Les CNIL européennes haussent le ton contre le pistage de Facebook

Les CNIL européennes haussent le ton contre le pistage de Facebook

Après une décision de la justice belge, d'autres pays européens réclament que Facebook cesse de traquer les internautes en dehors de ses pages.

Facebook n'est pas encore sorti du bourbier européen.

L'autorité française de protection des données (la CNIL) a publié lundi une déclaration commune avec quatre de ses homologues européens concernant les règles de confidentialité du réseau social.

Elle fait suite à une décision de la justice belge, qui a demandé à Facebook de ne plus tracer les internautes non-inscrits sur le site américain. L'entreprise a finalement obtempéré il y a une semaine, en empêchant toute personne sur le territoire belge déconnectée du site d'accéder à ses pages.

Pas encore suffisant pour les cinq CNIL des Pays-Bas, de la France, de l'Espagne, de Hambourg et de la Belgique, qui réclament la généralisation du dispositif. «Le groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne», précise le communiqué.

Mesures de sécurité

En Belgique, la justice contestait l'utilisation par Facebook d'un «cookie», un micro-fichier qui conserve les données ou habitudes des internautes, baptisé «datr».

Principale critique: cette collecte concerne les personnes ne disposant pas de compte Facebook, et qui ne consentent donc pas à ce suivi. Il suffit de visiter une page du site (par exemple un évènement public) pour se voir déposer ce cookie sur son ordinateur et mobile. Facebook est ensuite capable de connaître les fréquentations en ligne de l'internaute, s'il se rend sur des sites contenant des modules du réseau social, comme le bouton «like».

De son côté, Facebook affirme qu'il collecte des cookies pour des raisons de sécurité. «Nous les utilisons afin de distinguer les véritables visites des fausses», expliquait la semaine dernière Alex Stamos, en charge de la sécurité chez Facebook. «Depuis cinq ans, ces cookies nous servent à empêcher la création de faux comptes, d'empêcher le vol de données ou l'organisation d'attaques par déni de service.» Facebook précise que ces cookies sont utilisés afin de surveiller le comportement d'un navigateur Web, et non d'un utilisateur précis. Pour Alex Stamos, «si le cookie nous informe qu'un navigateur a visité des centaines de sites en cinq minutes, cela nous indique qu'il s'agit probablement d'un robot».

Facebook a ajouté qu'il comptait faire appel de la décision de la justice belge et qu'il était prêt à discuter du sujet du cookie «datr» avec les autres autorités de protection des données.

Le groupe des CNIL européennes dénonce lui une «ingérence dans la vie privée des internautes» qui «n'est pas acceptable». Il réclame à Facebook de «prendre les mesures nécessaires pour se mettre en conformité avec la législation européenne, et ce sur tout le territoire de l'Union européenne.»

Le groupe enquête depuis presque un an sur les règles de confidentialité de Facebook. Ces investigations sont menées par chacune des CNIL, mais coordonnées par le groupe de contact. Leurs conclusions ne devraient pas être rendues avant l'année prochaine.

Réagissez à cet article

Source : http://www.lefigaro.fr/secteur/high-tech/2015/12/07/32001-20151207ARTFIG00299-les-cnil-europeennes-haussent-le-ton-contre-le-pistage-de-facebook.php

Objets connectés : les Français sont séduits mais restent méfiants

Objets connectés : les Français sont séduits mais restent méfiants

---

L'internet des objets, terrain de jeu de nombreuses start-up et d'entreprises industrielles, entre doucement dans les habitudes de consommation des Français.

Réalisé par le Credoc pour le compte du Conseil général de l'économie (CGE) et de l'Autorité de régulation des communications électroniques et des postes (Arcep), le baromètre du numérique 2015 vient de paraître.
Cette enquête, destinée à faire le point sur la diffusion des technologies de l'information dans la société française, s'est notamment portée sur l'accueil réservé par les consommateurs aux objets connectés.
Il en ressort que 6 % des Français utilisent déjà des outils leur permettant de commander à distance des appareils électroniques présents à leur domicile. Un chiffre qui reste modeste et qui n'a augmenté que de deux points depuis la dernière étude réalisée en 2011.
Sans surprise, les jeunes adultes (8 %), les plus diplômés (8 %), les cadres supérieurs (13 %) et les habitants de la région parisienne (10 %) sont les plus friands de ces solutions domotiques. Quant à leur adoption prochaine, 33 % des Français déclarent l'envisager (contre 25 % en 2011). Les 12 à 17 ans (60 %), les hauts revenus (40 %) et les habitants de la région parisienne (40 %) sont sur ce point les plus catégoriques.

