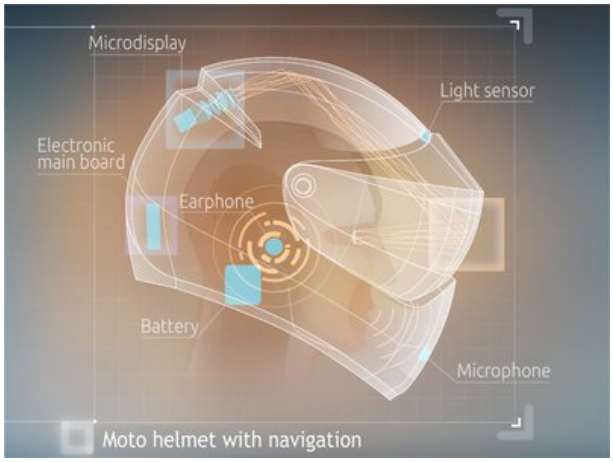
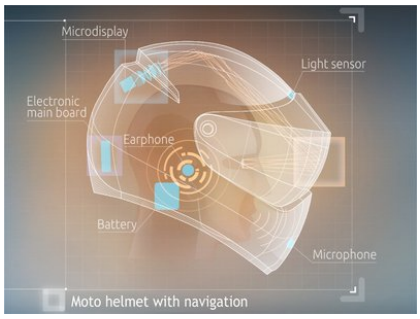
Un casque moto connecté à réalité augmentée prévu pour cet été



Un casque moto connecté à réalité augmentée, prévu pour cet été

La société russe Livemap annonce avoir levé 300 000 dollars pour commercialiser son produit phare. La sortie de son casque de moto affichant des éléments visuels sur la visière du conducteur est prévue pour cet été.

La société russe Livemap développe un produit très particulier pour les conducteurs de deux-roues. Il s'agit d'un casque intégrant plusieurs technologies comme la réalité augmentée ou encore, le contrôle de services grâce à la voix. Le dispositif peut se relier au GPS et afficher un itinéraire sur la visière du conducteur.



Après avoir développé de premiers concepts, la start-up indique que son produit est désormais prêt à être commercialisé. Elle précise au site américain Techcrunch avoir levé la somme de 300 000 dollars auprès du ministère des Sciences de Russie, afin de procéder à la mise sur le marché de son dispositif.
Grâce à ces fonds, Livemap indique s'être notamment concentrée sur le dispositif permettant de projeter des images sur la visière. Son dernier prototype devrait être présenté au printemps prochain, pour une commercialisation au trimestre suivant.

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

Source : http://pro.clubic.com/actualite-e-business/investissement/actualite-746953-casque-moto-realite-augmentee-levee-fonds.html
Par Olivier Robillart

Obsolescence programmée – Dénoncez et ne soyez plus complice

Obsolescence programmée – Dénoncez et ne soyez plus complice

L'obsolescence programmée regroupe l'ensemble des techniques visant à réduire la durée de vie ou d'utilisation d'un produit afin d'en augmenter le taux de remplacement.La demande ainsi induite profitera au producteur, ou à ses concurrents, ce qui explique certains cas de cartels. Le secteur bénéficie alors d'une production plus importante, stimulant les gains de productivité et le progrès technique, qui accélère l'obsolescence des produits antérieurs.Cette stratégie n'est pas sans risques car elle implique un effort de recherche et développement, n'allant pas toujours dans le sens d'une amélioration du produit.
Il y a également un impact écologique direct. L'obsolescence programmée visant la surconsommation, elle est la cause d'un surplus de déchets, indépendamment de l'état de fonctionnement effectif des produits techniques mis au rebut ou de l'état d'usure des objets d'usage. Les circuits de recyclage ou de conditionnement des matières plastiques et des métaux, en particulier, ne prennent pas en charge le stockage des déchets informatiques, malgré l'abondance de matières premières de valeur qu'ils peuvent contenir comme le fer, l'aluminium, les métaux rares, etc.
L'exportation en masse de déchets des pays de grande consommation vers des zones géographiques où le stockage est négociable à moindre coût est d'autant plus problématique et expose classiquement les pays receveurs à des pollutions spécifiques sur les sites de décharge de grande envergure.
L'enquête de Cash Investigation dévoile la face cachée de l'obsolescence programmée, ou comment les fabricants d'électroménagers, de téléphones portables ou d'ordinateurs font souvent tout pour limiter la durée de vie de leurs produits. Pourquoi ? Pour que les consommateurs en rachètent toujours plus, et toujours plus rapidement.
Cash Investigation a notamment enquêté sur le géant Apple et d'autres grandes marques. Vous découvrirez que les techniques de l'obsolescence programmée sont variées et sophistiquées. Les conséquences sont claires, une surconsommation généralisée et au bout de la chaîne, de gros dégâts environnementaux pour la planète.

