Pourquoi le Big data va révolutionner les DRH | Le Net Expert Informatique

Pourquoi le Big data va révolutionner les DRH

Le Big data se met au service des ressources humaines. Aujourd'hui, les plates-formes collectent des données sur les candidats partout sur Internet. Une technologie qui va totalement bousculer la gestion de carrières et dynamiter le recrutement. Pour le meilleur, mais aussi pour le pire.

Depuis quelques années, les éditeurs de logiciels de gestion des ressources humaines, notamment ceux qui offrent leur service dans le cloud, s'intéressent au Big data. Certains utilisent des bases de données in-memory, d'autres ont mis en place des technologies type Hadoop afin d'offrir à leurs utilisateurs des capacités avancées d'analyse et de reporting sur les données RH.
Non seulement, ceux-ci peuvent davantage croiser des données entre les formations, les compétences, les salaires, les absences, mais ils peuvent aussi injecter, dans leurs analyses, des données captées sur Internet et sur les réseaux sociaux.
Dans le recrutement, le Big data permet déjà aux entreprises d'aller chercher les meilleurs candidats non plus dans le vivier de CV qui leur sont adressés, mais directement sur les forums et les réseaux sociaux.
Alors, pourquoi s'embêter à lire des CV quand un algorithme peut jouer les chasseurs de tête ou détecter les salariés « à risque » ? Ces méthodes prédictives tout droit venues du marketing débarquent dans les RH. C'est une véritable révolution qui s'apprête à voir le jour dans la profession.

Lire la suite….

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.
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 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 !

Menacé de chantage sur Skype, un lycéen se suicide| Le Net Expert Informatique

Menacé de chantage sur Skype, un lycéen se suicide

Après avoir été menacé par son interlocutrice virtuelle de voir une « vidéo intime » diffusée sur Internet s'il refusait de la payer, un jeune homme s'est donné la mort dans sa chambre.

Mercredi 4 juin, un peu avant 20 heures, à Castelsarrasin (Tarn-et-Garonne), un lycéen de 18 ans – qui s'appellerait Quentin – est attendu à la table familiale pour dîner. En l'absence de réponse à leurs appels, ses parents se rendent dans sa chambre. Et le découvrent dans une mare de sang, un couteau planté en plein coeur.
Quentin est déclaré mort peu après l'arrivée des secours. Les policiers qui leur font suite se concentrent sur son ordinateur portable, resté allumé. Ils y découvrent les causes probables de son suicide grâce à la fenêtre de conversation restée ouverte sur sa messagerie vidéo Skype : un chantage à la webcam.

Une jeune femme le menace de diffuser une vidéo intime
Les enquêteurs remontent le fil de la discussion et constatent que Quentin s'était filmé nu pour son interlocutrice. Celle-ci l'avait ensuite menacé de diffuser cet enregistrement sur internet s'il refusait de payer une certaine somme d'argent sur le champ. Pris de panique, Quentin se serait donné la mort pour éviter un scandale.
Le parquet de Montauban a ouvert une enquête préliminaire.
« La Dépêche du midi », qui avait d'abord évoqué l'hypothèse d'un chagrin d'amour avant de retenir celle du chantage, précise que la mère du lycéen l'aurait découvert avec une « corde au cou ». Mais évoque également, comme RTL, une « mare de sang ».
Le jeune homme, décrit comme un « très bon élève » de terminale au lycée professionnel de Beaumont-de-Lomagne, n'avait jamais parlé de suicide à ses proches. Les centres d'intérêt de son probable profil Facebook tournaient essentiellement autour des mangas.

Un scénario similaire à Brest, en 2012
Ce suicide rappelle un drame similaire survenu à Brest en octobre 2012. Un jeune homme de 18 ans s'était dénudé par webcam, sur Facebook, à la demande d'une jeune femme rencontrée en ligne qui faisait de même. Avant d'interrompre le « jeu » au bout de 10 minutes en le menaçant : « J'ai une vidéo porno de toi, si tu ne me donnes pas 200 euros, je vais détruire ta vie. »
Paniqué à l'idée de voir la vidéo diffusée à ses amis Facebook, le lycéen s'était pendu après avoir laissé un SMS d'adieu à ses parents. L'adresse IP de la femme provenait de Côte d'Ivoire, où des maîtres chanteurs connus sous le nom de « brouteurs » sont devenus des professionnels de ce genre de pratique.

Source : http://tempsreel.nouvelobs.com/faits-divers/20150605.OBS0251/menace-de-chantage-sur-skype-un-lyceen-se-suicide.html
Par Alexis Orsini

Une imprimante 3D pour personnaliser la mousse de votre café latte | Le Net Expert Informatique

Une imprimante 3D pour personnaliser la mousse de votre café latte

Un support de communication inattendu développé par la startup Coffee Ripples.