Un frein sur les objets connectés « santé »
La santé est un des principaux axes de développement de l'Internet des objets. Interrogés sur ces solutions, les Français les considèrent comme intéressantes lorsqu'elles sont destinées à recueillir des données permettant d'améliorer leur état de santé (28 %), à mieux gérer leur poids (24 %) ou bien leur sommeil (21 %).
En revanche, ils font preuve, à une écrasante majorité, d'une réelle défiance vis-à-vis des entreprises qui fabriquent et commercialisent ces objets connectés. 83 % estiment ainsi qu'elles feront un usage commercial des informations recueillies sur leur santé. Une opinion très ancrée chez les cadres supérieurs (92 %) et les plus diplômés (91 %). En outre, 78 % considèrent que ces entreprises sont incapables de garantir une parfaite protection de ces données personnelles et privées.

-

Réagissez à cet article
Source : http://business.lesechos.fr/entrepreneurs/web/7000261-objets-connectes-les-francais-sont-seduits-mais-restent-mefiants-205224.php

---

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela est une nouvelle messagerie qui prétend qu'elle peut cacher les métadonnées. Le concept est encore très expérimental, mais il est assez prometteur.

Vuvuzela est un concept de messagerie qui permet de communiquer en cachant les métadonnées. Elle est développé par David Lazar, un doctorant du MIT qui travaille sur le chiffrement et les systèmes distribués. Il a publié un papier qui décrit les principes de Vuvuzela.
Des protocoles comme TOR permettent d'avoir un certain anonymat, mais il reste vulnérable à une analyse du trafic. Avec Vuvuzela, la messagerie est spécialement conçue pour se protéger contre la surveillance gouvernementale sur les métadonnées. La NSA a admis a plusieurs reprises qu'il ne sert à rien de chiffrer les données si les métadonnées sont en clair.

Les métadonnées englobe de nombreuses informations, mais on peut les résumer par le fait qu'elle pointent vers l'identité d'une personne et les contacts de cette personne. Vuvuzela veut cacher les métadonnées, mais elle ne peut pas cacher 2 métadonnées. La première est le nombre d'utilisateurs connectés sans une conversation et la seconde concerne les utilisateurs actifs dans une conversation. Mais Vuvuzela réduit également ce problème en ajoutant des nuisances aux métadonnées.
Le concept est intéressant, mais il n'est pas prêt pour le déploiement. On peut suivre le projet sur Github.

Réagissez à cet article
Source : http://actualite.housseniawriting.com/technologie/2015/12/04/vuvuzela-une-messagerie-qui-cache-les-metadonnees/11327/

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html

Près de la moitié des Français confrontés à la cybercriminalité

Près de la moitié des Français confrontés à la cybercriminalité

Ransomware ou vol des données bancaires : près d'un Français sur deux (47%) a déjà été victime de cybercriminalité au cours de sa vie, selon l'étude annuelle Norton/Symantec révélée par Le Parisien / Aujourd'hui en France.

La cybercriminalité touche plus particulièrement les Français, puisque seulement quatre Européens sur dix sont confrontés à ce phénomène.
En détail, plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant qui permet au cybercriminel de demander de l'argent aux utilisateurs en échange de la décontamination de leur ordinateur, alors que 20% des Français confient avoir été victimes du vol de leurs données bancaires.
Ce rapport montre que les Français sont particulièrement méfiants vis-à-vis de la cybercriminalité. Plus de la moitié des sondés (55%) ont aujourd'hui plus peur de se faire voler leurs données bancaires en ligne que de se faire subtiliser leur portefeuille.
Plus de 17.000 consommateurs dans le monde ont été sondé cet automne pour les besoins de cette étude.

