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

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

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 ?

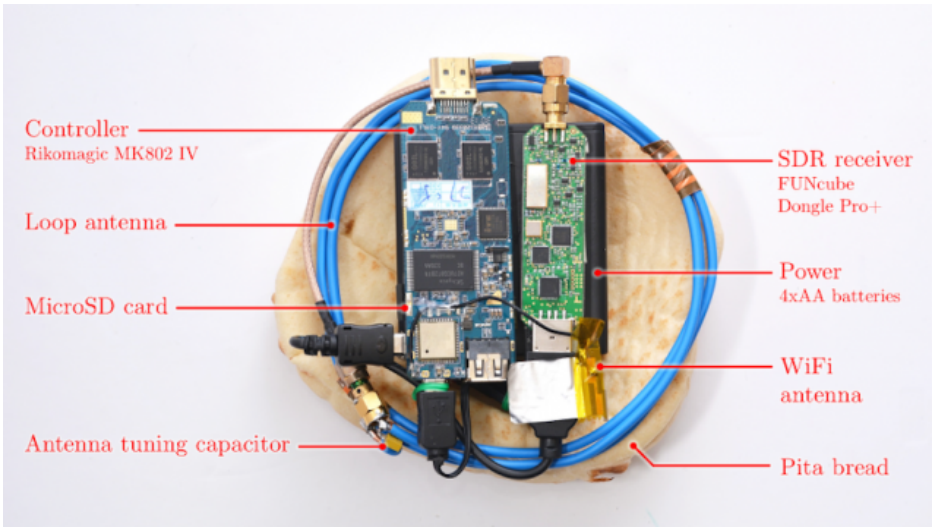
L'hebdomadaire rapporte que les écoutes se focalisaient sur certains pays, tels que les États-Unis ou le Moyen-Orient, et en délaissaient d'autres, comme le Japon. Le magazine souligne également le fait que ces écoutes n'ont pas été simplement employées dans le cadre de la lutte antiterroriste, mais 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

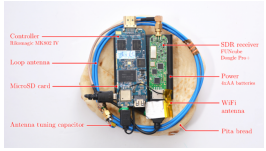


Pour pirater un ordinateur, une pita suffit

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

La Cnil interdit la géolocalisation du salarié en dehors du temps de travail | Le Net Expert Informatique

La Cnil interdit la géolocalisation du salarié en dehors du temps de travail

Par une délibération du 4 juin 2015, la Cnil a décidé de renforcer l'encadrement du recours au dispositif de géolocalisation.

La Commission nationale de l'informatique et des libertés (Cnil) constate le développement de dispositifs dits de géolocalisation permettant aux organismes privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules mis à leur disposition pour l'accomplissement de leur mission. Ainsi, l'employeur peut contrôler le respect des règles d'utilisation d'un véhicule par ses employés grâce à la géolocalisation.
Ce dispositif permet de collecter des données à caractère personnel et sont donc soumis aux dispositions de la loi du 6 janvier 1978.
Par délibération n° 2015-165 du 4 juin 2015, la Cnil a considéré qu'il était nécessaire de compléter la norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé.
Dans cette délibération, la Cnil précise que le recours au dispositif peut servir à justifier la réalisation d'une prestation auprès d'un client ou d'un donneur d'ordre, ou bien à lutter contre le vol du véhicule.
En outre, la Cnil interdit formellement aux employeurs de collecter des données de localisation en dehors du temps de travail du salarié, à savoir lors de ses temps de pause et du trajet entre son domicile et le lieu de travail.
La faculté de désactiver la fonction de géolocalisation doit être laissée à l'employé. Toutefois, la Cnil souligne que des explications pourront être demandées au salarié lorsque les désactivations sont trop longues ou trop fréquentes.
Enfin, les employeurs publics et privés devront se conformer au nouveau dispositif avant le 17 juin 2016.

Source : http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/206288-la-cnil-interdit-la-geolocalisation-du-salarie-en-dehors-du-temps-de-travail.html

---

Comment la France écoute (aussi) le monde | Le Net Expert Informatique

Comment la France écoute (aussi) le monde

Révélations sur un vaste plan de la DGSE pour intercepter les communications internationales passant par les câbles sous-marins : lancé en secret par Nicolas Sarkozy, il vient d'être légalisé par François Hollande en toute discrétion.

