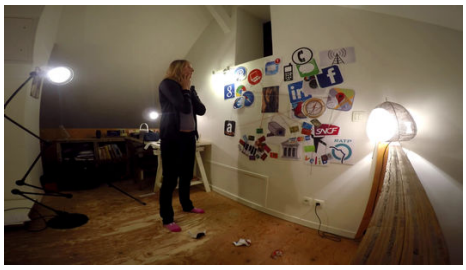
Comment je suis devenu invisible (sur le Net) Replay du 28 mars 23h35

	Comment je suis devenu invisible (sur le Net) Replay du 28 mars 23h35

Peut-on encore, en 2016, échapper à la surveillance de masse sans renoncer totalement aux outils bien pratiques que sont le téléphone et l'ordinateur ? C'est la question que s'est posée la journaliste Alexandra Ranz dans le très efficace documentaire Comment je suis devenue invisible.

Echapper à la surveillance, qu'elle soit « *étatique ou commerciale* », s'avère un véritable parcours du combattant, constate rapidement la journaliste. Si les mesures de base d'« *hygiène numérique* » que lui conseillent des activistes sont simples – utiliser la navigation privée, doter son téléphone d'un mot de passe –, l'ampleur de la surveillance dont elle fait l'objet, comme chacun, la pousse rapidement vers des méthodes plus élaborées.

Le replay sur pluzz.fr jusqu'au dimanche 3 avril 2016

Echapper aux cinquante caméras de vidéosurveillance qu'elle croise sur un trajet à vélo ? C'est possible, mais il faut porter un masque. Naviguer sur Internet de manière anonyme ? Oui, en utilisant le navigateur anonyme Tor. Empêcher la RATP, la SNCF et l'Etat de savoir où elle se rend ? Oui, là encore, à condition d'abandonner son passe Navigo et de payer son billet de transport en liquide. De toute façon, la carte bancaire est un outil de surveillance ultra-performant, qui donne des informations sur tous nos achats : poubelle, là aussi.

Outil de flicage

Reste l'outil de flicage par excellence, qui est aussi l'accessoire indispensable du XXIe siècle : le téléphone portable. Un nettoyage des applications et un réglage précis des paramètres de confidentialité n'y changent pas grand-chose. « *Le réseau des opérateurs mobiles n'est pas du tout sécurisé* », explique le spécialiste Karsten Nohl, lors d'une rencontre des « hacktivistes » du Chaos Computer Club. « *Avec simplement votre numéro de téléphone, on peut savoir où vous êtes* » – démonstration à l'appui. Pire, renchérit le spécialiste en sécurité informatique Bruce Schneier, « *votre téléphone sait avec qui vous couchez si votre partenaire en a un aussi* ». Pour devenir invisible, il faut l'abandonner.

Même en prenant les mesures les plus radicales, impossible de déjouer totalement les yeux qui nous espionnent, car surveillance d'Etat ou des entreprises, tout se mêle. « *Les entreprises qui gèrent les plates-formes collectent en permanence des données sur nous. Qui aurait imaginé que Facebook, destiné à nos loisirs, deviendrait la source principale des services de renseignement ?* », s'étonne David Lyon, professeur de sociologie.

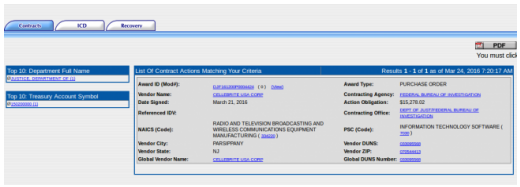
Alors, faute de pouvoir échapper à la surveillance, au moins peut-on lutter contre, et le documentaire nous emmène, dans un certain désordre, à la rencontre de militants. Au Musée de la Stasi, à Berlin, dirigé par un ancien opposant à la police secrète est-allemande, Jörg Drieselmann, la question est évidente : « *Est-ce qu'il y avait des moyens d'échapper à la surveillance ?* » Une longue pause. « *Non. Mes parents m'ont appris dès mon plus jeune âge qu'il fallait que je mente quand j'étais en public : ne dis surtout pas ce que tu penses, dis-leur ce qu'ils veulent entendre. Il n'était pas possible de vivre en RDA sans que cela laisse des séquelles psychiques.* » Restent, cependant, des outils et des attitudes qui fonctionnent, sans devenir asocial ou complotiste, montre le documentaire. Le chiffrement, d'abord, seule protection efficace contre les oreilles indiscrètes. Mais aussi l'action politique, le choix de « *se cacher en subvertissant le système* »… [Lire la suite]