Cash Investigation – La mort programmée de nos appareils
Emission diffusée sur France 2 le 22 Octobre 2012
présentée par Elise LUCET

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

Source : http://www.inexplique-endebat.com/article-cash-investigation-la-mort-programmee-de-nos-appareils-le-lobby-du-sel-106398577.html

Des cybercriminels dérobent 25M$ à des banques russes

	Des cybercriminels dérobent 25M$ à des banques russes

Un groupe de cybercriminels baptisé Anunak a réussi à infiltrer les réseaux informatiques et à détourner les distributeurs automatiques d'institutions bancaires en Russie et dans des pays voisins. Il a également ciblé des terminaux point de vente de revendeurs américains et européens.

Un groupe de cybercriminels très aguerris a volé plus de 25 millions de dollars en piratant l'infrastructure de plusieurs institutions financières russes et de pays de l'ancien bloc soviétique, et en détournant des systèmes de points de vente appartenant à des revendeurs américains et européens. Des chercheurs de l'entreprise russe spécialisée dans la cybercriminalité Group-IB, et de l'entreprise de sécurité néerlandaise Fox-IT, ont baptisé le groupe Anunak, d'après le malware qui a servi de base au set d'outils utilisé par les pirates.
En général, les cybercriminels ciblent les clients des institutions financières, mais le groupe Anunak s'est attaqué directement aux institutions elles-mêmes, s'infiltrant dans leurs réseaux informatiques, jusqu'aux postes de travail et aux serveurs. Grâce à cet accès, le groupe a pu transférer des fonds sur des comptes dont ils avaient le contrôle, réussissant même dans certains cas, à détourner des distributeurs de billets automatiques sur lesquels ils ont pu ensuite retirer frauduleusement de l'argent. « Depuis 2013, ce groupe est parvenu à infiltrer les réseaux de plus de 50 banques russes et de 5 systèmes de paiement, et deux de ces institutions ont été privées de leur licence bancaire », a déclaré l'entreprise de sécurité russe Group-IB dans un rapport publié lundi. « À ce jour, le montant total du vol dépasse le milliard de roubles (environ 25 millions de dollars), la plus grande partie ayant été volée au cours du second semestre de 2014 ».