L'entreprise Coffee Ripples a mis au point une machine qui permet d'écrire le message de votre choix sur la mousse d'un café : The Ripple Maker. Un site et une app mobile permettent d'uploader et adapter le message désiré. Celui-ci est alors imprimé sur la surface de la boisson en poudre de café, combinant ainsi les technologies de l'impression 3D et du jet d'encre. Coffee Ripples mise sur un prix de vente de 999 USD avec un abonnement annuel de 75 USD pour permettre aux commerces d'utiliser pleinement toutes les fonctionnalités et s'attirer le capital sympathie des clients. Retrouvez plus d'information sur le site de de la startup.
Coffee Ripples profite ainsi d'un emplacement peu investi pour communiquer, tout en surfant sur un art de plus en plus populaire. Il suffit pour cela de jeter un œil au hashtag #latteart sur Instragram. Lufthansa a d'ores et déjà signé pour cette technologie dans le but d'imprimer le logo de la compagnie sur les cafés des voyageurs de première classe.

Source : http://lareclame.fr/132138-coffee-ripples-un-cafe-pour-instagram-sans-filtre

Première forte condamnation pénale d’atteinte à la E-réputation | Le Net Expert Informatique

L'excellent site Légalis.net vient de rendre public un jugement du Tribunal correctionnel de Paris en date du 24 novembre 2014, qui a condamné à 2 ans de prison avec sursis, 3 ans de mise à l'épreuve ainsi que 50 000 € de dommages-intérêts à verser aux victimes et 27 000 € pour participation aux frais de justice des plaignants.

Les faits en bref

Il s'agit d'une femme qui n'a pas supporté d'être quittée par son amant. Elle s'est donc déchaînée contre lui, en n'hésitant pas à user de toute la technique d'internet pour usurper son identité et créer à son nom des comptes sur des réseaux sociaux (Facebook, Viadeo, LinkedIn, Twitter), harcelant sa famille, sa nouvelle compagne et même l'employeur de cet homme, ainsi que de nombreux autres agissements tels que du harcèlement téléphonique, montrant pour le moins le manque de stabilité psychologique de l'intéressée.

L'affaire avait été classée par le Procureur de la République sous la condition que la personne se tienne tranquille, ce qu'elle a été incapable de faire et elle a continué ses agissements nuisibles, d'où les poursuites et cette lourde condamnation.

Quant la méchanceté rejoint la lâcheté

Ce cas d'espèce n'est pas aussi particulier ni exceptionnel qu'on pourrait le penser. Même si les faits ne sont pas toujours portés devant la justice et médiatisés, notre expérience de nettoyeurs de net nous apporte de nombreux cas de réel acharnement de personnes qui ont le goût de nuire ou la haine suffisants pour chercher à détruire des personnes, par exemple à démolir la vie de la femme qui a osé demander le divorce contre eux, ou encore qui se sont juré qu'ils auraient la peau d'un dirigeant d'entreprise en proférant les plus graves accusations non fondées et qui continuent à le faire, sur des sites hébergés à l'étranger, alors même qu'ils sont déjà lourdement condamnés pour diffamation en correctionnelle puis en appel.

La technique du pseudonyme – ou ici celle de l'usurpation d'identité – donne très souvent aux personnes malfaisantes l'impression grisante de puissance et d'impunité (voir notre actualité du 26 février 2010 : Sur le Web 2.0 c'est carnaval tous les jours). Ce qui permet ainsi de nuire en toute impunité et en toute lâcheté…

Il y a encore la possibilité de publier sur des sites hors d'atteinte du droit français, ce qui rend les choses encore plus compliquées et plus longues à neutraliser. Mais il faut savoir qu'une telle neutralisation, même si elle est plus longue, est rarement impossible.

Dans le cas de la jurisprudence que nous évoquons, on a eu affaire à une personne suffisamment instable et incontrôlable pour qu'elle laisse des traces et qu'on remonte très vite à son identité. Mais les cas sont hélas fréquents où il est impossible d'identifier rapidement l'auteur de telles manœuvres de démolition. Il faut alors saisir la justice, avec tous les délais et les frais que cela suppose pour que, au cours de l'enquête, le juge ordonne des mesures pour remonter jusqu'à l'auteur des faits, notamment par voie d'injonction aux hébergeurs ou aux opérateurs de réseaux.

Une décision de justice exemplaire

Malgré ces réserves, il faut saluer cette décision de justice comme exemplaire au sens fort du terme : elle doit servir d'exemple pour toute personne qui serait tentée de nuire avec autant d'acharnement contre des personnes.