Réagissez à cet article

Source : *Echapper à Big Brother, une gageure*

---

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*

L'innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016

L'innovation, une arme contre le terrorisme ? Emission sur BFM Business du 23 mars 2016

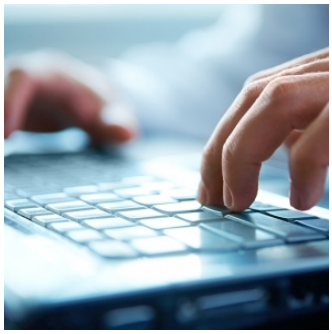
Deuil national en Belgique au lendemain des attaques qui ont fait 31 morts et 270 blessés tandis que l'enquête s'accélère.
Deux frères kamikazes, auteurs des tueries à l'aéroport et dans le métro, ont été identifiés grâce à leurs empreintes digitales. Alors, comment prévenir un nouvel attentat comme celui de Bruxelles ?

La lutte contre le terrorisme passe par le renseignement et la surveillance sur le terrain. Mais les effectifs semblent insuffisants et épuisés. Reconnaissance faciale, logiciels d'analyse comportementale… l'une des armes efficaces contre le terrorisme ne serait-il pas l'innovation ? — Avec: Gérôme Billois, membre et administrateur du CLUSIF. Frédéric Simottel, éditorialiste high-tech BFM Business. Matthieu Marquenet, COO de Smart Me Up. Jean-Baptiste Huet, BFM Business. Et Jean-Louis Missika, adjoint à la mairie de Paris en charge de l'innovation. — Les Décodeurs de l'éco, du mercredi 23 mars 2016, présenté par Fabrice Lundy, sur BFM Business.

Réagissez à cet article

Source : *L'innovation, une arme contre le terrorisme ? — 23/03*

Big Data : gare à vos données personnelles !



Big Data : gare à vos données personnelles !

Les marques, enseignes et sites Web cherchent à capter un maximum d'informations sur leurs clients. Leur objectif ? Vous vendre plus en vous soumettant des offres et promotions personnalisées. À la clé, des bons plans ou du harcèlement ? Débat.

Renseigner votre mail pour participer à un jeu concours, indiquer votre numéro de portable pour ne rater aucune vente privée, ou encore remplir un formulaire pour intégrer un programme de fidélité : il ne se passe pas une semaine où un magasin ou une marque ne vous sollicitent pour obtenir des informations personnelles sur vous, votre famille et vos habitudes de consommation. Et sur le Web, même combat. Les sites Internet ont même un avantage puisqu'ils peuvent obtenir des informations via les fameux cookies et ainsi savoir quel site vous avez visité ou encore quels sont les produits que vous avez regardés sur la Toile.

Peut-être avez-vous déjà remarqué que le fameux ordinateur ou la paire de bottes que vous convoitez se retrouve dans un carré de pub les heures ou les jours suivants votre session de surf ?

Globalement, les Français communiquent facilement et de façon importante des informations sur eux. C'est ce que révèle l'enquête 2015 « Les Français et leurs données personnelles » réalisée par Ipsos pour Elia Consulting. Plus exactement, les résultats démontrent qu'il y a un décalage entre la méfiance grandissante des utilisateurs sans pour autant qu'ils changent leur comportement. Ainsi, paradoxalement, les Français renseignent fréquemment et en quantité leurs données personnelles, malgré leur opposition de principe à leur utilisation par les entreprises et la conscience des risques qui y sont associés. 74% déclarent partager régulièrement des données personnelles, ce qui s'explique souvent par la contrainte de fournir ces informations pour terminer un acte d'achat ou bénéficier d'un service (73% des Français renseignent leurs données personnelles pour terminer un acte d'achat). D'ailleurs, seul un internaute sur trois prend le temps de lire les conditions générales de vente ou de modifier les paramètres de sécurité de leurs réseaux sociaux et smartphones (33% dans les deux cas).