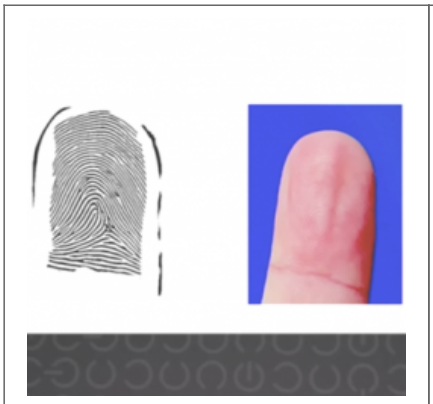
Un arsenal d'outils au service du piratage
Tout commence par l'infection des ordinateurs des salariés avec des logiciels malveillants, lesquels servent ensuite de point d'accès au réseau interne, aux serveurs et aux comptes de domaine actifs. Et le groupe Anunak ne lésine pas sur les outils : scanners de réseau, keyloggers, logiciels pour cracker les mots de passe, backdoors SSH, programmes de contrôle à distance, avec en plus, la plupart du temps, le framework Metasploit pour tester les failles et réaliser des exploits. Mais, leur principal outil est un cheval de Troie nommé Anunak. Celui-ci est basé sur le malware Carberp, conçu pour dérober des informations d'identification sur les sites de banque en ligne et dont le code source a été rendu public en juin 2013. Les chercheurs de Group-IB pensent que le groupe Anunak comprend sûrement des membres de l'ancien gang Carberp, éclaté en 2013 après des conflits internes.
Les attaquants utilisent plusieurs méthodes pour infecter les ordinateurs avec le Trojan Anunak. Par exemple, le téléchargement de logiciels malveillant quand les ordinateurs se connectent à certains sites (autrement appelé drive-by downloads) via des kits d'exploits (les chercheurs pensent que le groupe a injecté du code malveillant sur le site php.net en 2013 pour attaquer les visiteurs) ; des faux e-mails avec des pièces jointes malveillantes à en-tête de la Banque centrale de la Fédération de Russie ; l'installation d'autres programmes malveillants en utilisant les services de botnets. « Les cybercriminels sont de mèche avec plusieurs propriétaires de botnets pour diffuser massivement leurs programmes malveillants », ont expliqué les chercheurs de Group-IB. « Ils achètent aux propriétaires de botnets des informations sur les adresses IP des ordinateurs sur lesquels il y a déjà des logiciels malveillants contrôlés par le botnet et ils vérifient si les adresses IP appartiennent à des institutions financières ou gouvernementales. Si le malware du botnet se trouve dans les plages d'adresses que le groupe veut cibler, ils paient le propriétaire du réseau de zombies pour qu'il diffuse leur logiciel malveillant ».

Le vol de données de cartes de crédit confirmé
Depuis le début du second trimestre 2014, le groupe Anunak a également ciblé des revendeurs aux États-Unis, en Australie et en Europe, l'objectif étant d'infecter les terminaux points de vente avec leurs logiciels malveillants et de voler des données de cartes de paiement au moment des transactions. « Plus d'une quinzaine de violations potentielles ont été identifiées, dont une douzaine aux États-Unis, et le vol de données de cartes de crédit a été confirmé dans trois de ces cas », ont déclaré les chercheurs dans leur rapport. Le groupe a également compromis les ordinateurs de trois entreprises du secteur des relations publiques et des médias basées aux États-Unis. « Ils cherchaient peut-être des informations qu'ils pouvaient exploiter sur le marché boursier », ont déclaré les chercheurs. « Nous n'avons aucune preuve du piratage de banques en Europe occidentale ou aux États-Unis, mais les attaquants peuvent très bien utiliser les mêmes méthodes pour cibler des banques hors de Russie », ont mis en garde les chercheurs.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cybercriminels-derobent-25m$-a-des-banques-russes-59699.html
Par Jean Elyan

Un hacker parvient à reproduire des empreintes digitales à partir de photos



Un hacker parvient à reproduire des empreintes digitales à partir de photos

Il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales.

On savait déjà quil était possible de récupérer les empreintes digitales d'une personne ayant touché une surface lisse, comme un verre ou un smartphone. Mais un hacker allemand a montré qu'il était possible de voler ces caractéristiques biométriques spécifiques à partir d'une simple photo.
Lors de la 31e convention annuelle (27-30 décembre, Hambourg, Allemagne) du Chaos Computer Club, la plus grande association de hackers européens, un hacker du nom de Jan Krissler, également connu sous le pseudonyme de « Starbug », a expliqué comment reproduire les empreintes digitales d'une personne à partir de simples photos.
Pour sa démonstration, il a copié l'empreinte de la ministre de la Défense allemande, Ursula Von der Leyen.
En effet, il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales. Étant donné que ces empreintes peuvent être utilisées pour l'authentification biométrique, « Starbug » estime que sa démonstration va vraisemblablement obliger « les politiciens à porter des gants lors de leurs apparitions publiques ».
Pour réussir son exploit, Jan Krissler a utilisé le logiciel VeriFinger disponible dans le commerce. Comme source, il est reparti d'un gros plan du pouce de la ministre, pris lors d'une conférence de presse donnée en octobre dernier, plus d'autres photos prises sous des angles différents pour restituer une image complète de l'empreinte digitale.

