou d'un groupe, et appelle un comptable de niveau assez bas dans hiérarchie, à qui il demande, dans le cadre d'une opération soi-disant très confidentielle, un virement urgent vers un pays étranger. Bien souvent, il s'agit de la Chine, ou de Chypre, mais cette fois, le pseudo directeur financier a réclamé que les règlements soient effectués sur le compte d'une banque en République tchèque. « Cet homme connaissait parfaitement la procédure à suivre et la personne à contacter au sein du groupe Michelin pour pouvoir effectuer cette modification en toute discrétion », a rapporté une source proche de l'affaire. Une enquête a été ouverte et confiée à la police judiciaire de Clermont-Ferrand.

Michelin n'est pas le premier groupe à être victime d'une telle escroquerie, « la plus redoutable » et qui requiert « une autorité naturelle, un certain aplomb et […] un don pour la comédie », expliquait récemment aux « Echos » le SRPJ de Clermont-Ferrand. Pour le service régional de police judiciaire, ces arnaques sont de trois types : outre « l'arnaque au président », on trouve l'escroquerie « à la nigériane » ou encore le détournement de la nouvelle norme Sepa , l'espace de paiement unique européen.

La fédération française bancaire a récemment mis en ligne une vidéo afin de prévenir les escroqueries aux ordres de virement :

Selon l'Office central pour la répression de la grande délinquance, quelque 700 faits ou tentatives ont ainsi été recensés entre 2010 et 2014. Le montant des préjudices atteignait, en août dernier, plus de 250 millions d'euros. Le cabinet KPMG (audits et expertises comptables) avait révélé cette année en avoir été victime, pour un préjudice de 7,6 millions d'euros.

Denis JACOPINI et son équipe vous propose des formations pour sensibiliser les salariées à ce type de pratiques cybercriminelles.

N'hésitez pas à me contacter pour organiser une session de formation. (Denis JACOPINI)

Source :

http://www.lesechos.fr/finance-marches/banque-assurances/0203910698411-michelin-victime-de-larnaque-au-president-1060501.php

Arnaques sur Internet : 30% des sites sont dans l’illégalité

Arnaques sur Internet : 30% des sites sont dans l’illégalité

Les arnaques sur internet se multiplient. De faux sites imitent les couleurs et le logo d'autres sites fiables, pour attirer les internautes.

Le mauvais habit qui arrive, les délais de garantie non-respectés ou encore des soldes avec des prix gonflés… Tous ces litiges du commerce sur Internet représentent la moitié des cas traités par le site Lesarnaques.com. Attention aussi au vol de vos coordonnées bancaires et à une nouvelle arnaque, plus inattendue, le faux nom de site internet.

Une copie conforme d'un site connu

Prenez un site très prisé, RueduCommerce.com par exemple, transformez-le un tout petit peu, en RDCommerce.com, et les internautes s'y perdent très vite. Un internaute avait acheté une couette à 100 euros qui n'est jamais arrivée. « Pour moi c'était le même site, c'était Rueducommerce. Les couleurs étaient identiques, tout comme le logo. Il y avait une très bonne promotion donc je me suis dit c'était une affaire », raconte-t-il.

Et pour se faire rembourser, c'est le parcours du combattant. Si bien que ces sites frauduleux en profitent. Le temps qu'une victime s'aperçoive de la supercherie, envoie des courriers recommandés, fasse appel à des associations et porte plainte et le temps que des dizaines de plaintes débouchent enfin sur une enquête, puis sur un jugement au tribunal, il peut très vite s'écouler un an. Souvent, les fraudeurs sont basés à l'étranger, ils sont quasiment intouchables.

Comment éviter les arnaques

« Ce n'est parce que vous avez un site web où tout est écrit en français, que forcément il est basé en France. Il faut regarder les conditions générales. Si vous n'avez pas d'adresses ou d'information sur le site, il ne faut pas faire d'achats », conseille Joël Guillon, président du site Lesarnaques.com.

