Affaire United : selon le FBI, un hacker a modifié en vol la puissance d’un réacteur – Le Monde Informatique | Le Net Expert Informatique

Un hacker a modifié en vol la puissance d’un réacteur

Selon une note du FBI, en trois ans, le chercheur en sécurité Chris Roberts a réussi à pirater une vingtaine de fois les systèmes informatiques d'avions de ligne. Le dernier en date, sur un vol d'United Airlines entre Denver et Chicago, a entraîné son interpellation à la sortie de l'avion le 15 avril 2015.

Le FBI soupçonne aujourd'hui le chercheur en sécurité Chris Roberts, fondateur et CTO de One World Labs, d'avoir modifié la puissance d'un des réacteurs du vol d'United Airlines du 15 avril dernier entre Denver vers Chicago. M. Roberts avait été interpellé par le FBI à sa descente d'avion suite à un tweet suggérant qu'il avait scanné les systèmes informatiques (EICA) d'un Boeing 737. Cette arrestation et la saisie de tout son matériel informatique semblent faire suite à des dysfonctionnements relevés par United Airlines. Interrogé par le FBI, le chercheur, justement spécialisé dans les failles de sécurité des systèmes embarqués en aéronautique, a indiqué avoir réussi à accéder une vingtaine de fois aux systèmes informatiques d'avions de ligne.

Le 17 avril, l'agence fédérale américaine a obtenu un mandat pour perquisitionner les locaux du chercheur. Dans sa demande de mandat, le FBI révèle des informations provenant des trois interrogatoires de M. Roberts. Il n'a pas encore été accusé d'un crime, même si United Airlines l'a interdit de vol sur ses avions. On ne sait pas encore si l'incident impliquant le moteur de l'avion a eu lieu ou si l'avion aurait pu être en danger à la suite de celui-ci.

Un tweet dévastateur

Dimanche dernier, M. Roberts a écrit sur Twitter que «au cours des cinq dernières années, mon seul but a été d'améliorer la sécurité des avions … compte tenu de la situation actuelle, on m'a conseillé de ne pas en dire plus. » La défense du chercheur en sécurité est assurée par Nate Cardozo, un avocat travaillant avec l'Electronic Frontier Foundation. M. Cardozo a déclaré que son client n'était pas disponible pour commenter autre chose que ce qu'il a écrit sur Twitter.

En ce qui concerne l'incident de moteur, l'agent spécial Mark S. Hurley a écrit dans la demande de mandat que M. Roberts a indiqué qu'il avait connecté son PC portable au système de divertissement en vol (In Flight Entertainment System ou IFE) de l'avion United Airlines en utilisant le Seat Electronic Box (SEB), qui se trouve sous certains sièges passagers. Après le piratage du système IFE, il a accédé aux autres systèmes de l'avion, précise l'agent spécial. M. Roberts « a déclaré qu'il avait modifié le code du Thrust Management Computer (TMC) de l'avion pour modifier la puissance des moteurs », ajoute M. Hurley. « Il a déclaré qu'il a commandé avec succès le système pour consulter et modifier les commandes de vol (CLB ou climb command). Un des moteurs de l'avion a commencé à augmenter sa puissance, « entrainant un mouvement latéral ou sur le côté de l'avion lors d'un de ces vols », précise le mandat de perquisition. L'agent Hurley écrit encore que M. Roberts a précisé qu'il avait compromis 15 à 20 fois des systèmes IFE de 2011 à 2014. Selon l'agent spécial, les systèmes IFE compromis sont fabriqués par Thales et Panasonic (les moniteurs vidéo installés à l'arrière de sièges passagers), .

Un boitier SEB forcé sous le siège passager

Les problèmes judiciaires de Chris Roberts ont vraiment commencé le 15 avril quand il a écrit un tweet suggéré qu'il sondait les systèmes d'un Boeing 737/800 d'United Airlines lors d'un vol Denver/Chicago. Il a ensuite poursuivi son voyage de Chicago vers Syracuse (dans l'état de NY). Entretemps le département Cyber Security Intelligence d'United Airlines qui avait vu ce tweet faisant référence au système EICAS, a envoyé une équipe de sécurité interpeller M. Roberts à sa sortie de l'avion pour le remettre au FBI.

Après son interpellation, un agent spécial a examiné la cabine de première classe où avait voyagé M. Roberts vers Chicago. Les boitier SEB sous les sièges 2A et 3A montraient des signes d'effraction. « Le SEB sous le siège 2A a été endommagé » indique le mandat de perquisition. « L'enveloppe extérieure de la boîte a été ouverte d'environ 1,27 cm, et une des vis de fixation était manquante ». Redevenu très prudent, M. Roberts a affirmé aux agents du FBI qu'il n'avait pas compromis le réseau de l'avion sur le vol à destination de Chicago, selon le mandat. En février et mars dernier, le FBI avait déjà interrogé Chris Roberts qui avait également affirmé avoir réussi à pirater les systèmes IFE à bord d'avions.