Réagissez à cet article
Source : http://www.lejdc.fr/france-monde/actualites/societe/techno/2015/11/30/pres-de-la-moitie-des-francais-confrontes-a-la-cybercriminalite_11685497.html

---

Le ransomware CryptoWall donne la migraine aux forces

de l’ordre

Le #ransomware CryptoWall donne la migraine aux forces de l’ordre

Bâti sur un labyrinthe de serveurs proxy, ce botnet est, pour l'instant, difficile à neutraliser. Pour se protéger, il faut faire des sauvegardes, mais pas n'importe comment.

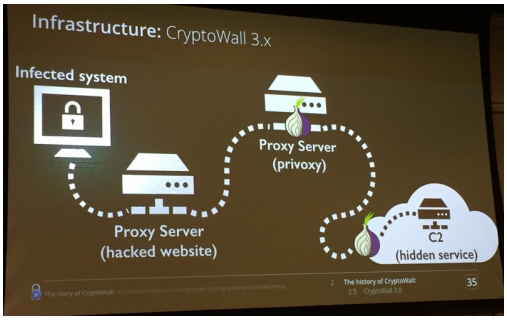
C'est l'un des plus importants « rançongiciels » du moment, et il le sera certainement encore pour un bout de temps. Car les pirates qui se cachent derrière ce néfaste malware ont mis en place un système pour l'instant assez inviolable et diaboliquement efficace. Bienvenue dans l'univers de CryptoWall.

Le chercheur en sécurité Yonathan Klijnsma de la société Fox IT est l'un de ceux qui essayent de pister ses auteurs. Il a profité de la conférence Botconf 2015, qui se déroule actuellement à Paris, pour présenter ses dernières analyses.

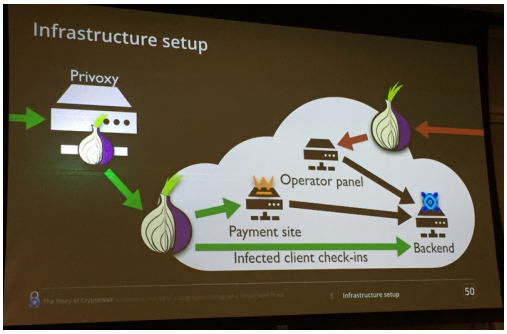
GK — Yonathan Klijnsma

Sur le principe, CryptoWall — qui existe actuellement dans sa version 4.0 — n'a rien d'original. Apparu pour la première fois en novembre 2013, ce code malveillant fonctionne un peu comme son aïeul Cryptolocker. Il infecte les ordinateurs et chiffre les fichiers qui s'y trouvent, ainsi que les noms de ces fichiers. Pour cela, il s'appuie sur les algorithmes AES 256bit et RSA 2048bit. Pour avoir une chance de récupérer ses données, il faut passer à la caisse. Plusieurs moyens de paiement sont acceptés : bitcoin, litecoin, UKash, moneypak, paysafecard, etc.
Ce qui rend ce malware si difficile à terrasser, c'est son infrastructure sous-jacente, composée d'une multitude de serveurs proxy en cascade, des intermédiaires qui servent essentiellement à brouiller les pistes. *« C'est un vrai labyrinthe. On ne sait jamais si la ressource que l'on a détectée est le véritable serveur de commande et contrôle, ou simplement un autre proxy »*, explique Yonathan Klijnsma.

Autre subtilité : le premier niveau de proxy est constitué de serveurs Web piratés. *« Ce sont de vrais sites totalement légitimes. Les propriétaires, évidemment, ne savent pas que leurs serveurs ont été détournés par des pirates. C'est assez malin de leur part, car cela complique le démantèlement du botnet. On ne peut pas simplement tirer le cordon. Il faut contacter chaque administrateur un par un »*, souligne le chercheur en sécurité.



© DR



© DR

Derrière le serveur Web piraté se trouve un autre proxy qui va faire le lien avec le réseau d'anonymisation Tor, dans lequel les pirates ont planqué toute leur infrastructure d'administration : les clés de chiffrement, le paiement, la diffusion de malware, etc. Tous ces « services » sont créés sous la forme de services Tor cachés (Tor Hidden Service). *« Pour les forces de l'ordre, c'est techniquement très difficile d'identifier les serveurs qui se cachent derrière »*, souligne Yonathan Klijnsma.
Pour avoir une chance de démanteler le réseau, il faut donc utiliser des méthodes d'investigation plus classiques, par exemple en infiltrant des forums de discussion. Mais cette méthode prend du temps et n'est pas forcément couronnée de succès.

