Plusieurs centaines de sites enregistrent l’intégralité des actions de visiteurs

	Plusieurs centaines de sites enregistrent l’intégralité des actions de visiteurs

Une étude menée par des chercheurs de l'université de Princeton montre que des sites très populaires recourent à des scripts qui enregistrent le moindre mouvement de souris.

La pratique s'appelle session replay, littéralement « rejouer une session ». Elle consiste à enregistrer l'intégralité des actions d'un visiteur sur un site Web : les endroits où il clique bien sûr, mais aussi ses mouvements de souris, ce qu'il ou elle tape dans un formulaire de série et à quelle vitesse… Des données qui permettent de « revoir », en vidéo, comment un internaute s'est comporté en reproduisant l'intégralité de sa session sur le site…[lire la suite]

Réagissez à cet article

Source : *Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs*

Votre télévision connectée vous espionne… même éteinte ?

	Votre télévision connectée vous espionne… même éteinte ?

Dans plus de 25 % des cas, votre télévision connectée vous espionne et elle diffuse de nombreuses informations vous concernant sur Internet. Pire, vous n'avez aucune idée des informations recueillies, des personnes qui reçoivent ces données et de ce qu'elles font avec.

Une heure avec une télévision connectée

[…] il se trouve que nous achetons déjà ce genre d'appareils, et ces objets connectés en savent long sur nous. En une heure seulement, Avira a constaté qu'une smart TV fouinait et relevait une quantité d'informations sur son domicile : A ouvert trois ports vulnérables sur Internet ; à scanné le réseau du domicile pour trouver d'autres objets connectés ; à recueilli 750 pages d'informations textuelles sur la personne qui utilise l'appareil et sa façon de l'utiliser ; à envoyé ces informations à 13 serveurs, dont nombre sont inconnus ; à transféré les informations aux services non activés et n'ayant pas de compte utilisateur inscrit ; pire encore, la télévision a effectué tout cela alors que personne dans la maison ne l'utilisait activement…[lire la suite]

Réagissez à cet article

Source : *ZATAZ Votre télévision connectée vous espionne… même éteinte ? – ZATAZ*

Une faille permet d’écouter 77 % des smartphones Android

	Une faille permet d’écouter 77 % des smartphones Android

Voilà qui risque d'augmenter la paranoïa de celles et ceux qui pensent qu'ils sont écoutés, via leur smartphone, à tout moment de la journée : les chercheurs de MWR Labs ont découvert une nouvelle faille majeure qui toucherait plus des trois quarts des smartphones Android en circulation. Une faille que Google a comblée, mais seulement dans Android 8.0 Oreo.

Le problème de cette nouvelle faille, c'est qu'elle est très facilement exploitable par un développeur malintentionné : il ne s'agit pas d'une attaque à proprement parler mais d'un souci dans les autorisations données aux applications.

Le service Android MediaProjection au centre de cette nouvelle faille

Les chercheurs de MWR Labs ont découvert que Google, qui développe Android, a réalisé un changement majeur dans les autorisations d'un des services les plus anciens d'Android : MediaProjection. Ce service est en mesure d'enregistrer l'audio ainsi que l'écran du smartphone et est utilisé par certaines applications….[lire la suite]

Réagissez à cet article

Source : *Une faille permet d'écouter 77 % des smartphones Android*

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

---

Ce dispositif donne aux services de renseignement français un moyen d'analyser automatiquement les métadonnées des communications Internet, notamment pour lutter contre le terrorisme.

De nouvelles oreilles pour le renseignement. Longtemps inactives, les boîtes noires sont désormais en cours de déploiement. Francis Delon, le président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'a révélé à l'occasion d'une conférence organisée à Grenoble. Il précise qu'une première boîte noire a été activée «début octobre», à l'issue d'un «travail qui a duré plusieurs mois».

Prévu par l'article 851-3 du Code de la sécurité intérieure, le dispositif a été particulièrement critiqué en amont du vote de la loi renseignement de 2015. Il permet aux services de renseignement d'analyser de grandes quantités de métadonnées (relatives au contexte d'un message, comme son origine ou sa date d'envoi) à la volée, afin de détecter une éventuelle menace terroriste. Francis Delon se veut néanmoins rassurant. «Les données récoltées sont des données de connexion anonymisées, recueillies de façon non ciblée pour être mises dans une sorte de grande marmite étanche», a-t-il résumé, par une métaphore de son cru…[lire la suite]

Réagissez à cet article

Source : *Loi renseignement : une première «boîte noire» activée pour surveiller les communications*

Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés

La faille de sécurité « HomeHack » permettait de prendre le contrôle de n'importe quel objet connecté du fabricant coréen LG. Mais appliquée aux robots aspirateurs, elle serait un moyen offert aux hackers d'observer l'intérieur des maisons.