Cette affaire devrait en n'en pas douter, impacter le monde de la sécurité aérienne dans les prochains mois, voire années, et aboutir au renforcement des règles dans ce domaine.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-affaire-united%C3%82%C2%A0-selon-le-fbi-un-hacker-a-modifie-en-vol-la-puissance-d-un-reacteur-61170.html
Par Serge Leblal avec IDG NS

Les PME connaissent les risques informatiques mais ne

réagissent pas| Le Net Expert Informatique

Les PME connaissent les risques informatiques mais ne réagissent pas

Bien que les petites et moyennes entreprises soient conscientes des menaces qui pèsent sur leurs systèmes d'information, le baromètre Ipsos-Navista montre qu'elles ne consacrent qu'un budget dérisoire à leur protection.

Une récente étude menée par Ipsos-Navista auprès des PME françaises indique que 99% d'entre elles sont équipées en informatique et que les postes clients et terminaux mobiles qu'elles utilisent sont connectés à Internet. 82 % des entreprises interrogées permettent à leurs salariés de se connecter à n'importe quel site web. Elles sont en outre 80% à voir des terminaux mobiles utilisés dans leurs murs et à leur donner accès à leur réseau dans 2 cas sur 3. Autant dire qu'elles laissent la porte grande ouverte aux menaces de tous types. Pourtant, 9 sociétés sur 10 évaluent bien l'usurpation des mots de passe et l'utilisation frauduleuse ou malveillante de leurs ressources informatiques comme un risque. Par ailleurs, 76% des gérants se savent pénalement responsables de l'utilisation d'internet dans leur entreprise.

Une PME sur deux n'a pas de pare-feu

Malgré ce contexte de fort équipement, d'accès ouvert au web et de conscience des risques, les PME françaises sont loin de faire ce qu'il faut pour se protéger. Elles sont par exemple une grande majorité à utiliser la messagerie native de leur FAI, ou un web mail peu sécurisé. Plus grave encore sur le plan juridique, les trois quarts d'entre elles sont incapables de dire où sont sauvegardées les pièces-jointes échangées avec leurs clients, sans garantie de confidentialité. La liste égrenée par l'étude Ipsos-Navista ne s'arrête pas là. Elle précise aussi que 26% des petites et moyennes entreprises ne possèdent pas d'anti-virus, qu'elles ne sont que 36 % à utiliser un antiphising et 52 % un pare-feu.

50€ par an et par salariés pour la sécurité

Dans ces conditions, on comprend pourquoi le budget annuel que les PME allouent par employé à la sécurité informatique n'excède pas les 50€ par an pour plus de la moitié d'entre elles. L'étude relève que la « légèreté de ce budget est à considérer au regard des sommes que coûteraient en moyenne une violation des données de l'entreprise, pouvant atteindre parfois plusieurs millions d'euros ». 11 % des entreprises interrogées déclarent avoir déjà été victimes d'actes de malveillance. Un chiffre qui ne prend pas en compte les sociétés qui n'ont pas rendu publique les attaques dont elles ont fait l'objet ni celles qui ne s'en sont pas aperçu.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Vous souhaitez participer à une de nos formations ?
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.distributique.com/actualites/lire-securite-les-pme-connaissent-les-risques-mais-ne-reagissent-pas-23077.html

Alerte: Nouveaux courriels de phishing au nom d’Apple (iTunes) | Le Net Expert Informatique

Des fraudeurs envoient des courriels au nom d'Apple (iTunes) afin de s'emparer des données d'accès à votre compte.
Par ces courriels, les destinataires sont informés que leur compte n'a pas pu être validé et que celui-ci a été bloqué. Les escrocs demandent de suivre un lien et de fournir des données personnelles (nom d'utilisateur et mot de passe) sous prétexte de pouvoir réactiver leur compte.

Le SCOCI conseille :
1. Effacez le courriel !
2. Si vous soupçonnez quelqu'un d'être en possession de vos données d'accès à votre compte, veuillez immédiatement prendre contact avec le support d'Apple.
3. Soyez prudents avec tous les courriels qui vous demandent de cliquer sur un lien Internet pour contrôler vos données personnelles. En règle générale, ceci est l'œuvre de fraudeurs.
4. Contrôlez toujours l'adresse Internet (URL) sur laquelle vous êtes redirigés (cf. rectangle rouge sur l'image). De manière générale, si vous devez vous connecter à un compte en ligne, inscrivez l'URL vous même dans votre navigateur plutôt que de cliquer sur un lien qui vous est transmis par courriel.
5. Signalez ces cas au SCOCI par le biais de son formulaire d'annonce en ligne afin que nous puissions analyser ces courriels et faire fermer au plus vite les sites frauduleux.