Il n'y a pas que la NSA. La France aussi écoute le monde. Après une enquête de plusieurs semaines, « l'Obs » révèle que :
– Début 2008, Nicolas Sarkozy a autorisé la DGSE à espionner les communications internationales transitant par les câbles sous-marins qui relient l'Europe au reste du monde. Un plan de 700 millions d'euros sur cinq ans (2008-2013) a été lancé par le service secret pour installer des stations d'interceptions à l'arrivée des câbles en France (notamment à Marseille, Penmarch et Saint-Valéry-en-Caux).
– Au moins cinq câbles majeurs ont été mis sur écoute pendant cette période avec l'aide de l'opérateur Orange et du groupe Alcatel-Lucent dont le TAT14 vers les Etats-Unis ; le I-Me We vers l'Inde ; le Sea-Me-We 4 vers l'Asie du Sud-est ; et le ACE vers l'Afrique de l'Ouest.
– La DGSE a passé un grand accord de coopération avec le GCHQ britannique. C'est une annexe secrète au traité de défense dit de Lancaster House, signé le 2 novembre 2010 par Nicolas Sarkozy et David Cameron.
– François Hollande a autorisé la DGSE à étendre ces opérations à d'autres câbles dans un nouveau plan quinquennal (2014-2019). L'article L-854-1 de la toute nouvelle loi sur le renseignement vise à les légaliser en catimini.
C'est un plan classé « très secret », exposé ici pour la première fois. Un projet de la Direction générale de la sécurité extérieure (DGSE) autorisé par Nicolas Sarkozy il y a sept ans et poursuivi sous François Hollande, qui explique leur surprenante modération après la révélation de leur mise sur écoute par la NSA. Une vaste entreprise française d'espionnage que la loi sur le renseignement, adoptée le 24 juin, vient de légaliser en catimini.
Cette histoire de l'ombre, « L'Obs » a pu la reconstituer grâce aux témoignages anonymes de plusieurs responsables actuels et passés. Il y est question de stations clandestines installées par la DGSE sur les côtes françaises pour « écouter » les câbles sous-marins, de la complicité de grandes entreprises hexagonales, des accords secrets entre le service français et ses homologues anglo-saxons et de l'indigence du contrôle parlementaire…

La France à la traîne
L'affaire commence début janvier 2008, dans le bureau du chef de l'Etat, à l'Elysée. Nicolas Sarkozy a réuni le Premier ministre, François Fillon, le patron de la DGSE, Pierre Brochand, et quelques collaborateurs. Au menu : l'avenir des services spéciaux français. Leur problème ? Ils sont devenus (presque) sourds. Ils ont de plus en plus de mal à écouter les communications mondiales…
Lire la suite….

S o u r c e : http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html?cm_mmc=EMV-_-NO-_-20150701_NLNOACTU08H-_-exclusif-comment-la-france-ecoute-aussi-le-monde#xtor=EPR-1-Actu8h-20150701

WHOIS : vos informations personnelles bientôt publiques ? | Le Net Expert Informatique

WHOIS : vos informations personnelles bientôt publiques ?

L'ICANN pourrait bientôt modifier le système du WHOIS. Le régulateur propose notamment d'interdire aux propriétaires de sites « à but commercial » de s'enregistrer via proxy, soit de façon anonyme. Le texte ne laisse pas les associations insensibles, qui y voient une menace pour ceux qui s'expriment librement sur leurs sites.

WHOIS est souvent décrit comme l'annuaire d'Internet. Lors de l'enregistrement d'un nom de domaine, un internaute doit renseigner diverses informations personnelles, de son état civil à son numéro de téléphone en passant par son adresse de domicile. Ces informations alimentent les bases de données des registres de noms de domaine, et sont consultables via l'outil WHOIS.
Pour des questions évidentes de protection de la vie privée et de confidentialité, les données fournies par le propriétaire d'un nom de domaine ne sont pas accessibles au public. Les registres de renseignement proposent fréquemment en option la possibilité de s'enregistrer via proxy. Les seules tierces personnes alors en mesure d'accéder aux bases de données non anonymisées sont celles détenant une autorisation légale, tel qu'un mandat judiciaire.
Mais cette situation connaîtrait ses derniers jours. L'ICANN prévoit en effet de modifier le système en profondeur. Le régulateur étudie actuellement un projet, lequel envisage notamment que les noms de domaine « utilisés dans un but commercial soient inéligibles à l'enregistrement proxy/privacy ». En d'autres termes, les propriétaires de sites contenant un quelconque élément transactionnel ne pourront plus s'enregistrer de façon anonyme : leurs informations personnelles devront être publiques.