Si la méthode est aussi facile à réaliser que ce qu'a montré le hacker, elle pourrait remettre en question l'usage des empreintes digitales pour la sécurisation de certains accès. Et dans ce cas, il faut garder ces options de détournement en mémoire. Mais, même si la reproduction des empreintes digitales s'avère viable pour forcer l'accès d'un système, aussi bien un smartphone qu'un lieu très sécurisé, l'exploit accompli par le hacker au 31C3 ne signifie pas pour autant que leur usage est devenu brusquement obsolète.
Les systèmes de sécurité parfaits n'existent pas, et les empreintes digitales ont encore leur place dans la sécurisation des systèmes. Dans un grand nombre de situations, on peut renforcer la sécurité en ajoutant des codes PIN, et il est toujours temps de coupler les solutions biométriques existantes avec des codes ou d'autres protections par mots de passe pour multiplier les niveaux de sécurité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-hacker-parvient-a-reproduire-des-empreintes-digitales-a-partir-de-photos-59753.html
Par Jean Elyan

Les hackers iraniens montent en puissance

Les hackers iraniens montent en puissance

Les pirates informatiques iraniens montent en puissance et ont déjà dérobé des données « hautement sensibles » lors d'attaques contre des gouvernements et des entreprises aux Etats-Unis, en Chine ou en France, affirme aujourd'hui une société américaine de cyber-sécurité. « A mesure que les capacités de l'Iran en matière de cyber-attaque se transforment, la probabilité d'une attaque qui aurait un impact dans le monde réel, à un niveau national ou mondial, augmente très rapidement », met en garde Cylance.

Selon son rapport, l'opération « Cleaver » menée depuis deux ans par des hackers basés à Téhéran leur a déjà permis de conduire une « importante campagne d'infiltration et de surveillance » dans une longue liste de pays qui compte également Israël, l'Arabie Saoudite, l'Allemagne ou l'Inde. Leurs attaques ont ciblé les gouvernements mais également les entreprises du secteur militaire ou pétrolier ainsi que des infrastructures stratégiques (aéroports, hôpitaux…), énumère la société qui affirme avoir des « preuves » que la sécurité aérienne a été par exemple particulièrement « compromise » en Corée du Sud et au Pakistan.

« Les capacités techniques de l'opération Cleaver évoluent plus vite que toutes les précédentes tentatives iraniennes », assure Cylance, selon qui cette offensive répond aux cyber-attaques subies par Téhéran en provenance d'Israël ou des Etats-Unis et visant son programme nucléaire controversé. L'attaque du virus informatique « Stuxnet », qui avait frappé l'Iran vers 2010-2011, aurait ainsi « ouvert les yeux » des autorités de Téhéran en révélant leur vulnérabilité et les a conduits à « contre-attaquer » en lançant l'opération « Cleaver », explique le rapport, selon qui le soutien du régime à cette offensive ne fait aucun doute.

Plusieurs grandes entreprises américaines, dont Apple ou la banque JPMorgan ont récemment été victimes de cyber-attaques dont l'origine n'a pas été formellement identifiée, suscitant des mises en garde croissantes des autorités.

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

Source : http://www.lefigaro.fr/flash-actu/2014/12/03/97001-20141203FILWWW00452-les-hackers-iraniens-montent-en-puissance.php
Par Gilbert Kallenborn

Reprenez le contrôle de votre identité en ligne avec IndieHosters

Reprenez le contrôle de votre identité en ligne avec IndieHosters

Quand on s'inscrit avec un des géants du web comme Google ou Facebook, on souscrit à beaucoup plus qu'un seul service. On peut par exemple utiliser les mêmes identifiants pour s'enregistrer partout sur le web. C'est très pratique. Sauf que si votre compte se fait un jour pirater ou supprimer, vous perdez votre mail et tous les accès aux différents services que vous utilisez. IndieHosters veut vous aider à reprendre le contrôle de votre identité en ligne sans perdre le côté pratique.