En cas de doute sur une usurpation d'identité ou de doute sur une arnaque, n'hésitez pas à contacter Denis JACOPINI expert informatique assermenté.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/2015/2015-05-15.html

---

Big Data et données

personnelles: l’Europe harmonise ses règles | Le Net Expert Informatique

Big Data et données personnelles: l’Europe harmonise ses règles

La future réglementation européenne encadrant l’usage des données à caractère personnel imposera de nouvelles contraintes aux entreprises. Mieux vaut s’y préparer.

Au sein des 28 Etats membres de l’Union européenne, les CNIL nationales veillent, entre autre choses, à la protection des données à caractère personnel.
Mais la globalisation de l’économie et sa digitalisation imposent un cadre réglementaire lui-même global. Ainsi, cette année, un règlement européen unifiant la protection des données personnelles entre les pays de l’UE devrait voir le jour.
L’objectif de ce projet est d’accroître le contrôle des utilisateurs sur leurs propres données, en leur accordant un droit à l’oubli, un droit à la portabilité et un droit à être informé en cas de défaillance des systèmes gérant leurs informations.

Les entreprises devront se mettre en conformité
Pourquoi est-ce important ? Parce que le Big Data et ses traitements statistiques montent en puissance, notamment auprès des équipes marketing des entreprises.
Ces analyses ont pour objectif de profiler les consommateurs, en collectant également des données personnelles sur Internet, pour leur proposer une de nouveaux services personnalisés. Les internautes pourront donc demander à supprimer certaines données.
Surtout, le prochain règlement européen obligera toutes les entreprises exploitant des informations personnelles à révéler leurs failles en cas de dysfonctionnement de leurs systèmes (panne, piratage…).
En somme, quand les entreprises étaient jusqu’alors soumises à des formalités, elles devront, dès la mise en application du règlement, se mettre en conformité pour pouvoir répondre à ces nouvelles exigences.
« Les entreprises vont devoir mettent en place des dispositifs démontrant le respect la protection des données à caractère personnel et assurant leur traçabilité », résume Garance Mathias, avocat à la Cour.

Vous souhaitez vous former à la protection des données personnelles, vous mettre en conformité avec la CNIL, n’hésitez pas à consulter nos **formations en protection des données personnelles** et **formations en cybercrimnalité** sur le sujet

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://bfmbusiness.bfmtv.com/entreprise/big-data-et-donnees-personnelles-l-europe-harmonise-ses-regles-886590.html
Par Eddye Dibar

Sécurité : il est urgent de ne plus négliger le facteur humain ! | Le Net Expert Informatique

Sécurité : il est urgent de ne plus négliger le facteur humain !

Dans sa dernière étude intitulée « Le Facteur Humain », Proofpoint indique que les pirates ont, l'an denier, décidé d'opérer au niveau des entreprises, et non plus auprès du grand public. Ils se sont donc concentrés sur les processus de partage d'informations utilisés par les cadres, tout en privilégiant la sophistication des attaques, et non plus leur volume.