Pratiques parce qu'ils nous simplifient la vie et qu'on peut les piloter depuis une simple application mobile, les objets connectés sont aussi potentiellement de véritables chevaux de Troie dans notre intimité.
Les experts de l'entreprise de cybersécurité Check Point ont révélé une faille de sécurité, « HomeHack », via laquelle il était possible de prendre le contrôle à distance d'un aspirateur LG Hom-Bot et d'espionner l'intérieur d'une maison au moyen de la caméra intégrée, comme le montre cette vidéo :
http://www.youtube.com/embed/BnAHfZWPaCs
Communiqué à LG en juillet dernier, le problème a depuis été corrigé par le constructeur en septembre, mais une question demeure : comment être certain que les objets connectés qui nous entourent sont assez sécurisés ? En effet, il est régulièrement proposé aux clients de synchroniser l'ensemble de leurs appareils sur un même système, ici l'application mobile SmartThinQ de LG, disponible sur Android et iOS…[lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité permet aux hackers de vous espionner via des aspirateurs connectés*

Privacy Shield : Le transfert de données Europe-USA suffisamment sécurisé ?

	Privacy Shield : Le transfert de données Europe-USA suffisamment sécurisé ?

Pour le Conseil national du numérique, le Privacy Shield doit être « renégocié » car l'accord n'offre pas de garanties suffisantes à la protection des données.

A l'occasion du premier bilan annuel du Privacy Shield et de ses garanties, le **Conseil national du numérique** (CNNum) exprime sa divergence.
L'accord de transfert d'une partie des données entre l'Union européenne et les Etats-Unis, qui a succédé au dispositif Safe Harbor à partir du 1er août 2016, « doit être renégocié », selon le comité consultatif d'experts en charge d'éclairer les pouvoirs publics sur le numérique.
Celui-ci dit partager les inquiétudes d'autres organisations comme les CNIL européennes (fédérées à travers le G29), la commission des libertés civiles du Parlement européen et des associations de défense des droits.
« Le Privacy Shield présente un trop grand nombre de zones d'ombre et ne donne pas suffisamment de garanties à la protection des données personnelles des Européens », souligne par voie de communiqué le CNNum.
L'accord en l'état est *« faible, susceptible d'annulation sur les mêmes fondements que son prédécesseur ».*
Le Safe Harbor avait été invalidé fin 2015 par la Cour de justice de l'Union européenne (CJUE).
La collecte massive et indifférenciée de données pratiquée par les services de renseignement américain, une pratique mise à jour par les révélations d'Edward Snowden relative au cyberespionnage américain, était au coeur de ce dossier.
Le Privacy Shield n'offrirait toujours pas de garanties satisfaisantes dans ce domaine.

Bouclier percé ?

Lors de négociations qui ont précédé l'adoption du Privacy Shield en juillet 2016, la Commission européenne avait obtenu des autorités américaines une avancée présumée : la collecte de masse de données devait être écartée au profit d'une collecte ciblée.
Mais cette avancée n'est qu'une *« simple directive présidentielle »* prise par l'ancien locataire de la Maison Blanche, Barack Obama, souligne le CNNum dans son communiqué. Sur le fond, *« le droit américain reste largement inchangé »* en la matière.
« Les évolutions législatives et jurisprudentielles récentes, combinés à la position affichée par la nouvelle administration [Trump] » sont *« un signal politique particulièrement préoccupant. »*
Le CNNum fait notamment référence aux évolutions à venir de la législation américaine en matière de données, dont le titre VII du FISA Amendments Act (FAA).Il est censé expirer à la fin de l'année mais pourrait être reconduit.
Ces dispositions incluent la controversée « section 702 », qui autorise la surveillance large de tout ressortissant d'un pays étranger.
Une section qui a notamment servi de fondement aux programmes de surveillance Prism et Upstream de la National Security Agency (NSA) que Snowden avait dévoilés à partir de mi-2013.
Le Conseil national du numérique s'inquiète également de *« la vacance de postes clés en charge de la supervision du dispositif côté américain »* et de *« l'effectivité des mécanismes de recours. »*
Des problématiques de souveraineté sont également soulevées par l'organisation.
Les données constituent un actif essentiel de l'économie numérique. Or les flux de données d'Europe sont *« massivement captés par les États-Unis »*, souligne l'organisation.
Cette asymétrie des transferts de data avait déjà été constaté dans le cadre du Safe Harbor…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Transfert de données Europe-USA: le CNNum rejette le Privacy Shield | Silicon*