Il existe de nombreuses alternatives aux identifications de Facebook et Google. Elles s'appellent OpenID ou Mozilla Personna. Le problème avec ces outils, c'est qu'ils demandent d'être hébergés sur un serveur en ligne et qu'ils doivent être régulièrement mis à jour. Les compétences techniques demandées dépassent bien souvent les bases des internautes avertis et c'est une galère qui décourage même les utilisateurs les plus motivés.
Aujourd'hui, si vous allez chez un hébergeur connu comme OVH ou Gandi, vous aurez droit en un seul clic à une adresse mail, un hébergement pour un site web, une base de données et WordPress ou quelques logiciels libres.
IndieHosters veut aller encore plus loin en proposant tous les outils qui vous permettent de gérer votre identité en ligne. Et pour garantir la confidentialité des données, ils vous offrent en prime un certificat TSL (identique à celui utilisé pour les opérations bancaires en ligne par exemple). Vos données vous appartiennent et elles ne sont pas accessibles pour l'hébergeur. Et comme vous bénéficiez d'un serveur chez IndieHosters, vous pouvez également en profiter pour créer votre blog.
Quand vous souscrivez chez IndieHosters, le serveur se trouve chez une personne et vous pouvez déménager de serveur en allant chez quelqu'un d'autre en un seul clic. Pour l'instant, ils ne sont que 2 chez IndieHosters : Pierre Ozoux et Michiel de Jong. Dans les mois qui viennent, IndieHosters accueillera de nouveaux hébergeurs indépendants et proposera de plus en plus de logiciels libres accessibles et administrables par des débutants, comme Owncloud, la solution alternative à Dropbox.
Pour se développer, ils ont lancé une campagne de financement participatif sur IndieGogo. Et j'ai rencontré Pierre Ozoux alors qu'il était de passage à Toulouse pour qu'il m'explique son projet.
Le but avoué d'IndieHosters est que chaque personne puisse créer son propre nom de domaine, son adresse email, son système d'enregistrement en ligne et finisse un jour par quitter Google, Facebook et consorts. Si vous voulez rejoindre ce mouvement, dépêchez-vous, la campagne de financement se termine dans quelques jours seulement.

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

Source : http://www.gizmodo.fr/2014/12/18/reprenez-le-controle-de-votre-identite-en-ligne-avec-indiehosters.html

---

MegaChat : la messagerie anti-NSA signée Kim Dotcom

MegaChat : la messagerie anti-NSA signée Kim Dotcom

Le sulfureux fondateur du défunt MegaUpload annonce le lancement d'une messagerie chiffrée capable d'échapper à la curiosité des services de renseignement, NSA en tête.

Kim DotCom signe son retour. Après avoir – en apparence du moins – négocié l'arrêt des attaques par déni de service contre les réseaux Sony PlayStation et Xbox Live avec les hackers de la Lizard Squad, le sulfureux fondateur du défunt site de téléchargement MegaUpload promet l'arrivée imminente d'un nouveau service de messagerie électronique et de discussion instantanée sécurisé par chiffrement. Un service baptisé MegaChat qui entre dans la croisade de Kim Dotcom visant à garantir aux internautes une confidentialité totale de leurs échanges numérique. Rappelons que ce dernier a déjà lancé un service de stockage chiffré, Mega.
Pour passer à travers les mailles du filet de la NSA et d'autres services de renseignement, cette alternative cryptée à Skype permettra aux internautes, dès début 2015, d'utiliser cette messagerie ultra-sécurisée dotée de fonctionnalités d'appels audio et de visioconférence.
Elle autorisa également « le transfert de fichiers à haute vitesse via un navigateur Web », a promis Kim Dotcom, dans un message publié sur Twitter. Pas besoin donc d'installer un logiciel spécifique sur son ordinateur ou sa tablette, notent nos confrères d'ITespresso. De manière sécurisée, les utilisateurs pourront, grâce au chiffrement intégral des données, envoyer, lire et partager des fichiers (audio, vidéos,…).