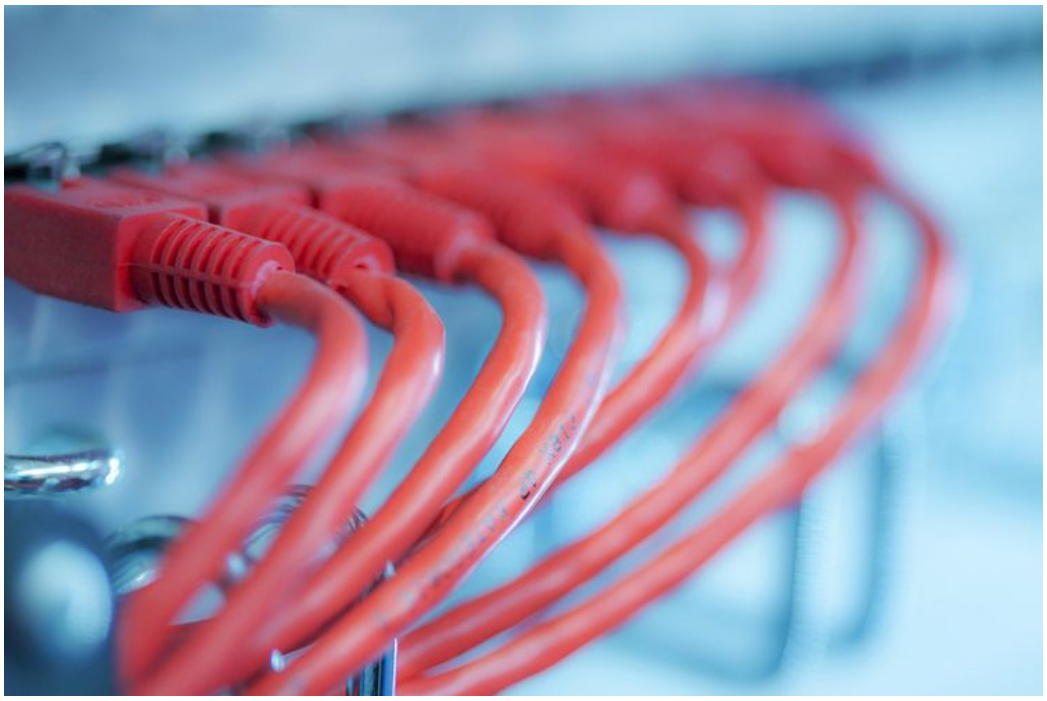
Pour vérifier la fiabilité d'un site, « pensez à les appeler sur la fiabilité d'un produit. Si le téléphone sonne dans le vide, c'est déjà qu'il y a un vrai service derrière », ajoute-t-il. Autre conseil : au moment où l'on fait un achat sur un site web, une page s'ouvre pour demander le numéro de carte bleue. « À ce moment-là, en haut de votre page à gauche, avant le nom de domaine se trouve « https » qui correspond à 'secure' ».

Par Anaïs Bouissou

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.rtl.fr/culture/web-high-tech/arnaques-sur-internet-30-des-sites-sont-dans-l-illegalite-7775018016

Données c'est donner…



Données c'est donner…

Fondateurs de réseaux sociaux ou de sites de rencontre, tous tentent d'exploiter les data des internautes. Des manipulations s'opèrent, à l'insu des utilisateurs… Les questions d'éthique et de droit restent posées.

En juin, Facebook révélait avoir mené une expérience psychologique sur près de 700 000 utilisateurs à leur insu.
L'idée: tester une potentielle «contagion émotionnelle».
Dans la foulée, le site de rencontre OKCupid affichait des «manipulations de profils» de ses internautes.
Christian Rudder, cofondateur du site, postait récemment un billet intitulé «Nous réalisons des expériences sur les êtres humains», affirmant : «si vous utilisez Internet, vous êtes l'objet de centaines d'expériences, à tout moment quel que soit le site.» De quoi faire frissonner.