L'anonymat, garant de la liberté d'expression
Alors que l'ICANN doit se prononcer le 7 juillet sur ce texte, l'Electronic Frontier Foundation appelle les internautes à s'y opposer. Selon l'EFF, le terme « but commercial » englobe un grand nombre de sites, et la vie privée de leurs propriétaires, des personnes physiques, seraient menacée. L'association prend pour exemple TG Storytime, un site destiné aux auteurs transgenres et hébergés par Joe Six-Pack, lui-même transgenre. Si l'ICANN devait modifier la régulation en vigueur, ses adresses, numéros de téléphone et mails seraient alors exposées à la vue de tous, trolls et harceleurs compris.
Le changement a été impulsé par les géants américains du divertissement, signale l'EFF, ce que l'ICANN ne cache pas. En effet, à de nombreuses reprises, le régulateur d'Internet écrit que cette proposition vise à faciliter le signalement de sites violant le droit d'auteur (ou toute autre propriété intellectuelle). Pour l'EFF, « ces entreprises veulent de nouveaux outils pour découvrir l'identité des propriétaires de sites Web qu'ils veulent accuser de violation de droit d'auteur et contrefaçon de marque, de préférence sans une ordonnance du tribunal ».
« L'avantage limité de cette évolution est manifestement compensé par les risques supplémentaires pour les propriétaires de sites, qui vont souffrir d'un risque plus élevé de harcèlement, d'intimidation et de vol d'identité ».
Il est vrai que, malgré les gardes fous prévus par l'ICANN, la plupart des informations fournies pour l'enregistrement d'un nom de domaine sont sensibles, tant IRL (In Real Life) que dans le monde virtuel. En appelant à s'opposer au texte, l'association entend faire réagir sur un recul de l'anonymat, qui affectera ceux qui portent des opinions impopulaires ou marginales mais aussi les lanceurs d'alerte et tous ceux susceptibles de dénoncer « la criminalité et la corruption ».

Source : http://www.linformaticien.com/actualites/id/37199/whois-vos-informations-personnelles-bientot-publiques.aspx
Par Guillaume Périssat

L’anonymat du WHOIS remis en question à l’ICANN | Le Net Expert Informatique

	L’anonymat du WHOIS remis en question à l’ICANN

Une proposition de l'ICANN s'est attiré les foudres des commentateurs et de l'EFF. La suggestion propose de rendre impossible l'anonymisation des données personnelles sur le service WHOIS pour les sites à vocation commerciale.

Le service WHOIS est un outil particulièrement utile pour savoir qui se cache derrière un nom de domaine et comment contacter les responsables d'un site. Fourni par les registres de noms de domaines, il permet d'interroger les bases de données des bureaux d'enregistrement afin de connaître le nom et l'identité de la personne ou de la société détenant le nom de domaine, ainsi que certaines informations de contacts.
Ces informations ne sont pas forcement accessibles à tout le monde : dans de nombreux cas et pour éviter de voir ces informations personnelles à l'air libre, les bureaux d'enregistrement proposent un service d'enregistrement via proxy permettant de dissimuler au public les données et de les réserver aux seules personnes munies d'autorisations légales fournies par un service judiciaire national. Le service agit donc comme un écran afin d'offrir un moyen de contacter le propriétaire du nom de domaine tout en protégeant ses données personnelles.
Mais une proposition de l'ICANN, ouverte depuis mardi aux commentaires publics, envisage de revenir sur le fonctionnement de ce système en ouvrant à tous les données WHOIS des sites à but commercial. Selon l'EFF, cette règle s'appliquant « à tous les sites commerciaux » pourrait toucher de nombreux petits administrateurs de sites et de communautés en ligne qui ont choisi de mettre en place de la publicité ou un système de dons pour subvenir au coût de leur site.
L'EFF cite ainsi l'exemple de TG Storytime, un paisible site de fanfiction à destination des communautés LGBT, qui pourrait ainsi se voir obligé de révéler certaines informations personnelles liées à l'administrateur du site si la nouvelle proposition était approuvée par l'ICANN.

L'EFF dans la boucle
L'EFF explique que ce changement est notamment soutenu par le secteur du divertissement, qui entend ainsi simplifier les procédures judiciaires à l'égard des sites diffusant des contenus constituant des infractions relatives à la propriété intellectuelle. Outre le risque que cette proposition peut faire peser sur les données personnelles des utilisateurs, on peut également évoquer les dangers relatifs à la cybersécurité.
Cedric Pernet, dans son ouvrage sur les Advanced Persistent Threat, citait ainsi les informations de service WHOIS parmi la liste des sources utiles aux attaquants pour préparer leurs attaques, en leur permettant d'identifier précisément le bureau d'enregistrement d'un site, un numéro de téléphone ou encore le nom de l'employé chargé d'administrer le nom de domaine.Autant d'informations utiles pour une attaque de type spear phishing.
La proposition est ouverte aux commentaires jusqu'au 7 juillet, et suscite déjà un certain engouement de la part des opposants à ce changement de politique, qui ont déjà posté des milliers de commentaires invitant l'ICANN à refuser cette proposition.

Source : http://www.zdnet.fr/actualites/l-anonymat-du-whois-remis-en-question-a-l-icann-39821566.htm
Par Louis Adam

La première soirée Implant Party débarque à Paris | Le Net Expert Informatique

La première soirée Implant Party débarque à Paris

La première « implant party » française a été organisée à Paris dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Le concept, se faire implanter une puce sous la peau pour différentes applications du quotidien.

