ESET intègre un bouclier anti-ransomware et rejoint « No More Ransom »

ESET intègre un bouclier anti-ransomware et rejoint « No More Ransom »

En prenant part au projet « No More Ransom », ESET fournit un outil qui permet d'analyser les impacts d'une attaque par des ransomwares. Les utilisateurs n'en mesurent la gravité qu'une fois qu'ils ont été infectés. Grâce à cet outil, ESET espère les sensibiliser en amont, afin de limiter les infections de ce type.

De plus, ESET renforce la sécurité de ses utilisateurs en ajoutant une couche de sécurité supplémentaire capable de bloquer les ransomwares. La fonctionnalité est disponible gratuitement et sans intervention de l'utilisateur dès maintenant pour les solutions de sécurité Windows destinées aux particuliers.

Le bouclier anti-ransomware d'ESET contrôle et évalue toutes les applications exécutées en utilisant l'heuristique comportementale. Il bloque activement tous les comportements qui s'apparentent à une attaque par ransomware et peut également forcer l'arrêt des modifications apportées aux fichiers existants (c'est-à-dire leur chiffrement).

Activé par défaut, le bouclier anti-ransomware ne demande l'intervention de l'utilisateur qu'une fois la menace détectée en lui demandant d'approuver ou non son blocage.

Pour plus d'informations à propos de notre bouclier anti-ransomware et de l'implication d'ESET au sein de l'organisation « No More Ransom », n'hésitez pas à nous contacter.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Les États peuvent-ils imposer aux FAI une obligation générale de conservation des données ?

	Les États peuvent-ils imposer aux FAI une obligation générale de conservation des données ?

Dans un arrêt, la Cour de justice de l'Union européenne considère que les États ne peuvent pas imposer une « conservation généralisée et indifférenciée » des données de connexion. Celle-ci doit se faire de façon «ciblée, limitée et avec des garde-fous.

L'accès aux données de connexion ne peut pas être « open bar ». Tel est, en somme, le sens de l'arrêt que la Cour de justice de l'Union européenne vient de rendre ce mercredi 21 décembre. Pour les magistrats, il n'est pas possible d'imposer aux fournisseurs d'accès à Internet une « *conservation généralisée et indifférenciée* » des données de connexion de leurs clients. Celle-ci doit être extrêmement ciblée et fortement délimitée pour éviter des dérives. Rappel des faits.
C'était le 8 avril 2014. Dans son mémorable arrêt *Digital Rights Ireland*, la Cour de justice de l'Union européenne manifestait sa volonté jurisprudentielle de protéger les droits des internautes, en invalidant la directive européenne de 2006. Celle-ci obligeait les États membres à exiger des opérateurs qu'ils conservent un journal des données de connexion de leurs clients pour que la police et la justice puissent y avoir accès.
S'appuyant sur la Charte des droits fondamentaux de l'Union européenne, la cour jugeait que cette obligation était disproportionnée et offrait un cadre insuffisant pour la protection de la vie privée et des données personnelles des citoyens européens. Grâce à cet arrêt, plusieurs États ont suspendu ou révisé leur législation pour intégrer l'avis de la cour suprême communautaire. D'autres nations ont en revanche choisi de ne pas bouger, à l'image de la France.

CC Harald Deischinger

Sollicité dans le cadre de deux affaires jointes (C-203/15 Tele2 Sverige et C-698/15 Secretary of State for Home Department/Tom Watson e.a), l'avocat général de la Cour de justice de l'Union européenne, le Danois Henrik Saugmandsgaard Øe a considéré au mois de juillet que les États membres avaient bien le droit d'exiger la conservation de toutes les métadonnées mais uniquement s'ils se conforment aux impératifs fixés par l'arrêt *Digital Rights Ireland*.
Une analyse que la Cour de justice de l'Union européenne a refusé de suivre. Dans un arrêt rendu le 21 décembre, l'institution communautaire n'a en effet pas suivi l'avocat général. Elle déclare que les États ne peuvent pas imposer aux fournisseurs d'accès à Internet une obligation générale de conservation de données, que ces données soient relatives au trafic ou qu'elles concernent la localisation. Pour le dire autrement, l'accès aux données n'est plus « open bar »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Les États ne peuvent pas imposer aux FAI une obligation générale de conservation des données — Politique — Numerama

Snowden conçoit une coque d’iPhone anti-espionnage – L’Express L’Expansion

Cette coque a pour objectif de protéger les données de nos smartphones. Un premier prototype sera rendu public d'ici un an.