OKCupid est un site basé sur des questions auxquelles l'on répond en tant qu'utilisateur, sur tous sujets – de la propreté du bac à douche, à la fellation ou encore à l'usage du LSD. Plus l'internaute répond, plus l'Algorithme Magique est susceptible de lui proposer l'âme sœur. Soit. Et de fait, sur une base aussi riche, il est possible d'envisager une pertinence ethno-sociologique à ces expériences in vivo qui posent bien entendu des questions éthiques. Peut-on utiliser les données d'innocents internautes qui viennent chercher une cour de récréation / une rencontre sur les réseaux sociaux ?
Ces thèmes ont été largement discutés. Ce qui choque, c'est la position «de plein droit» que s'accordent les géants du Net, s'affichant dans une normalité sur le thème: «Oui, nous utilisons vos données, et alors ?» Et alors… ? Bizarrement, c'est aussi ce que répondent nombre d'internautes quand ont les avertis de l'impact de leurs clics. Faites le test. Expliquez à une personne non avertie que ses données sont transmises à l'annonceur quand il en like la pub. Réponse probable : «Qu'est-ce qu'on s'en fout ?»

Pourtant quand le juriste-activiste autrichien Max Schrems a demandé à Facebook de lui envoyer une compilation de ses données, **il a reçu un fichier de plus de mille pages** contenant ses informations présentes sur le site, y compris celles qu'il pensait avoir supprimées. Il a déposé une plainte cet été, rappelant que les questions éthiques posées par ces intrusions impliquent d'abord une prise de conscience de l'individualité et du droit des internautes.

DATA EN MASSE
Avec respectivement 1,2 milliard et 4 millions d'utilisateurs, les américains Facebook et OKCupid bénéficient d'un corpus qui combinent âge, sexe, CSP, habitat (urbain, rural), habitudes de consommation, et même religion. Autant de données croisées qui feraient rêver n'importe quel statisticien.
Stéphanie ESTOURNET

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://ecrans.liberation.fr/ecrans/2014/10/17/donnees-c-est-donner_1115973?xtor=rss-450

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La firme à la pomme a été épinglée plusieurs fois par la Commission pour sa pratique abusive des caméras de surveillance, même dans les espaces de repos des salariés.

Il fut un temps où Apple dénonçait à grands coups de publicités la surveillance généralisée d'une société, comme dans 1984. La firme à la pomme semble aujourd'hui avoir zappé ces beaux principes…

La Cnil annonce en effet avoir mis en demeure Apple Retail France pour sa pratique abusive des caméras de surveillance dans ses boutiques et pour le manque d'information des salariés. Les caméras « ne sont pas orientées uniquement vers les zones sensibles (apporte d'accès ou coffre-fort) mais filment de manière directe et constante les postes de travail » mais aussi la salle de repos d'une des boutiques.

Cette surveillance, « est disproportionnée au regard de la finalité de prévention des atteintes aux personnes et aux biens. Si la surveillance de zones sensibles est justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut intervenir que dans des circonstances exceptionnelle », assène la Commission.

Surveillance disproportionnée

Ce n'est en fait pas la première fois que la firme est épinglée par la Commission informatique et Libertés. En décembre 2013, elle faisait déjà l'objet d'une mise en demeure portant sur le dispositif de vidéosurveillance des salariés installé au sein de l'Apple Store d'Opéra à Paris. « Il était notamment demandé à la société de réorienter certaines caméras qui filmaient en permanence des salariés et de leur délivrer une information complète », explique la Cnil.

En février 2014, la société a justifié s'être mise en conformité avec ses obligations pour le magasin, entraînant la clôture de la mise en demeure. Mais des contrôles menés en mai et juin derniers dans d'autres magasins français du géant « ont révélé que la société n'avait pas adopté des mesures de conformité similaires à l'ensemble de ses magasins. L'information des salariés sur le dispositif demeurait lacunaire et certaines caméras continuaient à filmer des salariés à leur poste de travail sans justification particulière ».

« La persistance de ces manquements » a conduit la Commission à mettre à nouveau en demeure la société « de modifier l'intégralité des dispositifs de vidéosurveillance de ses 16 magasins sur le territoire national ».