Sommes-nous en train d'assister à un tournant dans le domaine de l'interface homme/technologie ? Jusqu'à maintenant (sauf cas extrême), les modifications corporelles se cantonnaient aux tatouages, aux piercings ou écarteurs et à la chirurgie esthétique.
Mais depuis quelques mois, une nouvelle tendance née dans les pays scandinaves devient de plus en plus populaire, les Implant Party. Un concept qui consiste à se faire implanter une puce NFC sous la peau et permettre à son porteur d'interagir avec de nombreuses technologies de notre quotidien.

Une puce NFC sous la peau
Ce weekend, Paris a accueilli sa première implant party dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Chacun pouvait venir se faire implanter une puce NFC par un spécialiste formé à cette opération.
Bien entendu, pas question de faire n'importe quoi et l'opération, facturée 200 euros, est effectuée dans des conditions d'hygiène drastiques et dans un environnement totalement stérilisé. Le biohacker (nom donné à la personne qui reçoit l'implant) se voit injecter une puce NFC grosse comme un grain de riz sous la peau après une anesthésie locale. Une fois l'opération effectuée, il devient possible pour le porteur de la puce d'interagir sans contact avec les équipements NFC qui l'entoure.

Des applications multiples, notamment dans le domaine professionnel
Déverrouiller son smartphone, ouvrir une porte, allumer un ordinateur ou encore payer un petit achat du quotidien d'un simple geste de la main, voilà ce que permet la technologie implanté dans le biohacker.
Ce mouvement d'un nouveau genre a été créé en Suède par l'association à but non lucratif Bionyfiken. 400 salariés suédois se sont récemment vus proposer la possibilité de se faire implanter une puce NFC pour entrer dans leurs locaux, payer leur repas ou faire des photocopies. Si jamais le biohacker regrette son acte, il est possible de se faire enlever la puce.

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

Source : http://www.begeek.fr/les-implant-party-debarquent-a-paris-172890

Compter une population seulement avec le Wi-Fi | Le Net Expert Informatique

Compter une population seulement avec le Wi-Fi

Plus besoin de se baser sur le nombre de smartphones connectés dans une certaine zone pour compter des groupes de personnes. La découverte de chercheurs de Santa Barbara se base uniquement sur le signal Wi-Fi.

L'idée est assez simple sur le papier : analyser les variations des ondes Wi-Fi d'une certaine zone pour compter les personnes présentes. Partant du principe que chacun altère légèrement les ondes par sa présence, les chercheurs de l'université de Californie Santa Barbara ont mis au point un modèle mathématique pour estimer le nombre d'individus dans une zone donnée. Le professeur d'ingénierie informatique Yasamin Mostofi et son équipe ont disposé deux spots Wi-Fi à deux extrémités d'une aire de 70 mètres carrés. Grâce à l'analyse de leurs ondes, les ingénieurs sont ensuite parvenus à estimer le nombre de personnes présentes dans la zone en temps réel. Et ce même si les individus étaient en mouvement.

Un outil pour la sécurité ?

En fait, la découverte répond à un besoin : celui de connaître l'étendu d'un groupe de personnes dans une manifestation ou dans un lieu public. La sécurité de certains événements pourrait en être accrue, selon les chercheurs, grâce à la notion de temps réel qu'apporte l'invention, même si les méthodes de comptage par les données télécoms se rapprochent déjà de ces objectifs. D'autant que le Wi-Fi ne peut s'étendre sur une surface aussi large que celles qui voient défiler des manifestants. L'aspect sécuritaire ne concernerait donc que les petits événements. Son seul avantage étant la prise en compte des individus sans smartphone.

Le Wi-FI rendra-t-il les bâtiments plus verts et plus intelligents ?

Vers des bâtiments plus intelligents

C'est en réalité dans un autre domaine que la découverte pourrait changer la donne. Les bâtiments intelligents seraient, en effet, à même de bénéficier d'une telle invention. Comme l'explique le professeur Mostofi dans le communiqué de l'université : « les stores intelligents pourraient se servir du dénombrement des utilisateurs du lieu pour mieux s'adapter par exemple ». Savoir précisément le nombre d'occupants d'un lieu ou le nombre de consommateurs dans un magasin permettrait à la fois une consommation d'énergie plus efficace mais également une nouvelle opportunité marketing. Les écrans publicitaires pourraient, en effet, se moduler selon la population présente pour ne citer que cet exemple.

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

Source :
http://www.atelier.net/trends/articles/compter-une-population-seul-wi-fi_436129?utm_source=emv&utm_medium=mail&utm_campaign=lettre_toute_zone