Pour l'instant, ce cyberracket constitue donc quasiment le crime parfait. Les auteurs sont tellement insouciants qu'ils n'hésitent pas à se moquer ouvertement de leurs victimes, en les félicitant — sur l'un des écrans d'alerte — d'avoir rejoint *« la grande communauté CryptoWall »*.

Un malware d'origine russe ?

Certains éléments techniques semblent indiquer que les auteurs de CryptoWall — ou une partie d'entre eux — se trouvent en Russie. Un mécanisme dans le code évite, en effet, qu'il ne s'installe sur des ordinateurs qui se trouvent en Russie, en Biélorussie, en Ukraine ou au Kazakhstan. Ce type d'exception est typique pour des cybercriminels qui ne souhaitent pas avoir de problèmes avec les forces de l'ordre locales. *« En même temps, on ne peut jamais être sûr à 100 %. Cela pourrait être un faux indice »*, ajoute le chercheur.
En tant qu'utilisateur, pour se prémunir contre un fléau tel que CryptoWall ou consorts, le mieux c'est de faire des sauvegardes régulières de ses fichiers. Mais attention : pas n'importe comment. Il faut éviter les sauvegardes automatiques sur un disque en réseau sur lequel l'ordinateur est connecté en permanence. *« Dans ce cas, le malware ne va pas seulement chiffrer le contenu de l'ordinateur, mais aussi les sauvegardes »*, explique le chercheur. L'idéal, c'est donc de faire des sauvegardes régulières, mais à la main.

Réagissez à cet article
Source : http://www.01net.com/actualites/cryptowall-le-ransomware-qui-donne-la-migraine-aux-forces-de-l-ordre-934345.html
Gilbert KALLENBORN

La menace cyber-terroriste n’a jamais été aussi vaste

La menace cyber-terroriste n’a jamais été aussi vaste

Général d'Armée, Marc Watin-Augouard a cofondé en 2007 le Forum international de la cyber-sécurité. À l'heure des attentats, il revient sur les menaces de cyber-terrorisme qui pèsent sur les entreprises.

Le cyber-terrorisme est-il une réalité aujourd'hui ?

On le voit apparaître aujourd'hui autour de quatre phénomènes. Le premier, c'est l'atteinte aux contenus, comme l'effacement de sites. Suite aux attentats de janvier, 19.000 sites ont été effacés en France suite à des intrusions sur les serveurs, avec parfois la modification de données pour diffuser de la propagande ou de l'incitation au terrorisme. Le second phénomène, c'est l'utilisation du web par les terroristes à des fins d'organisation. Daesh n'aurait pas son visage actuel s'il n'existait pas un réseau mondial lui permettant de diffuser de l'information et des ordres. Le troisième aspect, c'est le recours des terroristes à la criminalité du cyber-espace pour se financer : vols de données bancaires, escroquerie, etc. Enfin, même si c'est une menace encore rare, il existe un danger d'attaque visant à bloquer ou saboter du matériel : en 2012, 30.000 ordinateurs de l'entreprise saoudienne Saudi Aramco ont été détruits à distance par des activistes. La menace cyber-terroriste n'a donc jamais été aussi vaste.

Toutes les entreprises peuvent-elles être concernées par ces menaces ?

Il ne faut jamais oublier que si une entreprise peut être une cible potentielle, elle peut être aussi un vecteur qu'on utilise pour mener une attaque en rebond. Regardez la chaîne américaine de magasins Target, qui a été victime en 2014 d'une cyber-attaque massive : elle a été touchée parce qu'on s'est d'abord infiltré chez un prestataire qui s'occupait de la climatisation des points de vente. Une entreprise peut donc être visée simplement parce qu'elle est sous-traitante de la « vraie » cible.

Quel est aujourd'hui le niveau de préparation des entreprises françaises face à ces cyber-menaces ?

