La France, terrain de jeu privilégié des espions chinois

La France, terrain de jeu privilégié des espions chinois

Au début du mois, « l'Obs » dévoilait l'existence d'un centre d'écoutes des services de renseignement chinois en banlieue parisienne. Si la Chine a démenti les affirmations de l'hebdomadaire, l'exécutif français n'a absolument pas réagi. Une passivité qui dit bien la liberté d'action dont bénéficient en France les espions chinois. Impossible de prendre le risque d'une brouille diplomatique avec Pékin pour une vague affaire d'espionnage compte tenu des enjeux commerciaux.

Lors de la visite du président chinois, Xi Jinping, à Paris en mars 2014 – Orban Thierry-POOL/SIPA

Une annexe de la « NSA chinoise » en banlieue parisienne ! Au début du mois de décembre, l'Obs dévoilait l'existence de ce que l'hebdomadaire croyait être un centre d'écoutes des services de renseignements chinois.

« C'est une totale invention !, tonne Monsieur Wu, chargé de communication de l'ambassade de Chine en France, Ces installations ne font qu'assurer le système de communication de l'ambassade. Cela permet des connexions sécurisées. Cela a été fait en totale conformité avec la législation française. Nous respectons les lois françaises. J'ai sous les yeux les papiers datés du 11 octobre 2002 qui attestent de l'autorisation donnée par l'Autorité de régulation des télécoms qui est parfaitement au courant de ces installations. Il n'y a là bas que des diplomates, aucun militaire. Tout est transparent ». Quand nous lui demandons, si la totale transparence et la bonne volonté chinoise pourraient aller jusqu'à nous laisser visiter ces installations, Monsieur Wu hésite tout de même… avant de répondre par la négative ! La transparence a des limites…

Paradoxalement, du côté français, on est encore moins prolixe. Interrogé sur l'existence supposée d'un bâtiment des renseignements chinois sur le territoire français, le quai d'Orsay répond « pas de commentaires ». En théorie, le ministère de l'Intérieur, les Affaires étrangères et les services de renseignement français sont parfaitement au courant de l'existence de cette annexe de l'ambassade de Chine et les autorités françaises auraient même validé l'installation de ces antennes.

Les « grandes oreilles » de Pékin en France… *par LeNouvelObservateur*

Si l'Obs surévalue sans doute en partie la menace représentée par les trois paraboles perchées sur ce bâtiment de Chevilly-la-Rue au point d'en faire une annexe de la « NSA chinoise » – on « souhaite » à Pékin de disposer d'autres moyens pour espionner Paris –, l'article de l'hebdomadaire, que l'on sent largement alimenté par la DGSI, dit bien toute la frustration et l'impuissance du contre-espionnage français face au pillage d'informations exercées par l'Empire du Milieu en France. Compte tenu du poids économique que représente la Chine pour la France, les espions chinois opèrent en effet relativement tranquillement sur le territoire français au grand dam du contre-espionnage français.

La France n'a tout simplement pas les moyens de se payer une brouille diplomatique avec Pékin au prétexte de trois paraboles installées en banlieue parisienne. Les milliards de contrats commerciaux signés avec les Chinois valent bien quelques sacrifices… Ce laisser-faire relève néanmoins de l'humiliation permanente pour les services français, contraints d'avaler toutes les couleuvres chinoises.

Non que Pékin ne possède pas, comme les Américains, mais aussi comme la France, de « grandes oreilles » un peu partout dans le monde, et prioritairement dans les pays et les dictatures amies du régime. En 2008, dans son ouvrage Les services secrets chinois, Roger Faligot estimait déjà que la Chine jouait dans la cour des grands avec les Etats-Unis et la Russie en matière de renseignement électro-magnétique. Six ans plus tard, les budgets du renseignement chinois ont explosé et les techniciens ont progressé, formés depuis les années 80 par le BND allemand et même jusque dans les années 90 par… la NSA américaine.

Selon Roger Faligot, la Chine a mis en place au fil des ans une « armée populaire des cyberguerriers » : « Ce service dépend de l'armée populaire de libération. Il est organisé en deux départements qui travaillent sur le renseignement de guerre et l'interception des communications. Ils procèdent en envoyant des virus qui permettent de pirater des informations ou de bloquer des sites gênants. Ils opèrent également en mode "testing" en piratant des systèmes pour étudier la capacité de réaction de l'ennemi. Nous sommes ici en plein volet de guerre psychologique et idéologique ».

Une guerre surtout économique désormais, comme l'avait illustré en septembre dernier une enquête de Franck Renaud et Hervé Gattegno parue dans Vanity Fair. Les journalistes avaient mis la main sur un rapport de la délégation interministérielle à l'intelligence économique (D2IE) sur les objectifs et méthodes chinoises pour piller les innovations technologiques françaises. Un espionnage d'une toute autre ampleur que le renseignement d'origine électro-magnétique. Cette instance signale chaque année plusieurs dizaines de vols ou tentatives de vols de données par captation ou indiscrétion. Toutes les techniques d'espionnage seraient utilisées. De la simple « oreille baladeuse » chinoise dans les trains Thalys ou Eurostar largement fréquentés par les industriels, aux « agents de charme » chargés de séduire les élites industrielles, à l'organisation de voyage de tourisme industriel, l'infiltration d'étudiants chinois dans les universités françaises, le vol de matériels informatiques ou bien encore des méthodes de « phishing » très sophistiquées. Il faut aussi ajouter l'incroyable « pouvoir de persuasion » des Chinois pour imposer à leurs partenaires des transferts de technologies lors de la signature de contrats commerciaux ou la création de joint-ventures, de filiales communes.

« La Chine est déterminée à devenir indépendante de l'Occident en matière d'innovation technologique. Elle est donc avide de connaissances, de savoir-faire et de procédés à faire venir en Chine ou à absorber à l'étranger » précisait le rapport de la D2IE. De leur côté, « les entreprises françaises, attirées par ce marché qu'elles envisagent immense (…) et par les coûts de main-d'œuvre locaux inférieurs aux coûts européens, sont souvent prêts à transférer leur technologie et leur savoir-faire, fournissant ainsi un avantage à leurs concurrents chinois ».
Paris se rassure en estimant que Pékin n'a pas encore les capacités d'exploiter à plein les renseignements politiques, économiques ou industriels qu'ils obtiennent, la Chine se limitant pour l'instant à du rattrapage technologique et à des copies de mauvaise qualité. Mais les énormes moyens affectés à la cyberguerre servent aussi le renseignement économique notamment par le biais de piratages informatiques massifs ainsi que le vol de propriété intellectuelle.

