Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

	Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

Edward Snowden, l'ancien agent du renseignement américain réfugié en Russie, a dénoncé samedi 25 juin les lois antiterroristes adoptées par les députés russes. Ces dernières relèvent selon lui de « Big Brother » et de la « surveillance de masse », et a demandé qu'elles ne soient pas promulguées.

« La nouvelle loi russe Big Brother constitue une violation inapplicable et injustifiable des droits qui ne devrait jamais être promulguée », a écrit sur Twitter le lanceur d'alerte, qui a fui les Etats-Unis pour révéler l'ampleur de la surveillance menée par les services de renseignement américains.
« La surveillance de masse ne marche pas. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité », a-t-il insisté dans un second message.

Des lois extrêmement répressives

Adoptés vendredi lors de la dernière séance de la Douma (chambre basse) avant les législatives du 18 septembre, les projets de loi en question obligent en particulier les opérateurs de télécommunications et internet à stocker les messages, appels et données des utilisateurs pendant six mois pour les transmettre aux *« agences gouvernementales appropriées »* à leur demande.
Les réseaux sociaux se voient également obligés de stocker les données pendant six mois, selon l'un de ces textes qui doivent encore être approuvés par le Conseil de la Fédération (chambre haute) et promulgués par M. Poutine.
Ce délai de six mois *« n'est pas seulement dangereux, il est inapplicable »*, a prévenu M. Snowden, qui avait été critiqué, par le passé, pour ne pas critiquer assez sévèrement le régime de Vladimir Poutine.
Ces lois ont été dénoncées par l'opposition russe comme une tentative de *« surveillance totale »* de la part des autorités, mais aussi par les entreprises du numérique qui ont critiqué un coût exorbitant.
Elles introduisent par ailleurs des peines de prison pour la non-dénonciation d'un délit, abaissent l'âge de la responsabilité pénale à 14 ans et introduisent des peines allant jusqu'à sept ans de détention pour la*« justification publique du terrorisme »*, y compris sur internet.
Article original Le Monde

Réagissez à cet article

Original de l'article mis en page : Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse »

Bulletin sécurité du 13 juin 2016 du CERTFR

Bulletin sécurité du 13 juin 2016 du CERTFR

La S . G . D . S . N (Agence nationale de la sécurité des systèmes d'information) met régulièrement à notre disposition ses avis et alertes sur de nouvelles vulnérabilités détectées.
Voici le dernier bulletin d'actualité : CERTFR-2016-ACT-024

1 – Sonde de détection d'intrusions réseau – Comment implémenter les points de mesure ?

Une sonde de détection d'intrusions réseau est un équipement passif, elle ne s'insère donc pas en coupure sur un flux de production. Il est donc nécessaire, pour implémenter les points de mesure définis, d'assurer une duplication en temps réel de l'activité réseau à analyser.
Deux techniques différentes existent pour dupliquer un trafic réseau : la première, généralement appelée « port miroir », est logicielle, et s'appuie sur les équipements réseau déjà en place ; la seconde, généralement appelée « tap », s'appuie sur des boîtiers matériels dédiés à cette fonction. Nous allons voir les avantages et les inconvénients de ces deux solutions.

Port miroir

La majorité des commutateurs du marché permettent de configurer une recopie logicielle de tout ou partie du trafic sur un ou plusieurs ports physiques dédiés. Le port miroir peut être un choix peu coûteux, si les équipements existants d'un réseau disposent déjà de cette fonctionnalité.
Toutefois, la recopie logicielle du trafic n'est pas sans risque. En effet, si l'équipement atteint sa limite de capacité sur ses fonctions « principales » (comme par exemple : la commutation de paquets, le routage, etc.), des fonctions annexes comme la recopie de paquets peuvent être dégradées, entraînant dans un tel cas des pertes sur l'activité à superviser.
La recopie logicielle peut également altérer le signal, car les couches basses réseau sont analysées et traitées par les commutateurs. Cette technique ne garantit donc pas la recopie de l'intégralité du trafic commuté sur le réseau de production. Étant donné qu'un seul paquet perdu sur un flux volumineux peut empêcher l'analyse par la sonde ou l'évader, il est primordial de considérer ce problème et de superviser la charge des commutateurs, si cette technique est mise en place.
La mise en place d'un port miroir sur un équipement du réseau augmente aussi la consommation de ressources : cela peut donc également dégrader le réseau de production. Une attention particulière doit être apportée au fond de panier, car le débit total commuté par l'équipement est décuplé.
D'autre part, il est important d'intégrer les ports miroirs dans les procédures d'exploitation : lors du remplacement d'un équipement ou d'un changement de configuration, il faut s'assurer que la recopie est toujours opérationnelle et qu'il n'y a pas de perte d'une partie des flux.
Une erreur de configuration peut également autoriser des communications depuis le réseau de duplication, voire même entre la sonde et le réseau de production.
Par contre, la mise en oeuvre d'un port miroir peut se faire sans interruption du réseau en production à superviser, à condition de disposer de suffisamment de ports physiques libres au niveau des commutateurs où les points de mesure sont effectués.