« Skype est obligé de fournir des backdoors »
« Vous ne pouvez faire confiance à aucun fournisseur de services en ligne installé aux Etats-Unis pour [garantir la confidentialité] de vos données », a souligné Kim Dotcom. « Skype n'a pas le choix. Ils sont obligés de fournir des backdoors au gouvernement américain ». A en croire l'homme d'affaires d'origine allemande, MegaChat serait donc un des seuls services Internet capables de garantir l'intégrité des données de ses membres, et de les préserver des manœuvres d'espionnage des autorités gouvernementales, Etats-Unis en tête.
Rappelons que selon des informations relayées par Der Spiegel et issues des documents confidentiels dévoilés par Edward Snowden, la NSA a réussi à contourner, dès la fin 2011, la sécurité de Skype pour permettre à l'agence américaine de mettre en place une collecte de données à grande échelle sur le système de communications, propriété de Microsoft.

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

Source : http://www.silicon.fr/megachat-messagerie-anti-nsa-kim-dotcom-104829.html

---

Accès administratif aux données de connexion: rassuré

avec le décret ?

	Accès administratif aux données de connexion: rassuré avec le décret ?

Le décret sur l'accès administratif aux données de connexion, en lien avec l'article 20 de la LPM, a été publié le 24 décembre. La cyber-surveillance tend à se généraliser malgré la vigilance de la CNIL.

C'est un grand classique quel que soit le gouvernement : la tentation de faire passer des décrets juste avant Noël pour éviter de faire trop de bruit. Mais le tour de passe-passe n'a pas échappé à des médias vigilants sur la protection de la vie privée comme NextInpact.

Dans le JORF en date du 26 décembre, on découvre le décret 2014-1576 « relatif à l'accès administratif aux données de connexion » (qui avait été approuvé le 24 décembre).
Une belle tentative de mettre en œuvre en catimini d'ici le premier janvier 2015 ce qui avait provoqué une polémique sur la protection des droits civils à l'ère numérique dans le cadre de l'examen du projet de loi sur la programmation militaire (LPM).
Adopté en décembre 2013, le texte dense intègre un article 20 au contour flou qui a des répercussions sur la vie civile : l'accès par les autorités – sans décision judiciaire – aux données de connexion des internautes.
Une approche qui suscitait des craintes sur l'encadrement de l'accès aux données à caractère personnel. Gare à la dérive cyber-sécuritaire, estimait des associations professionnelles du secteur IT comme Renaissance Numérique ou l'ASIC à l'époque.
Ainsi, la loi prévoit initialement l'accès par l'administration aux « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques ». Le champ des données surveillées n'était pas limité aux seules données de connexion, mais pouvait concerner l'ensemble des données stockées par l'utilisateur : documents sur le cloud, mails, échanges sur les réseaux sociaux, pseudos, mots de passé, etc.

L'élargissement de la cyber-surveillance reste d'actualité avec la publication du décret associé à l'article 20 de la LPM. Le régime d'exception de l'accès administratif aux données de connexion – jusqu'ici associé principalement à la lutte antiterroriste – est généralisé : « Les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses et sont accessibles à un nombre de plus en plus important d'organismes. »
Et ce, pour des finalités très différentes » au nom de divers intérêts nationaux : « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

Le spectre du Big Brother serait écarté partiellement avec les nouveaux éléments fournis dans le décret du 24 décembre sur « l'accès administratif aux données de connexion ». Celui-ci limite la collecte d'information aux données de connexion (identité de la personne, date et heure de communication, etc.) mais il reste néanmoins à préciser l'exact périmètre des données recueillies.

Bonne nouvelle : le décret semble écarter les risques de droit de regard sur les contenus.
De même, la DGSE, la DGSI ou tout autre service de police judiciaire ne pourront pas directement installer des logiciels d'espionnage (« mouchards ») de manière intensive sur les réseaux des opérateurs.
Selon l'avis de la CNIL rendu le 4 décembre (sur ce qui était à l'époque un projet de décret) mais qui vient juste d'être publié dans le prolongement de la promulgation du décret, il en résulte que « cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes ».
L'autorité française en charge de la protection des données personnelles reste vigilante. « Elle appelle l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques. »
L'année 2015 va mal démarrer alors que le gouvernement prépare une loi sur le numérique. L'occasion d'éclaircir le débat ? Dans le cadre de la consultation gouvernementale ouverte au grand public pour élaborer cette loi, on espère un peu plus de transparence à propos de cette extension de la cyber-surveillance.