Derrière chaque touriste chinois, un espion potentiel ?
En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue anglaise, l'unité aurait compromis jusqu'à 141 entreprises dans vingt grands secteurs industriels, en dérobant un volume considérable d'informations relevant de la propriété intellectuelle. L'infrastructure de commandement et de contrôle de cette unité compterait de 850 à 1 000 machines situées dans 13 pays. Le coût de ce pillage informatique des entreprises américaines était estimé à au moins 24 milliards de dollars en 2012. L'unité 61046, chargée notamment du suivi de l'Europe, fonctionne sans doute sur le même principe avec la même efficacité, mais est moins connue.
Elle a néanmoins permis aux espions chinois d'accéder aux ordinateurs du président de la Commission européenne, du ministère français des Finances en mars 2011et même de l'Elysée en juillet 2012, causant à l'époque une panique certaine dans les couloirs de la présidence. Chaque attaque est l'occasion pour les services occidentaux d'identifier les priorités des services chinois ainsi que les commanditaires pour mieux connaître leur organisation encore très nébuleuse.
Un an plus tard, dans une mise à jour de son rapport, la société Mandiant disait avoir constaté une « mise en sommeil » pendant quelques mois des activités de l'Unité 61398 suite à la publication de son rapport et aux protestations américaines. De même, toutes les adresses IP des cyberattaques chinoises qui ont frappé les Etats-Unis depuis ont été modifiées, suggérant un changement de stratégie des renseignements chinois.
Mais l'espionnage informatique continue. En octobre dernier, une société américaine de cybersécurité privée identifiera une nouvelle unité de espions informatiques chinois baptisée « groupe Axiome » : « Axiome est chargé de diriger les opérations de cyberespionnage très sophistiquées contre de nombreuses grandes entreprises, des journalistes, des groupes écologistes ou pro-démocratie, des sociétés de logiciels, des établissements universitaires et des organismes gouvernementaux dans le monde entier ». Cibles prioritaires : les Etats-Unis, l'Europe et les voisins asiatiques.
Le Washington Post dévoilera quelques jours plus tard une note du FBI destinée aux industriels américains les alertant sur cette unité de cyberpirates que le FBI considérait comme directement liée aux services de renseignements chinois et jugeait plus performante que l'unité 61398.

Une forme d'espionnite aigüe qui oblige les services français à une attention de tous les instants. Très récemment la lettre spécialisée Intelligence online rapportait l'escapade à Saint-Nazaire d'une équipe du service culturel de l'ambassade de Chine, venue célébrer l'anniversaire de la construction d'un bateau de croisière chinois. La délégation se serait tellement attardée à « mitrailler » le porte-hélicoptères Mistral destiné à la Russie que cela aurait fini par éveiller les soupçons de la DGSI. De la surveillance à la paranoïa, il n'y a parfois pas loin…

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

Source : http://www.marianne.net/La-France-terrain-de-jeu-privilegie-des-espions-chinois_a243309.html
par Régis SOUBROUILLARD – Marianne

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

L'arrêt rendu ce matin par la Cour de Justice de l'Union européenne en matière de vidéosurveillance risque d'avoir de douloureux effets en France. Il remet en effet en cause les efforts du ministère de l'Intérieur pour se passer de la CNIL dans l'installation des caméras de « vidéoprotection. »

Les faits examinés par la CJUE visait le cas d'un Tchèque ayant installé une caméra de surveillance chez lui, mais dont le champ de vision débordait sur la voie publique. Les flux étaient stockés sur disque dur, chez lui. Par ce biais, ce particulier avait finalement permis à la police d'identifier une personne suspectée d'avoir caillassé les fenêtres de sa maison. Cependant, la CNIL locale lui a infligé une amende, faute pour ce particulier d'avoir zappé le consentement préalable des personnes filmées. On pourra revoir notre actualité sur les solutions proposées par la Cour, mais l'important n'est peut-être pas là car l'arrêt est supposé provoquer un vent de panique en France, au ministère de l'Intérieur. Explication.

Vidéosurveillance, donnée personnelle, traitement automatisé

La Cour a en effet posé qu'en principe la vidéosurveillance relevait du champ d'application de la directive de 1995 sur les données personnelles, du moins « dans la mesure où elle constitue un traitement automatisé ». Cette analyse fait suite à un développement très logique :
La donnée personnelle embrasse « toute information concernant une personne physique identifiée ou identifiable. »
Est réputée identifiable « une personne qui peut être identifiée, directement ou indirectement, notamment par référence […] à un ou plusieurs éléments spécifiques, propres à son identité physique.»
Du coup, « l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel (…) dans la mesure où elle permet d'identifier la personne concernée ». En clair, une caméra de vidéoprotection capte donc des données à caractère personnelles quand les personnes filmées sont identifiées ou identifiables.
Mais y a t-il pour autant traitement automatisé de ces données ? La directive de 95 définit ce traitement par « toute opération ou [tout] ensemble d'opérations […] appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement […] la conservation ». La CJUE considère donc qu' « une surveillance effectuée par un enregistrement vidéo des personnes (…) stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue (…) un traitement de données à caractère personnel automatisé. »

Fort de ces enseignements, auscultons le régime français.

Les contrariété du régime français de la « vidéoprotection »
Une circulaire du 14 septembre 2011 décrit le cadre juridique applicable à l'installation de caméras de vidéoprotection, terme officiel pour repeindre de manière plus sympathique les outils de vidéosurveillance. Cette circulaire est importante puisqu'elle définit les (rares) cas où les autorités doivent effectuer une déclaration préalable auprès de la CNIL, et quand elles peuvent (très souvent) s'en passer.
Deux hypothèses sont envisagées par cette circulaire qui vient faciliter l'application du Code de la sécurité intérieure : des caméras installées sur la voie publique, des caméras installées sur des lieux non ouverts au public.

Les caméras installées sur la voie publique

Les caméras installées sur la voie publique (et dans des lieux ou établissements ouverts au public) nécessitent l'autorisation préalable du préfet après avis de la commission départementale de la vidéo protection. Donc sans passer par la CNIL.
Cependant, parfois, ce passage CNIL est nécessaire. Le ministère de l'Intérieur, épaulée par un avis du Conseil d'État (non public et concernant les caméras dans les prisons) l'estime inévitable seulement « si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment). »
Décodons : en France, lorsque le flux permet l'identification via un système de reconnaissance faciale (ou de plaque d'immatriculation), il faut passer par la CNIL. L'Intérieur en déduit naturellement que « le seul fait que les images issues de la vidéoprotection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéoprotection lui-même. »

On le voit, ce point est en exacte contradiction avec ce que vient de juger la CJUE : des personnes, une caméra, un flux, un stockage, nous voilà déjà plongé jusqu'au cou en Europe dans le règne du traitement automatisé de données personnelles. La France, pourtant un État membre, estime qu'il n'y a pas de traitement automatisé (donc pas de passage par la CNIL) faute de flux couplé à une reconnaissance faciale ou de plaque d'immatriculation. Un critère totalement surabondant !

Les caméras installées dans les lieux non ouverts au public

La circulaire précitée évoque aussi les caméras installées dans les lieux non ouverts au public (soit partout ailleurs que les voies publiques, la résidence privée ou la voiture). Ce régime n'est pas de la compétence de l'Intérieur, mais celui-ci donne malgré tout des pistes : il faut là encore l'avis de la CNIL « lorsque ces personnes sont identifiables ».