« Aucune suite ne sera donnée à cette procédure si Apple France se conforme à la loi dans le délai de deux mois qui lui est imparti », ajoute la Cnil. Dans le cas contraire, la firme pourrait écoper de sanctions financières.

Voila de quoi tendre encore un peu plus les relations entre Apple et ses salariés français. En 2012 déjà, ces derniers s'étaient mis en grève. En cause, des revendications sur les salaires et les conditions de travail. Les syndicats négociaient avec la direction la mise en place de différents dispositifs, dont l'attribution de tickets restaurant et d'un 13e mois. Les salariés ont finalement obtenu une concession : des tickets restaurant d'un montant de 8,50 euros…

Par Olivier Chicheportiche

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.zdnet.fr/actualites/la-cnil-met-en-demeure-apple-france-accuse-de-surveiller-en-permanence-ses-salaries-39808739.htm

Certains sites facturent jusqu’à 80€ de plus l’achat depuis un mobile

Certains sites factureraient jusqu’à 80€ de plus l’achat depuis un mobile

Une étude dénonce l’absence de transparence des sites de e-commerce et de réservation d’hôtels pratiquant la tarification dynamique. Plus de la moitié des services analysés applique des prix différents en fonction des acheteurs.

Dans les souks, il n’est pas rare d’avoir des prix à la tête du client. Mais au moins, on peut négocier. Sur Internet, on apprend que les prix peuvent varier selon le type de terminal utilisé, le système d’exploitation ou les données personnelles des Internautes. C’est ce que démontre une équipe de chercheurs du College of Computer and information Science de l’université du Nord-Est à Boston (USA).

L’étude révèle que, sur les 16 sites américains observés, 9 modifient les prix en fonction du type de visiteur. Ainsi, le service de réservation d’hôtels Travelocity réduit ses tarifs de 15 dollars pour les utilisateurs d’iPhone ou d’iPad. Le distributeur Home Depot facture jusqu’à 100 dollars supplémentaires les internautes naviguant à partir d’un terminal mobile. Cheaptickets et Orbitz, deux sociétés de voyages en ligne, ajoutent 12 dollars en moyenne à la note des clients ne disposant pas de comptes sur leurs sites.
Enfin, Expedia et Hotels.com manipulent les résultats de recherches afin de mettre en avant des hôtels plus chers. Cela dans l’optique de tester l’impact de telles méthodes sur les internautes.

Un manque de transparence
La pratique du « Dynamic pricing », ou tarification dynamique, est bien connue et n’a rien d’illégale. D’ailleurs, elle est antérieure à Internet, puisque des coupons de réduction dans un supermarché constituent également une forme de tarification personnalisée. En revanche, Internet, le Big data et les traceurs ont permis d’affiner la technique en se servant, entre autres, des adresses IP des visiteurs, de leur localisation géographique, de leur historique (navigation et achats), ou encore de la plateforme utilisée.
Ce que les chercheurs pointent du doigt n’est donc pas la pratique en tant que telle, mais le manque de transparence autour de celle-ci. La tarification dynamique peut permettre d’obtenir des produits à de meilleurs prix, à condition d’être au courant de sa mise en œuvre. Autrement, des clients peuvent se retrouver à payer plus cher pour le même produit, sans s’en rendre compte.
Certains e-commerçants, comme Amazon par exemple, gardent secrète leur méthode de calcul des tarifs. En 2011, des consommateurs s’étaient plaints d’avoir payé des prix différents pour le même DVD, livré dans les mêmes conditions. Le géant américain avait alors remboursé la différence. Un an plus tard, Orbitz se retrouvait à son tour sous le feu des projecteurs car le service mettait en avant des hôtels jusqu’à 30% plus cher lorsqu’un visiteur effectuait une recherche à partir d’un Mac. Depuis, la société affirme avoir mis un terme à cette pratique.
Plus récemment, les sociétés de location de voitures Avis, Goldcar, Entreprise, Sixt, Europcar et Hertz se sont fait taper sur les doigts pour avoir appliqué des prix différents selon l’endroit où se trouvait le consommateur. Une différence de traitement injustifiée selon l’Union européenne. Cette dernière avait alors sommé les six sociétés de respecter les lois du marché unique sur le vieux continent.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/e-commerce/actualite-735329-commerce-etude-prix-utilisateur.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_28/10/2014&partner=-&svc_position=720502960&svc_misc=-&crmID=639453874_720502960&estat_url=http%3A%2F%2Fpro.clubic.com%2Fe-commerce%2Factualite-735329-commerce-etude-prix-utilisateur.html

