Protection contre la Fuite des données, priorité pour les entreprises ?

	Protection contre la Fuite des données, priorité pour les entreprises ?

Prévention des pertes de données des collaborateurs mobiles. Quand la mobilité oblige à la Data Loss Prevention.

La mobilité est à la fois un besoin et un défi pour les entreprises qui se battent pour créer une force de travail réellement fluide et entièrement digitale. Aujourd'hui, presque tous les collaborateurs travaillent avec un ou plusieurs périphériques mobiles contenant des informations d'entreprise, qu'il s'agisse d'un téléphone mobile, d'un ordinateur portable ou d'une tablette. L'un des premiers défis qui en découlent pour la direction informatique tient au fait que l'accès à distance aux données et aux e-mails se fait, par nature, « hors » du périmètre de l'entreprise, et qu'il est par conséquent très difficile de s'en protéger. La multitude des périphériques utilisés, en elle-même, complique la surveillance et le suivi des données d'entreprise consultées, partagées ou utilisées.

Data Loss Prevention : se concentrer sur les données

L'une des approches, choisie dans certaines entreprises, consiste à intégrer ces périphériques à une stratégie d'environnement de travail en BYOD. Les utilisateurs peuvent choisir le périphérique, le système d'exploitation et la version de leur choix, puisqu'il s'agit de leur propre périphérique. Malheureusement, cette approche peut en réalité créer des problèmes supplémentaires de sécurité et de DLP (prévention des pertes de données). En effet, de nombreux utilisateurs n'apprécient pas (voire interdisent) que leur employeur gère et/ou contrôle leur périphérique, pire encore, d'y installer des logiciels professionnels comme les programmes d'antivirus et de **VPN**.

Par conséquent, pour réussir, la stratégie de protection des données doit se concentrer sur la sécurisation des données uniquement, quel que soit le périphérique ou le mode d'utilisation. Dans un environnement d'entreprise, une grande majorité des données sensibles transitent dans les e-mails et leurs pièces jointes. Ainsi, une stratégie de protection des données réussie doit chercher à gérer et contrôler la passerelle par laquelle transitent les données, à savoir, ici, le compte d'e-mail d'entreprise.

Autre option : implémenter une suite d'outils de gestion de la sécurité mobile, ce qui permet de placer des mécanismes de sécurité sur la passerelle d'e-mail, et d'autoriser la création de règles de sécurité pour surveiller et contrôler la façon dont les informations d'entreprise sont traitées sur chaque périphérique.

Data Loss Prevention : Stratégie DLP tridimensionnelle

Une stratégie « DLP tridimensionnelle », surveille et contrôle le contenu transféré via un périphérique sur la base de critères précis. Par exemple, on peut limiter l'accès au contenu ou aux fichiers depuis le compte e-mail d'entreprise en fonction du pays, puisque les utilisateurs qui voyagent avec leur périphérique sont susceptibles d'accéder aux données et aux systèmes sur des réseaux Wi-Fi non sécurisés. Il est également possible de contrôler le contenu sur la base des mots clés qui figurent dans les e-mails (comme des numéros de sécurité sociale ou des numéros de contrat), afin d'interdire les pièces jointes ou le contenu incluant ce type d'information sur les périphériques mobiles. Comme les pièces jointes d'e-mail contiennent la majorité des informations sensibles transmises d'un périphérique à un autre, ce point est crucial lorsqu'il s'agit de protéger l'utilisation des périphériques dans l'environnement de travail. La troisième dimension est la surveillance du contexte, qui permet d'identifier et d'interdire le contenu pour des expéditeurs/destinataires spécifiques.

Ce type de considération permet de limiter les risques liés aux pertes de données et aux problèmes de sécurité pour cette partie des activités professionnelles Bien que cette approche ne suffise pas à contrôler et à sécuriser entièrement les banques de données d'une entreprise, la sécurité mobile va jouer un rôle de plus en plus vital pour la réussite des stratégies complètes de protection des données, au fur et à mesure que davantage de périphériques s'intègrent à nos habitudes de travail.

(Par Eran Livne, Product Manager LANDESK)

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Data Loss Prevention – Data Security BreachData Security Breach

---

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

dénonce une loi « Big Brother » et la « surveillance de masse »

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

Réagissez à cet article

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

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 apparaître 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

---

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 entraînerait 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

Réagissez à cet article

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

Facebook regarde dans quels magasins vous faites vos courses

	Facebook regarde dans quels magasins vous faites vos courses

---

Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.

Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d'un carrousel – pour indiquer à l'internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s'inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d'afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s'y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l'occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu'environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n'a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n'est d'ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Moutain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l'utilisateur et de sa géolocalisation.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

Pourquoi l’inventeur du Web rêve d’un autre Internet ?

	Pourquoi l’inventeur du Web rêve d’un autre Internet ?