La Place Beauvau pose ici deux critères cumulatifs :
D'une part des images qui font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage.
D'autre part, une identification possible parce que le lieu est fréquenté par des personnes « dont une partie significative est connue du responsable du système de vidéoprotection ou des personnes ayant vocation à visionner les images enregistrées. »

Cependant, ces deux critères ne se retrouvent pas dans les textes fondateurs :
Si la captation n'est pas un traitement selon l'Intérieur, la loi de 1978 tout comme la directive disposent que la collecte et la transmission le sont bien.
Le critère de la « connaissance » des personnes filmées par celui derrière la caméra est quelque peu restrictif : une reconnaissance indirecte est normalement suffisante, d'autant que même si personne ne peut identifier Mme Michu sur son écran de contrôle, elle aura son image et pourra le faire par la suite.

Enfin, le critère de la « partie significative » n'est pas intégré dans les textes socles.
Bref, l'arrêt rendu ce matin par la CJUE devrait naturellement amener la CNIL à se pencher plus en profondeur sur le régime français, et l'Intérieur à revoir le périmètre de ses yeux électroniques. D'autres actualités seront à suivre en fonction des retours obtenus auprès de ces deux acteurs.

Consultez l'arrêt de la Cour de Justice de l'Union Européenne de l'affaire C-212/13

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

Source : http://www.nextinpact.com/news/91367-quand-videosurveillance-europeenne-contrarie-videoprotection-francaise.htm#/page/1
par Marc Rees

Un autre programme secret de la NSA cible les réseaux GSM mondiaux

	Un autre programme secret de la NSA cible les réseaux GSM mondiaux

Des documents livrés par Edward Snowden évoquent un programme d'espionnage secret de la NSA. Appelé Auroragold, il cible les membres du GSMA pour recueillir des informations confidentielles sur les failles et les systèmes de cryptage, exploitées ensuite pour s'infiltrer dans les réseaux mobiles.

Selon des informations contenues dans des documents livrés par l'ex-consultant Edward Snowden, la NSA a lancé une campagne secrète pour intercepter les communications internes d'opérateurs et d'acteurs du secteur de la téléphonie mobile dans le but d'infiltrer leurs réseaux partout dans le monde. Dans un article publié samedi par le site The Intercept, qui a également mis en ligne les documents concernés, l'Agence nationale de sécurité américaine a mené, dans le cadre d'un programme appelé Auroragold, des opérations encore jamais rendues publiques.
Deux unités – Wireless Portfolio Management Office et Target Technology Trends Center – mises sur pied par la NSA, ont été chargées de surveiller de près les membres de la GSM Association, espionnant plus de 1200 adresses emails. L'objectif était d'intercepter dans les entreprises visées des messages internes et de recueillir des informations sur les failles de sécurité des réseaux et le cryptage des communications.
Les derniers documents indiquent qu'en mai 2012, sur les 985 réseaux de téléphonie mobile mondiaux, la NSA avait récolté des informations techniques sur 70 % d'entre eux. Mis à part les pays de quelques opérateurs ciblés – Libye, Chine et Iran – le document fourni par l'ancien consultant de l'agence américaine, toujours réfugié en Russie, ne contient aucun nom d'entreprises. Ces opérations d'espionnage ont permis à la NSA de récupérer des documents IR.21 utilisés par les membres de la GSMA pour signaler des failles de sécurité dans leurs réseaux. Les IR21 contiennent également des détails sur les solutions de cryptage utilisées par les opérateurs mobiles. D'après les documents d'Edward Snowden, la NSA, qui n'a pas répondu à une demande de commentaire, s'est servie de ces informations pour contourner le cryptage des communications.

Espionnage tous azimuts
Depuis juin 2013, de nombreux rapports et articles basés sur les documents fournis par Edward Snowden montrent l'étendu des opérations d'espionnage menées par la NSA sur Internet et les réseaux télécoms à travers le monde. Ils ont aussi permis de savoir que la NSA avait piraté les courriels de dirigeants de pays alliés des États-Unis et de découvrir qu'elle avait infiltré les réseaux et les systèmes d'entreprises étrangères, comme c'est le cas du constructeur chinois Huawei. L'an dernier, divers articles parus dans ProPublica, The Guardian et The New York Times, ont révélé que, pendant plusieurs années, la NSA s'était employée à affaiblir les normes de sécurité pour faciliter les opérations d'espionnage à grande échelle du gouvernement américain. Par exemple, des articles publiés en septembre 2013 par le Guardian et le NYT indiquent, sur la base des documents de Snowden, que la NSA a créé sa propre version du standard Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), un générateur de nombres aléatoires utilisé en cryptographie. Cette norme, approuvée pour un usage mondial en 2006, contiendrait une porte dérobée permettant à la NSA de s'introduire dans les systèmes de communications. Dès 2007, certains spécialistes et l'éditeur lui-même, RSA Security, recommandaient de désactiver par défaut le Dual_EC_DRBG. Des documents divulgués par Edward Snowden l'an dernier ont également apporté la preuve que la NSA pouvait espionner le trafic GSM chiffré avec l'algorithme A5/1.

Fin novembre, Symantec et Kaspersky Labs ont révélé l'existence d'un malware baptisé Regin, probablement développé par les États-Unis. Actif depuis au moins six ans, Regin cible les réseaux cellulaires GSM pour espionner les gouvernements, les infrastructures des opérateurs de téléphonie mobile, des instituts de recherche, des entreprises et des particuliers. En plus de ces opérations secrètes, la NSA espionne collectivement les conversations téléphoniques des citoyens américains. Le mois dernier, le directeur de la NSA, Michael Rogers a déclaré que l'agence ne prévoyait pas de réviser son programme de collecte : un projet de loi déposé devant le Sénat pour encadrer cette collecte n'a pas abouti.
Glenn Greenwald et Laura Poitras, les deux éditeurs et fondateurs du site The Intercept, ont déjà aidé Edward Snowden à diffuser ses documents par le biais de différents médias.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-autre-programme-secret-de-la-nsa-cible-les-reseaux-gsm-mondiaux-59530.html
Par Jean Elyan / IDG News Service

La justice européenne va

encadrer la vidéosurveillance depuis le domicile – Next INpact

	La justice européenne va encadrer la vidéosurveillance depuis le domicile – Next INpact

Jeudi, la Cour de Justice de l'Union dira si une caméra située dans une propriété privée qui surveille également une partie de l'espace public échappe ou non aux règles de protection en matière de traitement des données à caractère personnel.

Le déploiement des solutions de vidéosurveillance personnelles se démocratisant, une affaire tranchée demain par la Cour de Justice de l'Union européenne méritera une certaine attention. Le cas examiné est né en Tchécoslovaquie.

Un certain M. Ryneš, agacé que les vitres de sa maison soient brisées à maintes reprises avait installé un système de vidéosurveillance. Les flux étaient enregistrés sur disque dur à partir de caméras captant l'entrée de sa maison, celle de la maison d'en face, mais également une partie de la voie publique.