TAP

Un TAP garantit la recopie stricte du signal reçu : aucune analyse des couches au-delà de celle physique n'est réalisée. Le signal est régénéré électriquement pour des TAP cuivre, et la lumière est divisée sur deux chemins pour les TAP fibre. La mise en oeuvre d'une duplication de trafic sur un réseau en production nécessite une brève interruption du lien à superviser : celle-ci correspond au temps nécessaire pour placer le boîtier TAP en « coupure », c'est-à-dire sur le chemin de câble.
Pour les TAP alimentés, un défaut d'alimentation arrête la duplication, mais le TAP reste passant pour le lien coupé, moyennant généralement une microcoupure de quelques millisecondes.
Pour les TAP fibre, une partie de la lumière incidente étant réfléchie et l'autre réfractée, le signal est affaibli en fonction de proportions précisées dans la documentation du TAP.
Contrairement au port miroir, le TAP garantit également l'isolation entre le réseau de production et le réseau de détection.
Le prix d'un boîtier de duplication de trafic (TAP) varie entre une centaine d'euros et un millier, en fonction du type de média à dupliquer.

Conclusion

En conclusion, bien que ces deux méthodes permettent la duplication du trafic, il est conseillé de privilégier l'utilisation d'équipement dédié afin de garantir la séparation entre le réseau de production et le réseau de détection, ainsi qu'une recopie à l'identique des flux réseau.

2 – Rappel des avis émis

Dans la période du 06 au 12 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-190 : Vulnérabilité dans VLC Media Player
- CERTFR-2016-AVI-191 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-192 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-193 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-194 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-195 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-196 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-197 : Vulnérabilité dans Citrix Xenserver
- CERTFR-2016-AVI-198 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-199 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

---

Réagissez à cet article

Original de l’article mis en page : Bulletin d’actualité CERTFR-2016-ACT-024

Que change le brexit pour la protection des données personnelles ?

	**Que change le brexit pour la protection des données personnelles ?**

Le nouveau règlement européen sur les données personnelles, qui doit entrer en vigueur en mai 2018, ne s'appliquera peut-être jamais au Royaume-Uni. Le pays devrait, une fois sorti, conserver sa propre législation, basée sur les directives européennes antérieures. Cela pourrait obliger le Royaume-Uni à conclure un accord spécifique avec l'UE à 27, sous peine de se voir infliger des restrictions dans le transfert de données avec les pays de l'UE.

Le Royaume-Uni se retrouverait ainsi dans la même position que lesEtats-Unis, dont l'accord avec l'UE (Safe Harbor) a été remis en cause à l'automne pour être remplacé par le Privacy Shield, qui devrait entrer en vigueur cet été. L'adhésion à ces accords conditionne la possibilité de transférer des données personnelles de citoyens de l'UE aux Etats-Unis.
Si le Safe Harbor a été remis en cause, c'était notamment à cause des questions de surveillance de masse aux Etats-Unis. Soit le Royaume-Uni choisit de se rapprocher du modèle américain sur les questions de surveillance et de données personnelles, soit il se cale sur les standards européens.
Dans le premier cas, il faudrait que les grandes entreprises américaines (Google, Apple, Facebook, Microsoft…), dont la plupart des datacenters sont à Dublin, en Irlande, les rapatrient au Royaume-Uni, comme le note le site de la radio publique irlandaise RTE. La présence de ces datacenters en Irlande doit rassurer les Européens, puisque l'Irlande, elle, n'est pas concernée par le Brexit. Ce sont donc les standards européens qui s'appliquent.
Avant la sortie effective, rien ne change. « A moyen terme, les choses vont rester très stables. Le Royaume-Uni met en oeuvre la directive européenne sur les données personnelles depuis plus de 20 ans. La suite dépendra des accords qui seront négociés entre le Royaume-Uni et l'UE. Le cadre réglementaire ne changera donc pas pendant un bon bout de temps », assure à L'Express Daniel Kadar, avocat associé au cabinet Reed Smith.
Article original de Raphaële Karayan

Réagissez à cet article

Original de l’article mis en page : Ce que le Brexit va changer pour les géants du Web – L’Express L’Expansion

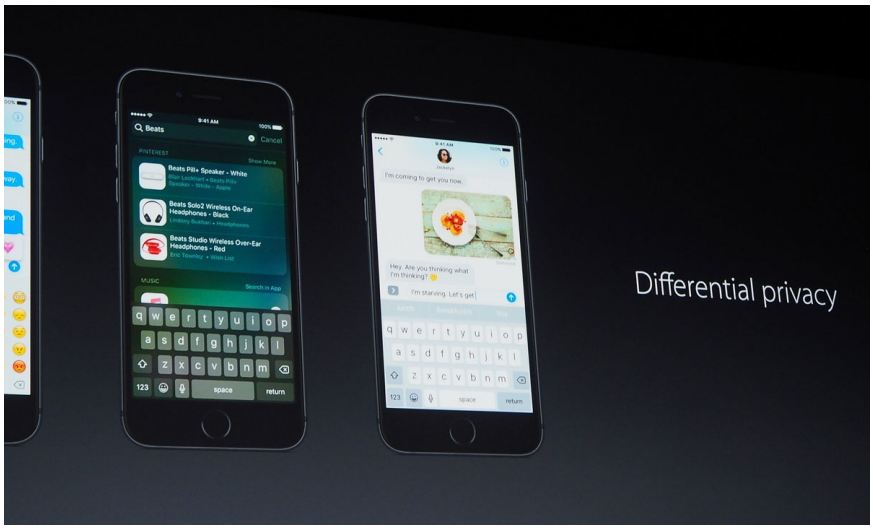
---

Finalement Apple collectera des données personnelles, avec votre accord

Finalement Apple collectera des données personnelles, avec votre accord

---

Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.



Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.
Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.
Cependant les nouvelles fonctionnalités de suggestion et d'identification d'iOS 10 ne peuvent se prétendre pertinentes sans avoir accès à un minimum de données !
Les techniques de « differential privacy » mises en oeuvre pour iOS 10 ne permettront pas une identification de l'utilisateur qui fournit ses données mais Apple, selon Recode, vous- demandera votre accord avant d'attaquer toute collecte d'information.
Dans un premier temps, le type de données collectées sera limité à quatre domaines :
– les nouveaux mots ajoutés au dictionnaire personnel d'iOS,
– les émoticônes utilisées,
– les liens profonds marqués comme public dans les applications,
– les suggestions de recherche dans les notes.
Pour ne pas rater le train de l'intelligence artificielle, Cupertino ne pouvait pas rester à l'écart d'une forme de collecte et d'exploitation de données. Cependant, ne souhaitant pas en faire directement commerce ni renier ses grands principes, Apple se doit de naviguer entre deux eaux et d'innover dans ce domaine.
On est encore loin de la façon de procéder de compagnies comme Google et Facebook !
Article original de bpepermans

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Finalement Apple collectera des données personnelles, avec votre accord | Slice42

Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

	Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

---

Particulièrement actif en Asie, ce malware est notamment parvenu à se frayer un chemin jusqu'au Google Play Store.

Android a pourtant initié depuis plusieurs années un grand nettoyage de son Google Play Store et a revu les règles et procédures d'accès des applications, mais certains malwares parviennent encore à contourner les garde-fous mis en place. Trend Micro alerte ainsi sur une famille de malware baptisés Godless, qui sont distribués entre autres via le Google Play Store et des applications malveillantes.

Trend Micro explique que Godless dispose de plusieurs exploits lui permettant d'affecter les appareils Android, ce qui le rend potentiellement dangereux pour tous les téléphones disposant d'une version antérieure à Android 5.1.
Le malware est généralement distribué via des applications proposées sur le Google Play store. La présence de celui-ci n'est pas détectée, car lorsque l'application est uploadée vers le playstore, elle ne contient aucun code malveillant à proprement parler. Mais une fois l'application installée, celle-ci va se mettre à jour et télécharger alors le « payload » contenant l'exploit de la vulnérabilité choisie par les cybercriminels.
Le malware tentera d'exploiter celle-ci pour acquérir les droits root sur la machine : il s'en sert par la suite pour installer des applications ou pour diffuser des publicités.
La France est relativement épargnée par ce malware, qui est principalement actif en Asie, notamment en Inde et en Indonésie. Mais Trend Micro estime que plus de 850.000 terminaux Android ont été infectés par ce malware à travers le monde. Outre les applications qui parviennent à le distribuer sur le Google Play Store officiel, celui-ci est évidemment diffusé sur les magasins d'application tiers.
Article original de Louis Adam

Réagissez à cet article

Original de l'article mis en page : Godless : un nouveau malware qui infecte plus de 850.000 terminaux Android – ZDNet

Enquête sur l’algo le plus flippant de Facebook

Enquête sur l’algo le plus flippant de Facebook

Si la section « Vous connaissez peut-être » vous faisait parfois flipper en vous proposant des profils précis et éloignés de vos réseaux habituels, vous n'avez encore rien vu.
La section « Vous connaissez peut-être » (« People you may know ») de Facebook est une source inépuisable de spéculations. Cette fonction, en apparence sympathique puisqu'elle nous propose d'ajouter de nouveaux amis, semble détenir des informations très personnelles sur chacun d'entre nous.
• Une journaliste de la rédaction s'est ainsi vu proposer un flirt dont elle n'avait pas noté le téléphone dans son portable ;
• un autre collègue s'est vu proposer un pote qu'il n'a pas revu depuis 10 ans et qui venait de lui envoyer un mail ;
• une autre enfin, sa femme de ménage, dont elle a le numéro de téléphone dans son portable, mais avec laquelle elle n'a jamais eu aucune interaction en ligne.
Beaucoup ont aussi vu apparaitre des gens rencontrés sur des applis de rencontre comme Tinder ou Grindr. Plutôt embarrassant, non ?

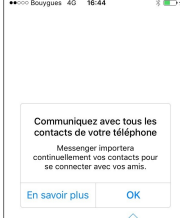
Folles rumeurs

Entre nous, les mots de « magie noire » et « espionnage » sont prononcés. Sur Internet, les rumeurs les plus folles circulent sur la façon dont cet algorithme plutôt intrusif fonctionnerait.
• Il existerait un « profil fantôme » de chacun d'entre nous, pré-rempli et automatiquement activé dès notre inscription.
C'est la théorie d'un utilisateur de Reddit. Il raconte avoir créé un profil anonyme avec un mail jamais utilisé et s'être vu proposer plein de contacts connus.
• A Rue89, on en formule une autre pour se faire peur : Facebook nous proposerait aussi les personnes qui nous « stalkent » (espionnent en ligne) ou que nous avons récemment « stalkées ».
Je découvre que cette rumeur existe déjà, et que beaucoup d'utilisateurs y croient dur comme fer. Facebook l'a toujours démentie.
• Dans le même genre, la sérieuse BBC affirmait, via des témoignages concordant et une société de sécurité informatique, que Facebook se connectait à des applications type Tinder ou Grindr pour vous faire des suggestions d'amis.
Un journaliste du Huffington Post a fait la même hypothèse. Ce que le réseau social a nié avec force.
Fabrice Epelboin, spécialiste des médias sociaux et entrepreneur du Web, croit les dires de Facebook, comme Vincent Glad :
« Ce serait très dangereux économiquement. Facebook n'est pas une société idiote, elle prend des risques calculés. »
Pour lui, l'explication est beaucoup plus simple :
« Quand on "date" quelqu'un sur Tinder, on lui donne bien son numéro avant, non ? Facebook se connecte en fait à votre répertoire. »
Ah bon ?