Inventeur du Web il y a plus de 25 ans, Tim Berners-Lee regrette le pouvoir quont pris sur lui les états et les grandes entreprises comme Google ou Facebook. Il souhaite pousser vers un Web plus déconcentré et plus sûr pour ses utilisateurs.

Mais qu'a-t-on fait d'Internet ? C'est la question que se posent régulièrement des pionniers du Web, qui rêvaient de changer le monde et qui l'ont effectivement fait, sans toujours bien savoir si c'est pour le meilleur ou pour le pire. Internet a apporté son lot incontestable d'améliorations dans la vie sociale, en permettant aux citoyens de s'informer davantage, de partager des connaissances et d'entrer plus facilement en contact les uns avec les autres. Mais il est aussi devenu un moyen inédit de surveillance de la population, et une machine libérale qui favorise les plus gros dans une économie plus que jamais mondialisée.

Parmi ceux qui semblent avoir quelques regrets figure l'inventeur du World Wide Web, Tim Berners-Lee. L'homme, qui a créé la première page Web il y a plus d'un quart de siècle, s'est désolé dans le New York Times de ce qu'était devenu en partie Internet. « Il contrôle ce que les gens voient, crée des mécanismes sur la manière dont les gens interagissent. Ce fut génial, mais l'espionnage, le blocage de sites, le détournement du contenu des gens, vous faire aller sur les mauvais sites web… tout ça mine complètement l'esprit d'aider les gens à créer », condamne-t-il.

NOUS N'AVONS PAS UN PROBLÈME TECHNOLOGIQUE, NOUS AVONS UN PROBLÈME SOCIAL

Berners-Lee voit un problème majeur dans le développement du Web qu'il a créé ; la possibilité pour les états ou de grandes entreprises de prendre le contrôle et d'imposer leur puissance. Pour les états, il s'agit par exemple de la possibilité qu'ils ont de bloquer l'accès à des sites internet (comme c'est désormais fréquent en France), ou de traquer les communications pour identifier ou géolocaliser des dissidents. Concernant les entreprises, le souci est davantage dans le pouvoir immense que des Facebook ou Google ont sur les populations du monde entier, en étant les principaux vecteurs d'informations, et en glanant des informations de plus en plus précises sur les habitudes et les pensées de chacun.

Pour défendre l'idée de repenser Internet, l'ingénieur a donc participé cette semaine à la conférence Decentralized Web Summit de San Francisco, organisée notamment par la fondation Internet Archive, et des acteurs impliqués dans le bitcoin et la blockchain. Mais il prévient que la solution ne sera pas seulement technique. « Le Web est déjà décentralisé », rappelle-t-il. « Le problème c'est la domination d'un moteur de recherche, d'un grand réseau social, d'un Twitter pour le microblogging. Nous n'avons pas un problème technologique, nous avons un problème social ».

« Nous sommes au bord de découvrir qu'une entreprise peut en arriver au point où en réalité elle contrôlera tout ce que chacun d'entre nous voit », s'était déjà inquiété Berners Lee dans une interview à GeekWire. « Elle décidera des posts de ses amis et des articles de journaux qu'une personne voit, et nous réalisons que nous parlons d'une seule grande multinationale qui a soudainement le contrôle complet sur la perception qu'a quelqu'un de la planète sur laquelle il habite. C'est une bataille constante et nous en sommes très proches tout le temps ».

UN PAIEMENT PLUS FLUIDE POUR UN INTERNET PLUS SAIN

Pour aider à réinventer le Web, Tim Berners-Lee rêve notamment d'un réseau social respectueux de la vie privée des utilisateurs et de leur liberté d'expression. Il est membre du conseil d'administration de MeWe, qui se rêve en Facebook éthique. D'autres technologies décentralisées peuvent aussi aider, comme Tor bien sûr, mais aussi des initiatives comme ZeroNet, qui prétend héberger un Web non censurable en utilisant BitTorrent et du chiffrement, ou MaidSafe, qui utilise aussi une architecture P2P et un système d'échange monétaire baptisé SafeCoin.

À cet égard, Tim Berners-Lee espère aussi voir prospérer un Web où le paiement électronique serait beaucoup plus aisé, et sans intermédiaires à qui verser des commissions (ce qui était à l'origine l'idée du bitcoin, même s'il manque de fluidité dans la validation des transactions). « Imaginez un monde où le fait de payer pour des choses serait facile des deux côtés », demande-t-il, en faisant remarquer que « le modèle publicitaire est le seul modèle pour trop de gens sur le web actuellement ».

Les journaux, par exemple, devraient pouvoir proposer de faire payer quelques centimes pour lire un article, ce qui rapporterait davantage que la publicité, offrirait davantage d'espace d'affichage pour l'information, et éviterait de tracer l'internaute. Or aujourd'hui, le jeu des commissionnements et des empilements d'intermédiaires fait qu'il est pratiquement impossible d'avoir sur internet la fluidité de paiement offerte par l'argent liquide.