Les résultats de cette étude prouve que le comportement des utilisateurs, et pas uniquement les failles d'un système ou d'un logiciel donné, a une incidence significative sur la sécurité des entreprises. « Le facteur humain constitue l'un des éléments clés des programmes de sécurité, alors qu'il est souvent celui que l'on néglige le plus, indique Nick Hayes, Christopher McClean et Claire O'Malley. C'est bien là le problème. En effet, les solutions de sécurité se révèlent fondamentales si vous souhaitez protéger votre environnement de travail, mais ne sont d'aucune utilité si des actions humaines viennent les affaiblir ».
Malgré cela, de nombreuses entreprises adossent leur sécurité uniquement sur des technologies avec passerelle et n'optent pas pour des solutions de blocage, de protection contre les attaques ciblées, de détection et de gestion des menaces (qui sont toutes basées sur les utilisateurs plutôt que sur l'infrastructure).
L'étude révèle également que les cadres constituent une cible privilégiée. L'an dernier, ils ont été deux fois plus ciblés qu'en 2013, et leurs clics sur des liens dangereux ont doublé. Du côté des services, ce sont ceux dédiés à la vente, aux finances et à l'approvisionnement (chaîne logistique) qui ont été plus touchés. Proofpoint note que les attaques se produisent surtout pendant les heures de travail. La plupart des messages malveillants étant envoyés lors des heures de travail, principalement le mardi et le jeudi matin. Le mardi constitue la journée la plus critique, avec 17 % de clics de plus que les autres jours.
Au final, même si les utilisateurs sont plus vigilants, les cybercriminels sont aussi capables de s'adapter rapidement. Ainsi, le nombre de mails intégrant des pièces jointes douteuses, et non plus des URL (notifications, avertissements à caractère financier), s'est multiplié. L'an dernier, durant certains jours, Proofpoint a même constaté une augmentation de 1 000 % du volume des pièces jointes malveillantes. Cette année, la donne est différente, les fausses sollicitations par mail faisant état de réception de fax ou de messages vocaux, voire d'alerte à caractère financier (facture, relevés de comptes, etc.).
« Il existera toujours une personne qui cliquera sur un lien, et permettra ainsi aux menaces de se propager auprès des utilisateurs, confirme Kevin Epstein, Vice-Président en charge de la gouvernance et de la sécurité avancée chez Proofpoint. L'approche de Proofpoint est efficace car nos systèmes sont capables d'identifier les individus concernés, de localiser ces derniers et de déterminer les actions en cours. Ainsi, nous permettons aux organisations de se protéger activement, ainsi que de prendre, en temps réel, les mesures adéquates ».

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

Source :
http://www.infodsi.com/articles/155558/securite-est-urgent-plus-negliger-facteur-humain.html

Les «usines à clics» tournent à plein régime aux Philippines | Le Net Expert Informatique

Les «usines à clics» tournent à plein régime aux Philippines

Les « usines à clics » aux Philippines produisent en masse de faux comptes pour les réseaux sociaux. De nombreuses célébrités, des personnalités politiques, de grandes entreprises et même de simples internautes en manque de fans, usent et abusent de cette contrefaçon numérique afin accroître leur popularité sur la Toile.

Un journaliste du magazine en ligne New Republic a enquêté aux Philippines sur les « usines à clics », ces fabriques singulières qui créent à la chaîne de faux comptes « clef en main » et inondent les réseaux sociaux de recommandations bidons, de « j'aime » chimériques, de fans fictifs et de suiveurs imaginaires.

Le prix d’un faux profil n’excède pas 1€50, et n’importe quel internaute ou de grandes entreprises peuvent ainsi, en quelques clics, gonfler artificiellement leur visibilité sur la Toile. Une activité frauduleuse en plein essor qui s’appuie sur un réseau d’intermédiaires peu scrupuleux, comme le démontrait récemment le magazine Envoyé Spécial sur France Télévisions, qui a surpris une start-up française spécialisée dans la revente d’abonnés virtuels, en pleine transaction.

Selon les conditions d’utilisation des réseaux sociaux, le commerce de faux profils en ligne est formellement interdit. Mais les autorités des Philippines considèrent que ces règlements n’ont aucune valeur juridique sur leur territoire. Pour elles, c’est donc un négoce illicite mais pas illégal.

Un fléau pour les géants d’Internet

Ce marché noir de la « web réputation » menace maintenant l’économie numérique mondiale, il serait nuisible aux activités des entreprises qui ont depuis longtemps investi dans les réseaux sociaux.

C’est un fléau, selon les géants du web, qui ne parviennent pas à endiguer le phénomène, particulièrement pour Facebook, Twitter et Google, dont les modèles économiques reposent exclusivement sur des offres publicitaires ciblées pour le commerce en ligne.

Les usines à clics fonctionnent comme de vraies entreprises, avec un personnel qualifié qui est composé principalement de

jeunes informaticiens diplômés gagnant cinq fois le salaire d'une femme de ménage.

Les patrons, eux, profitent pleinement des infrastructures technologiques implantées dans le pays par de grandes compagnies américaines comme Microsoft. Un miracle économique inattendu de la délocalisation, conclut ironiquement le journaliste de New Republic. Les « usines à clics » sont devenues en quelques années les principaux moteurs de la croissance aux Philippines.