Un aspirateur à données, via votre téléphone

On résume. Il faut imaginer l'algorithme de Facebook comme un aspirateur à données géant.

*Visages et Facebook — **Pixabay/CC0***
*Dans un article du Washington Post, qui fait référence en la matière, il **est expliqué** que l'algorithme de « Vous connaissez peut-être » est basé sur la « science des réseaux ».*
En définissant les réseaux auxquels on appartient, Facebook calcule nos chances de connaître telle ou telle personne. Et il peut même prédire nos futures amitiés. Un peu de probabilités et c'est dans la boîte.
« Ce n'est pas de la magie, mais juste des mathématiques très pointues », apprend-on.



Avertissement de Messenger, dont la « synchronisation » permet au contact de « se connecter sur Facebook »
*En fonction des amis que l'on a, de nos interactions plus ou moins fortes et fréquentes avec eux, de l'endroit où on vit, des lieux où on a étudié et travaillé, l'algorithme fait ses calculs. Il tente aussi de définir les personnes « clés » de votre réseau, celles qui vous présentent aux autres. Enfin, il utilise votre géolocalisation, ce qui a **probablement mené** ce lundi à l'arrestation du voleur de la voiture d'un internaute, qui est apparu dans ses suggestions d'amis.*
Surtout, depuis qu'il est arrivé sur votre mobile, via les applis Facebook et Messenger, le réseau social a un tas d'autres informations à mettre sous la dent de leur algo : vos contacts téléphoniques et vos mails.
Vous l'avez autorisé, probablement sans en avoir conscience, au moment de l'installation de l'une et/ou l'autre application.

Le test ultime : le Nokia de Xavier de La Porte

Comme c'était un jour de pluie, j'ai voulu tester la puissance de cet algorithme qui marche donc sur deux pieds :
• La « science des réseaux » ;
• des tonnes de données « scrapées » de notre mobile notamment.
Je décide de créer un compte avec un numéro de téléphone et avec un faux nom. Le mien est déjà lié à un compte, donc Facebook le refuse.
*En effet, il est interdit, en théorie, de créer un faux compte ou de doublonner, selon sa politique de « l'identité réelle » — les personnes transgenres en **savent** malheureusement quelque chose.*
Il y a une personne dans ces bureaux qui n'a pas lié son compte Facebook à son numéro. J'ai nommé : Xavier de La Porte. Il possède un charmant Nokia cassé sur le dessus.

Le téléphone de Xavier, bolide de la protection des données
« J'ai 20 contacts dessus, seulement ma famille et mes amis proches », jure-t-il.
Il n'est évidemment pas question d'applications quelconques. Avec le numéro de Xavier, Facebook accepte la création du compte de « Mathilde Machin », 21 ans.

« Mathilde Machin », couverture très discrète
Et là, un truc vraiment effrayant arrive : des dizaines de contacts sont proposés, amis, famille, collègues de bureau, sources de Xavier. Ils ne sont pas dans son répertoire. Et ne sont pas non plus tous amis avec lui sur Facebook. A partir de là, deux hypothèses s'offrent à moi :
• Son compte a été lié un jour à ce numéro de téléphone, et Facebook se rend compte qu'il s'agit de la même personne. Il lui propose logiquement d'ajouter les amis du compte de Xavier.
Mais, Facebook refuse d'ouvrir deux comptes avec le même mail ou le même numéro. Il s'agirait d'une sorte de faille de sécurité, puisque le téléphone sert justement à sécuriser votre compte. Et cela n'expliquerait pas pourquoi Mathilde Machin se voit proposer des personnes qui ne sont pas dans les amis Facebook de Xavier.
• Les contacts proposés sont ceux qui possèdent le numéro de Xavier dans leur répertoire. Et qui ont donné à Facebook l'autorisation de scraper leurs données. Ce qui veut dire que l'algorithme de suggestion est tellement puissant qu'il réussit, en quelques secondes, à « inverser » la recherche.
Facebook, après s'être creusé les méninges un moment — c'est un peu technique —, me confirme la dernière hypothèse.
*C'est vertigineux. Mais inscrit noir sur blanc dans les flippantes« **Confidentialités et conditions** » de Facebook. Qui autorisent l'application à utiliser les « données que vous importez ou synchronisez de votre appareil », type répertoire, mais aussi :*
*« Les contenus et informations que **les autres personnes** fournissent lorsqu'elles ont recours à nos services notamment des informations vous concernant, par exemple **lorsqu'elles partagent une photo de vous, vous envoient un message ou encore lorsqu'elles téléchargent, synchronisent ou importent vos coordonnées.** »*

Un algo gourmand

Facebook m'explique donc que l'algorithme se nourrit aussi des données que les autres ont sur vous (votre mail, votre numéro). Pour le dire autrement, quelqu'un qui a votre contact et l'importe dans son appli Facebook va probablement apparaître dans vos suggestions d'amis. C'est aussi fou que les rumeurs. Facebook insiste sur le fait que :
• Le processus est transparent ;
• l'algorithme, gentil, ne cherche qu'à vous faire retrouver vos amis et échanger avec eux ;
• « Facebook ne possède pas et n'utilise pas » votre numéro de téléphone, il s'en sert pour mettre en relation des profils ;
• et les paramètres de votre compte sont personnalisables.
Un samedi soir, vous êtes tombée amoureuse d'un ami d'ami. Le lendemain, vous demandez à l'ami commun son numéro. Vous hésitez à envoyer un message, vous bloquez plusieurs jours. Sachez donc que ce mec, à qui vous n'avez rien envoyé, vous a peut-être déjà vu apparaître dans « Vous connaissez peut-être ». Et qu'il a déjà peur de vous.
Article original de Alice Maruani Rue 89

Réagissez à cet article

Original de l’article mis en page : Enquête sur l’algo le plus flippant de Facebook – Rue89 – L’Obs

---

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Quelques trucs et astuces simples, mais efficaces, pour protéger votre ordinateur, téléphone et tablette.