Crédit photo de la une : CC Kristina D.C. Hoeppner

Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Pourquoi linventeur du Web

L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l’un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l’univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu’à l’auteur de l’attaque, se révèle souvent compliqué.

Lorsqu’un incident survient, il est généralement difficile pour l’entreprise de définir qui a accédé à son système d’information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d’utilisateurs internes bénéficiant d’un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l’incident soit le résultat d’une action malveillante d’un utilisateur interne, d’une erreur humaine ou d’une faille, dès lors que l’entreprise n’est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l’enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l’incident.

L’examen approfondi des logs : remonter les étapes d’une attaque
Lorsqu’une faille est avérée, l’entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l’attaque. En pratique, trier les informations peut prendre des jours – en d’autres termes, cela revient à chercher une aiguille dans une botte de foin.

L’intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu’ils ne peuvent pas être présentés dans leur format original, l’intégrité des données de logs peut être remise en question lors d’une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n’ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l’information cruciale peut manquer et ce chainon manquant peut empêcher l’entreprise de reconstituer tout le cheminement de l’incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d’accès étendus, voire sans aucune restriction au système d’information, aux bases de données, et aux couches applicatives, les cybercriminels s’octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l’entreprise (financières, clients, personnelles, etc.).

L’analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l’analyse comportementale permettent aux entreprises d’analyser l’activité de chacun des utilisateurs, et notamment les événements malveillants, dans l’intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l’activité des utilisateurs en temps réel pour comprendre ce qu’il se passe sur leur réseau. Si l’entreprise est victime d’une coupure informatique imprévue, d’une fuite de données ou encore d’une manipulation malveillante de base de données, les circonstances de l’événement sont immédiatement disponibles dans le journal d’audit, et la cause de l’incident peut être identifiée rapidement.
Ces journaux d’audit, lorsqu’ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d’une procédure judiciaire, mais ils assurent à l’entreprise la possibilité d’identifier la cause d’un incident grâce à l’analyse des données de logs.
Lorsque ces journaux sont complétés par de l’analyse comportementale, cela offre à l’entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel.
Article original de Balázs Scheidler

Réagissez à cet article

Original de l’article mis en page : Recouvrer les traces d’une attaque informatique : l’investigation peut s’avérer complexe et coûteuse

---

L’État crée encore un nouveau fichier secret de données personnelles

L'État crée encore un nouveau fichier secret de données personnelles

Le gouvernement a fait connaître vendredi la création d'un fichier de données personnelles utilisé pour les services de renseignement intitulé « #BCR-DNRED », dont le contenu et la portée sont confidentiels. Il s'agit d'un fichier permettant les enquêtes contre la fraude douanière, orienté vers les crimes graves.

Le gouvernement a fait publier vendredi au Journal Officiel un décret n° 2016-725 du 1er juin 2016 qui ajoute un 13e fichier à la liste des fichiers confidentiels de données personnelles mis en œuvre par l'État, « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* ».
Comme le veut la règle, on ne sait strictement rien de ce fichier si ce n'est qu'il est baptisé « BCR-DNRED » et sera utilisé par les « *services du ministère des finances et des comptes publics (administration des douanes et droits indirects) traitant de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la prolifération des armes de destruction massive* ».
L'acronyme BCR-DNRED est sans aucun doute une référence à la Direction nationale du renseignement et des enquêtes douanières (DNRED), rattachée à Bercy. Considérée comme un service de renseignement, elle est chargée notamment de collecter des informations sur les les grands trafics de contrebande, et de lutter contre les flux financiers clandestins.

UN FICHIER CONTRE LE TRAFIC

JORF n°0128 du 3 juin 2016
texte n° 87

Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED »

NOR: CNIX1614799X
ELI: Non disponible

Avis favorable avec réserve.

L'avis « favorable avec réserve » de la Cnil.

On imagine donc que le fichier BCR-DNRED s'inscrit dans une politique de croisement d'informations concernant de possibles trafics internationaux illicites de biens ou d'argent qui transitent par la France, avec une orientation plus spécifique vers la recherche de financements de crimes graves.
La Cnil, qui n'a pas le droit de publier son avis, a émis un avis « favorable avec réserve », ce qui veut dire qu'elle a estimé qu'au moins sur certains points, le fichier projeté n'était pas conforme à la loi de 1978 sur la protection des données personnelles. Elle avait déjà émis des réserves non publiées concernant les deux derniers fichiers créés par l'État, le fichier CAR relatif au suivi des prisonniers créé en novembre 2015, et le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT) modifié quelques jours plus tôt.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : L'État crée encore un nouveau fichier secret de données personnelles — Politique — Numerama