Une amende infligée par la CNIL tchèque

Dans la nuit du 6 au 7 octobre 2007, nouveau vandalisme à l'aide d'une fronde. Les enregistrements sont remis à la police qui parvient à identifier des suspects. Problème, l'un d'eux conteste la légalité des procédures auprès de l'Office tchèque pour la protection des données à caractère personnel. Et pour cause : ces enregistrements ont été effectués sans son consentement alors qu'il était sur la voie publique.
La CNIL locale lui donne raison et inflige une amende à M. Ryneš. Ce dernier attaque cependant cette décision devant la Cour suprême administrative tchèque, laquelle, prise d'un doute, a saisi la Cour de justice pour savoir si ces enregistrements constituaient ou non un traitement de données couvert par la directive 95/46 sur les données personnelles. Celle-ci en effet, ne s'applique pas quand le traitement est effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

L'analyse de l'avocat général

Pour l'heure, l'avocat général a déjà conclu que le traitement de données à caractère personnel effectué par ce Tchèque ne relevait pas de la notion d' « exercice d'activités exclusivement personnelles ou domestiques », une des exceptions à la directive en question. Du coup, a contrario, ce système de vidéosurveillance devrait entrer dans le plein champ de ce texte européen.
Si la Cour suit cette analyse, cela ne signifiera pas nécessairement que l'amende infligée au responsable du traitement sera légitimée. Il faudra en effet déterminer si d'autres articles de cette directive ne peuvent être appelés en renfort pour légitimer cette installation effectuée sans le consentement des personnes filmées (article 7 f) de la directive).

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

Source : http://www.nextinpact.com/news/91283-la-justice-europeenne-va-encadrer-videosurveillance-depuis-domicile.htm

---

Indétectable et envahissant : le successeur des cookies est là, le fingerprinting

Indétectable et envahissant : le successeur des cookies est là, le fingerprinting

Excédé par le tracking publicitaire des sites marchands, vous pestez contre les cookies ? Le Fingerprinting ou « empreinte » s'apprête à leur succéder. Cookies ou pas, vous n'échapperez donc pas au traçage.

Qui ne s'est jamais érigé en défenseur des bandeaux publicitaires. Certaines publicités peuvent même vous rappeler intégralement, quel que soit le site sur lequel vous vous rendez, la liste des produits que vous avez consultés sur un site marchand. Le ciblage publicitaire connaît un succès foudroyant auprès des annonceurs, mais il suscite aussi l'agacement car il révèle l'efficacité du traçage systématique des internautes via les cookies.
Des plugins tels que Lightbeam ou Collusion permettent de se faire une idée de l'intense pistage réalisé par une multitude d'agences et de prestataires divers, que l'on subit lorsque l'on surfe sur un site. Depuis quelques mois, tous les sites de contenus et autres sites marchands sont contraints par la Cnil d'afficher un bandeau pour vous avertir de l'utilisation de cookies, incitant les internautes à activer l'option Do not Track de Firefox, à installer des plugins tels que Ghostery, BetterPrivacy ou NoScriptSecurity Suite, afin de se démettre de l'emprise des publicités.
L'extension Lightbeam pour Firefox identifie 245 sites tiers impliqués pour la visite de 21 sites Web seulement. Chaque site Web pose un cookie pour son fonctionnement interne, mais bien davantage pour tous ses partenaires commerciaux

Fingerprinting, l'après cookies, est déjà là
Pour l'instant, selon les chiffres compilés par AT Internet, le taux d'acceptation des cookies en Europe atteint encore 92%. Une proportion négligeable pour les publicitaires, mais qui ne les empêche pas d'envisager l'après cookie. Le futur, c'est le fingerprinting, une solution qui est, sur le papier, imparable. Le service conserve sur ses serveurs les principales caractéristiques de son poste de travail de chacun des internautes, des caractéristiques qui constituent l'empreinte numérique de son poste. Système d'exploitation, navigateur, résolution d'écran, une visite sur le site Panopticlick de l'EFF donne une petite idée de l'étendue des informations que votre ordinateur peut transmettre au serveur, sur simple requête.

Elles sont très largement suffisantes pour identifier à coup sûr un internaute qui revient sur le site. Poser un cookie sur le poste devient inutile, il suffit de vérifier cette configuration à chaque connexion.

L'approche peut sembler extrêmement coûteuse en ressources, puisque toutes les données doivent être analysées et stockées sur le serveur, mais les technologies Big Data rendent aujourd'hui cette approche centralisée totalement possible. En France, des acteurs tels que Criteo ou AT Internet affirment ne pas utiliser cette solution technique.

« D'un point de vue technique, le fingerprinting est une alternative sur laquelle nous nous sommes penchés » reconnaît Mélanie Claisse, chef de produit chez AT Internet. Elle souligne néanmoins : « Il reste aujourd'hui malgré tout des zones d'ombre sur des aspects fondamentaux du respect de la vie privée, comme la transparence vis-à-vis des internautes, et surtout, sur leur capacité à accepter ou non la collecte d'informations es concernant, aussi anonymes soient-elles. De ce fait c'est une technique qu'AT Internet n'utilisera pas tant que ces zones d'ombre ne sont pas levées. »

Une prudence qui n'est pas de mise chez un certain nombre d'acteurs du Web. Des chercheurs de KU Leuven et de Princeton ont ainsi débusqué un code Javascript de fingerprinting sur 5 282 des 100 000 sites qu'ils ont expertisés. Des services tels que AddThis, Ligatus exploitent les API JavaScript Canvas, initialement destinées à dessiner des graphiques sur une page HTLM, afin de générer une empreinte unique.

Votre ordinateur vous trahit
Pour ceux qui douteraient de la fiabilité des techniques de fingerprinting, les chercheurs de l'INRIA, du laboratoire IRISA et de l'INSA-Rennes viennent de mettre en ligne le site Am I Unique ? Celui-ci réalise un calcul de votre signature, votre empreinte et vous dit si celle-ci est véritablement unique et donc s'il vous expose au traçage.
Les résultats sont étonnants. Même avec une configuration de type PC sous Windows 7 avec Google Chrome, un serveur va facilement pouvoir vous repérer à votre prochaine venue sur le site, sans qu'aucun cookie n'ait été posé sur le poste.
Derrière le site Am I Unique ?, un chercheur de l'INRIA, Benoit Baudry. Celui-ci participe au projet européen Diversify, qui étudie la problématique de la diversité logicielle.

Les chercheurs visent à diversifier les logiciels afin d'améliorer leur résistance aux bugs et aux cyberattaques.

Application de cette recherche, Benoit Baudry cherche comment déjouer le fingerprinting grâce à cette diversité dans le projet Blink : « Globalement, il y a deux stratégies possibles pour déjouer le fingerprinting : soit on va mentir au serveur, soit chercher à le tromper. Mentir au serveur, c'est très simple, on lui renvoie de fausses informations. Le problème, c'est : d'une part, vous risquez d'avoir des problèmes d'affichage du site car ces informations sont utiles à l'affichage des pages, d'autre part, il faut envoyer des informations cohérentes pour ne pas être identifié comme un tricheur par le serveur qui va alors mettre en place d'autres stratégies pour vous reconnaître. »

Autre approche possible, ne pas mentir au serveur, mais le prendre à son propre jeu. La première stratégie c'est de présenter strictement la même signature pour l'ensemble des internautes. C'est ce que fait le Tor Browser, une version spécifique de Firefox qui surfe via le réseau Tor. Absolument tous ses utilisateurs ont un seul et même fingerprint. De fait, un serveur n'est pas capable de distinguer un individu unique dans la masse.