Wifi gratuit ? Votre meilleur ennemi ! En général, les réseaux Wi-Fi que l'on trouve dans les lieux publics ne sont pas bien protégés. Ils se basent souvent sur des protocoles de chiffrement trop simples ou parfois pas chiffrés du tout. Les pirates peuvent ainsi accéder à chacune des informations que vous envoyez sur Internet : e-mails importants, données de carte bancaire, voire données d'identification permettant d'accéder à votre réseau d'entreprise. Une fois que les pirates disposent de ces renseignements, ils peuvent accéder à vos systèmes en votre nom, diffuser des programmes malveillants, ou facilement installer des logiciels infectés sur votre ordinateur si le partage de fichiers a été activé.

Quelques bons gestes à respecter face à un Wifi gratuit

D'abord, utilisez un réseau privé virtuel (VPN). Un VPN est indispensable lorsque vous accédez à une connexion non sécurisée, comme un point d'accès wifi. Même si un pirate réussit à se placer en plein milieu de votre connexion, les données qui s'y trouvent seront chiffrées, donc illisibles. Mails, mots de passe, ou simplement ce que vous visitez ne seront pas lisibles. J'utilise moi même plusieurs dizaines de VPN différents. Je peux vous proposer de tester Hide My Ass, ou encore VyprVPN. Un test de VPN disponibles pour votre ordinateur, tablette ou encore smartphone dans cet article. Dernier conseil, même si vous ne vous êtes pas activement connecté à un réseau, le matériel wifi équipant votre ordinateur, votre téléphone portable, votre tablette continuent de transmettre des informations. Bref, désactivez la fonctionnalité wifi si vous ne l'utilisez pas.

Activez l'option « Toujours utiliser HTTPS » sur les sites Web que vous visitez fréquemment ou qui nécessitent de saisir des données d'identification. Les pirates ne savent que trop bien que les utilisateurs utilisent les mêmes identifiants et mots de passe pour les forums, leur banque ou leur réseau d'entreprise.

Pour finir, lorsque vous vous connectez à Internet dans un lieu public, via un Wifi gratuit il est peu probable que vous souhaitiez partager quoi que ce soit. Dans ce cas, vous pouvez désactiver les options de partage dans les préférences système. (Kaspersky)

Article original de Damien Bancal

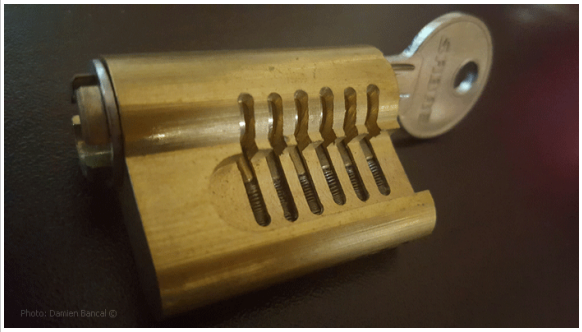
Réagissez à cet article

Original de l'article mis en page : Wifi gratuit, protégez votre connexion – Data Security Breach

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Vol de ses données personnelles – Plusieurs sources ont révélé récemment la mise en vente sur le web de plus de 117 millions de profils d'utilisateurs LinkedIn dérobés en 2012. Ce type d'actualité rappelle que personne n'est à l'abri d'un vol de ses données personnelles qui risquent d'être utilisées à des fins illicites. Cette question est d'autant plus cruciale à l'heure où le nombre de logiciels malveillants, ransomwares et autres virus explose. Aujourd'hui, 67 % des Français sont soucieux quant à la protection de leurs informations personnelles sur internet et 83 % d'entre eux sont hostiles à la conservation de ces données (Source : Institut CSA).



Malgré cette méfiance, dans un monde où l'utilisation d'Internet est devenue omniprésente, les utilisateurs ont tendance à exposer très facilement leur vie privée et leurs données personnelles – parfois par paresse ou par mégarde, mais souvent par manque d'information. Il existe cependant des moyens simples et efficaces de limiter ces risques.
Michal Salat, Threat Intelligence Manager chez Avast, commente : « ***Les sphères privées et professionnelles se fondent de plus en plus, poussant fréquemment les utilisateurs à accéder à leurs plateformes de travail depuis des terminaux personnels ou à utiliser leurs appareils professionnels à la maison par exemple. Or, en adoptant ces comportements, les internautes exposent davantage leurs données personnelles.***«