Des données pour quoi faire ?

Les Big Data, ou mégadonnées en français, désignent l'ensemble des informations que l'on peut capter et représentent le nouvel or noir des professionnels. En effet, l'objectif pour ces derniers consiste à bien cerner un client et lui glisser ainsi la bonne offre ou le bon service, au bon moment, et avec le bon prix. Amazon teste même un service aux États-Unis où le client reçoit un produit sans l'avoir commandé, en fonction de son historique d'achats. Libre à lui de le garder – dans ce cas, il sera débité dans les jours suivants – ou de le renvoyer si le produit ne lui convient pas.

En France, nous n'en sommes pas encore là. L'usage des mégadonnées reste encore peu développé, faute de moyens techniques et financiers à allouer à ce sujet. L'idée serait plutôt, dans le secteur du commerce, d'utiliser la « smart data », autrement dit celle qui fera la différence pour déclencher une intention d'achat chez le consommateur.

Pour illustrer l'usage des mégadonnées, prenons un cas pratique avec Monoprix par exemple. L'enseigne envoie à tous les porteurs de la carte de fidélité des bons de réduction. Or, ces fameux coupons nominatifs ont été définis en fonction des informations fournies initialement (genre, âge, situation matrimoniale, etc.) et des derniers achats effectués par le consommateur. Ainsi, un homme n'aura, en théorie, pas de réduction pour du maquillage. Et s'il consomme surtout des plats cuisinés, ces derniers se retrouveront dans ses bons de réductions.

Manque de transparence ?

Toujours selon l'enquête Ipsos, les Français sont parfaitement conscients que leurs données personnelles peuvent être utilisées. D'ailleurs, 9 sondés sur 10 (92%) pensent que les informations qu'ils renseignent peuvent être utilisées ou conservées pour un usage futur par le fournisseur de services. Mais dans la majorité des cas, les Français se sentent mal informés sur l'utilisation qui en est faite.

L'utilisation des données par les professionnels reste en réalité un jeu à double tranchant. En effet, si votre magasin d'électronique préféré vous envoie des promotions qui ne vous intéressent absolument pas, il y a fort à parier que vous allez vite couper toute relation avec lui. Pas forcément ne plus acheter chez lui, mais il ne pourra plus vous contacter pour vous inciter à venir en point de vente ou à vous rendre sur son site Web. Par ailleurs, même si les professionnels ont en leur possession de nombreuses données sur vous, ils font attention à ne pas devenir trop intrusifs. Imaginons que vous êtes en train de chercher un nouveau parfum et que la vendeuse vous lance : « Vous avez acheté depuis deux ans uniquement des fragrances sucrées, celui-ci est très différent ». D'un côté, vous bénéficieriez d'un conseil super personnalisé mais, d'un autre côté, vous réaliseriez que la dame en face de vous que vous ne connaissez pas sait beaucoup de choses sur vous…

Vigilance de mise

Si dans les faits, il devient presque impossible de ne fournir aucune donnée personnelle, il convient, néanmoins, de réfléchir à qui vous les donnez, de vérifier dans les petites lignes à quoi elles serviront, et d'identifier les gains que cela vous apportera. En effet, comme les professionnels veulent un maximum d'informations pour mieux vous cerner, ils proposent… [Lire la suite]

Réagissez à cet article

Source : *Big Data : gare à vos données personnelles !*

Des données personnelles de développeurs trouvés dans des caméras de surveillance

Des données personnelles de développeurs trouvés dans des caméras de surveillance

---

Gmail, Dropbox et comptes FTP, voici ce qu'ont laissé des développeurs dans les entrailles des caméras sur lesquelles ils travaillaient. Des informations personnelles qui montrent le manque de vigilance de ces techniciens, ayant utilisés leurs comptes privés lors du développement de ces caméras… Une affaire qui pourrait faire tâche sur les CV de ces indélicats !