Autre piste possible, et c'est l'objet de la recherche de Benoit Baudry, c'est tout simplement de changer de configuration à chaque visite. Cet expert de la diversité logicielle travaille sur une solution qui génère automatiquement une configuration qui fonctionne réellement, avec un comportement le plus proche possible de ce qu'attend l'internaute, mais qui, du point de vue du serveur, est différente et donc, impossible à tracer. « Le fingerprint est unique et stable dans le temps » ajoute le chercheur. « Notre recherche porte sur la stabilité dans le temps. On veut faire évoluer le fingerprint de l'utilisateur dans le temps, mais sans renvoyer de fausses informations. On doit donc faire varier sa configuration pour faire évoluer son fingerprint. » Automatiquement, les paramètres du navigateur, les polices de caractère installées, la liste des plugins et même l'OS vont varier.

Le chercheur s'appuie notamment sur des machines virtuelles pour générer cet environnement automatiquement parmi une liste de configurations disponibles. Demain, il pourrait avoir recours à Docker, une solution plus légère pour générer ces configurations. C'est aussi le rôle de Am I Unique ? que de collecter des configurations « réelles » afin d'amasser un stock de fingerprint (anonymes, bien entendu) et générer ces configurations. Une stratégie du mal contre le mal pour lutter contre le fingerprinting.

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

Source : http://pro.clubic.com/webmarketing/publicite-en-ligne/actualite-742853-fingerprinting-cookies.html
par Alain Clapaud

Gmail et Inbox : Google va-t-il trop loin ?

Gmail et Inbox : Google va-t-il trop loin ?

Google vient de lancer Inbox, une version nouvelle et plus structurée de Gmail. La solution soulève de nombreuses questions autour de l'utilisation et de la protection des données personnelles et notamment : quel est l'objectif de Google avec Inbox ?

Inbox présente un grand nombre de fonctionnalités intéressantes : une bonne classification des e-mails, un algorithme intelligent, une interface plus ergonomique et facile à utiliser, en particulier à partir d'un téléphone mobile. Cependant, il subsiste quelques zones d'ombre, que ce soit avec Gmail ou Inbox.
Google se positionne parmi les acteurs qui protègent la vie privée de ses utilisateurs, alors qu'il met tout en œuvre dans ses outils pour analyser leur comportement. Nous savons tous que les données qui transitent dans nos e-mails sont analysées et utilisées, soit pour classer nos e-mails, soit pour nous envoyer/identifier une publicité ciblée. Google analyse les données et doit donc les stocker pour y avoir accès à tout moment.

Peut-on continuer à parler de vie privée lorsqu'il n'y a ni option ni moyen d'interdire l'accès à mes données ?
Inbox propose à l'utilisateur de faire le tri et de filtrer les e-mails commerciaux et les newsletters, que celui-ci peut désormais recevoir dans des catégories (« promotions », « réseaux sociaux », etc.). Pourtant, Google pousse des publicités vers les utilisateurs grâce à ce même outil. Alors Google est-il vraiment impartial lorsque Inbox filtre et classifie les e-mails ? La publicité est tout de même l'un des principaux revenus de Google… AdWords a d'ailleurs évolué pour devenir la principale source de revenus de Google et les recettes publicitaires totales de Google ont dépassées les 50 milliards de dollars en 2013, faisant de lui le leader, bien loin devant ses concurrents.
La principale différence entre Google Inbox et Gmail résulte dans l'affichage des publicités : apparemment, il n'y a pas de pub dans Inbox alors qu'il y en a toujours dans Gmail. Cela signifie-t-il que les publicités sont cachées… peut-être dans ce que Google appelle les « Bundle » (groupement de plusieurs emails) ? Car, il est difficile de croire que Google va supprimer l'affichage des publicités dans l'un de ses principaux services. Par contre, il est fort probable qu'ils continuent à utiliser l'une de leurs tactiques bien rodées qui consiste à promouvoir de nouvelles offres sans publicité au départ…
Avec Inbox, Google offre un algorithme, une classification et de nombreuses autres fonctionnalités d'un très bon niveau. Toutefois, sur le marché du filtrage des e-mails (de l'anti-spam à la solution de graymail management), seul Google a besoin de lire le contenu des e-mails alors que les autres acteurs se basent sur sa structure et d'autres paramètres pour définir sa nature. Par ailleurs, les pure-players qui offrent des solutions identiques de filtrage des e-mails, ne tirent aucun bénéfice de la publicité. Ils sont donc impartiaux dans la classification, aucun émetteur ne sera mis en avant au détriment d'un autre. Ainsi, le contenu des e-mails n'influence pas les contenus et les publicités lors des connexions du navigateur. On peut facilement comparer cette situation avec une affaire du passé concernant le paiement de Google vers AdBlock.
Les débats autour de la protection de la vie privée et des données personnelles n'ont jamais été aussi présents. Les solutions du type Gmail et Inbox sont largement utilisées par le grand public parce qu'elles sont gratuites et performantes. Toutefois, les utilisateurs n'ont pas forcément pris conscience de l'utilisation de leurs données. Quand une solution est gratuite, cela signifie que l'utilisateur est le produit… Si cela peut être acceptable pour le grand public (à voir sur le long terme), dans le monde de l'entreprise, la confidentialité des données doit être prise au sérieux. Le choix d'une solution de graymail management doit se faire en connaissance de cause.

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

Source : http://www.journaldunet.com/ebusiness/expert/59293/gmail-et-inbox–google-va-t-il-trop-loin.shtml

Détecter et analyser les émotions sur internet

	Détecter et analyser les émotions sur internet

Détecter et analyser les émotions humaines au départ de sites internet, c'est ce que propose Getsmily, une nouvelle spin-off de l'Université catholique de Louvain. « Avec plus d'un milliard de sites web sur la toile, le besoin pour les entreprises de nouer des liens forts avec leurs publics devient primordial. Et La construction de ces liens commence par la compréhension des comportements et des émotions de ces audiences. Les émotions nous animent au quotidien et guident nos actions, plus souvent qu'on ne le pense », confie David Frenay, le chercheur UCL à la base de la technologie et CTO de la startup.