Edward Snowden continue son combat contre la surveillance. L'ancien analyste de la NSA et lanceur d'alerte, qui a levé le voile sur les pratiques d'écoute massive à travers le monde, travaille à la réalisation d'une nouvelle coque d'iPhone. Son atout: elle est capable de protéger les données du téléphone qu'elle abrite.

Pour ce projet, Edward Snowden s'est associé au hacker Andrew « Bunnie » Huang. Dans un rapport, les deux hommes précisent que le mode avion est loin d'être efficace contre le piratage. « Croire au mode avion d'un téléphone hacké équivaut à laisser une personne ivre juger de sa capacité à conduire », indiquent-ils.

Contrôler les signaux envoyés à l'iPhone

Le système, encore au stade d'étude, a été présenté à l'occasion d'une conférence le 21 juillet. L'objet est un périphérique sous logiciel libre qui se pose à l'emplacement de la carte SIM. Il permet ensuite de contrôler les signaux électriques envoyés aux antennes internes du téléphone et donc de savoir si le téléphone partage des informations avec des tiers, sans que vous en soyez conscients.

Une alerte est envoyée dès lors qu'une transmission anormale est détectée.
Mashable explique que « lorsque le mode avion est activé et que les connexions réseaux sont supposées être désactivées, une alerte est envoyée dès lors qu'une transmission anormale est détectée ». L'anomalie repérée, le périphérique peut même éteindre le téléphone immédiatement.

Journaliste, activiste et lanceur d'alerte

L'outil, dont le premier prototype devrait être rendu public d'ici un an, a été pensé pour venir en aide aux journalistes, activistes et lanceurs d'alerte « pour détecter quand leurs smartphones sont surveillés et trahissent leurs localisations ».

Le programme d'espionnage américain de la NSA, révélé par Edward Snowden a, permis la collecte de données personnelles de millions de citoyens, ainsi que des institutions et chefs d'Etats étrangers. Ces révélations ont montré que ces collectes dépassaient le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques.

Article original de l'express

Réagissez à cet article

Original de l'article mis en page : Snowden conçoit une coque d'iPhone anti-espionnage – L'Express L'Expansion

Ma vie disséquée à travers mes données personnelles

Ma vie disséquée à travers mes données personnelles

Plusieurs centaines de fois par jour, nous générons des données qui disent où nous allons, ce que nous faisons, avec qui nous mangeons et ce que nous avons pris comme dessert.

La NSA. Google. Les opérateurs téléphoniques. Nos banques. La DGSE. Les cartes de fidélité. Le Pass Navigo. La vidéosurveillance. Du lever au coucher, on sait depuis quelques années que nos vies se copient en temps presque réel dans des bases de données, parfois sans notre véritable consentement. L'anonyme dans la foule est de moins en moins flou.
À quoi ressemble une vie contemporaine, et donc numérisée ? Dessine-t-elle un portrait fidèle de ce que je suis ? Est-ce même encore possible, en 2014, de le savoir ?

Vendredi matin, mon réveil sonne. Mon premier réflexe : allumer mon iPhone. Son réflexe ? Se géolocaliser. Il répète l'opération plusieurs fois dans la journée, si l'option n'a pas été désactivée, afin d'*« améliorer ses performances et proposer des informations utiles en fonction des lieux où vous êtes »*.

Apple n'assure que les données sont stockées sur mon iPhone, accessible uniquement par moi, et non dans un « datacenter ». La vague certitude que le détail de mes allers et venues n'est pas mémorisé dans un lieu que j'imagine froid, vaste et à l'autre bout du monde est une maigre consolation.

Pour accéder à ce menu : Réglages > Confidentialité > Services de localisation > Services système > Lieux fréquents.