L'affaire reste à suivre car le jugement a été frappé d'appel : on aura donc sans doute prochainement des nouvelles de ce cas et la confirmation ou l'infirmation de la sentence par la Cour d'appel de Paris.

Le jugement : http://www.legalis.net/spip.php?page=breves-article&id_article=4672
La décision de justice intégrale : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4671

Source : http://www.les-infostrateges.com/actu/15072025/e-reputation-premiere-forte-condamnation-penale-assortie-de-dommages-interets

Une loi pour vous espionner… | Le Net Expert Informatique

Une loi pour vous espionner…

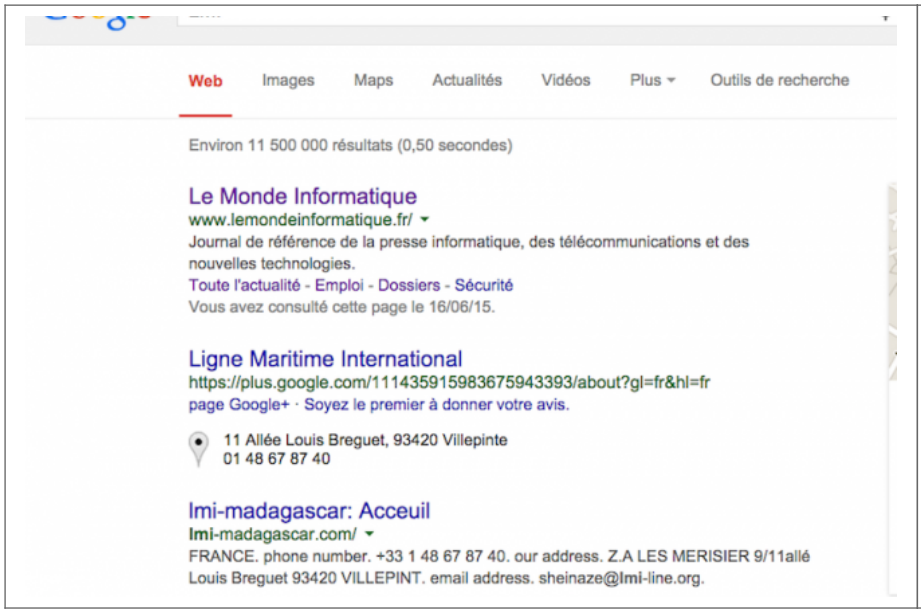
Alors que les révélations sur les activités de la NSA en France se multiplient et que le terrorisme frappe à nouveau, le gouvernement vient de faire voter une loi sur le renseignement qui autorise de nouvelles techniques d'espionnage très intrusives. Enquête sur ces nouveaux dispositifs controversés.

«Inacceptables.» C'est en ces termes attendus que l'Elysée a qualifié les écoutes de l'agence américaine NSA sur la France, révélées à partir du 24 juin par l'organisation WikiLeaks et les journaux Mediapart et Libération. L'ensemble de la classe politique a réagi à l'unisson aux premières publications de documents concernant les interceptions par la NSA, entre 2006 et 2012, des conversations des trois présidents successifs Jacques Chirac, Nicolas Sarkozy et François Hollande, ainsi que des cas d'espionnage économique. «Ces pratiques portent atteinte à la confiance entre alliés», a fustigé le …
Lire la suite….

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

Source : http://www.lefigaro.fr/actualite-france/2015/07/03/01016-20150703ARTFIG00179-loi-renseignement-comment-vous-allez-etre-espionnes.php

Les pratiques de Google dénoncées par 2 universitaires | Le Net Expert Informatique



Les pratiques de Google dénoncées par 2 universitaires

Selon une étude réalisée par deux universitaires, Google porte préjudice aux consommateurs en favorisant ses propres services.

Un rapport publié par deux universitaires américains met en cause les méthodes de Google. Ils pointent notamment une pratique du moteur de recherche qui consiste à inclure avec des résultats de recherche généraux des liens redirigeant vers ses propres services.
Selon l'étude parrainée par Yelp, lui-même plaignant dans le procès antitrust que l'UE a intenté au moteur de recherche, ce favoritisme vis à vis de ses propres services ne nuisent pas seulement aux concurrents, il nuit également aux consommateurs. L'étude révèle ainsi que les utilisateurs ont 45 % de chance de plus de cliquer sur les résultats de recherche organiques générés par le moteur de recherche de Google que sur des résultats mettant en avant les propres services de la firme de Mountain View, comme c'est le cas actuellement. « On peut estimer qu'en tirant parti de sa position dominante dans la recherche afin de promouvoir ses propres contenus, Google réduit le bien-être social, parce qu'il réserve aux consommateurs des résultats de qualité inférieure et les moins bonnes occurrences », ont constaté les chercheurs. L'étude « apporte la preuve empirique » que la place accordée dans certains cas par Google à ses propres produits porte préjudice aux utilisateurs. « On ne peut donc pas dire qu'un tel comportement soit favorable à la concurrence », ont déclaré Tim Wu, professeur à la Columbia Law Schéol, et Michael de Luca, professeur assistant à la Harvard Business Schéol.