Source : http://www.rfi.fr/asie-pacifique/20150506-philippines-usine-clics-commerce-fans-internet-reseaux-sociaux/?aef_campaign_date=2015-05-06&aef_campaign_ref=partage

_user&ns_campaign=reseaux_sociaux&ns_linkname=editorial&ns_mch
annel=social&ns_source=twitter

Enjeux et défis du web profond | Le Net Expert Informatique

Le web profond (Deep Web) désigne le sous-ensemble d'internet qui n'est pas indexé ou mal indexé par les grands moteurs de recherche comme Google, Yahoo ou Bing,…On sait que cet ensemble de données reste difficilement mesurable mais qu'il occupe un espace très supérieur à celui de l'ensemble des sites web bien indexés par les moteurs classiques. Certaines études avancent un ratio de 80% de Deep Web contre 20% de web de surface à l'image de la partie immergée d'un iceberg…

Profond comme le web

Le contenu du deep web demeure hétérogène. On y trouve de grandes bases de données, des bibliothèques volumineuses non indexées par les moteurs en raison de leur tailles, des pages éphémères, mal construites, à très faible trafic ou volontairement rendues inaccessibles par leurs créateurs aux moteurs traditionnels.
D'après une étude récente de la Darpa, l'agence américaine en charge des projets de défense, plus de 60 millions de pages à vocation criminelle ont été publiées depuis deux ans dans les profondeurs du web. Les moteurs de recherche classiques, Google en tête, utilisent des algorithmes d'indexation dérivés du puissant Pagerank qui s'appuient sur une mesure de popularité du site ou de la page.
Cette approche qui a fait le succès de Google va de fait exclure les pages à faible trafic, éphémères ou furtives. Ce sont précisément ces pages qui sont utilisées par les acteurs de la cybercriminalité pour diffuser de l'information tout en restant sous les radars des grands moteurs. Lorsque cette information concerne une activité criminelle, c'est dans le Dark Web qu'elle sera dissimulée et rendue accessible aux seuls clients potentiels via des outils d'anonymisation spécialisés comme Tor. Le web profond réunit donc de la donnée légitime, souvent de haute qualité lorsqu'il s'agit de bases de données scientifiques volumineuses peu ou mal indexées par les moteurs.
Il réunit de la donnée sécurisée accessible seulement par mot de passe mais aussi de la donnée clandestine issue de trafics et d'activités criminelles. Cet ensemble informationnel hétérogène intéresse depuis longtemps les grands acteurs du numérique, chacun avec une motivation spécifique. L'accès au web profond constitue un élément stratégique du dispositif global de lutte contre la cybercriminalité qui reste l'une des grandes priorités de l'administration américaine. Les efforts pour obtenir des capacités de lecture du web profond se sont concrétisés avec le développement en 2014 du moteur de recherche Memex tout droit sorti des laboratoires de la Darpa.

Memex, le moteur Darpa

Dans son communiqué officiel publié le 9 février 2014 [1], l'agence Darpa décrit Memex comme « le moteur qui révolutionne la découverte, l'organisation et la présentation des résultats de recherche en ligne. Le programme Memex imagine un nouveau paradigme, où il est possible d'organiser rapidement et intelligemment un sous-ensemble de l'internet adapté à l'intérêt d'une personne ».

Le moteur est construit autour de trois axes fonctionnels:
1. l'indexation de domaines spécifiques,
2. la recherche de domaines spécifiques
3. la mise en relation de deux premiers axes

Après plus d'un an d'utilisation en phase de test par les forces de l'ordre américaines, Memex a permis de démanteler un réseau de trafiquants d'êtres humains. Durant la finale du Super Bowl, Memex a servi pour détecter les pages associées à des offres de prostitution. Ses outils d'analyse et de visualisation captent les données invisibles issues du web profond puis tracent la graphe des relations liant ces données. De telles fonctionnalités s'avèrent très efficaces pour cartographier des réseaux clandestins de prostitution en ligne.

D'après les récents communiqués de la Darpa, Memex ne traite pour l'instant que les pages publiques du web profond et ne doit donc pas être associé aux divers outils de surveillance intrusifs utilisés par la NSA. A terme, Memex devrait offrir des fonctionnalités de crawling du Dark Web intégrant les spécificités cryptographiques du système Tor. On peut raisonnablement imaginer que ces fonctions stratégiques faisaient bien partie du cahier des charges initial du projet Memex dont le budget est estimé entre 15 et 20 millions de dollars… La Darpa n'est évidemment pas seule dans la course pour l'exploration du web profond. Google a parfaitement mesuré l'intérêt informationnel que représentent les pages non indexées par son moteur et développe de nouveaux algorithmes spécifiquement adaptés aux profondeurs du web.

Google et le défi des profondeurs

Le web profond contient des informations provenant de formulaires et de zones numériques que les administrateurs de sites souhaitent maintenir privés, hors diffusion et hors référencement. Ces données, souvent très structurées, intéressent les ingénieurs de Google qui cherchent aujourd'hui à y avoir accès de manière détournée. Pour autant, l'extraction des données du web profond demeure un problème algorithmiquement difficile et les récentes publications scientifiques des équipes de Google confirment bien cette complexité. L'Université de Cornell a diffusé un article remarquable décrivant une infrastructure de lecture et de copie de contenus extraits du web profond [2],[3].