---

CyberCercle du 8 octobre 2014 – Décryptage du rapport interministériel sur la lutte contre la cybercriminalité

CyberCercle du 8 octobre 2014 – Décryptage du rapport interministériel sur la lutte contre la cybercriminalité

Le 8 octobre dernier, Denis JACOPINI s'est rendu au Décryptage du rapport interministériel sur la lutte contre la cybercriminalité organisé par le CyberCercle.

Le CyberCercle a reçu mercredi 8 octobre 2014, Myriam QUEMENER, Magistrat, membre du groupe de travail auteur du rapport interministériel sur la lutte contre la cybercriminalité, membre de la Commission Numérique à l'Assemblée Nationale, et Maître Christiane FERAL-SCHUHL, avocat, ancien Bâtonnier du Barreau de Paris, co-présidente de la Commission Numérique à l'Assemblée Nationale, pour un petit-déjeuner-débat sur le thème :
« DECRYPTAGE DU RAPPORT INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE »

Cette conférence s'est déroulée dans les salons du Bateau MAXIM'S en présence d'une cinquantaine d'auditeurs, notamment des représentants de la magistrature, de la Gendarmerie nationale, de la D2IE, de l'ANSSI, du ministère de la Défense, et des entreprises partenaires des forces de sécurité dans la lutte contre la cybercriminalité.
Retrouvez Myriam QUEMENER par video sur notre chaîne YouTube : « Quels sont selon vous les points forts du rapport interministériel sur la lutte contre la cybercriminalité publié en juillet 2014 ? »

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.defense-et-strategie.fr/index.php?option=com_content&view=article&id=567:cybercercle-du-8-octobre-2014-decryptage-du-rapport-interministeriel-sur-la-lutte-contre-la-cybercriminalite

---

Outlook Web App ciblé par des attaques de phishing sophistiquées – Le Monde Informatique

Outlook Web App ciblé par des attaques de phishing sophistiquées

Selon les chercheurs de Trend Micro, un groupe de pirates sévit à l'encontre d'agences militaires, ambassades et d'entreprises liées à la défense nationale et des médias internationaux utilisant Outlook Web App d'Office 365.

Afin de voler les identifiants de messagerie des employés de nombreuses organisations publiques, parapubliques mais également privées, un groupe d'espions a mis en place des techniques de phishing avancées.
Selon des chercheurs de l'entreprise de sécurité Trend Micro, qui ont baptisé cette campagne Operation Pawn Storm dans un document publié la semaine dernière, le groupe à l'origine de ces attaques opèrerait depuis au moins 2007. Au cours de ces années, ils ont utilisé différentes techniques pour atteindre leurs objectifs, notamment des campagnes de phishing pour propager des malwares sous forme de pièces jointes Microsoft Office malveillantes, l'installation de backdoors type SEDNIT ou Sofacy, ou des exploits plus sélectifs pour infecter des sites légitimes.