Je constate la réception, pendant la nuit, de iMessages dont je préférerais qu'ils ne soient pas lus par d'autres. Apple m'assure qu'ils sont chiffrés et être incapable elle-même de les lire. Mais en même temps, la NSA a ajouté l'entreprise à son programme Prism, qui permet d'accéder de manière privilégiée aux données de plusieurs géants du Web, en octobre 2012.
Ce n'est pas tout : Apple a récemment détaillé la manière dont l'entreprise répond aux demandes de données des autorités. On y apprend que même les passages au « Genius Bar », le service après-vente d'Apple, sont mémorisés.
Sur la table du petit déjeuner, l'iPhone a remplacé le dos de la boîte de céréales. Les corn-flakes ne pouvaient pas savoir où j'habitais. L'iPhone, si : chacune de mes localisations, implacablement consignées dans sa mémoire, lui permet de situer mon « domicile » sur une carte. Les corn-flakes n'étaient pas l'allié objectif de mon patron. L'iPhone, lui n'indique le temps nécessaire pour rejoindre un autre lieu qu'il a identifié : *« Si vous partiez maintenant, il vous faudrait 20 minutes pour arriver sur votre lieu de travail. »*
La pluie me pousse vers la station de métro. Le portique s'ouvre après le passage du badge. Le Pass Navigo, gratuit, est recommandé à tous les utilisateurs réguliers de la RATP ; il est associé à toute son identité. Il ne sauvegarde que mes trois dernières validations aux portiques de la RATP.
La raison ? Un combat de dix ans avec la Commission nationale de l'informatique et des libertés (CNIL) qui s'est efforcée de limiter l'appétit en données de la RATP. Un Navigo « découverte », anonyme mais coûtant 5 euros existe, mais il est difficile de se le procurer.
Mes trajets de métro, mes séances ciné… Tout est stocké quelque part.
Arrivée 26 minutes plus tard sur mon lieu de travail. Le badge à l'accueil fait biper la porte. Un son qui devrait me rappeler que toutes mes allers et venues sont consignées également dans une base de données.
Renseignements pris, on m'assure que mon chef ne peut y avoir accès, même si certains ont tenté, mais les données servent, en cas de problème, à savoir qui est entré dans le bâtiment. J'ai essayé, en vain, d'avoir le détail des données associées à mon badge, mais je n'ai reçu aucune réponse.
À peine arrivé au bureau, je prévois déjà d'aller au cinéma le lendemain. En cherchant les horaires, je me fais la réflexion que ma carte UGC Illimité doit enregistrer l'ensemble des informations et des files que je suis allé voir.
Cette recherche personnelle devient donc professionnelle : hélas, impossible de savoir quelles données sont conservées. Les conditions générales d'abonnement, qui sont rarement lues, n'en font pas mention. Et impossible de savoir où réclamer l'accès à mes données. UGC n'est d'ailleurs pas d'une très grande aide : *« Tout le monde est à Cannes »*, me répond-on quand j'essaie d'en savoir plus.
Ces exemples d'organismes pas très enthousiastes à l'idée de répondre à mes demandes ne sont pas isolés. Je ne rends vite compte du nombre effarant de bases de données dans lesquelles figurent des bribes de mon existence, ainsi que de la réticence (ou l'incompréhension) de certains organismes.
La loi informatique et libertés de 1978 prévoit pourtant explicitement un droit quasiment inconditionnel d'accès aux données personnelles. En cas de refus ou au bout de deux mois sans réponse, je peux même saisir laCNIL, qui peut *« faire usage de ses pouvoirs de contrôle et de sanction »*. Et même, en dernier recours, le procureur de la République.
La composition de mon déjeuner est stockée pendant treize mois
À l'heure du déjeuner, nouveau big caractéristique : celui de ma carte de cantine. Là aussi, l'historique de mes consommations est gardé pendant treize mois. Que peut donc faire le chef avec mes pâtes fraîches achetées en juin 2013 ? *« Oh, nous n'en faisons rien, mais je peux vous sortir tous vos tickets. »*
Passage ensuite à la pharmacie. La carte Vitale, obligatoire pour obtenir le remboursement des médicaments, enregistre la transaction. En jaugeant ce qu'est capable de faire la Sécu avec les données de ses assurés, j'imagine que mon achat d'aujourd'hui va rejoindre ceux que j'ai faits tout au long de ma vie dans les serveurs de l'assurance-maladie.
Analyse épidémiologique avec le Sniiram (Système national d'information inter-régimes de l'Assurance maladie) ou surveillance de la fraude chez les consommateurs avec Erasme, la Sécu mouline mes données, sûrement pour mon bien. Et certains espèrent même pouvoir y accéder pour leur bien à eux dans le cadre d'une ouverture des données publiques…
La loi permet aux organismes détenteurs de nos données de facturer leur envoi, à un coût qui ne doit pas dépasser leur coût de reproduction. La plupart des gens autour de moi n'ont qu'à se connecter à leur espace client, sur Internet, pour accéder à leurs factures détaillées. Mon opérateur (BbYou) me propose également ces documents… Mais les numéros de téléphone de mes correspondants y sont expurgés de leurs deux derniers chiffres. Pour les ajouter , il m'en coûtera 7 euros… par facture.