L'extraction des données s'effectue selon plusieurs niveaux de crawling destinés à écarter les contenus redondants ou trop similaires à des résultats déjà renvoyés. Des mesures de similarités de contenus sont utilisées selon les URL ciblées pour filtrer et hiérarchiser les données extraites. Le système présenté dans l'article est capable de traiter un grand nombre de requêtes sur des bases de données non adressées par le moteur de recherche classique de Google [4].

A moyen terme, les efforts de Google permettront sans aucun doute de référencer l'ensemble du web profond publiquement accessible. Le niveau de résolution d'une requête sera fixé par l'utilisateur qui définira lui même la profondeur de sa recherche. Seuls les contenus privés cryptés ou accessibles à partir d'une identification par mot de passe demeureront (en théorie) inaccessibles à ce type de moteurs profonds.

Vers une guerre des moteurs?

Les grandes nations technologiques ont pris en compte depuis longtemps les enjeux stratégiques de l'indexation des contenus numériques. Peu bruyante, une « guerre » des moteurs de recherche a bien lieu aujourd'hui, épousant scrupuleusement les contours des conflits et les concurrences de souverainetés nationales. La Chine avec son moteur Baidu a su construire très tôt son indépendance informationnelle face au géant américain.

Aujourd'hui, plus de 500 millions d'internautes utilisent quotidiennement Baidu à partir d'une centaine de pays. La Russie utilise massivement le moteur de recherche Yandex qui ne laisse que peu de place à Google sur le secteur du référencement intérieur russe puisqu'il détient plus de 60% des parts du marché national. En 2014, Vladimir Poutine a souhaité que son pays développe un second moteur de recherche exclusivement contrôlé par des capitaux russes et sans aucune influence extérieure. Plus récemment, en février 2015, le groupe Yandex a déposé une plainte contre Google en Russie pour abus de position dominante sur les smartphones Android. Yandex reproche en effet à Google de bloquer l'installation de ses applications de moteur de recherche sur les smartphones fonctionnant sous Android. Les constructeurs sont contraints aujourd'hui à pré-installer sur leurs machines les Google Apps et à utiliser Google comme moteur par défaut sous Android…

Le moteur face aux mégadonnées

La course à l'indexation des contenus du web profond apparaît comme l'une des composantes stratégiques de la guerre des moteurs. Si la géopolitique des données impose désormais aux nations de définir des politiques claires de stockage et de préservation des données numériques, elle commande également une vision à long terme de l'adressage des contenus. La production mondiale de données dépassera en 2020 les 40 Zo (un zettaoctet est égal à dix puissance vingt et un octets). L'évolution de cette production est exponentielle: 90% des données actuelles ont été produites durant les deux dernières années. Les objets connectés, la géolocalisation, l'émergence des villes intelligentes connectées et de l'information ubiquitaire contribuent au déluge de données numériques. La collecte et l'exploitation des mégadonnées (le terme officiel français à utiliser pour big data) induiront le développement de moteurs polyvalents capables d'indexer toutes les bases de données publiques quelle que soient leurs tailles et leurs contenus.

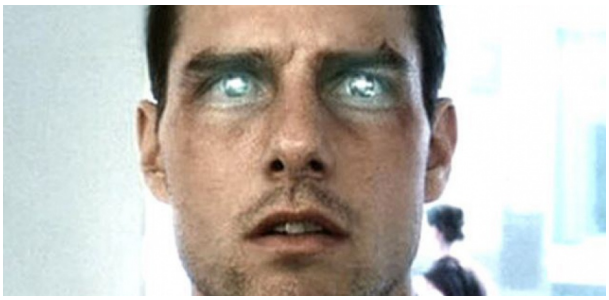
Le moteur de recherche doit être considéré aujourd'hui comme une infrastructure de puissance stratégique au service des nations technologiques. Qu'attend l'Europe pour développer le sien?