Dans ses dernières attaques de phishing, le groupe a utilisé une technique particulièrement intéressante, ciblant les organisations qui utilisent Outlook Web App (OWA), une composante du service Office 365 proposé par Microsoft. Pour chaque attaque, le groupe a créé deux faux domaines : un premier, qui reproduit un site Web tiers connu des victimes – par exemple le site d'une conférence dans un secteur de l'industrie qui les intéresse – et un second, similaire au domaine utilisé pour le déploiement d'Outlook Web App par l'organisation visée. Les attaquants ont ensuite créé des courriels contenant un lien vers le faux site tiers sur lequel ils hébergeaient un code JavaScript non malveillant dont le but était double : ouvrir le site légitime dans un nouvel onglet et rediriger l'onglet déjà ouvert du navigateur Outlook Web App vers une page de phishing. « Le code JavaScript faisait croire aux victimes que leur session OWA était close, et la page malveillante leur demandait de se reconnecter en tapant à nouveau leurs identifiants », ont écrit les chercheurs de Trend Micro dans leur document.
« Les attaquants ont réussi à rediriger les victimes vers de fausses pages Outlook Web App en agissant sur les propriétés d'ouverture des pages de leurs navigateurs ».

Une technique de phishing multi-navigateurs
Selon les chercheurs, cette technique n'exploite aucune vulnérabilité et fonctionne avec tous les navigateurs courants dont Internet Explorer, Mozilla Firefox, Google Chrome et Safari d'Apple. Cependant, il faut deux conditions pour que ce mode opératoire fonctionne : « Les victimes doivent utiliser OWA et ils doivent cliquer sur les liens intégrés au volet de prévisualisation OWA », ont-ils expliqué. L'attaque est redoutable parce que l'onglet du navigateur ne permet pas aux victimes de voir que leur session OWA est illégitime et ils ont peu de chance de se rendre compte que l'URL a été usurpée avant de rentrer leurs identifiants. « De plus, les attaquants ont pris soin d'utiliser des noms de domaine très similaires à ceux choisis par les organisations ciblées pour leurs pages de log in OWA, et dans certains cas, ils ont même acheté des certificats SSL légitimes, de sorte que les navigateurs des victimes affichent aussi les indicateurs de connexion sécurisée HTTPS pour les sites de phishing », ont encore ajouté les chercheurs de Trend Micro.

Parmi les personnes visées, on trouve des employés de l'entreprise militaire privée américaine Academi, anciennement connue sous le nom de Blackwater ; l'Organisation pour la sécurité et la coopération en Europe (OSCE) ; le Département d'État des États-Unis ; le fournisseur du gouvernement américain Science Applications International Corporation (SAIC) ; une société multinationale basée en Allemagne ; l'ambassade du Vatican en Irak ; des médias de radiodiffusions de plusieurs pays ; les ministères de la Défense de la France et de la Hongrie ; des responsables militaires pakistanais ; des employés du gouvernement polonais et des attachés militaires de différents pays. Parmi les appâts utilisés par les assaillants, les chercheurs ont identifié des événements et des conférences bien-connus pour lesquels les victimes pouvaient avoir un intérêt.
« Mais, ce n'est pas tout : les assaillants ont combiné leur tactique de phishing à diverses attaques éprouvées afin de compromettre les systèmes et entrer dans les réseaux pour y voler des données », ont déclaré les chercheurs de Trend Micro.
« Les variantes de SEDNIT utilisées ont été semble-t-il très efficaces car elles ont permis aux pirates de voler des informations sensibles sur les ordinateurs des victimes en évitant de se faire repérer ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-outlook-web-app-cible-par-des-attaques-de-phishing-sophistiquees-59081.html

---

Est-ce que votre site Internet est en règle avec la

CNIL ?

Est-ce que votre site Internet est en règle avec la CNIL ?
Est-ce que votre site Internet est en règle vis à vis de la loi informatique et libertés ?
Des grands changements ont eu lieu ces derniers mois.

Un grand pas vers la détection des fraudes nommé ArgyleDB

Un grand pas vers la détection des fraudes nommé ArgyleDB

L'éditeur Argyle Data a lancé sa solution de détection des fraudes reposant sur le SGBD Accumulo créé par la NSA ainsi que sur le moteur de requêtes SQL distribué Presto développé par Facebook.