Fruit de plusieurs années de travail au sein du laboratoire de vision par ordinateur du professeur Benoit Macq de l'UCL, cette technologie a séduit des investisseurs privés ainsi que le Fonds d'investissement VIVES II qui ont décidé d'injecter un demi-million d'euros dans la société. Les applications marketing rendues possibles grâce à la technologie UCL, unique en son genre, vont mener l'équipe de GetSmily à la conquête du world wide web. « La compréhension des émotions humaines et les leviers qui les activent sont des atouts majeurs pour le responsable marketing moderne. Le marketing reprend donc un rôle central au sein des entreprises qui sont résolument tournées vers l'avenir », confirme David Hachez, co-fondateur et CEO de GetSmily.
Lancée en septembre 2014, la spin-off GetSmily donne accès à un indicateur de performance émotionnelle novateur baptisé l'Emoscore. Celui-ci est obtenu grâce aux Emolytics (contraction des mots « emotions » et « analytics ») qui intègrent un algorithme unique et scientifiquement solide. La technologie a déjà séduit plusieurs entreprises telles que Foto.com, Europ Assistance, VOO, La Loterie Nationale, Sherpa, Quick Step, Lampiris ou encore Rossel Advertising.
GetSmily résulte d'un projet de recherche dans le domaine de la vision par ordinateur (vision artificielle), accompagné pendant deux ans par le Louvain Technology Transfer Office (LTTO). « Cette nouvelle spin-off démontre le rôle important que joue le LTTO pour assurer avec succès le transfert de technologie issu de la recherche UCL. Le soutien de la région wallonne (DG06), notamment par le biais de son programme First Spin-Off et du fonds proof-Of-Concept nous a permis de concrétiser ce projet qui offre de belles perspectives de développement », déclare Anne Bovy, co-directrice du LTTO et directrice de l'administration de la recherche de l'UCL. Les investisseurs qui rejoignent GetSmily vont lui permettre d'accélérer son développement international et aideront l'équipe à résoudre les challenges techniques qui s'annoncent. « Investir dans une startup du web confirme la volonté de notre fonds d'être un acteur dans ce secteur en pleine ébullition tout en soutenant le développement d'une spin-off de l'UCL », souligne Philippe Durieux, CEO de VIVES II.

A propos de GetSmily
Les Emolytics de GetSmily permettent aux propriétaires de sites internet de mesurer les émotions de leur audience ainsi que leurs comportements de surf. GetSmily, qui compte déjà 5 personnes à son bord, propose son produit Emolytics en 14 langues en mode SaaS (Software as a service) avec les plans Free, Start, Pro et Enterprise. Les données statistiques anonymes collectées sont traitées pour prendre forme dans un rapport. Ce dernier guide les entreprises dans la mesure de la qualité de la relation avec leurs audiences/publics, par l'intermédiaire d'un KPI unique appelé Emoscore, ainsi qu'à la prise de décision stratégique (marketing, communication, technique et/ou managériale).

Les fondateurs :
– David Hachez, CEO de GetSmily. Il a déjà à son actif quelques initiatives dont Raz*War, lancé en 2009 et repris par un fonds d'investissement privé en 2012
– David Frenay, ingénieur civil biomédical, master en physique et en gestion à l'UCL, bachelier en mathématique et médaillé aux Olympiades internationales. Il est à l'origine de la technologie de détection des émotions et occupe aujourd'hui le poste de CTO

A propos de VIVES – Louvain Technology Fund et du LTTO
– VIVES – Louvain Technology Fund est un fonds d'investissement technologique multi-sectoriel qui investit dans les spin-offs de l'UCL et dans les start-up en Belgique et dans les pays limitrophes. L'objectif du fonds est d'investir dans le développement de start-up, depuis la validation technologique jusqu'à la maturité commerciale. Les fonds (VIVES 1 de 15 millions d'euros et VIVES 2 de 43 millions d'euros) sont gérés par la Sopartec, la société de transfert de technologie de l'UCL. Infos : http://www.vivesfund.com.

– Le Louvain Technology Transfer Office (LTTO), regroupant la Sopartec et l'administration de la recherche de l'UCL, couvre l'entièreté du processus de transfert de technologie : financement des contrats de recherche, identification des inventions dans les laboratoires, protection et gestion de la propriété intellectuelle, maturation technologique et commercialisation (par le biais de licences et/ou spin-off). Plus précisément, la Sopartec coordonne la gestion des accords de licence et la maturation technologique des projets de spin-offs de l'UCL. Plus de 60 spin-offs, qui génèrent aujourd'hui, plus de 3.000 emplois, ont été créées en se basant en tout ou en partie sur des résultats des recherches menées à l'UCL. Il s'agit notamment de Ion Beam Application (IBA), IRIS Groupe, IBT, Telemis, Viridaxis, Promethera, GreenWatt, Keemotion, Iteos Therapeutics, DelfMens, Novadip Biosciences, etc. Infos : http://www.ltto.com.

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

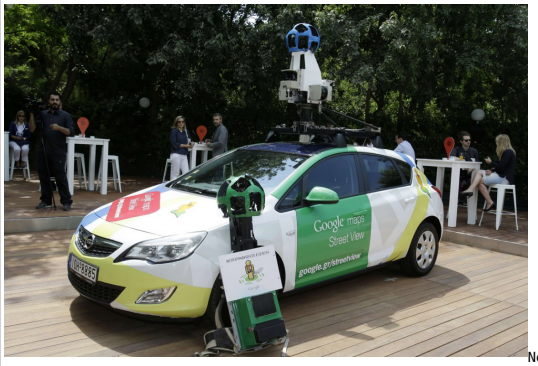
Source : http://www.bulletins-electroniques.com/actualites/77248.htm

Vous avez peur de Facebook ? Méfiez-vous plutôt de… tout

Vous avez peur de Facebook ? Méfiez-vous plutôt de… tout

« En réponse aux nouvelles lignes directrices de Facebook et en vertu du code de la propriété intellectuelle, je déclare que mes droits sont attachés à toutes mes données personnelles, dessins, peintures, photos, textes, musiques… publiés sur mon profil. Pour une utilisation commerciale, mon consentement écrit est nécessaire. »

Le message s'est répandu comme une traînée de poudre sur le réseau social, depuis l'arrivée d'une nouvelle politique de confidentialité. 240 mots qui seraient censés mettre à l'abri l'internaute contre une éventuelle réutilisation de ses données personnelles, mais qui n'ont « aucune valeur juridique », pointe la Commission nationale de l'informatique et des libertés (Cnil).
Pour autant, ce message (qui a déjà sévi en 2012) révèle un malaise des Français face à Facebook. Comme après le (faux) bug qui a suscité une panique sur le réseau social, les internautes ne sont pas à l'aise avec l'utilisation de leurs données personnelles.
Un sondage BVA, diffusé par « 20 minutes », pointe ainsi que 58% des Français ont une mauvaise opinion de Facebook. Celui qui compte 28 millions d'utilisateurs dans l'Hexagone voit son image bien plus écornée qu'Amazon ou Apple. Pis, Google s'en tire avec une perception « plutôt bonne » auprès de 81% des sondés. Erwan Lestrohan, directeur d'études de BVA Opinion, explique au quotidien :
Sur Google, on entre des mots-clés. Sur Apple et Amazon, des données bancaires. Facebook est la seule [plateforme] sur laquelle on stocke de nombreuses données privées. Ça génère un peu plus d'inquiétudes et ça touche plus à l'affect. »



Ne pas oublier le (condamné) Google

Cette crainte réelle se justifie en partie. Dans ses conditions d'utilisation, le réseau social prévoit que l'internaute lui « donne l'autorisation d'utiliser » les informations personnelles, dont les photos, qui sont partagées sur la plateforme.
Néanmoins, il faut reconnaître que Facebook a fait de nombreux efforts pédagogiques pour expliquer ses pratiques et surtout permettre aux utilisateurs de mieux se saisir des paramètres de confidentialité. Ainsi, la nouvelle politique d'utilisation des données s'est accompagnée d'une page – intitulée « Vous avez le contrôle » – permettant de mieux comprendre et appréhender les retords paramètres. En somme, une sorte de tutoriel géant sur l'utilisation avancée de Facebook.