Selon un article de Forbes, des développeurs ayant travaillé sur la création du software pour les caméras Motorola Focus 73 ont fait preuve d'un manque de vigilance flagrant au moment de finaliser leur travail, juste avant la commercialisation de ce modèle. Des experts de « Context Information Security » sont parvenus à accéder aux entrailles des caméras, et on pu en extraire plusieurs informations suprenantes. Les développeurs y avaient laissé trainer leurs identifiants Gmail, Dropbox et FTP d'entreprise.
Les caméra, facilement piratées et contrôlables à distance pour quiconque ayant un minimum de connaissance dans le domaine, ont apporté la preuve de la négligence de ces développeurs, comma l'a expliqué le responsable de Context Information Security :
Les comptes laissés dans le firmware sont apparus comme étant des comptes de développeurs partagés, utilisés pour recevoir les alertes de mouvement et les extraits de vidéo pour leurs tests. Nous n'avons pas accédé à ces comptes pour des raisons légales, mais nous avions tout ce qu'il nous fallait pour le faire. (…) On ne s'attend pas à ce qu'une entreprise de développement utilise ce type de comptes pour ce genre d'activité et ils n'auraient certainement pas du être laissés dans le firmware final.
Un constat d'autant plus affligeant que les mots de passe utilisés pour la sécurité des caméras et ces comptes Gmail sont plus que décevants : « 000000 » ou « 123456 ».

Réagissez à cet article

Source : *Gmail : des données personnelles de développeurs trouvés dans des caméras de surveillance – 1001Web*

Le « friend finder » de Facebook devient illégal en Allemagne

	**Le « friend finder » de Facebook devient illégal en Allemagne**

La plus haute cour de justice allemande a déclaré illégal l'outil de recherche d'amis « friend finder » du réseau social américain Facebook.

Le comité de la Cour fédérale d'Allemagne a jugé que la fonction de recherche d'amis de Facebook viole la loi sur la publicité, a rapporté le journal britannique The Guardian.

© FLICKR/ MOMPL

Facebook: cachez-moi cette sirène que je ne saurais voir!

En accédant au carnet d'adresses de l'utilisateur, le « friend finder » récolte tous les contacts et leur envoie des invitations leur proposant de s'inscrire sur le réseau social. C'est ce mécanisme de collecte d'adresses électroniques et son utilisation dans un but marketing qui a été condamné.

La cour a conclu que cette pratique de marketing était trompeuse, confirmant les décisions de deux tribunaux de Berlin de 2012 et 2014, qui avaient constaté que Facebook violait les lois allemandes sur la protection des données et sur les pratiques commerciales déloyales.

La Cour fédérale a également déclaré que Facebook n'avait pas informé d'une façon adéquate les membres du réseau sur le mécanisme qui utilise les données de leurs contacts.

© AP PHOTO/ DAPD, JOERG KOCH

Facebook dévoile les sujets de discussion les plus populaires en 2015

Le représentant officiel de Facebook en Allemagne a, à son tour, déclaré que la société attendait le rapport explicatif de la décision finale et qu'elle l'étudierait les solutions « pour évaluer tout impact sur les services ».

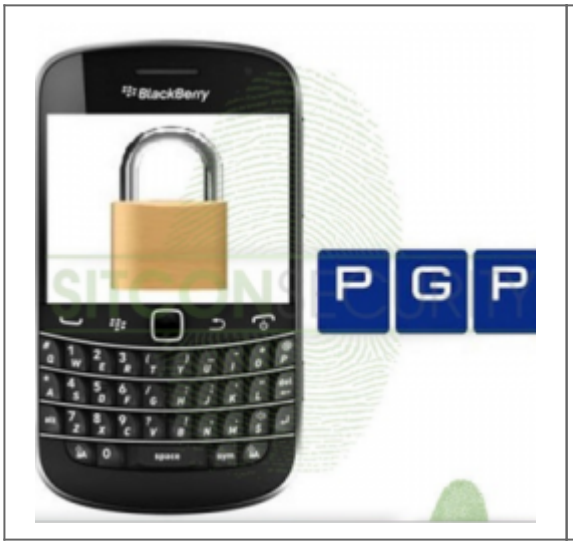
C'est une vraie victoire pour l'association de protection des consommateurs allemands VZBV (Verbraucherzentrale Bundesverband) qui menait ce combat depuis 2010. En outre, elle ne compte pas arrêter sa lutte contre les géant d'Internet et souhaite maintenant vérifier les mécanismes de LinkedIn et Twitter.