Il y a une prise de conscience : nos entreprises sont en train de prendre très au sérieux ces dangers. C'est le cas tout d'abord des opérateurs d'importance vitale, qui travaillent dans les secteurs critiques, et qui doivent mettre en place des règles dans le cas de la loi de programmation militaire. Ces règles doivent d'ailleurs être aussi respectées par leurs sous-traitants, ce qui créé un effet de diffusion de l'hygiène informatique. Les entreprises ont également en face d'elles des assureurs qui s'intéressent de plus en plus à ces risques. Aujourd'hui, beaucoup d'entreprises s'organisent donc en commençant à faire remonter à l'échelon stratégique ce qui était considéré parfois comme un simple rouage technique. C'est positif.

Le problème, c'est que la cyber-sécurité coûte cher…

Oui, elle a un prix, mais les résultats d'une cyber-attaque aussi. Il y a des arbitrages à opérer. Mais si l'on se plonge dans le guide de l'hygiène informatique publié par l'Agence nationale de la sécurité des systèmes informatiques, on voit que nombre de ces prescriptions ne coûtent rien. Et qu'elles permettent d'annihiler 85 % des risques. Cela débute souvent avec la sensibilisation des personnels : une grande partie des cyberattaques est le fait de collaborateurs malveillants ou d'erreurs humaines dont les personnels sont les porteurs. L'arnaque de l'escroquerie au président commence par exemple par une interaction humaine. Le bon sens, l'organisation, la réflexion, cela n'a pas de coût.

Née dans la foulée des attentats de janvier, la loi sur le renseignement a brusqué les entreprises du numérique, notamment avec ces « mouchards » que sont les boîtes noires susceptibles d'aspirer des données. Comment réagissez-vous ?

Je comprends qu'on puisse dire que c'est une mauvaise loi, mais c'est de loin la meilleure. Et face aux problèmes qui sont aujourd'hui les nôtres, la question d'une éventuelle évasion à l'étranger de clients qui craindraient pour la confidentialité de leurs données me semble dépassée depuis quelques jours. On a trop souvent compris que cette loi reposait sur l'aspiration massive de données, ce n'est pas le cas : les boites noires ne transmettent pas de données nominatives et n'agissent que lorsque des algorithmes signalent des signaux faibles de comportement terroriste. Le point positif, c'est que cette loi amène opérateurs et hébergeurs à dialoguer avec l'État et que cela crée une co-responsabilité qui aidera à lutter contre les cyber-menaces.

Justement, n'y a t'il pas un problème de culture du web : né du militaire, il a aussi pris un virage libertaire. Comment concilier ces deux visages ?

Dans une pile électrique, il y'a deux pôles opposés, mais leur interaction crée la lumière. C'est la même chose dans le cyber-espace : il y a deux pôles, un sécuritaire et un libertaire. La peur est la fille de la sécurité, l'audace est la fille de la liberté. Il nous faut trouver la sagesse, l'équilibre. Aujourd'hui, nous avons besoin d'entendre les deux voix, et notamment celle des libertaires qui disent qu'il ne faut pas faire n'importe quoi au nom de la sécurité absolue. Le trop sécuritaire tuerait en effet le potentiel de croissance du web. Mais un cyber espace sans règles serait dominé par la loi du plus fort, avec des conceptions de la justice parfois très différentes. Dans le contexte actuel, il ne faut pas laisser les choses partir dans tous les sens : les actions contre Daesh menées par les Anonymous nous « arrangent » aujourd'hui, mais elles peuvent nous porter préjudice demain. Un des enjeux majeurs, c'est d'harmoniser la régulation mondiale du web. C'est une urgence. Il faut mettre fin au Far-West.

Réagissez à cet article

Source : http://www.lejournaldesentreprises.com/editions/44/chutier/la-menace-cyber-terroriste-n-a-jamais-ete-aussi-vaste-04-12-2015-275472.php

---

Le français Seolane détecte et neutralise les drones

malveillants

Le français Seolane détecte et neutralise les drones malveillants

L'entreprise a développé une station fixe au sol qui détecte la signature électromagnétique de ces engins volants. Sa solution intègre aussi un drone volant fourni par le groupe Eca qui se chargera d'identifier et de filmer le pilote avec une caméra embarquée.