Vol de ses données personnelles
Pour éviter que cela n'arrive, les utilisateurs doivent d'abord se protéger des menaces extérieures à leur appareil en commençant par créer un mot de passe ou un code PIN sur les écrans et les applications mobiles, limitant ainsi l'accès aux données en cas de perte ou de vol. Mais encore faut-il qu'il soit suffisamment compliqué pour ne pas être déchiffré trop facilement. C'est pourquoi il est recommandé d'utiliser des mots de passes complexes – combinant lettres, chiffres, caractères spéciaux et majuscules – et qui ne reprennent pas non plus des informations personnelles facilement accessibles en ligne, telle que la date de naissance ou le prénom de ses enfants. Il est également important de changer ses codes régulièrement.
Il faut garder en tête que les cybercriminels sont à l'affût de la moindre faille à exploiter pour récolter des gains et cherchent très souvent à récupérer des informations bancaires. C'est pourquoi les internautes doivent à tout prix éviter de sauvegarder leurs coordonnées bancaires dans leurs terminaux, quels qu'ils soient. A titre d'exemple, beaucoup d'utilisateurs PayPal ont perdu de grosses sommes d'argent lorsque des hackers ont réussi à se connecter à leurs PC via un compte TeamViewer piraté et se sont servi des identifiants enregistrés pour transférer l'argent depuis les comptes PayPal.

Les pirates parviennent à créer des e-mails d'hameçonnage très sophistiqués notamment grâce à la collecte d'informations personnelles publiques disponibles sur le web – accessibles sur les réseaux sociaux par exemple. Il est alors essentiel pour l'utilisateur de poster le moins d'informations possibles sur Internet ou de s'assurer que celles-ci sont en mode privé. Il est également crucial de supprimer ses comptes s'ils ne sont plus utilisés, car bien qu'abandonnés, ces profils restent en ligne et des personnes malintentionnées pourraient usurper l'identité de l'internaute ou nuire à sa réputation en ligne en utilisant des informations sensibles contre lui.
La protection de la vie privée et des données personnelles (vol de ses données personnelles) implique une modification du comportement des internautes à commencer par de meilleures méthodes de gestion de mots de passe, une vigilance accrue sur leur utilisation d'Internet et des informations personnelles partagées publiquement – comme sur les réseaux sociaux. Au-delà des bonnes pratiques, il existe des solutions qui répondent aux problématiques liées à la vie privée. Cependant face aux menaces, il n'appartient qu'à nous de nous discipliner et de tout mettre en œuvre pour protéger nos données personnelles.

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Devenir maître dans l'art de protéger sa vie privée sur le net – Data Security BreachData Security Breach

Attention ! Le Cloud est espionné

	Attention ! Le Cloud est espionné

Les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Si vous n'êtes pas propriétaire du hardware, vous n'êtes pas propriétaire des données, selon une étude de Bitdefender.

L'éditeur de solutions de sécurité informatique affirme que les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Les révélations de l'affaire Snowden sur les capacités d'interception des données de la part de la NSA et de ses agences partenaires ont incité les propriétaires d'infrastructures et les fournisseurs de services, ainsi que les utilisateurs, à s'assurer que leurs données sont échangées sans encourir de risque de confidentialité et qu'elles sont stockées sous forme chiffrée. Régulièrement, les chercheurs s'attaquent à des protocoles très utilisés ou à leur mode de mise en œuvre. Des failles sont ainsi découvertes de manière récurrente et corrigées à plus ou moins brèves échéances, comme dans le cas de vulnérabilités bien connues telles que Heartbleed ou Logjam, qui ont entraîné le déploiement massif de correctifs à une échelle jusque-là inédite.
Mais les entreprises, et par conséquent, leurs clients, sont-elles vraiment protégées une fois que ces failles sont corrigées ? Existe-t-il des méthodes dissimulées et plus ou moins légales que les organismes d'État et certaines grandes entreprises bien informées seraient susceptibles d'utiliser pour passer outre les protocoles TLS / SSL, censés protéger les échanges d'informations ? Bref, espionnage dans le Cloud possible ?
Le 26 mai 2016, lors de la Conférence HITB à Amsterdam, Radu Caragea, Chercheur en sécurité des Bitdefender Labs, a démontré lors d'un POC (preuve de concept), que la communication protégée peut être déchiffrée en temps réel, en utilisant une technique qui ne laisse pratiquement aucune empreinte et qui reste invisible pour presque tout le monde, sauf peut-être pour des auditeurs de sécurité particulièrement vigilants.

Espionnage dans le cloud : Quelles conséquences pour votre sécurité ?
Cette attaque permet à un fournisseur de services cloud mal intentionné (ou sur lequel on a fait pression pour qu'il donne des accès à des agences gouvernementales) de récupérer les clés TLS utilisées pour chiffrer chaque session de communication entre votre serveur virtualisé et vos clients (même si vous utilisez Perfect Forward Secrecy !). Si vous êtes un DSI et que votre entreprise externalise son infrastructure de virtualisation auprès d'un prestataire de service, considérez que toutes les informations circulant entre vous et vos utilisateurs ont pu être déchiffrées et lues pendant une durée indéterminée.
Il est impossible de savoir dans quelle mesure vos communications ont pu être compromises et pendant combien de temps, puisque cette technique ne laisse aucune trace anormale derrière elle. Les banques et les entreprises qui gèrent des dossiers de propriété intellectuelle ou des informations personnelles, ainsi que les institutions gouvernementales sont les secteurs susceptibles d'être particulièrement touchés par cette faille.