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

Source : http://www.itespresso.fr/acces-administratif-donnees-connexion-rassure-publication-decret-85710.html

Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

	Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

Ils sont de plus en plus jeunes et stupides puisque incapables d'évaluer les risques liés à l'objet de leurs forfaits. Avec la création de la cellule de lutte contre la cybercriminalité, nombre d'entre eux apprennent désormais à leurs dépens que certains actes ne restent jamais impunis.

Les faits remontent au lundi 15 septembre 2014 dans la zone ACI, une cité résidentielle censée pourtant être sous surveillance accrue au regard de ses occupants, pour la plupart, des ressortissants étrangers (missions diplomatiques, organisations internationales, etc.). Mais qu'importe pour les malfrats désormais regaillardis par les nombreuses failles du dispositif sécuritaire dans la capitale et surtout, par des décisions pour le moins controversées des plus hautes autorités de la République.
C'est donc en plein jour, aux environs de 14 heures dans la zone indiquée que trois individus armés ont envahi un magasin de vente de téléphones portables de grandes valeurs et autres accessoirs electroniques dont des clés USB, des chargeurs, des puces, cartes mémoires, etc.
Les deux premiers tinrent la gérante en joue pendant que le troisième dévalisait litteralement la boutique. Ils purent ainsi emporter des appareils d'une valeur marchande de plusieurs dizaines de milliers de nos francs ainsi que la somme de 35.000 F CFA en espèces. Et ils repartirent sans être inquietés. Mission accomplie? Loin s'en fallait !

La victime décida de porter plainte contre X au niveau de la Brigade d'Investigation judiciaire (BIJ) et, naturellement, la nature des objets volés aidant, l'affaire fut confiée à la Cellule de lutte contre la Cybercriminalité dirigée par l'Inspecteur divisionnaire Papa Mambi Keïta surnommé « l'Epervier du Mandé». Commença alors la cyber-traque !

Nous ne cesserons jamais de le dire: les objets électroniques sont de véritables traîtres. Ils sont susceptibles de tout révéler sur leurs propres utilisateurs. Et le saviez-vous ? Il est même possible d'ouvrir le micro de certains téléphones à distances. Quant aux puces, cartes mémoires ou clés USB, elles peuvent être également activées de loin. A ce stade, certains commentateurs comparent déjà notre époque à celle décrite par l'auteur de roman de science fiction, Georges Orwell dans «1984» avec le fameux « Big Brother » désormais présent dans la légende contemporainne*.
Naturellement, ces méthodes de surveillance necessitent des équipements adéquats, une collboration accrue des services techniques et surtout, une bonne dose d'intelligence; un aspect de la question qui ne fait nullement défaut au niveau de la cellule de lutte contre la cybercriminalité.

Mettant ainsi toutes ces aptitudes à contribtion, les enquêteurs parvinrent à identifier un nommé Souleymane Doumbia comme utilisateur d'un des objets volés. Il fut interpellé dans les heures qui suivront et sa victime l'identifia formellement comme étant un de ses agresseurs. Il était inutile de nier les faits. Mais comment diantre les enquêteurs sont-ils parvenus jusqu'à lui ? C'est bien la question qu'il se pose encore à l'heure actuelle. Difficile de trouver réponse à cette intérrogation. Et pour cause, « Big Brother » est passé par là. Ses complices, quant eux, attendent à leur tour d'être arrêtés. Une question de jours.

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

Source : http://maliactu.net/mali-arrestation-de-braqueurs-dans-la-zone-aci-big-brother-est-passe-par-la/

Doit-on avoir peur de Facebook ?

Doit-on avoir peur de Facebook ?

Tous les jours vous utilisez Facebook et tous les jours vous donnez au réseau social de nouvelle informations sur vous. Tout ce que vous faîtes est observé de près et analysé par le site. Alors, devez-vous avoir peur de Facebook ?