Ce drone intervient dès lors que la station fixe a détecté un drone malveillant. © Seolane

Le survol illégal de drones au-dessus de bases militaires, centrales nucléaires et autres sites sensibles a mis à jour la nécessité d'identifier et de neutraliser les intrus. « *Ce marché devrait peser d'ici cinq ans entre 500 millions et un milliard d'euros* », estime Wilfrid Rouger, le fondateur et directeur général de Seolane une PME française créée en 2007 à Maisons-Laffitte (Yvelines).
Constituée d'une dizaine de personnes, l'entreprise est spécialisée dans l'intégration de systèmes de détection de signaux et de géolocalisation pour le transport et la sécurité. Le mois dernier, elle a remporté la première édition du concours Startup Challenge organisé le mois dernier par le salon Milipol, dédié à la sûreté des Etats.
Le prix récompense sa solution Dronelnt qui détecte, caractérise, traque et neutralise les drones malveillants avec une station fixe au sol. En cas de survol illégal d'un site, cette dernière va détecter la signature électromagnétique du drone et le localiser par radiogoniométrie. Une technique qui recourt à plusieurs capteurs pour localiser la position du drone par triangulation.

Drone fourni par Eca.

« *Nous avons lancé ce développement technologique il y a deux ans* », indique Wilfrid Rouger. Ce dernier a noué un partenariat avec le groupe Eca qui fournit un drone d'intervention. Fonctionnant de concert avec la station au sol, ce dernier dispose d'une autonomie allant jusqu'à 1h30 selon le modèle. Pour identifier le pilote et le filmer, l'engin volant embarque une caméra qui fonctionne de jour comme de nuit.
« *Plusieurs tests ont été réalisés avec succès avec la Gendarmerie nationale sur différents sites dont une centrale nucléaire* », fait valoir le directeur général de Seolane qui reçoit des demandes provenant de sites Seveso, aéroports et autres bases militaires qui s'inquiètent de l'explosion annoncée des vols illégaux de drones et des menaces terroristes.

Réagissez à cet article
Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article,I1602,Zoom-c1901a7c9c9d76e3b257db6e81734942.htm
Par Eliane Kan

Les 7 cyber menaces les plus exploitées chaque jour | Le

Net Expert Informatique

Les 7 cyber menaces les plus exploitées chaque jour

Les cyber-attaques qui frappent les Etats ou les grandes entreprises ont beau être celles qui font le plus régulièrement l’actualité, les cybercriminels usent tout autant de techniques d’escroqueries plus basiques mais tout aussi efficaces, ciblant les individus. La plupart des gens n’étant pas assez informés sur les cyber menaces ou ne suivant pas les mesures de cybersécurité classiques, restent la proie des hackers via des failles pourtant très connues, et exposent leur entreprise à des attaques beaucoup plus importantes.

A ceux qui se reconnaîtraient – ou l’un de leurs collègues ou amis – dans l’un des 7 profils décrit ci-dessous, il est encore temps de perfectionner vos compétences en matière de cybersécurité !

J’ai tendance à cliquer très (trop) rapidement
Un clic peut être suffisant pour être infecté par un virus ou pour être redirigé vers un site web malicieux. Les hackers sont très bons pour créer des contenus destinés à leurrer les utilisateurs et les inviter à cliquer. Ce contenu piégé peut être un message important – paraissant venir d’une personne ou d’une société que vous connaissez bien et en laquelle vous avez confiance – technique que l’on appelle le spear phishing. Il peut aussi simplement s’agir d’un spam, d’une publicité proposant une promotion trop belle pour être vraie ou encore d’une fausse enquête vous demandant de donner certaines informations personnelles.
Aussi, avant de cliquer, une bonne précaution à prendre est de survoler le lien hypertexte avec sa souris pour voir apparaître l’URL de destination et ainsi vérifier sa légitimité. Les liens de phishing incluent toujours une petite erreur dans l’écriture du lien qui va donc mener vers un site factice ou infecter votre PC avec un malware. Deuxième précaution : portez plus d’attention aux comportements inhabituels. Une entreprise connue ne demande jamais des mots de passe et autres informations sensibles et n’envoie pas d’emails comportant des fautes d’orthographe ou des images de mauvaise qualité, etc. En d’autres termes, au moindre doute, ne cliquez pas !