Télétravail et protection des données personnelles

Le télétravail pose certaines questions concernant d'abord le droit du salarié à la déconnexion mais aussi sur la protection des données. La barrière de plus en plus floue entre outils personnels et outils professionnels avec la collecte d'informations impose de revoir le régime juridique de la protection des données. Explications par François Alambret, Counsel chez Bryan Cave Paris.

L'essor du télétravail a accru la nécessaire protection des données personnelles. Si ces deux sujets se complètent, ils ne doivent éclipser les autres aspects de la digitalisation des relations de travail.

Le développement du télétravail

Le télétravail n'a pas attendu l'émergence d'internet pour exister mais il s'est incontestablement développé par la conjonction de différents facteurs : les progrès des outils technologiques individuels, l'individualisation des relations du travail et l'accroissement des centres urbains et leur congestion concomitante.

Poussé d'abord par les revendications des salariés, le télétravail a été organisé par les entreprises par le biais d'accords collectifs ou de chartes (informatiques ou sur la qualité de vie au travail), puis reconnues par les organisations syndicales au niveau européen et national (accord cadre européen sur le télétravail du 16 juillet 2002 et accord national interprofessionnel du 19 juillet 2005). Enfin, encadré par le législateur par le biais des lois du 22 mars 2012, du 8 août 2016 (Loi travail dite loi « El-Khomri ») et les ordonnances Macron en cours de promulgation.

Cette dernière étape législative vise encore à simplifier le recours au télétravail, notamment par le biais d'un accord ou d'une charte d'entreprise en dispensant ensuite les parties d'un avenant au contrat de travail (voir article 24 de l'ordonnance n°3 du 31 aout 2017 modifiant les articles L.1222-9 et suivants du code du travail).

L'employeur n'est plus tenu, non plus, de supporter le coût de ce télétravail, ce qui autorise le salarié « de facto » à utiliser son propre matériel informatique (avec les conséquences afférentes en termes de confidentialité et de sécurité).

La protection des données personnelles

Dès son apparition, le télétravail s'est heurté aux problématiques de la protection des données informatiques. Cette contrainte a d'ailleurs été rappelée expressément par les partenaires sociaux dans leur premier accord européen (point 5 de l'accord cadre du 16 juillet 2002) et national (article 5 de l'accord national interprofessionnel du 19 juillet 2005).

Et de fait, le télétravail accroît les risques sur la protection des données de façon à la fois structurelle et technique. Structurellement, par le mode même d'organisation du travail (qui augmente les communications digitales au détriment de communications directes et orales dans l'entreprise) et techniquement car le salarié demeure à distance des services informatiques de l'entreprise et peut dorénavant utiliser ses propres matériels informatiques avec les risques qui en découlent.

Le règlement communautaire sur la protection des données en date du 27 avril 2016 (souvent dénommé GDPR « Global Data Protection Regulations ») prend acte de la digitalisation croissante de la société et de ses nouvelles formes de travail. Il renforce les mesures de protection à l'égard des personnes et donc vis-à- vis des salariés et des télétravailleurs.

L'imbrication des deux notions/ le rôle de l'entreprise

Ces deux sujets (télétravail et protection des données) s'accompagnent et s'encouragent mutuellement. Le renforcement de la protection des données offre des garanties nécessaires au développement du télétravail.

Toutefois, ce cadre législatif et réglementaire posé, c'est aux acteurs de l'entreprise de s'en saisir et de le façonner.

A eux de négocier et de rédiger un accord collectif ou une charte permettant une mise en œuvre fluide mais aussi sécurisée du télétravail, dans le respect du nouveau règlement communautaire du 27 avril 2016.