« En plus de Facebook, d'autres services utilisent cette forme de publicité pour attirer de nouveaux utilisateurs. Ils doivent maintenant probablement repenser leurs systèmes », a déclaré Klaus Mueller, président de VZBV.

Réagissez à cet article

Source : *Le « friend finder » de Facebook devient illégal en Allemagne*

Les Blackberry PGP déchiffrés par la Police hollandaise



Les Blackberry PGP déchiffrés par la Police hollandaise

Commercialisés par de nombreux vendeurs en ligne, les smartphones Blackberry embarquant en surcouche le standard de chiffrement de messagerie PGP seraient loin d'assurer un échange confidentiel des données. Tout du moins pour la Police hollandaise qui a confirmé être en mesure de les déchiffrer.

Les oreilles des défenseurs de la vie privée vont encore siffler. Des enquêteurs de la Police hollandaise ont en effet confirmé à Motherboard être en mesure d'accéder aux messages chiffrés envoyés depuis un terminal Blackberry sur lesquel le standard de chiffrement PGP est intégré en surcouche. « Nous sommes capables d'obtenir des données chiffrées depuis les terminaux Blackberry PGP », a fait savoir Tuscha Essed, responsable presse du Netherlands Forensic Institute (NFI), qui assiste la Police dans la recherche de preuves pour ses enquêtes en Hollande. L'information était parue initialement en décembre sur le blog misdaadnieuws.com où plusieurs documents sourcés NFI ont été publiés.

Le fait que les emails chiffrés puissent être lus et les messages effacés retrouvés, ne semble en tout cas pas perturber outre mesure les fournisseurs de Blackberry PGP. « Nous n'avons pas été affecté. Nos services sont complètement sécurisés et nous n'avons jamais été compromis », a indiqué un porte-parole de GhostPGP dans un mail à Motherboard. « Nous utilisons le dernier chiffrement PGP du moment qui est aussi impossible à déchiffrer. Nos clients sont très satisfaits du niveau de sécurité fourni », a quant à lui indiqué un représentant de TopPGP.com.

Réagissez à cet article

Source : *Les Blackberry PGP déchiffrés par la Police hollandaise – Le Monde Informatique*

Utiliser Internet à des fins personnelles peut être un motif de licenciement

Utiliser Internet à des fins personnelles peut être un motif de licenciement

---

La justice européenne confirme à nouveau que dans un cercle professionnel, la direction a un droit de regard sur les échanges électroniques des salariés. Les e-mails ou autres services de communication en ligne peuvent être surveillés.

La Cour européenne des droits de l'homme (CEDH) vient de débouter un plaignant dont le licenciement avait été motivé par une utilisation indue de ressources professionnelles. Ce dernier avait utilisé à des fins personnelles, et pendant les heures de travail, des outils professionnels mais également la connexion de l'entreprise, entre autres services en ligne.
Le plaignant, un ingénieur roumain en charge des ventes, utilisait en particulier Yahoo Messenger pour converser avec des clients mais surtout avec des connaissances personnelles. La décision de la Cour met ainsi en avant le fait que l'employé échangeait très régulièrement des messages « avec son frère et sa fiancée et portant sur des questions personnelles telles que sa santé et sa vie sexuelle ».
La société a mis fin au contrat de son collaborateur au motif que son règlement intérieur interdisait l'usage de ces mêmes ressources à des fins personnelles. Cet argument a été soutenu par la justice d'autant qu'elle ne qualifie pas d'abusif le fait qu'un employeur souhaite vérifier que ses employés accomplissent leurs tâches professionnelles pendant les heures de travail.

Stress travail e-mail email

La CEDH estime donc que la surveillance des communications du salarié était légitime dans la mesure où elle est considérée comme raisonnable. Cela signifie que l'employeur a cherché à préserver la productivité de ses salariés sans pour autant instaurer de politique rigide de surveillance des communications. La Cour précise que cette attention portée à l'encontre du collaborateur était organisée dans le cadre d'une procédure disciplinaire.
En France, le régime est très similaire. La justice valide régulièrement des licenciements lorsque des salariés utilisent trop souvent leurs outils informatiques pour des motifs personnels. Il est en général question de navigations régulières et conséquentes pour des tâches qui ne sont en rien en rapport avec le travail.