J’ignore toujours les demandes de mises à jour
Les fournisseurs de solutions de sécurité investissent en permanence pour renforcer la sécurité de leurs produits face aux cyber-attaques et publient des patchs et mises à jour pour résoudre chaque problème rencontré. Toutefois, si ces mises à jours ne sont pas installées par les utilisateurs eux-mêmes, ceux-ci resteront vulnérables aux attaques. Les navigateurs web sont le meilleur exemple d’outils utilisés au quotidien et pouvant facilement être exploités par les hackers. Lorsque l’on sait que seulement 10% des utilisateurs d’Internet Explorer utilisent la dernière version du navigateur, il est évident que les failles à exploiter pour les hackers sont nombreuses.

Je suis friand de free Wi-Fi
Les espaces de free Wi-Fi nous ont permis d’être plus connectés ou encore d’éviter les frais de connexion exorbitants lorsque nous sommes à l’étranger. Ces connexions étant ouvertes à tout le monde et en continu, il est très facile pour les hackers d’intercepter les données qui transitent via le Wi-Fi. Utiliser le Wi-Fi gratuit, c’est bien, mais il est clairement recommandé de ne pas consulter son compte en banque ou encore réaliser des achats en ligne avec sa carte d’identité lorsque l’on est connecté via un réseau Wi-Fi public. Dès lors que vous utilisez régulièrement un réseau de Wi-Fi public pour travailler, vous devez être en mesure de vous connecter à un VPN pour renforcer la sécurité de votre connexion.

J’utilise des applications gratuites
Si vous êtes fan des dernières applications, jeux ou gadgets, vous devez savoir que certaines applications gratuites peuvent être infectées par des malwares. Celles-ci permettent aux hackers de collecter vos données à des fins malveillantes, sans que cela ne vous soit jamais notifié. Aussi, il est recommandé de télécharger des apps issues de sources connues.

J’utilise le même mot de passe pour tous mes comptes en ligne
Les hackers savent pertinemment que la plupart des gens réutilisent les mêmes mots de passe pour plusieurs sites. Ils vont ainsi dérober un mot de passe sur un site peu sécurisé et essayer d’utiliser ce même mot de passe sur des sites de vente très connus ou des réseaux sociaux sur lesquels vous pourriez avoir un compte, jusqu’à ce qu’ils trouvent des informations personnelles, financières ou même liées à votre entreprise. Le meilleur moyen de se prémunir de ce type de risques est d’utiliser des mots de passe compliqués et personnalisés pour chaque site web.
Il existe de nombreux conseils en ligne pour savoir comment créer des mots de passe fort et facilement mémorisables.

Je ne verrouille jamais ma session
Le moyen le plus facile de dérober des données de valeur ou de pénétrer dans la vie privée d’une personne est d’accéder physiquement à son ordinateur non verrouillé puis de copier ses données ou de se connecter aux sites sur lesquels le mot de passe est enregistré et dont l’accès se fait automatiquement. Cela ne nécessite aucune compétence technique et, même si la personne mal intentionnée est repérée par une caméra, cela ne permet absolument pas de la tenir pour responsable, en partant de la faille. Le conseil ici est évident, ne jamais laisser sa session ouverte sur son PC lorsque l’on s’absente.

Je partage énormément (trop) en ligne
Quel est le nom de jeune fille de votre mère ? Le nom de votre premier animal de compagnie ? Le nom de votre première école ? Ce sont autant de questions de sécurité qui vous permettent de récupérer votre mot de passe oublié, et il serait bien dommage que quelqu’un puisse retrouver ces informations sur votre profil Facebook. Si vous êtes accro aux réseaux sociaux, mais que vous souhaitez vous protéger ainsi que votre entreprise des nombreuses menaces en ligne, vous pourriez commencer par restreindre l’accès à vos publications, à vos amis uniquement. Faites un nouveau tour sur votre profil et reconsidérez à quel point telle ou telle information pourrait être utile si elle tombait entre de mauvaises mains.

De la même manière, informez-vous sur les termes et conditions des sites que vous fréquentez régulièrement dans la mesure ou certains d’entre eux pourraient déclarer collecter vos données et les utiliser pour de la publicité voire même les partager avec des sociétés tierces.

La cybersécurité commence avec vous !
Aussi avancée que soit la technologie, ce que l’utilisateur fait reste la plus grande partie de l’équation à résoudre. Les sites web que vous utilisez et l’entreprise pour laquelle vous travaillez peuvent faire le maximum pour assurer la protection de vos données, ils restent toutefois dépendants de vos actes. L’humain est le maillon faible de la sécurité, et pour changer cela nous devons tous prendre nos responsabilités et jouer notre rôle. Les bonnes pratiques de cybersécurité qui commencent à la maison, avec nos données et terminaux personnels, peuvent être facilement étendues à nos vies professionnelles.