Mais traiter ces deux thèmes isolément méconnaît l'ampleur des bouleversements de la digitalisation de la société et des relations du travail…[lire la suite]

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Télétravail et protection des données personnelles – LE MONDE DU DROIT : le magazine des professions juridiques*

Campagne d’espionnage de grande envergure sur Internet

	Campagne d’espionnage de grande envergure sur Internet

Les chercheurs ESET® ont détecté des campagnes d'espionnage liées à FinFisher, le célèbre spyware également connu sous le nom de FinSpy. Sept pays sont infectés.

FinFisher est un spyware (logiciel espion) **commercialisé en tant qu'outil de surveillance et d'intrusion informatique.**Il est **vendu à une vingtaine d'organismes gouvernementaux** à travers le monde. ESET pense qu'il a également été utilisé par des régimes autoritaires.

Les capacités d'espionnage de FinFisher s'étendent à :

• la surveillance via les webcams et les microphones (images retransmises en direct)

• l'enregistrement de frappe (keylogger)

• l'exfiltration des fichiers

Ce logiciel espion a reçu un certain nombre de modifications via des correctifs dans sa dernière version. Elles améliorent ses fonctions pour se montrer plus intrusif. FinFisher peut ainsi rester sous le radar de détection des solutions de sécurité et empêcher une analyse approfondie de son comportement. L'innovation la plus importante reste la méthode pour pénétrer les machines ciblées.

Lorsqu'un utilisateur ciblé est sur le point de **télécharger une application populaire telle que WhatsApp®, Skype® ou VLC Player®**, il est **automatiquement redirigé vers le serveur de l'attaquant. La victime installe alors une version qui inclut un malware de type Trojan et se trouve ainsi directement infectée par FinFisher.**

Mécanisme d'infection de la dernière variante de FinFisher

« Sur deux des sept campagnes menées, les logiciels espions se sont propagés au moyen d'une attaque man-in-the-middle. Autrement dit, les communications sont interceptées à l'insu des parties concernées. Nous pensons que **les principaux fournisseurs d'accès à Internet de ces deux pays ont joué un rôle crucial dans cette infection** », explique Filip Kafka, Malware Analyst chez ESET et à l'origine de cette recherche.

Ces campagnes sont les premières à révéler publiquement la probable implication (volontaire ou pas) d'un fournisseur d'accès à Internet dans la diffusion de malwares. « Les campagnes FinFisher sont des projets de surveillance perfectionnés et tenus secrets. Les méthodes utilisées associées à la portée de ces attaques en font une menace sans précédent », poursuit Filip Kafka.

Par le passé, ESET a publié un certain nombre d'articles sur les campagnes FinFisher. Vous pouvez les consulter ici. Les experts ESET ont également rédigé un article détaillé sur cette nouvelle campagne. Pour plus de détails, notre cybersecurity leader Benoît Grunemwald peut répondre à vos questions.

Note pour les éditeurs:

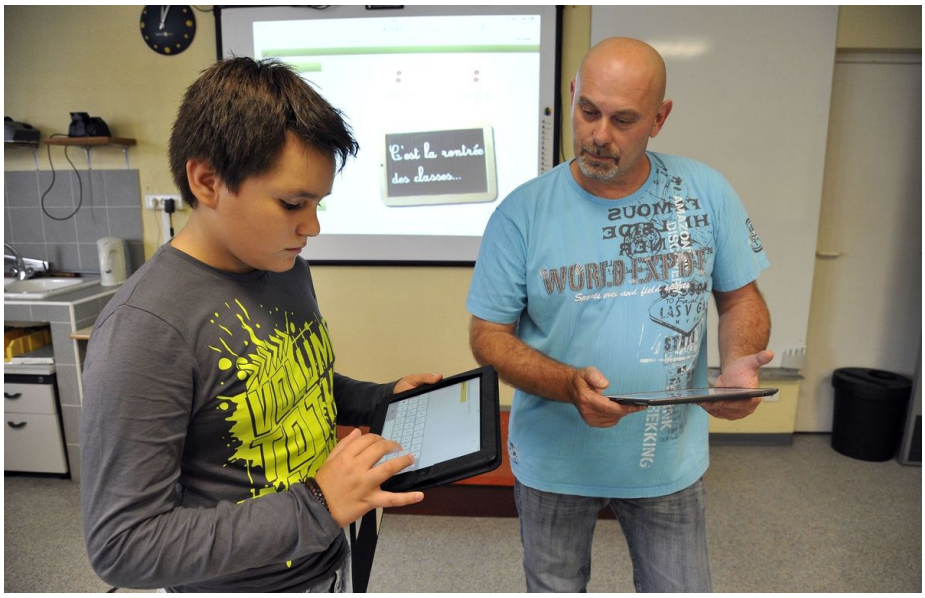
FinFisher, le soi-disant malware du gouvernement et l'approche de l'industrie de la sécurité sont sous les feux de la rampe. Pour ESET, il n'existe pas de malware dans la mesure où ce programme a été acheté d'une part puis modifié et détourné d'autre part par des individus mal intentionnés.