Réagissez à cet article

Source : *Utiliser Internet à des fins personnelles peut être un motif de licenciement*

Plus fort que les cookies, découvrez les super-cookies

	***Plus fort que les cookies, découvrez les super-cookies***

Dans un précédent bulletin d'actualité [1], était présenté comment les cookies HTTP (ou témoins de connexion), pouvaient être utilisés à des fins de profilage de l'utilisateur, dans le but notamment de pouvoir lui proposer du contenu ciblé. Après un bref rappel, cet article se propose de parcourir plus largement les mécanismes complémentaires existants à l'heure actuelle, à des fins de sensibilisation aux problématiques de vie privée sur l'Internet, et dans l'optique de permettre la prise des précautions d'usage adaptées à son utilisation au quotidien, dans un contexte professionnel comme personnel.

Techniques de pistage – Cookies – et évolutions

La technique la plus utilisée en matière de pistage d'utilisateurs sur l'Internet repose sur l'exploitation des cookies. Nous rappelons que le terme cookie désigne une variable utilisée par un serveur HTTP pour sauvegarder des informations sur la session HTTP courante. Il est composé d'une paire obligatoire nom/valeur, et d'attributs optionnels, comme la date d'expiration, le domaine et le chemin. Ces informations sont créées et mises à jour lors des échanges entre un serveur et un client Web grâce à des en-têtes dédiés du protocole HTTP (« Set-Cookie », « Cookie ») [2].
Le premier cas d'usage des cookies est tout à fait nécessaire à la navigation sur de nombreux sites Web, par exemple pour le maintien d'une session applicative ou la mémorisation d'un panier d'achats, on parle alors de « cookies de premier niveau ». Il existe cependant d'autres cas d'utilisations controversés sur le plan du respect de la vie privée. En particulier, l'usage de « cookies tiers » (ou « tierce partie ») [1], notamment dans l'optique d'établir des statistiques de consultation, peut permettre par exemple d'offrir des services de publicité ciblée. Ces cookies sont reconnaissables en particulier à leur domaine d'appartenance différent de celui de la page consultée, et peuvent parfois permettre d'identifier finement un utilisateur donné (par exemple cookies Google).

D'autres mécanismes permettent la conservation de données utilisateur, qui exploitent d'autres modes de création et de stockage que les cookies HTTP. On regroupe généralement ceux-ci sous le terme « supercookie ». Ils s'appuient notamment sur l'utilisation :
• mécanismes de stockage local dédiés à des applications Web au-dessus du protocole HTTP, comme Adobe Flash (« Local Shared Objects », également appelés « cookies Flash »), Microsoft Silverlight (« Silverlight Isolated Storage ») ou encore HTML5 (« HTML5 storage ») ;
• d'objets dans le contenu des pages Web, comme la propriété « window.name » en JavaScript, qui peut être détournée pour stocker temporairement des informations ;
• du cache du navigateur et de l'historique de navigation, pour stocker sous forme encodée des informations ;
• de HSTS (« HTTP Strict Transport Security ») [3], mécanisme de politique de sécurité pour HTTP, permettant à un serveur de demander le passage vers HTTPS via un champ d'en-tête HTTP (« Strict-Transport-Security »), mais dont une utilisation détournée permet à tiers contrôlant plusieurs domaines d'identifier de façon unique un utilisateur [4].

Cette liste, non exhaustive, montre bien qu'il existe de nombreuses façons de stocker des données issues de la navigation Web, et qu'un simple nettoyage des cookies HTTP via le navigateur ne peut pas suffire à effacer proprement l'ensemble de celles-ci. D'ailleurs, on parle de « cookie zombie » pour désigner des cookies HTTP qui sont régénérés après leur suppression grâce à l'utilisation des supercookies. L'application Evercookie [5], par exemple, illustre cela, permettant la propagation des cookies HTTP dans autant que mécanisme de stockage que possible afin d'assurer la résilience de l'information.