Espionnage dans le Cloud : Premières découvertes
Cette nouvelle technique, surnommée TeLeScope, a été développée par l'éditeur dans le cadre de ses recherches et permet à un tiers d'écouter les communications chiffrées avec le protocole TLS, entre l'utilisateur final et une instance virtualisée d'un serveur. Cette technique n'est opérationnelle qu'avec les environnements virtualisés fonctionnant au-dessus de l'hyperviseur. Ces infrastructures sont extrêmement répandues et sont proposées par les géants de l'industrie tels qu'Amazon, Google, Microsoft ou DigitalOcean, pour ne citer qu'eux. Si la plupart des experts de l'industrie s'accordent pour dire que la virtualisation est l'avenir, aussi bien en termes de stockage, que de déplacement et de traitement de gros volumes de données, ce type de solutions fait déjà partie du quotidien de nombreuses entreprises.
Plutôt que d'exploiter une faille dans le protocole TLS, cette nouvelle technique d'attaque repose sur l'extraction des clés TLS au niveau de l'hyperviseur par une inspection intelligente de la mémoire. Même si l'accès aux ressources virtuelles de la VM est une pratique déjà connue (accéder au disque dur de la machine, par exemple), le déchiffrement en temps réel du trafic TLS, sans mettre en pause la machine virtuelle de manière flagrante et visible, n'avait jamais été réalisé jusqu'alors.
La découverte de ce vecteur d'attaque a été possible en recherchant un moyen de surveiller des activités malveillantes depuis le réseau de honeypots de l'éditeur, sans altérer la machine et sans que les pirates puissent comprendre qu'ils sont surveillés. Un administrateur réseau ayant accès à l'hyperviseur d'un serveur hôte pourrait surveiller, exfiltrer et monétiser toutes les informations circulant depuis et vers le client : adresses e-mail, transactions bancaires, conversations, documents professionnels confidentiels, photos personnelles et autres données privées.

Espionnage dans le Cloud : Comment cela fonctionne-t-il ?
Normalement, la récupération des clés à partir de la mémoire d'une machine virtuelle nécessiterait de mettre en pause la VM et de décharger le contenu de sa mémoire sur un fichier. Ces deux processus sont intrusifs et visibles par le propriétaire de la VM (de plus ils enfreignent le SLA – Service Level Agreement). L'approche des chercheurs repose sur les mécanismes de Live Migration, disponibles au sein des hyperviseurs modernes, qui nous permettent de réduire le nombre de pages nécessaire pour le vidage de la mémoire de l'ensemble de la RAM, à celles modifiées lors de l'établissement d'une liaison TLS.
« ***Au lieu de mettre la machine en pause (ce qui entrainerait une latence notable) et de réaliser un vidage complet de la mémoire, nous avons développé une technique de différentiel de la mémoire qui utilise des fonctions de base déjà présentes dans les technologies de l'hyperviseur,*** » explique Radu Caragea. « ***Ensuite, bien que cela permette de réduire le volume de vidage mémoire de giga-octets à méga-octets, le temps nécessaire pour écrire une telle quantité de données sur un espace de stockage reste non négligeable (de l'ordre de quelques millisecondes) et c'est pourquoi nous montrons comment 'déguiser ' le processus pour le faire passer pour une latence du réseau, sans qu'il soit nécessaire de stopper la machine.*** »

Atténuation des risques
L'attaque TeLeScope n'exploite pas de faille lors de l'implémentation du protocole TLS et ne tente pas de contourner le niveau de chiffrement de l'implémentation TLS via des attaques par repli (downgrade attacks). Au lieu de cela, elle exploite une caractéristique de l'hyperviseur pour exfiltrer les clés utilisées par le protocole pour chiffrer la session. Notre POC révèle un écart fondamental qui ne peut être corrigé ou atténué sans réécrire les bibliothèques de cryptographie qui sont déjà en cours d'utilisation. La seule solution à ce jour est, en premier lieu, de bloquer l'accès à l'hyperviseur – en exécutant votre propre hardware à l'intérieur de votre propre infrastructure.
Article original de Damien BANCAL

Denis JACOPINE est Expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

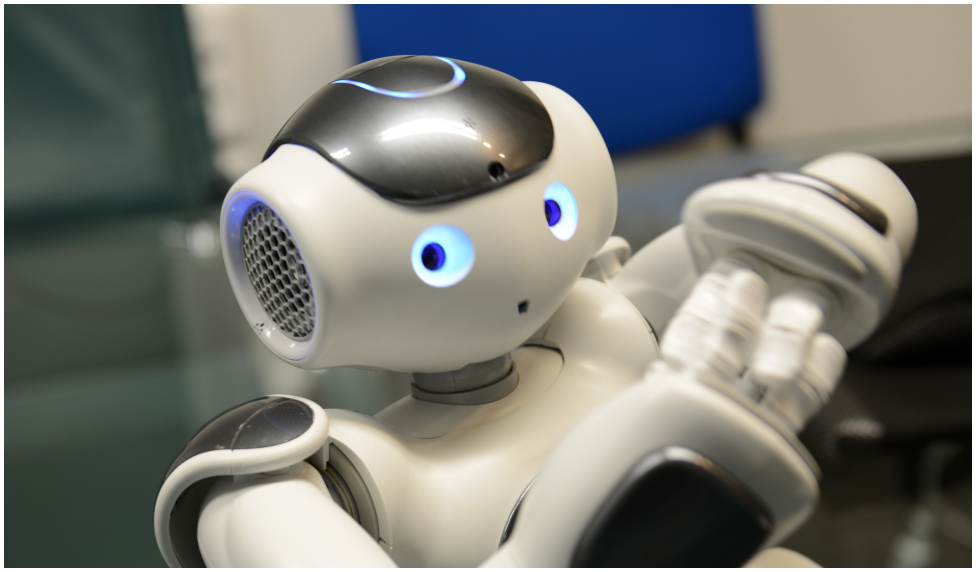
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Espionnage dans le Cloud – ZATAZ

Faut-il que les robots et les Intelligences Artificielles payent des cotisations sociales ?