Lire la réponse d'ESET à une lettre ouverte adressée à Bits of Freedom, un groupe de défense des droits numériques…[lire la suite]

Réagissez à cet article

Source : ESET

Les données personnelles des écoliers français vont-elles échapper à Google?



Les données personnelles des écoliers français vont-elles échapper à Google?

Une «note interne» diffusée en mai ouvrait la possibilité aux entreprises du numérique de collecter des données scolaires. Les parents d'élèves avaient protesté auprès du ministre de l'Education. Jean-Michel Blanquer compte revoir la politique en la matière.

Pas d'école pour Google, Facebook, et autres géants du numérique, regroupés sous l'appellation Gafa. Jeudi, le porte-parole du gouvernement a indiqué que le ministre de l'Education Jean-Michel Blanquer comptait limiter l'accès de ces entreprises aux données scolaires des élèves.

Le ministre compte « revenir sur une circulaire [en fait, une lettre interne] signée deux semaines avant les présidentielles, qui ouvre très largement, peut-être trop largement l'accès des Gafa dans l'école », a expliqué Christophe Castaner.

Publicités ciblées

Rappel des faits : le 12 mai dernier, Matthieu Jeandron, délégué au numérique éducatif, adresse une lettre aux délégués académiques du numérique. Dans ce courrier, révélé par le Café pédagogique, il explique qu'il n'y a pas « de réserve générale sur l'usage des outils liés aux environnements professionnels chez les grands fournisseurs de service du web ». Un peu plus loin, il indique qu'il ne voit pas de « blocage juridique de principe à la connexion d'un annuaire avec l'un de ses services ».

En clair, cela signifie que Google, Facebook, et autres entreprises du numérique auraient pu collecter des listes d'élèves avec leurs noms, leurs classes, voire même leurs notes dans le cadre de travaux effectués en ligne. Ces données peuvent rapporter de l'argent : par exemple, on peut imaginer que Google, ayant connaissance des difficultés d'un élève, lui « propose » des publicités ciblées sur les cours en lign…[lire la suite]

Réagissez à cet article

Source : *Les données personnelles des écoliers français vont-elles échapper à Google?*

ACCReD, le mégafichier de données personnelles qui suscite la polémique

	ACCReD, le mégafichier de données personnelles qui suscite la polémique

---

Un décret paru dans le Journal officiel en pleine torpeur du mois d'août. La création d'ACCReD, mégafichier ciblant des milliers d'individus, a été discrète, voire escamotée.

Pourtant, comme l'a repéré Europe 1, ce nouveau traitement de données personnelles est loin d'être anecdotique.

Menace terroriste oblige, il doit améliorer le recoupement de fichiers déjà existants – celui des personnes recherchées, des antécédents judiciaires, des objets et véhicules signalés etc. – et en permettre une « consultation automatique et simultanée ». Au nom de la sécurité du territoire.

Mais un mois seulement après son apparition, la CNIL met déjà le holà. L'objectif d'ACCReD est certes « légitime », mais les moyens d'y parvenir suscitent quelques inquiétudes. Voici pourquoi.

Qui est fiché dans ACCReD ?

Tous les individus occupant un poste considéré comme « sensible » en France. Cette qualification est désormais élargie aux postes dans les aéroports, dans les centrales nucléaires mais aussi dans les événements festifs que ce soit des concerts, des festivals, des événements sportifs, etc…[lire la suite]

Que signifie ACCReD ?

Denis JACOPINI : (Automatisation de la Consultation Centralisée de Renseignements de Données)

Réagissez à cet article

Source : *Créé pendant l'été, un mégafichier de données personnelles suscite la polémique*