Autres techniques
Si les cookies (et assimilés) permettent d'obtenir une masse d'informations très intéressante, ils ne sont pas pour autant la seule source considérée par les entités cherchant à pister l'utilisateur. Il existe en particulier de nombreuses autres méthodes permettant d'identifier de façon unique un utilisateur, parfois à la granularité du terminal utilisé (téléphone, ordinateur, téléviseur connecté, tablette, etc.).
Ces méthodes peuvent être classées en cinq catégories [6] :
• entification générée par le client : certains terminaux ou applications clientes génèrent un identifiant unique pouvant être accessible par les services tiers à des fins publicitaires (advertising identifiers).
• Identification via des éléments réseau : certains équipements réseau situés entre le client et le serveur insèrent des éléments permettant, volontairement ou non, d'identifier l'utilisateur. Par exemple, l'utilisation du champ « X-Forwarded-For » dans l'en-tête HTTP précise l'adresse IP d'origine d'un client se connectant à travers un serveur mandataire.
• Identification par le serveur : certains serveurs ajoutent des pixels-espions [7], images de très petite taille généralement non repérables par l'utilisateur, qui permettent la génération de cookies tiers.
• Identification unique : certains services permettent à l'utilisateur de s'authentifier pour accéder à un ensemble de ressources (sites, applications), induisant ainsi la création d'un identifiant unique, censé faciliter la navigation (unique portail d'authentification, gestion des préférences utilisateur, etc.). On peut citer par exemple Facebook Connect, Windows Live ID, Google Account, etc.
• Identification statistique : certaines données issues du navigateur, de l'application ou encore du système d'exploitation permettent le calcul d'une empreinte entraînant la capacité à singulariser l'utilisateur. Ce calcul peut par exemple s'appuyer sur le User-Agent, la valeur du champ HTTP Accept, la politique de gestion des cookies, la résolution de l'écran, ou encore les extensions installées [8].

La directive 2002/58 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9][10] précise que l'utilisation de cookies est autorisée à condition que l'utilisateur se voie donner des informations claires et précises sur la finalité de ces cookies ainsi que les informations placées sur l'équipement terminal qu'il utilise. L'utilisateur pourra refuser l'utilisation de ces dispositifs, cependant cette disposition ne fait pas obstacle au stockage de données utilisées à des fins exclusivement techniques.
Techniquement, des solutions amont ont été proposées, comme l'en-tête HTTP « Do Not Track » (DNT, 2009), pour permettre d'indiquer à un site web qu'un utilisateur ne souhaite pas être tracé. Cependant, bien qu'intégré dans tous les navigateurs modernes, il est purement déclaratif et peut être ignoré par le site visité.
D'un point de vue pratique, une des solutions les plus simples afin de limiter ces traces est de bloquer les cookies tiers. Ces cookies ne sont généralement pas utiles pour la navigation et il est recommandé de les refuser par défaut [11].
Enfin, de nombreuses extensions pour navigateur permettent de limiter le suivi d'un utilisateur existant. Elles ont principalement pour effet :
• blocage des traceurs (DoNotTrackME, Disconnect, uBlock Origin, AdBlock),
• le blocage des scripts (NoScript, ScriptNo),
• la génération de fausses informations afin de brouiller le calcul des empreintes numériques (Random Agent Spoofer),
• le basculement automatique vers HTTPS si disponible (HTTPS Everywhere).

Références

Bulletin d'actualité CERTA-2010-ACT-005 (05 février 2010)
http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-005/CERTA-2010-ACT-005.html
RFC 6265 (HTTP State Management Mechanism) (avril 2011)
https://www.rfc-editor.org/rfc/rfc6265.txt
RFC 6797 (HSTS) (novembre 2012)
https://tools.ietf.org/html/rfc6797##section-14.9
How HSTS supercookies make you choose between privacy or security (02 février 2015)
https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
Evercookie (github)
https://github.com/samyk/evercookie
IAB Cookie White Paper (janvier 2014)
http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
Web beacon (9 janvier 2014)
https://www.iab.net/wiki/index.php/Web_beacon
Browser uniqueness
https://panopticlick.eff.org/browser-uniqueness.pdf
Directive 2002/58/CE (12 juillet 2002)
http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
Sites web, cookies et autres traceurs (CNIL)
http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/
Conseils aux internautes (CNIL)
http://www.cnil.fr/vos-droits/vos-traces/les-cookies/conseils-aux-internautes/