Facebook sait tout de vous. C'est un fait. En vous inscrivant sur le réseau social, vous fournissez de nombreuses informations vous concernant à l'entreprise de Mark Zuckerberg. Votre âge, votre nom, votre ville, votre sexe, mais ce n'est pas tout puisque, à chaque fois que vous publiez un message, un statut, que vous ajoutez un ami ou aimez une publication, Facebook le sait. Si vous avez activé la géolocalisation sur votre smartphone ou sur votre tablette, Facebook sait également où vous vous trouvez. Si vous cliquez sur un lien Public Ados sur Facebook, le réseau social sait que vous avez lu tel article, à telle heure, sur tel appareil, depuis tel endroit…

A quoi servent vos données ?
Mais alors, que fait Facebook avec toutes ces données sur vous. Et bien il les revend. Car ne l'oublions pas, le seul but de Facebook est de faire de l'argent, aucunement d'être un gentil samaritain qui permet aux amis de rester en contact. Facebook revend vos données à des annonceurs, qui peuvent ainsi cibler avec précision un public donné. Si une marque de cosmétiques française souhaite faire une campagne de pub destinée aux 15-20 ans, Facebook peut lui vendre un encart publicitaire optimisé, qui s'adressera seulement à la cible visée. Facebook enverra donc cette pub uniquement aux jeunes filles qui ont entre 15 et 20 ans, qui résident en France et qui suivent déjà des actualités liées à la mode.

Facebook s'engage à vous garder anonyme.
Toutefois, lorsque Facebook vend vos données, il s'engage à vous rendre anonyme. Ainsi, il peut dire à une marque que vous êtes une femme de 17 ans célibataire qui vit à Marseille, qui aime la mode et qui a 453 amis Facebook. Mais aucunement le réseaux social n'a le droit de communiquer le fait que vous vous appelez Marie Duchnoc, que vous êtes en couple avec Martin Truc et que votre numéro de téléphone est le 06 XX XX XX XX. En vous inscrivant sur Facebook vous avez accepté ce principe.

Supprimer vos données
La seule solution pour ne plus être espionné par Facebook, c'est se désabonner du réseau social. Toutefois, il peut y avoir un délai entre votre désinscription et la suppression de vos données. Un délai de 90 jours précise le site dans sa charte de confidentialité. Et même ce délai passé, il peut rester des traces de votre passage sur le site.
En effet, le message que vous avez envoyé à votre meilleure copine Marjorie le 6 avril 2011 à 15h42 sera conservé tant que votre copine Marjorie sera inscrite sur Facebook. Car ce message fait également partie de ses données à elle. Vous l'aurez compris, le système est tentaculaire. Autant dire qu'il est très difficile d'effacer l'intégralité de vos données du réseau social.

Litige avec Facebook
Mais n'oubliez pas que vous êtes le seul et unique propriétaire de vos données. En vous inscrivant sur Facebook vous acceptez uniquement que le réseau social les utilise. Il n'en est pas propriétaire. Si vous estimez que Facebook va trop loin avec vos données, que le réseau social à manqué à l'un de ses engagements, comme vous garantir l'anonymat à la revente de vos données, vous pouvez toujours les contacter via la page d'aide du site. Si la réponse que Facebook vous apporte ne vous convient pas, vous n'aurez qu'une seule solution : contacter un avocat et engager une procédure judiciaire. Toutefois, cela risque de vous coûter très cher, et Facebook, lui, a les moyens de se payer un procès.

Récupérer vos données
Vous pouvez également télécharger vos données Facebook afin de voir ce que le site sait sur vous via l'onglet « Paramètres » > « Général » > « Télécharger une copie de vos données sur Facebook ». Vous recevrez par mail l'intégralité de vos données Facebook. Tout ceci vous appartient, vous en faîtes ce que vous voulez, à l'exception bien sûr des photos que vous n'avez pas prises vous même (si vous avez uploadé des photos prises sur Google Image par exemple). N'allez surtout pas revendre la photo de Rihanna que vous aviez mise en photo de profil, sauf bien sûr si vous l'avez prise vous même… Ne faites pas avec les données des autres ce que vous ne voulez pas que Facebook fasse avec les autres !

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

Source : http://actu.ados.fr/news/facebook-confidentialite-charte-donnees-vente_article6861.html
Par Edouard Riaud