Evidemment, il convient de prendre au sérieux les empiètements sur la vie privée sur internet. Seulement, Facebook est loin d'être le seul acteur qui doit préoccuper les internautes. Google devrait même arriver en tête de ce classement.

L'Américain est en effet en capacité de dresser un incroyable profil des consommateurs en se basant sur son énorme base de données personnelles. D'abord, il dispose d'un historique de l'ensemble des recherches effectuées sur le web, mais aussi ses robots lisent les contenus des e-mails, tandis que les smartphones Android enregistrent les géolocalisations tout en comptant le nombre de pas… A ces couches pourraient bientôt s'ajouter les équipements Nest, permettant d'en savoir plus sur les pratiques dans la maison.
Effrayant ? C'est peu de le dire. Surtout que l'intégralité de ces informations sont croisées. C'est d'ailleurs pour cette raison que la Cnil a condamné le géant à 150.000 euros d'amende (soit 0.01% de ses recettes annuelles dans l'Hexagone).
L'ensemble de ces données sont utilisées afin de prédire ce que le consommateur va chercher, lire, acheter, faire…

Cinq ans et aucune avancée…
Google, Amazon ou Apple ne sont pas les seuls acteurs dont il convient de se méfier. Un large écosystème d'entreprises s'est créé avec pour seul objectif de traquer le comportement de l'internaute. Un graphique de la société de conseils Luma Partners met ainsi en lumière qu'un nombre impressionnant de sociétés se greffe à un contenu.

La Cnil a ainsi mis à disposition un outil de visualisation (http://www.cnil.fr/vos-droits/vos-traces/les-cookies/telechargez-cookieviz/) de l'impact d'une navigation internet, et de l'ensemble des acteurs qui entrent en jeu. De son côté, le Massachusetts Institute of Technology (MIT) propose un service (https://immersion.media.mit.edu) qui, à partir d'une adresse e-mail Gmail, Yahoo ou Microsoft, permet de déceler les liens entre personnes, ainsi que leur importance.
Dans l'idéal, il faudrait que l'internaute donne un accord manifeste à chaque site qui veut utiliser ses données personnelles », estime Olivier Cimelière, président du cabinet en communication Heuristik. « Mais plutôt que ce contrat moral, dit d'opt-in, c'est la politique d'opt-out qui prévaut sur les sites, c'est-à-dire que l'option est activée par défaut et que la désactiver est compliqué et fastidieux. »

Un avis de la Commission nationale de l'informatique et des libertés (Cnil) de 2009 demandait déjà aux fournisseurs de réseaux publicitaires d'adopter au plus tôt des mécanismes d'opt-in pour informer au préalable la pub ciblée. Cinq ans plus tard, la pratique ne semble pas appliquée par les géants, malgré un relais de l'avis auprès du G29 européen.

« La norme sociale a évolué »
Faut-il baisser les bras face aux pratiques des acteurs du net qui empiètent sur la vie privée ? « La vie privée peut être considérée comme une anomalie », a lâché Vinton Cerf, père fondateur du web devenu « chef évangéliste » chez Google, rejoignant les saillies régulières de Mark Zuckerberg, PDG et cofondateur de Facebook. « Les gens sont désormais à l'aise avec l'idée de partager plus d'informations différentes, de manière plus ouverte et avec plus d'internautes. […] La norme sociale a évolué », a-t-il notamment estimé.

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

Source et suite : http://obsession.nouvelobs.com/high-tech/20141201.OBS6646/vous-avez-peur-de-facebook-mefiez-vous-plutot-de-tout.html

Detekt : l’outil Anti-Espions d’Amnesty International, Digitale Gesellschaft, l’Electronic Frontier Foundation et Privacy International…

Detekt : l’outil Anti-Espions d’Amnesty International…

Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, ont lancé un outil anti-espion : Detekt.

Ce billet a été rédigé par Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

Imaginez que vous n'êtes jamais seul
Quelqu'un regarde par-dessus votre épaule, enregistre toute activité sur votre ordinateur, lit et écoute vos conversations privées sur Skype, allume le microphone et la caméra de votre téléphone portable pour vous surveiller, vous et vos collègues, sans même que vous vous en rendiez compte.
Pour des milliers de défenseurs des droits humains et de journalistes qui, aux quatre coins de la planète, s'efforcent de dévoiler des atteintes aux droits humains et des injustices choquantes, nul besoin de l'imaginer.
Ils sont victimes d'une nouvelle forme sophistiquée de surveillance illégale. Certains gouvernements utilisent déjà des technologies de pointe pour installer des espions virtuels dans leurs bureaux et leurs salons.
La plupart des personnes ciblées ne savent même pas qu'elles sont espionnées, jusqu'à ce qu'on leur montre des copies de courriels et de vidéos où elles apparaissent, avec leurs collègues. Ces documents ont été extraits subrepticement de leurs propres ordinateurs portables. Ces « preuves » refont souvent surface lorsque les militants sont passés à tabac dans des cellules sordides, sanctionnés pour leur travail légitime ou contraints d' »avouer » des crimes qu'ils n'ont pas commis.

Le militant des droits humains et blogueur Ahmed Mansoor est l'un d'entre eux.
Ressortissant des Émirats arabes unis, il a été relâché en 2011. Il avait été incarcéré parce qu'il avait signé une pétition en faveur de la démocratie et animait un forum de discussion en ligne, que le gouvernement avait bloqué un an auparavant sous prétexte qu'il hébergeait des commentaires critiques envers les autorités. Après sa libération, Ahmed Mansoor a découvert que ses déplacements étaient parfois surveillés et a été agressé physiquement à deux reprises. Il s'est plus tard rendu compte que son ordinateur avait été infecté par des logiciels espions qui permettaient aux autorités de surveiller chacun de ses mouvements. Sa messagerie et son compte Twitter étaient également piratés.
Ce type de logiciels espions sophistiqués est l'arme idéale contre les défenseurs des droits humains. Ils sont de plus en plus utilisés dans le monde, même dans des États qui proclament défendre les libertés fondamentales.
Ces logiciels sont développés et produits dans des pays comme le Royaume-Uni, l'Allemagne et l'Italie, pour être ensuite vendus à des gouvernements du monde entier, sans qu'aucune réglementation ne garantisse qu'ils ne serviront pas à faciliter des atteintes aux droits humains.

« Cette nouvelle forme de surveillance semble tout droit sortie de 1984 de George Orwell, et elle rencontre un vif succès. Auparavant, les gouvernements interceptaient des communications ; aujourd'hui, ils peuvent entrer dans les systèmes et tout surveiller comme s'ils se trouvaient dans la pièce », a déclaré Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

Et même si l'Union européenne s'est récemment engagée à adopter des réglementations sur le commerce des équipements de surveillance, cette technologie dangereuse se développe à un rythme effréné.