Une enquête de l'UE sur les pratiques de Google
Leur étude a été en partie financée par Yelp, un site qui permet aux utilisateurs de noter les entreprises locales qui est par ailleurs l'un des plaignants à l'origine de l'enquête antitrust menée justement par la Commission européenne sur les pratiques de recherche de Google. Des données fournies par l'équipe scientifique de Yelp ont également été utilisées dans cette enquête. Tous ces résultats ont été présentés par Yelp lors de l'Antitrust Renforcement Symposium organisé le week-end dernier à l'Université d'Oxford, comme l'a indiqué une porte-parole de l'université britannique. Le rapport a également été envoyé vendredi à la Commission européenne, laquelle a refusé d'en commenter les conclusions. Pour fonder leurs résultats, les chercheurs se sont basés sur des enquêtes par clic réalisées auprès de 2690 internautes invités à participer à des tests comparatifs sur la présentation des résultats de recherche. Les chercheurs ont ainsi présenté deux séries de résultats de recherche sur des requêtes concernant des entreprises locales. Selon l'étude, en volume, ces requêtes représentent environ un tiers des recherches réalisés à partir d'ordinateurs desktop et plus de la moitié des requêtes effectuées à partir de terminaux mobiles.
Actuellement, en ce qui concerne les résultats relatifs aux entreprises locales, « Google affiche généralement sept encarts commerciaux listant les résultats des services de recherche spécialisés de Google comme Google+ Local répartis en fonction de leur localisation », ont expliqué les chercheurs. Or Google qualifie ce panachage de résultats provenant de ses propres moteurs de recherche spécialisés dans les résultats de recherche généraux de « recherche universelle ». Dans la version alternative mise en place par les chercheurs, ceux-ci ont utilisé un plug-in permettant d'afficher dans le navigateur une carte et une liste de résultats de recherche basées sur le propre algorithme organique de Google, y compris des liens de sites tiers répertoriant des avis comme Yelp et TripAdvisor.

Tout n'est pas négatif
L'objectif du test était de montrer quel protocole de recherche délivrait l'information la plus pertinente pour le contenu concerné. Il a révélé que 32 % des utilisateurs cliquaient sur les résultats locaux tels que Google les affichaient actuellement tandis que 47 % cliquaient sur les résultats de la recherche alternative. « Cet écart de près de 50 % dans le nombre de clics représente un écart très important dans l'industrie du Web moderne », ont déclaré les chercheurs. « Il semble que la stratégie de Google consiste à déployer sa recherche universelle d'une manière qui dégrade le produit de façon à ralentir et à exclure les concurrents de son paradigme de recherche dominant », ont encore expliqué les chercheurs.

Cependant, tout n'est pas aussi négatif. Ainsi, les chercheurs ont estimé que « dans certains cas, comme l'affichage de l'heure ou celui d'une calculatrice, le favoritisme exercé par Google vis à vis de ses propres services ne porte pas préjudice aux consommateurs », ajoutant que l'affichage d'une calculatrice en haut d'une page de résultats de recherche est préféré par les utilisateurs. Google n'a pas immédiatement répondu à une demande de commentaire. La firme de Mountain View a toujours nié que ses pratiques violaient les règles européennes de la concurrence. C'est en 2010 que, suite aux plaintes formulées par ses concurrents, la Commission a ouvert une enquête antitrust sur les pratiques de recherche de Google. Et en avril le moteur de recherche a été formellement accusé d'avoir abusé de sa position dominante sur le marché de la recherche. La Commission a déclaré que « Google violait les règles européennes de la concurrence en favorisant systématiquement ses propres comparatifs de prix sur des produits par rapport à des services concurrents, au détriment des consommateurs et des services concurrents ». Une version expurgée des charges a été envoyée aux opposants de Google plus tôt ce mois-ci : ils avaient quatre semaines pour répondre. Et Google autant de temps pour répondre aux accusations de la Commission.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-les-pratiques-de-google-denoncees-par-2-universitaires-61631.html
Par Jean Elyan avec IDG NS

Reconnaissance faciale, une menace pour la vie privée ? | Le Net Expert Informatique

Reconnaissance faciale, une menace pour la vie privée ?

Pour le «Washington Post», les nombreuses applications capables de reconnaître les visages créent des bases de données biométriques dangereuses pour la «confidentialité numérique».