Faut-il que les robots et les IA payent des cotisations sociales ?

Comment financer la sécurité sociale lorsque les employés mis aux chômage par les robots ne versent plus de cotisations ? Pour Mady Delvaux, auteure dun projet de résolution qui sera débattu au Parlement européen, il est temps de faire cotiser les robots.

Faut-il reconnaître un droit spécifique des robots ? La commission du Parlement européen en charge des affaires juridiques (JURI), qui a établi un groupe de travail sur la robotique et l'intelligence artificielle, le pense. Elle prépare actuellement un rapport rédigé par l'eurodéputée luxembourgeoise Mady Delvaux (S&D), déposé le 31 mai dernier, qui demande à la Commission d'élaborer une proposition de directive sur des règles de droit civil sur la robotique. Le texte n'a pas encore été adopté en commission JURI, et devrait être débattu en séance plénière du Parlement européen le 12 décembre prochain.
Parmi ses dispositions, la proposition de résolution invite l'exécutif à réfléchir à la manière dont le modèle social européen peut évoluer, alors que « le développement de la robotique et de l'intelligence artificielle pourrait avoir pour conséquence l'accomplissement par des robots d'une grande partie des tâches autrefois dévolues aux êtres humains ».


Mady Delvaux, députée luxembourgeoise au Parlement Européen (groupe Socialistes & Démocrates)

UNE SITUATION PRÉOCCUPANTE POUR L'AVENIR DE L'EMPLOI ET LA VIABILITÉ DES RÉGIMES DE SÉCURITÉ SOCIALE

Actuellement, l'essentiel du financement de sécurité sociale, qu'il s'agisse du socle de base de l'assurance santé, de la retraite ou de l'assurance chômage, est assis sur une ponction d'une partie conséquente des salaires versés aux employés. C'est le salarié chargé de faire l'inventaire dans un hypermarché qui cotise pour être protégé le jour où son employeur jugera plus rentable de faire faire l'inventaire par un robot intelligent.
Paradoxe des paradoxes, l'employeur lui-même complète les cotisations par ses propres versements qui sont proportionnels aux salaires versés, ce qui fait qu'il doit cotiser lorsqu'il continue à payer l'humain (et cotiser d'autant plus lorsqu'il le paye bien), mais qu'il n'a plus rien à payer lorsqu'il le remplace par un robot.

DÉCLARER LES GAINS DE PRODUCTIVITÉ POUR MIEUX LES TAXER ?

Dès lors, si l'on considère que les emplois deviennent plus rapides à détruire qu'à créer dans une société toute obnubilée par l'ubérisation et les gains de productivité, cette « hypothèse s'avère préoccupante pour l'avenir de l'emploi et la viabilité des régimes de sécurité sociale, si l'assiette de contributions actuelle est maintenue », s'inquiète le rapport Delvaux.
L'eurodéputée luxembourgeoise propose donc à la Commission « d'envisager la nécessité de définir des exigences de notification de la part des entreprises sur l'étendue et la part de la contribution de la robotique et de l'intelligence artificielle à leurs résultats financiers, à des fins de fiscalité et de calcul des cotisations de sécurité sociale ». Dit autrement, les entreprises seraient taxées sur la part de leur chiffre d'affaires imputable aux productions automatisées, pour alimenter le pot commun de la sécurité sociale.

UN REVENU UNIVERSEL DE BASE FINANCÉ PAR LES ROBOTS

« Eu égard aux effets potentiels, sur le marché du travail, de la robotique et de l'intelligence artificielle, il convient d'envisager sérieusement l'instauration d'un revenu universel de base », ose même la députée socialiste, alors que la Suisse vient de rejeter la proposition par référendum, et qu'en France le débat est souhaité par Manuel Valls mais sans cesse repoussé.
Mais comment calculer les cotisations que les entreprises devraient reverser ? La question est extrêmement complexe et n'est pas aidée par l'annexe du rapport, où il est simplement précisé que les entreprises devraient être tenues de déclarer à l'administration :
• Le nombre de « robots intelligents » qu'elles utilisent ;
• Les économies réalisées en cotisations de sécurité sociale grâce à l'utilisation de la robotique en lieu et place du personnel humain ;
• Une évaluation du montant et de la proportion des recettes de l'entreprise qui résultent de l'utilisation de la robotique et de l'intelligence artificielle.

Or comment savoir, par exemple, si un rendez-vous enregistré dans l'agenda par Siri ou Cortana est un gain de productivité imposable au titre de la robotisation, parce qu'il aurait pu être inscrit par un(e) secrétaire, ou directement par le patron ou le cadre à travers un logiciel plus ou moins automatisé ? La fiscalité traditionnelle est déjà d'une complexité impressionnante, mais ce n'est rien en comparaison de ce que propose le rapport. Et pourtant, il faudra bien y réfléchir et trouver des solutions. À moins que la crise que nous traversons soit véritablement conjoncturelle et que se créent rapidement de nouveaux emplois durables difficilement remplaçables à court ou moyen terme. « Des emplois qui répondent à des besoins d'humanité », comme le défend le roboticien sud-coréen Jeakweon Han.
Crédit photo de la une : Stephen Chin
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Faut-il que les robots et les IA payent des cotisations sociales ? – Politique – Numerama