Detekt
En réaction au nombre croissant de militants arrêtés arbitrairement et interrogés avec violence sur la base d'informations soutirées illégalement, des experts en technologie se sont mis à jouer « au chat et à la souris » pour combattre la surveillance ciblant des personnes qui exercent leur droit à la liberté d'expression et d'association. Certains de ces experts se sont associés avec Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, afin de lancer un nouvel outil.
Detekt est un logiciel simple qui permet d'effectuer une analyse sur un ordinateur fonctionnant avec le système d'exploitation Microsoft Windows pour y trouver la trace de logiciels espions et alerter ses utilisateurs afin qu'ils puissent agir.

Selon Claudio Guarnieri, l'un des cerveaux qui a développé cet outil, Detekt répond à une demande d'aide croissante de la part des militants depuis 2012.

« Nous avons commencé à faire des recherches sur les pays qui commercialisent des équipements de surveillance et avons découvert qu'une société allemande en vendait aux autorités de Bahreïn, qui les avaient utilisés contre les manifestants durant le soulèvement [depuis février 2011]. Tout est parti de là, et cela nous a emmenés vers des pays comme le Maroc, la Tunisie, l'Éthiopie et quelques autres, qui s'en sont eux aussi servis », a déclaré Claudio Guarnieri.

« Tant de pays utilisent désormais ces technologies, qu'il serait plus simple de se pencher sur les autres. Si vous prenez une carte et placez un point rouge sur chaque pays concerné, cela fait froid dans le dos: Bahreïn, le Maroc, les Émirats arabes unis, Oman, l'Éthiopie, le Soudan, l'Ouzbékistan, le Kazakhstan, l'Azerbaïdjan, l'Indonésie, la Malaisie, l'Australie, l'Inde, le Mexique, Panama, le Royaume-Uni et l'Allemagne, entre autres. »

La Coalition contre l'exportation illégale de technologies de surveillance, dont Amnesty International est membre, estime que le commerce mondial des technologies de surveillance représente 4 milliards d'euros par an, et qu'il est en expansion.

FinFisher compte parmi les entreprises qui développent ce type de logiciels espions. Cette société allemande qui a appartenu à l'entreprise britannique Gamma International a conçu le logiciel espion FinSpy, grâce auquel il est possible d'effectuer un suivi des conversations sur Skype, d'extraire des fichiers de disques durs, d'enregistrer toute utilisation du microphone ainsi que les courriels, et même de prendre des captures d'écran et des photos en utilisant la caméra de l'appareil.
Selon des recherches menées par Citizen Lab et des informations rendues publiques par Wikileaks, FinSpy a permis d'espionner des militants et des avocats défenseurs des droits humains à Bahreïn – dont certains vivaient au Royaume-Uni.
C'est le cas de Saeed Al Shehabi, militant politique bahreïnite actuellement installé au Royaume-Uni. En juillet 2014, Privacy International a publié des informations indiquant que Gamma International avait vendu des services de logiciels aux autorités bahreïnites.

« Nous savions que les autorités surveillaient les militants à Bahreïn, mais nous ne pensions pas qu'il leur était possible de le faire ici, au Royaume-Uni. J'ai peur, parce qu'on ne sait jamais quelles informations ils ont recueillis, ni comment ils vont les déformer et s'en servir. Je ne me sens pas du tout en sécurité. Detekt me semble un outil très utile, et inestimable pour des militants comme moi », a déclaré Saeed.

Sécurité et droits humains
Les organisations qui dénoncent la surveillance ciblée illégale sont fréquemment accusées de développer des outils susceptibles d'entraver l'action légitime du gouvernement contre le crime organisé.

Toutefois, les experts comme Claudio Guarnieri s'accordent à dire que le problème est l'absence quasi totale de contrôle, de cadres juridiques et de lignes directrices quant à l'utilisation de ces technologies intrusives.

« La transparence n'est pas de mise pour savoir qui s'en sert et dans quelles circonstances. La seule chose que nous savons, c'est que ces technologies servent souvent à entraver le travail des militants et des journalistes. Nous souhaitons lancer un débat pour tenter de comprendre comment cela fonctionne, car tout se déroule dans le plus grand secret. Il faut plus de transparence sur les implications légales, morales et politiques de l'emploi de ces technologies », a déclaré Claudio Guarnieri.

Nous espérons que Detekt apportera un sentiment de sécurité aux défenseurs des droits humains, aux journalistes, aux avocats et aux militants, et qu'il permettra d'ouvrir le débat sur la nécessité de réglementer le développement, la vente et l'utilisation des technologies de surveillance.

« Ce marché échappe à tout contrôle. Il faut des réglementations légales solides pour qu'il soit en phase avec les normes relatives aux droits humains. Les conséquences négatives et les dangers du recours non réglementé à ces technologies puissantes sont énormes et celles-ci doivent être contrôlées », a déclaré Marek Marczynski.

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

Source : http://www.huffingtonpost.fr/genevieve-garrigos/detekt-un-nouveau-logiciel-dans-le-jeu-du-chat-et-de-la-souris-contre-big-brother_b_6235750.html
par Geneviève Garrigos Présidente Amnesty International France

---

Le système de reconnaissance biométrique du FBI est opérationnel

Le système de reconnaissance biométrique du FBI est opérationnel

Grâce aux outils du système NGI, le FBI pourra retrouver des criminels dans tous les Etats-Unis grâce à une empreinte, un scan d'iris ou une photo.

Le système NGI sera disponible dans tous les Etats-Unis d'ici à la fin 2014.
Après trois années de développement, le nouveau système de reconnaissance biométrique Next Generation Identification system) du FBI est opérationnel a annoncé le Bureau le 15 septembre 2014. Il a été conçu pour améliorer les possibilités d'identification biométriques explique le FBI dans son communiqué.
Il comporte deux nouveaux outils qui viennent s'ajouter aux bases de données d'empreintes digitales et de scans d'iris. Le premier concerne la reconnaissance faciale, l'Interstate Photo System (IPS) et le second, Rap Back, fournit des notifications écrites.

La base contiendra à terme 52 millions de photos.

Rap Back permet à toutes les autorités habilitées de recevoir des informations sur l'historique criminel de toute personne occupant un poste de confiance : un professeur, un conseiller bancaire…, explique le FBI dans son communiqué. Plus question de passer sous silence une arrestation pour conduite en état d'ivresse à 19 ans. Quant à IPS, il permet d'accélérer la recherche de criminels grâce à une base de données qui comptera 52 millions de photos d'ici à 2015.

En avril dernier, l'ONG Electronic Frontier Foundation émettait déjà quelques réserves sur cet outil. En premier lieu, elle dénonçait le mélange des genres puisqu'en plus des photos de criminels, celles de citoyens lambdas se trouvaient dans cette base. Elle s'inquiétait également du risque de « faux positif » compte tenu du taux de fiabilité du système qui n'est que de 85 %.

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

Source :
http://www.01net.com/editorial/626932/le-systeme-de-reconnaissance-biometrique-du-fbi-est-operationnel/#?xtor=EPR-1-NL-01net-Actus-20140916

Cécile Bolesse