«L'anonymat en public pourrait être une chose du passé.» Dans le Washington Post du 11 juin, Ben Sobel, chercheur au Centre sur la vie privée et la technologie de l'école de droit de Georgetown, consacre un article au risque qui pèse sur notre «confidentialité biométrique». Selon lui, les technologies de reconnaissance faciale se développent à la vitesse grand V sous l'impulsion du marketing individualisé. Et pas toujours de manière très légale…

Aux Etats-Unis, Facebook fait l'objet d'un nouveau procès en action collective, concernant la violation du droit à la protection des données personnelles de ses utilisateurs. En cause, le réseau social serait en train de créer «la plus grande base de données biométriques privées au monde» sans demander assez explicitement le consentement de ses utilisateurs comme l'explique le site Sophos. Le gouvernement américain et le département du Commerce auraient déjà invité des associations de défense de la vie privée ainsi que des représentants des grandes entreprises de ce secteur comme Google et Facebook pour essayer de réglementer l'usage de ces technologies.
Mais pour le moment, seul l'Illinois (2008) et le Texas (dès 2001) ont des lois interdisant l'utilisation de cet outil sans le «consentement éclairé» des utilisateurs, explique Ben Sobel. Selon lui, l'issue de ce procès, qui devra déterminer si Facebook a enfreint la «Biometric Information Privacy Act» (BIPA) de l'Illinois, déterminera l'avenir des applications de reconnaissance faciale sur le marché. Il encourage ainsi les Etats-Unis à adopter une loi fédérale pour garantir la «confidentialité biométrique» des Américains.

LE BOOM DES APPLICATIONS DE RECONNAISSANCE FACIALE
FaceNet (Google), Name Tag (FacialNetwork) ou encore Moments (Facebook). Toutes ces applications utilisent des algorithmes de reconnaissance faciale. Et pour les imposer sur le marché, les entreprises sont prêtes à tout pour mettre leur adversaire échec et mat.
FaceNet, la technologie développée par le géant Google, possède une précision de 99,63 % selon Ben Sobel. Elle est actuellement utilisée par Google Photos dans ses versions non européennes. Dans la même lignée, Name Tag, développé par FacialNetwork, ambitionne de fonctionner sur les Google Glass. Cette application permettrait de rassembler tous les profils sur les réseaux sociaux disponibles sur Internet (Twitter, Instagram, Google+ et sites de rencontres américains) selon un article du Huffington Post. Une application qui pourrait permettre d'avoir le profil social de quelqu'un en temps réel.
Parmi les fonctionnalités envisagées, il y aurait par exemple celle de révéler la présence de quelqu'un dans les bases de données criminelles. Pour le moment, Google a refusé que NameTag soit disponible sur ses Google Glass, pour des questions de problèmes de respect de la vie privée… Mais il n'est pas le seul à s'engouffrer dans ce marché.
Depuis 2011, Facebook utilise un système de suggestion de tags (identifications) sur les photos. Bien qu'interdit en Europe, Deepface, l'algorithme expérimental du réseau social, serait capable de reconnaître les gens à leur posture corporelle. De fait, son algorithme utilise ce que l'on appelle des «poselets». Inventés par Lubomir Bourdev, ancien chercheur de Berkeley œuvrant désormais chez Facebook IA Research. Ceux-ci repèrent les caractéristiques de nos visages et trouvent ce qui nous distingue de quelqu'un d'autre dans une pose similaire, explique un article de Numérama (http://www.numerama.com/magazine/33026-meme-de-dos-facebook-sait-vous-reconnaitre-sur-les-photos.html). Mais Facebook ne s'arrête pas là. En juin, le réseau social a présenté Moments, une application permettant de partager de manière privée des photos avec des amis utilisant elle aussi une technologie de reconnaissance faciale. D'ores et déjà disponible gratuitement aux Etats-Unis, elle permet à un utilisateur d'échanger avec ses amis des photos où ils figurent de manière synchronisée. Une vidéo en explique les rouages :

Moments ne devrait pas s'exporter en Europe de sitôt, puisque l'UE exige la mise en place d'un mécanisme d'autorisation préalable qui n'est pas présent sur la version américaine. Et ce, bien que les utilisateurs puissent désactiver les suggestions d'identification sur les photos, via les paramètres de leur compte.

L'INQUIÉTUDE AUTOUR DU SUCCÈS DE CES TECHNOLOGIES
En 2012, une recommandation formulée par le G29, qui réunit les commissions vie privée de 29 pays européens, mettait déjà en garde contre les dangers de la reconnaissance des visages sur les médias sociaux. Notamment concernant les garanties de protection des données personnelles, tout particulièrement les données biométriques. Pour le moment relativement bien protégés par la législation européenne, nous ne sommes pas pour autant épargnés par ces outils.