Source : http://www.globalsecuritymag.fr/Christophe-Jolly-Cisco-France-Les,20150728,54749.html
Par Christophe Jolly, Cisco France

Google For Education : un attrape-données personnelles ?

Google For Education : un attrape-données personnelles ?

Pour l'Electronic Frontier Foundation, Google profite de ses services Google For Education pour collecter et exploiter les données personnelles des élèves utilisateurs à son propre bénéfice et sans rapport avec l'enseignement. Google est pourtant signataire aux US d'un traité proscrivant ces pratiques.

Comme d'autres de ses concurrents, et notamment Microsoft, Google dispose d'une offre de services Cloud destinée spécialement aux acteurs de l'enseignement : Google For Education. Ce secteur est également un des principaux débouchés, aux Etats-Unis, pour le Chromebook.
Etudiants et enseignants sont depuis toujours des cibles de choix pour les fournisseurs de technologies. Mais Google pourrait aussi avoir un autre intérêt à être présent sur ce marché, un intérêt directement lié à son cœur de métier : la collecte et l'exploitation des données personnelles.

Chrome Sync par défaut sur Chromebook

Pour l'Electronic Frontier Foundation (EFF), Google a incontestablement dépassé les bornes en matière de données personnelles et surtout renié ses propres engagements. L'organisation vient à ce titre de saisir aux Etats-Unis le régulateur, la FTC.
En cause, les pratiques de la firme de Mountain View dans le cadre de son offre Google For Education. Selon l'EFF, Google piétine le « Student Privacy Pledge », un pacte signé par 200 entreprises, dont Google et qui encadre strictement les pratiques des fournisseurs en matière de confidentialité des données dans l'univers de l'enseignement.
Le « Student Privacy Pledge » proscrit ainsi la collecte, la conservation, l'utilisation et le partage des données personnelles des élèves hors des finalités touchant à l'enseignement. Google ne suivrait pas les règles en la matière, et ce de trois façons, juge l'EFF.
D'abord, lorsque les élèves se connectent avec leur compte Google for Education, la firme collecte les données personnelles des services non liés à l'enseignement et pour des finalités ne relevant pas non plus de l'enseignement.
Deuxième infraction : les ordinateurs Chromebooks disposent d'une fonctionnalité de synchronisation activée par défaut dans Chrome. Ce paramétrage permet ainsi à Google de collecter et d'exploiter intégralement l'historique de navigation, entre autres, des étudiants utilisant Google For Education. Et une fois encore sans que ces collectes de données relèvent des finalités admises.

Des pratiques trompeuses pour l'EFF

Enfin, Google a prévu dans les paramétrages d'administration de sa suite de services des paramètres autorisant sur les Chromebooks le partage des données des étudiants avec Google ainsi que des tiers. Or, le « Student Privacy Pledge » n'autorise pas un tel partage et une telle option n'aurait donc pas même dû être prévue à cet effet.
L'EFF demande donc au régulateur américain d'ouvrir une enquête sur les « agissements ou pratiques injustes et trompeurs » de Google, mais aussi d'exiger de la firme de détruire toutes les données des étudiants collectées jusqu'à présent en violation du « Student Privacy Pledge ».
Et cela pourrait faire beaucoup de données personnelles. Comme le rappelle ComputerWorld, Google revendiquait en octobre plus de 50 millions d'utilisateurs (élèves et enseignants) de Google For Education et 10 millions d'étudiants sur Chromebook.
Contacté par ComputerWorld, Google esquive les accusations formulées par l'EFF. La firme se déclare confiante dans le fait que ses outils respectent à la fois la loi et ses promesses, dont le Student Privacy Pledge.
Mais comme le signale l'EFF, Google a déjà reconnu au moins une mauvaise pratique et s'est engagé auprès de l'association à retirer l'activation par défaut de Chrome Sync sur les Chromebooks vendus aux établissements scolaires.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/google-for-education-un-attrape-donnees-personnelles-39829148.htm