Vulnérabilités critiques au sein de Juniper ScreenOS

Contexte

Le 18/12/2015, le CERT-FR a émis l'alerte CERTFR-2015-ALE-014 [1] concernant plusieurs vulnérabilités critiques impactant le système ScreenOS des équipements Juniper. D'après le bulletin de sécurité publié par Juniper [2], ces vulnérabilités ont été découvertes suite à un audit de code interne et auraient été introduites volontairement pour affaiblir la sécurité de ScreenOS. Il s'agit en l'occurrence de deux portes dérobées qui permettent de :
– contourner le mécanisme d'authentification en place au niveau des services SSH et Telnet,
– déchiffrer les communications entre un client et le service VPN d'un équipement Juniper vulnérable.

Marqueurs de détection

La société Fox-It propose des signatures au format Snort afin d'identifier toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée. Ces signatures sont cependant limitées au service Telnet. De plus, la vulnérabilité liée au service VPN étant exploitable après une interception passive du trafic chiffré, il n'est pas possible de détecter son exploitation.
Versions affectées
La porte dérobée permettant d'accéder à l'interface d'administration de l'équipement via le protocole Telnet ou SSH impacte le logiciel Juniper ScreenOS de la version 6.3.0r17 à 6.3.0r20.
La vulnérabilité permettant de déchiffrer les communications réseau liées au service VPN impacte le logiciel Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18 et les versions 6.3.0r12 à 6.3.0r20.
Ces vulnérabilités permettant un accès illégitime sont respectivement référencées par les identifiants CVE-2015-7755 et CVE-2015-7756.

Description des portes dérobées

CVE-2015-7755
La porte dérobée permettant d'accéder à l'interface d'administration d'un équipement Juniper vulnérable est localisée au sein du code de vérification des identifiants de connexion. Ce code compare le mot de passe saisie par l'utilisateur avec une chaîne de caractère codée en dur dans le système ScreenOS. Si elles sont identiques, l'accès est autorisé.
CVE-2015-7756
La seconde porte dérobée reposait sur une faiblesse du générateur de nombres aléatoires utilisé par l'algorithme de chiffrement et permettait à un attaquant d'accéder au contenu des communications VPN, obtenues à partir d'une écoute passive du trafic réseau.

Corrections

Le CERT-FR recommande d'appliquer les mesures préconisées dans le bulletin d'alerte CERTFR-2015-ALE-014.

Documentation

1
Bulletin d'alerte du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-014/index.html
2
Bulletin de sécurité de l'éditeur :
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
3
Versions de ScreenOS vulnérable :
https://isc.sans.edu/diary/Infocon+Yellow%3A+Juniper+Backdoor+(CVE-2015-7755+and+CVE-2015-7756)/20521
1 – Rappel des avis émis
Dans la période du 21 au 27 décembre 2015, le CERT-FR a émis les publications suivantes :
CERTFR-2015-ALE-015 : Campagne de messages électroniques non sollicités de type TeslaCrypt
CERTFR-2015-AVI-554 : Multiples vulnérabilités dans le noyau Linux de Debian
CERTFR-2015-AVI-555 : Vulnérabilité dans VMWare
CERTFR-2015-AVI-556 : Multiples vulnérabilités dans Citrix XenServer
CERTFR-2015-AVI-557 : Multiples vulnérabilités dans Cisco IOS et IOS XE
CERTFR-2015-AVI-558 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
CERTFR-2015-AVI-559 : Vulnérabilité dans Xen
CERTFR-2015-AVI-560 : Vulnérabilité dans Cisco IOS XE
CERTFR-2015-AVI-561 : Multiples vulnérabilités dans le noyau Linux de Fedora
CERTFR-2015-AVI-562 : Multiples vulnérabilités dans ISC Bind
CERTFR-2015-AVI-563 : Multiples vulnérabilités dans le noyau Linux de SUSE
Durant la même période, les publications suivantes ont été mises à jour :
CERTFR-2015-ALE-014-1 : Vulnérabilité dans Juniper ScreenOS (ajout de règles Snort dans les contournements provisoires.)
Gestion détaillée du document
28 décembre 2015 version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-052
CERT-FR
2015-12-28

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-052*

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*