Tous les jours, 350 millions de photos sont téléchargées sur Facebook, selon Ben Sodel. Or, le public semble majoritairement insouciant face à la diffusion de son identité (nom, image…), souligne InternetActu. A l'exemple de l'application How Old mise en ligne fin avril, qui se targue de deviner votre âge grâce à une photo. Corom Thompson et Santosh Balasubramanian, les ingénieurs de Microsoft à l'origine du projet, ont été surpris de constater que «plus de la moitié des photos analysées» par leur application n'étaient pas des clichés prétextes mais de vraies photos, rapporte le Monde.

Mais le succès (bien qu'éphémère) de cette application démontre bien que le public n'est pas vigilant face à la généralisation de la reconnaissance faciale. Un peu comme avec la diffusion des données personnelles au début de Facebook. Il ne s'agit pas tant du problème de stocker des photos d'individus que de mémoriser l'empreinte de leur visage. Entre de mauvaises mains, ces bases de données pourraient mettre à mal notre «confidentialité biométrique».

Source : http://ecrans.liberation.fr/ecrans/2015/06/26/reconnaissance-faciale-une-menace-pour-la-vie-privee_1337015
Par Camille PETTINEO

Les techniques du renseignement français se dévoilent un peu plus | Le

Net Expert Informatique

	**Les techniques du renseignement français se dévoilent un peu plus**

Le Nouvel Obs a publié dans ses colonnes une longue enquête faisant le point sur les écoutes et techniques mises en place par le renseignement français. Un rapide aperçu des capacités de la France en la matière.

Et le premier constat que l'on peut tirer, c'est que la France s'est évertuée à rattraper son retard sur les américains dès 2008. Comme le rapporte l'Obs, c'est en effet à cette date qu'a été lancée la première phase d'un plan initié par Nicolas Sarkozy afin de remettre en adéquation les méthodes et équipement des services de renseignement français, dont l'essentiel des ressources s'était concentré dans les années 80 et 90 sur l'interception des communications satellites.

Des satellites aux câbles

Plus intéressants que les communications satellites en effet, les câbles sous-marins sont devenus au cours de la première décennie des années 2000 l'axe privilégié de transit d'informations. Et comme le remarquaient certains observateurs, la France est particulièrement bien située à cet égard, disposant à la fois de nombreux câbles en direction de l'Afrique du Nord, ainsi qu'à travers le pacifique ou la méditerranée. Et dispose en plus de cela d'un acteur majeur du marché, Alcatel, qui selon l'Obs a participé à la mise en place de cette surveillance du réseau en formant les services du renseignement aux techniques de manipulation de la fibre.

Orange serait aussi venu prêter main-forte, l'opérateur gère en effet l'accès aux points d'arrivée de ces câbles sous-marins en France, qui en dénombre une douzaine. La technique utilisée n'a rien de révolutionnaire : il s'agit de l'extension numérique de la technique des « bretelles » : une ligne dédoublée, dont l'une des extrémités part directement vers un local de la DGSE.

L'Obs détaille le régime auquel ces écoutes étaient soumises : la commission nationale de Contrôles des Interceptions de Sécurité avait ainsi son mot à dire, et des règles étaient posées afin d'éviter les abus, notamment à l'égard des citoyens français. Mais face aux réalités et à l'ampleur du phénomène, la CNCIS se contentait de donner un avis par pays pour autoriser ou non les écoutes, simplifiant l'acheminement des données vers un datacenter dédié au traitement situé à Paris, boulevard Mortier. L'organe de contrôle, aujourd'hui remplacé par la CNCTR dans le cadre de la loi renseignement, pouvait aussi décider de limiter les écoutes à un thème précis.

Des écoutes encadrées ?