Mon activité sur Google, jour par jour, heure par heure. Google

Cette quête de mes données est sans fin. J'utilise Google des centaines de fois par jour. Normalement, j'ai désactivé la sauvegarde automatique de chacune de mes recherches. Je vérifie… Manqué : les 11 999 recherches effectuées dans Google depuis le 1er septembre 2012 sont là, à portée de clic depuis mon compte Google.
Requêtes personnelles et professionnelles se mélangent allégrement, et « cat eating quinoa » ou « scary manchot » côtoient « rapport de la Cour des comptes sur l'assiette des impôts locaux » ou « imprimé de changement de situation ameli ».
Prises individuellement, ces recherches font sourire ou consternent, paraissent étranges ou anodines, déplacées ou cryptiques. Mais en parcourant plusieurs pages, c'est tout simplement mes intérêts professionnels, mes lubies, mes passe-temps qui sont soigneusement classés par ordre chronologique. Me revient alors en mémoire le livre de l'artiste Albertine Meunier, qui compile trois ans de recherches Google. Et je désactive aussi sec la mémorisation de mes recherches.
La journée avance et les données continuent de s'égrener derrière moi. La carte de fidélité du supermarché qui garde l'historique de mes achats pour me profiler, mes écoutes sur Spotify, mon achat de billet de train à la SNCF, les centaines de caméras de vidéosurveillance devant lesquelles je passe chaque jour, mes données bancaires, celles de mon compte Apple…

L'ensemble des données liées à un abonnement Vélib LeMonde.fr

La soirée s'éternise, le dernier métro est passé. Je prends un vélo à la station la plus proche. La carte Vélib longue durée libère un vélo. Dans le même temps, les informations sur la prise du vélo sont envoyées au serveur de JCDecaux, en délégation de service public. Selon le publicitaire, les données relatives à la base de départ et à la base d'arrivée seront effacées dès que mon vélo sera rattaché sur la station d'arrivée. Ils gardent tout de même deux ans d'historique de mes contacts avec l'assistance Vélib.
Sur le chemin, je repense alors à mes données de géolocalisation sur mon iPhone. Il n'y a aucune raison pour que Google ne fasse pas la même chose. Chez moi, une recherche (sur Google) m'apprend que le géant de la recherche stocke bien ma géolocalisation en temps réel. Je me précipite sur mon historique de localisation. Rien, la carte qui s'affiche est vide. Par acquit de conscience, je demande le lendemain à une collègue qui possède un téléphone fonctionnant sous Android, donc Google, d'aller sur la même page que moi.

Des déplacements récents effectués dans Paris. Le Monde
Mon week-end dans L'Ain, mes sorties de course à pied, mes promenades, tout y est.
Elle ne peut pas retenir un cri : sur la carte de Paris, des centaines de petits points rouges, traces bien voyantes de tous ses déplacements. Pour illustrer cet article, j'active, heureusement non sans mal, la même fonctionnalité sur mon iPhone. Au bout d'un mois, tous mes déplacements sont minutieusement consignés chez le géant californien. Ma position quasiment minute par minute, à toute heure du jour et de la nuit. Mon week-end dans L'Ain, mes sorties de course à pied, mes promenades, tout y est.
Au terme de cette plongée ardue dans les traces ma propre existence, difficile de parvenir à une conclusion. Certes, avoir la liste de toutes les applications iPhone téléchargées depuis la création de mon compte n'est pas très intéressant, y compris pour moi. Oui, le détail de mes menus de cantine ne fera peur qu'à un nutritionniste. D'accord, je ne donne pas ces données gratuitement, et trouve formidablement pratique de pouvoir me repérer dans une capitale ou pouvoir écouter de la musique librement.

Des déplacement récents effectués en France. | Le Monde

Mais mises bout à bout, ces bases de données réunissent mes goûts, mes habitudes, mes obsessions, mes loisirs, mes centres d'intérêt. Dispersées sur des ordinateurs aux quatre coins du monde, ces données, souvent analysées, résistent encore aux croisements et recoupements divers. Mais pour combien de temps ?
Autre évidence : de plus en plus, les entreprises, les outils et les services que nous utilisons vont collecter nos données. Souvent activés par défaut, ces dispositifs ne nous laissent pas souvent le choix. Que faire, puisque personne ne peut vivre parfaitement déconnecté, ni ne peut passer maître dans la dissimulation de toutes ses traces ?
Article original de Alexandre Léchenet et Martin Untersinger

Réagissez à cet article

Original de l'article mis en page : Ma vie disséquée à travers mes données personnelles

---

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ?

Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama

---

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Le Massachusetts Institute of technology (MIT), aux États-Unis, et l'École polytechnique fédérale de Lausanne (EPFL), en Suisse, annoncent la création d'un nouveau réseau anonyme sur Internet, baptisé Riffle, encore plus rapide et sécurisé que Tor, la référence en la matière.

A l'image de Tor, le plus célèbre des réseaux de ce type, Riffle permet de surfer et de communiquer en théorie en parfait anonymat en s'appuyant sur le protocole de chiffrement "en oignon". Cela signifie qu'il est composé d'une multitude de couches de routeurs, autant de "noeuds" par lesquels transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. Les données personnelles de l'internaute (adresse IP, pays) ne peuvent ainsi plus être localisées par les sites visités. Cette alternative serait toutefois selon ses créateurs bien plus sécurisée et fiable que Tor et consorts.
Selon le MIT, l'avantage de Riffle repose sur ses serveurs, capables de permuter l'ordre de réception des messages rendant l'analyse du trafic encore plus complexe et favorisant donc l'anonymat des utilisateurs. Si, par exemple, les messages provenant d'expéditeurs Alice, Bob et Carol atteignent le premier serveur dans l'ordre A, B, C, ils peuvent être renvoyés dans un ordre complètement différent au serveur suivant, et ainsi de suite. Les utilisateurs du réseau deviennent alors en théorie parfaitement impossibles à identifier.
Dernier point non négligeable, Riffle proposerait une meilleure bande passante, garantissant une navigation plus fluide et des échanges de fichiers accélérés.
Cette annonce intervient alors que la sécurité de Tor a récemment été mise à mal par des chercheurs de la Northeastern University de Boston (États-Unis) qui a découvert plus d'une centaine de "nœuds-espions", en réalité des serveurs, capables d'identifier des services cachés et éventuellement de les pirater.
Davantage de détails sur Riffle, toujours en phase de développement, seront communiqués lors de sa présentation officielle à la conférence Privacy Enhancing Technologies Symposium (PETS), qui se déroulera du 19 au 22 Juillet à Darmstadt (Allemagne).
Article original de Etienne Froment

Réagissez à cet article

Original de l'article mis en page : Riffle, le nouveau réseau garanti plus anonyme et rapide que Tor | geeko

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.

Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au coeur d'une controverse d'experts.
Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités.
Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.
Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».
« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les liberté civiles.

L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.
Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thaï Duong.
Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »… [Lire la suite]

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

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

Vers une nouvelle plainte européenne contre Google

Vers une nouvelle plainte européenne contre Google

Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

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

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*

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

Android : Google Photos charge les clichés même après une désinstallation | Le Net Expert Informatique

Android : Google Photos charge les clichés même après une désinstallation

Google continue de charger sur ses serveurs les clichés capturés avec un smartphone Android même lorsque l'application Google Photos a été désinstallée.

A l'occasion de la conférence I/O, Google lançait un nouveau service baptisé Google Photos. Ce dernier, désormais dissocié de Google+, propose un espace de stockage illimité et se présente sous la forme d'une application mobile pour Android et iOS. Google est ainsi paré pour entrer en concurrence avec Facebook, Flickr, Microsoft ou Apple sur le domaine de la photo sur mobiles.
Sur le système d'exploitation Android, les développeurs ont choisi de ne pas placer les options de ce nouveau service directement au sein de l'application Google Photos mais de les ajouter dans les paramètres du compte Google. Cela signifie qu'un internaute désinstallant l'application après l'avoir testé devra effectuer une manipulation supplémentaire pour stopper le service. En effet, le magazine Nashville Business Journal explique qu'une fois l'application installée et activée, elle ajoute une option permettant d'autoriser le chargement des clichés vers les serveurs de Google. Mais lorsque Google Photos est désinstallée, l'option est toujours présente et bel et bien activée. Reste à savoir si dans une prochaine mise à jour Google rectifiera le tir.
Rappelons qu'avec Google photos, les clichés ne peuvent être publiés en privé. Google les masque en leur attribuant des URL supposées « indevinables », qu'il est possible de partager vers un tiers. Le dispositif a été révélé lorsqu'un internaute a réussi à accéder à ses photos supposées privées sans se connecter à son compte Google. Selon la firme de Mountain View, ces URL d'une quarantaine de caractères, seraient plus complexes qu'un mot de passe traditionnel.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.clubic.com/application-mobile/actualite-773600-android-google-photos-chargement-photos-desinstalaltion.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1067015562#pid=22889469