_____

[1] La présentation du moteur Memex par l'agence Darpa
http://www.darpa.mil/newsevents/releases/2014/02/09.aspx
[2] « Google's Deep-Web Crawl » – publication de l'Université Cornell
http://www.cs.cornell.edu/~lucja/publications/i03.pdf
[3] « Crawling Deep Web Entity Pages » – publication de recherche, Google
http://pages.cs.wisc.edu/~heyeye/paper/Entity-crawl.pdf
[4] « How Google May index Deep Web Entities »
http://www.seobythesea.com/2015/04/how-google-may-index-deep-web-entities/

Source : http://www.huffingtonpost.fr/thierry-berthier/enjeux-et-defis-deep-web_b_7219384.html
Par Thierry Berthier

Surveillance : votre œil vous trahira bientôt | Le Net Expert Informatique

	Surveillance : votre œil vous trahira bientôt

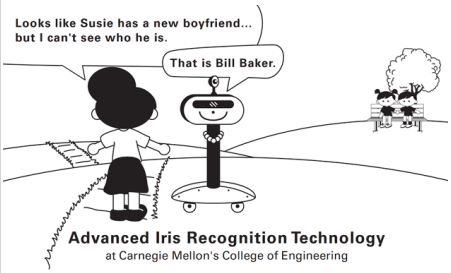
On n'arrête pas le progrès, mais en matière de surveillance, peut-on le qualifier comme tel ? La dernière trouvaille, repérée par « The Atlantic » fait un peu peur : a été mis au point un système permettant d'identifier une personne, à distance, par l'analyse de son œil. Rien de révolutionnaire, direz-vous ? Eh bien si, car les mots importants, dans la phrase précédente, sont : « à distance ».

La reconnaissance d'iris existe certes depuis longtemps, mais jusque là, il fallait que la personne à identifier coopère, qu'elle pose avec précision son œil sur un oculaire. Avec la machine mise au point par Mario Savvides, un professeur de l'université Carnegie Mellon, à Pittsburg, Etats-Unis, l'histoire sera très différente. A plus de dix mètres, assure-t-il, il est désormais possible d'analyser un iris avec la précision d'une empreinte digitale, avant de le confronter à une base de donnée.

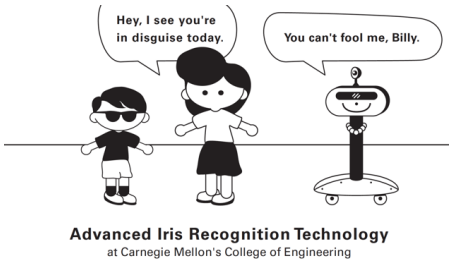
Dans une vidéo mise en ligne, le professeur d'ingénierie donne un exemple d'une utilisation possible d'une telle technologie : un policier repère un automobiliste au comportement suspect et lui demande de garer sa voiture. L'automobiliste jette un coup d'œil dans le rétroviseur et le policier en profite pour vérifier, sans avoir à sortir de son véhicule, s'il n'est pas fiché comme personne dangereuse…

On peut imaginer bien d'autres usages :
avant un match de foot, l'appareil vérifierait l'iris de chaque spectateur pénétrant dans le stade, afin de filtrer les éventuels hooligans fichés ;
un enfant est enlevé, son iris est livré aux autorités des frontières pour éviter qu'il ne soit emmené à l'étranger ;
dans une grande entreprise, une administration, ou un festival, seuls les propriétaires d'iris « VIP » pourraient accéder à certains espaces.
seuls les propriétaires d'ordinateurs ou de voitures pourront démarrer ces derniers, sans mot de passe, sans clé (et sans avoir à poser son oeil sur son volant) ;
à l'aéroport, les voyageurs pourront se passer de montrer leurs papiers.

Mais on peut craindre aussi des usages plus effrayants. Le service de presse de Carnegie Mellon a envoyé deux dessins à « The Atlantic ». Sur le premier, une jeune fille aperçoit un couple enlacé au loin : « On dirait que Susie a un nouveau petit ami… », dit-elle. Et la machine, ce robot-commère, lui dit : « Oui, c'est Bill Baxter ». Qui sait si la Susie en question n'est pas une femme politique et la héroïne du dessin une affreuse paparazzi ?



Autre dessin, la même jeune fille est face à un garçon grimé : « Eh, je vois qu'on s'est déguisé aujourd'hui ! ». La machine, froidement : « Tu ne m'aura pas, Billy ». Mignon ? Pas vraiment : une machine qui rend le déguisement obsolète ne peut guère être considérée comme un grand progrès pour la vie privée.



La police ne manquera pas de tester ce système, mais gageons qu'elle ne sera pas la seule à se pencher dessus. Les usages commerciaux, si cet appareil biométrique fonctionne, ne manqueront pas d'apparaître. On pense à ces scènes du film « Minority Report » où des publicités alpaguent les passants tout en s'adaptant à leurs goûts (« John Anderton ! Vous n'auriez pas envie d'une petite Guinness ? ») et où un hologramme, à l'accueil d'un magasin de vêtements, reconnaît les yeux que s'est greffés le héros, Tom Cruise, pour échapper à la police (« Hello Mr Yakomoto, contente de vous revoir chez Gap »).