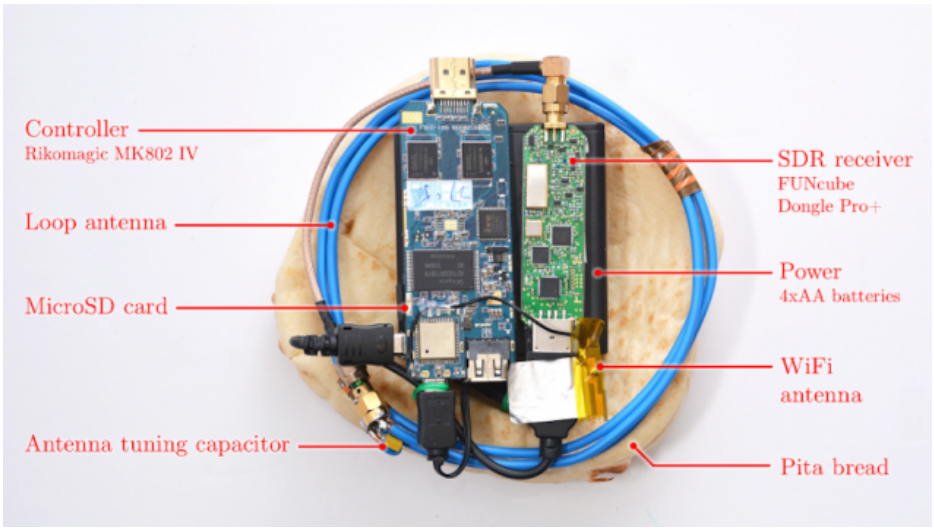
L'hebdomadaire rapporte que les écoutes se focalisaient sur certains pays, tels que les États-Unis ou le Moyen-Orient, et en délaissaient d'autres, comme le Japon. Le magazine souligne également le fait que ces écoutes n'ont pas été simplement employées dans le cadre de la lutte antiterroriste, mais aussi pour la promotion économique du pays. Une révélation qui peut faire sourire, alors que Wikileaks a révélé en début de semaine les indiscrétions de la NSA sur ces questions. On se demande même si ces révélations ne tombent pas à pic…

L'Obs donne les contours d'un vaste plan engagé par le renseignement français : en l'espace de 5 ans, à compter de 2008, 700 millions d'euros ont été débloqués dans le cadre ce plan et 600 embauches parmi les services. Et d'expliquer que François Hollande, lors de son arrivée au pouvoir en 2012, n'a pas remis en question cet effort et travaille au contraire à approfondir les premiers accords noués sous Sarkozy avec le GCHQ britannique, avec qui la France a établi en 2010 un traité militaire comprenant un discret volet sur l'échange d'informations dans le domaine du renseignement.

Une structure d'ampleur, que la loi renseignement, actuellement examinée par le Conseil constitutionnel, ne vient absolument pas remettre en cause.

Source : http://www.zdnet.fr/actualites/les-techniques-du-renseignement-francais-se-devoilent-un-peu-plus-39821892.htm
Par Louis Adam

Pour pirater un ordinateur, une pita suffit | Le Net Expert Informatique

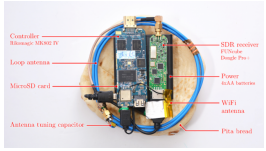


Pour pirater un ordinateur, une pita suffit

Selon une étude de l'université de Tel-Aviv, travailler dans un café pourrait s'avérer risqué pour la sécurité de votre ordinateur

Cette pita, qui donne l'apparence innocente que quelqu'un mange ostensiblement en face de vous dans le café de votre quartier, pourrait contenir un système d'espionnage informatique pouvant infiltrer les protocoles d'encodage les plus sécurisés de votre ordinateur.

Pire encore, ont déclaré les chercheurs de l'Université de Tel-Aviv, les utilisateurs de cet ordinateur ne peuvent pas faire grand chose pour se protéger.
« Des techniques d'atténuation… pourraient inclure des cages Faraday », des écrans en métal spécialement posés au sol qui bloquent les radiations… « Pourtant, la protection peu chère de PC de niveau commercial semble difficile », explique l'équipe.
Dans un article publié mardi, les chercheurs décrivent le très faible coût de l'équipement de type Radio Shack, que l'on peut facilement cacher dans un pain pita standard et qui peut être utilisé pour « lire » des impulsions électromagnétiques provenant du clavier d'un ordinateur standard, y compris les frappes sur le clavier afin de décrypter les documents sécurisés.
De manière amusante, l'Université de Tel-Aviv a appelé l'attaque PITA, Instrument portable pour l'acquisition de signaux.



L'étude, menée par les chercheurs Daniel Genkin, Itamar Pipman, Lev Pachmanov et Eran Tromer a été publiée pour coïncider avec une conférence majeure de sécurité informatique qui va avoir lieu à l'Université de Tel-Aviv (UTA) cette semaine.
« Nous avons pris avec succès des codes d'ordinateurs de divers modèles fonctionnant avec GnuPG (une source populaire d'encodage, en utilisant le standard d'encodage OpenPGP) en quelques secondes », a écrit l'équipe de l'UTA dans l'article, intitulé « Voler des codes de PC en utilisant une radio : des attaques électromagnétiques à moindre coût sur une exponentiation de fenêtres ».
En plus d'OpenPGP, l'équipe a été capable de dupliquer avec réussite les attaques sur d'autres systèmes d'encodages, très sécurisés, y compris RSA et ElGamal.
« L'attaque envoie quelques textes informatiques bien conçus et lorsque ces textes sont décryptés par la cible, ils entraînent l'occurrence de valeurs spécialement structurées dans le logiciel d'encodage », ont déclaré les chercheurs.
En utilisant un appareil qui peut recevoir des signaux radio, une simple radio ou une clé USB pouvant recevoir des émissions et les lire sur l'ordinateur, les chercheurs ont été capables d'observer les fluctuations dans le champ électromagnétique entourant l'ordinateur et de traduire ces fluctuations en frappes de clavier en utilisant un programme d'analyse.
L'article fournit des détails complets sur l'équipement nécessaire (tout est disponible et peu cher dans un magasin local d'électronique ou sur Internet), et sur la façon d'assembler et de connecter les parties, et même de les plier dans un pain pita.