Argyle Data a annoncé le lancement d'ArgyleDB, sa solution de surveillance et de détection des fraudes en temps réel taillé pour les environnements Hadoop et à forte volumétrie de données. La société indique avoir conçu son offre sur la base du système de gestion de base de données Accumulo, initialement développé par la NSA avant d'être récupéré en 2011 par la fondation Apache, mais également de Presto, la technologie Open Source utilisée par Facebook pour permettre d'analyser les données en utilisant des requêtes SQL et d'automatiser les futures requêtes sur les données en direct.
Argyle Data indique par ailleurs que sa solution supporte un ensemble d'algorithmes permettant de détecter une activité frauduleuse, à une échelle pétaflopique, en une quinzaine de minutes seulement contre 24 heures ou plus habituellement. L'année dernière, Argyle Data avait annoncé travailler sur une gamme de produits utilisant le machine learning sur une pile Hadoop afin de créer des applications capables d'ingérer des données et de les analyser en temps réale pour réduire la fenêtre de détection des fraudes et d'intrusion de plusieurs heures ou jours à quelques secondes.

Une levée de fonds de 4,5 millions de dollars
Parallèlement à ce lancement, Argyle Data a annoncé un nouveau tour de table financier qui lui a permis de lever 4,5 millions de dollars, portant à 21 millions de dollars le montant total des fonds levés depuis sa création en 2009. L'équipe de direction est également étoffée avec l'arrivée de Arshak Navruzyan, Ian Howells, Padraig Stapleton et Volkmar Scharf-Katz Navruzyan qui ont tous un solide vécu en matière d'analytique et de machine learning.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-argyledb-la-detection-des-fraudes-avec-des-technologies-de-facebook-et-la-nsa-59068.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Droit au déréférencement sur Google jugé à Paris

Droit au déréférencement sur Google jugé à Paris

Dans une ordonnance de référé datant du 16 septembre 2014, le Président du Tribunal de Grande Instance de Paris a enjoint Google France, de supprimer des liens renvoyant vers des contenus déjà jugés diffamatoires par un jugement du tribunal correctionnel du 13 mars 2014.

Google France avait tenté de faire valoir qu'elle n'avait qu'une activité de fourniture de prestations de marketing et de démonstration auprès d'une clientèle utilisant des services publicitaires. Cependant, le juge des référés a retenu que si la société Google Inc, sa société-mère, était l'exploitant du moteur de recherche, Google France avait pour activité la promotion et la vente d'espaces publicitaires liés à des termes recherchés au moyen du moteur édité par Google Inc. et assurait donc, le financement de ce moteur de recherche.
Google France avait argué que les demandeurs ne pouvaient contourner les conditions procédurales de la loi du 29 juillet 1881 (notamment l'article 53), dès lors qu'ils agissaient sur le fondement de la diffamation. Toutefois, le juge des référés a retenu qu'en aucun cas les demandeurs ne se fondaient sur la loi du 29 juillet 1881. En effet, ces derniers reprochaient simplement à Google France d'avoir mis à la disposition de ses utilisateurs des données à caractère personnel qui avaient déjà été jugées diffamatoires.. Ainsi, le Président du Tribunal de grande instance de Paris a estimé que les dispositions de la loi du 29 juillet 1881 précitée n'étaient pas applicables à Google France.

Le juge a donc consacré un droit au déréférencement dans les moteurs de recherche sur Internet en s'appuyant sur plusieurs fondements afin d'enjoindre Google France à déréférencer plusieurs liens renvoyant à des contenus diffamatoires :
– la Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
– la Loi n°78-17 du 6 janvier 1978 selon laquelle : « {Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soit, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdites. »}
– l'Arrêt du 13 mai 2014 de la Cour de justice des communautés européennes ;
– et la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette dernière directive européenne vise à assurer « une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée ».

Le juge des référés ordonna ainsi à la société Google France, sous astreinte, de faire procéder à la suppression des liens référencés litigieux. Cette décision, qui apparait quelques mois après l'arrêt innovant de la CJUE du 13 mai 2014, consacre pour la première fois en France, un droit au recours au juge des référés pour faire respecter ce droit au déréférencement des données à caractère personnel dans les résultats du moteur de recherche Google.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.legavox.fr/blog/e-reputation-et-droit/google-consecration-droit-dereferencement-donnees-16076.htm