Interrogé par « The Atlantic » sur les craintes que soulève cette technologie, Marios Savvides les balaye d'un argument pour le moins fataliste :
Les gens sont traqués, chacun de leurs mouvements, de leurs achats, de leurs habitudes, où ils se trouvent chaque jour, à travers leurs transactions par carte de crédit, leurs cartes de fidélité –si quelqu'un veut vraiment savoir ce que vous faites à n'importe quel moment de la journée, il n'a pas besoin de systèmes de reconnaissance faciale ou de reconnaissance d'iris. Tout ce qu'il faut est déjà en place. »

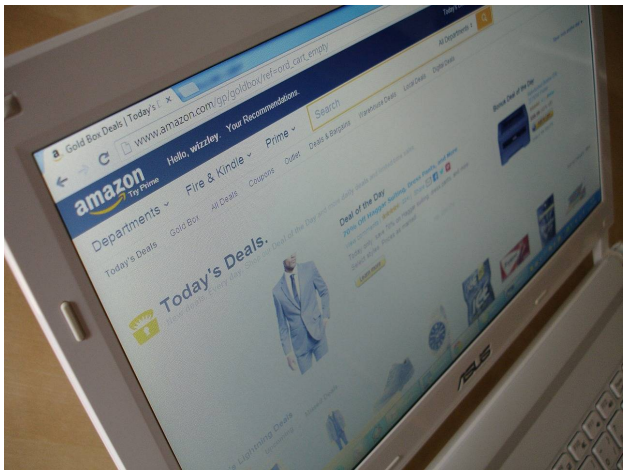
Autrement dit : bah, la surveillance de masse, un peu plus, un peu moins…
La mise en place d'un tel système de reconnaissance « à distance » sera facilité par la décision prise par plusieurs pays, il y a plusieurs années déjà, de constituer des bases d'iris. Aux Etats-Unis, depuis quatre ans, la police scanne ainsi les yeux des personnes condamnées à des peines de prison. Dans les Emirats arabes unis, l'iris est scanné à l'entrée et à la sortie du territoire. Et l'Inde va plus loin encore : ce sont les iris de l'ensemble de la population qui sont peu à peu associés, dans une base de donnée, à leur numéro unique d'identité.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150515.OBS9017/surveillance-votre-il-vous-trahira-bientot.html

Par Pascal Riché

96 % des consommateurs sont influencés par l’e-réputation des marques | Le Net Expert Informatique

	96 % des consommateurs sont influencés par l’e-réputation des marques

Les consommateurs sont de plus en plus nombreux à s'informer sur l'image des marques avant de procéder à un achat.

C'est une étude qui confirme ce que l'on pressentait. Les avis de consommateurs ont un impact réel sur l'acte d'achat : 80 % des consommateurs se renseignent en ligne avant de procéder à un achat. Et 96 % des internautes reconnaissent être influencés par l'e-réputation de la marque ! Selon une étude réalisée par l'IFOP pour le compte de l'agence Réputation VIP, les consommateurs sont désormais très nombreux à consulter les blogs et les forums de discussion. 85 % affirment qu'un avis négatif peut les dissuader d'acheter un produit.
Cette tendance à veiller sur la réputation d'une marque ou d'un produit est même en passe de devenir un sport national puisque « 58 % consultent Internet pour se faire une idée sur l'image d'une marque ou d'un magasin sans intention d'achat ».

Facebook et Twitter à la traîne
Trois types de contenus éditoriaux sont particulièrement prisés par les e-consommateurs : les forums (47 %), les blogs (17 %) et les réseaux sociaux (12 %). Facebook et Twitter ne semblent donc pas avoir l'influence qu'on leur prête habituellement. Ces chiffres soulignent par ailleurs la vitalité des forums de discussion que l'on croyait délaissés par les internautes.
Plus généralement, cette étude souligne l'incontournable rôle du e-commerce : 96 % des consommateurs déclarent avoir réalisé au moins un achat en ligne dans les douze derniers mois.

Méthodologie : Sondage IFOP pour Reputation VIP. Réalisé sur Internet, du 2 au 3 décembre 2014 auprès d'un échantillon de 1003 personnes, représentatif de la population française âgée de 18 ans et plus. Méthode des quotas (sexe, âge, profession).

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

Source : http://www.archimag.com/vie-numerique/2015/04/24/96-consommateurs-influenc%C3%A9s-e-r%C3%A9putation-marques
Par Bruno Texier

Facebook développe la

reconnaissance faciale… de dos ! | Le Net Expert Informatique

Capture d’écran du film « Mon nom est personne » (1973) (Tonino Valerii)	**Facebook développe la reconnaissance faciale… de dos !**