L'équipement détecte les fluctuations dans le champ électromagnétique émis par le matériel informatique (clavier et processeur) lorsque l'ordinateur essaie de décrypter les signaux (les modules d'encodage contiennent des composants qui peuvent être exploités pour fonctionner automatiquement lorsque le texte encodé est rencontré).

En envoyant ces textes pièges, les pirates peuvent voler les codes d'authentification sur l'ordinateur de l'utilisateur, leur autorisant un accès libre aux documents et aux données encodés.

Une attaque PITA pourrait probablement être utilisée par des pirates en cas d'une attaque qui « balaie » des données et les documents d'un ordinateur.

Si ces données sont encodées, il est peu probable que les pirates pourront les lire (en fonction de niveau de complexité du codage), mais avec des clés d'encodage, les pirates pourraient trouver des informations encodées comme des numéros de cartes de crédit ou des mots de passe.

La seule mise en garde est que la pita « espion » a besoin de se trouver à 50 centimètres de la cible.

Mais d'après l'équipe, la totalité de l'opération peut être réalisée en quelques secondes, rendant l'attaque parfaite pour les pirates dans les cafés où de nombreux utilisateurs d'ordinateurs profitent des installations électroniques, du wifi et de boissons pour travailler.

Un pirate pourrait obtenir les codes dans une attaque « en marchant », attaque menée en transportant une « pita empoisonnée » sur un plateau avec de la vraie nourriture. L'étude notait pourtant que la « qualité du signal variait fortement en fonction du modèle de l'ordinateur cible et de la position de logiciel espion ».

L'équipe de UTA n'est pas la première à penser à utiliser des impulsions électromagnétiques pour pirater des systèmes.

En 2014, des chercheurs de l'Université Ben Gourion (UBG) ont pu utiliser un programme pirate sur un téléphone portable pour collecter des radiations électromagnétiques provenant de claviers, de moniteurs et d'autres équipements pour lire des informations importantes.

L'équipe de l'UBG a démontré comment les données collectées par le programme espion, auparavant placé sur un ordinateur (à travers une attaque de phising ou une autre méthode), pouvaient être captées par un téléphone portable qui créait un réseau local en utilisant des impulsions émanant de matériel informatique.

Les informations du système cible pouvaient être captées, même s'il n'est pas connecté à internet ou à un réseau local (Ethernet).

Le pire, a déclaré l'équipe, est qu'il n'y a pas grand chose que les utilisateurs d'ordinateur puissent faire pour éviter ces attaques, si ce n'est éviter les cafés et garder leur ordinateurs loin des pitot.

Malheureusement, l'équipe a déclaré « qu'empêcher la fuite à un bas niveau de prévention est presque impossible » parce que mettre en place des mesures efficaces (comme des cages Faraday) serait très gênant à cause du matériel informatique excessif ou ralentirait la capacité au point que les utilisateurs seraient incapables d'accomplir le moindre travail.

« Même lorsqu'un programme cryptographique est sûr mathématiquement, ses mises en place peuvent être vulnérables à des attaques de réseaux secondaires qui exploitent des émanations physiques », a déclaré l'équipe. Le pirate « peut facilement viser les ordinateurs ».

« Nous avons testé de nombreux ordinateurs de modèles variés », et lorsqu'il s'agit d'une attaque PITA, chaque utilisateur d'ordinateur devrait se sentir concerné.

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

Source : http://fr.timesofisrael.com/pour-pirater-un-ordinateur-une-pita-suffit/
Par David Shamah

L'Afrique a besoin de cybersécurité| Le Net Expert Informatique

L'Afrique a besoin de cybersécurité

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.
Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.
Le Security Day, qui se tiendra les 15 et 16 mars 2016 à Dakar, sera l'occasion d'aborder l'ensemble de ces sujets.

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.
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 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 : Newsletter n°3 FIC
https://www.forum-fic.com/site/FR/Newsletter/S_inscrire_a_la_newsletter,C58881,I58949.htm