Privacy Shield : un « bouclier » troué à refuser !

	#Privacy Shield : un « bouclier » troué à refuser !

Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette décision, adoptée dans la plus grande précipitation, ne répond pas aux inquiétudes exprimées ces dernières semaines à tour de rôle par le groupe des CNILs européennes, le Parlement européen et différents gouvernements européens, ainsi que par les associations de défense des droits.

Le 6 octobre 2015 la Cour de justice de l'Union européenne avait annulé l'accord du « Safe Harbor » couvrant les transferts de données depuis 2000, estimant que celui-ci permettait une collecte massive des données et une surveillance généralisée sans offrir de voies de recours effectives aux États-Unis pour les individus concernés en Europe. Aujourd'hui, force est de constater que le Privacy Shield ne répond pas non plus aux exigences de la Cour de justice.
Sur les principes de respect de la vie privée qui incombent aux entreprises couvertes par le Privacy Shield, on peut se demander l'utilité même d'une telle décision dans la mesure où celle-ci ne se substituera pas aux clauses contractuelles types ni aux règles internes d'entreprises, moins contraignantes et actuellement en vigueur, mais qu'elle s'y ajoutera. Cela signifie que si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations qui lui incombent en matière de vie privée, elle pourra continuer à traiter des données avec les deux mécanismes internes cités plus hauts.
Mais le cœur de la décision se retrouve plutôt dans le chapitre sur l'accès aux données par les autorités publiques des États-Unis. Dans le texte, il n'est pas question de « surveillance de masse » mais plutôt de « collecte massive ». Or, si les États-Unis ne considèrent pas la collecte de masse comme de la surveillance, l'Union européenne, elle, par l'intermédiaire de sa Cour de justice, a tranché sur cette question en considérant, dans l'affaire C-362/14 Schrems c. Data Protection Commissioner, que la collecte massive effectuée par l'administration des États-Unis était de la surveillance de masse, contraire à la Charte des droits fondamentaux de l'Union européenne. Cette décision avait mené à l'invalidation du « Safe Harbor », et tout porte à croire que les voeux pieux et les faibles garanties d'amélioration exprimées par le gouvernement américain ne suffiront pas à rendre la décision du Privacy Shield adéquate avec la jurisprudence européenne.
Il en va de même sur la question des possibilités de recours. L'une des exigences de la CJUE, des CNIL européennes, du contrôleur des données personnelles et de la société civile était que toute personne concernée par un traitement de données avec cet État tiers puisse avoir la possibilité de déposer une plainte et de contester un traitement ou une surveillance illégale. Pour pallier cette sérieuse lacune du Safe Harbor, un mécanisme de médiateur (« #Ombudsperson ») a été instauré. L'initiative aurait été bonne si ce médiateur était réellement indépendant. Mais d'une part il est nommé par le Secrétaire d'État, d'autre part les requérants ne peuvent s'adresser directement à lui et devront passer par deux strates d'autorités, nationale puis européenne. L'Ombudsperson pourra simplement répondre à la personne plaignante qu'il a procédé aux vérifications, et pourra veiller à ce qu'une surveillance injustifiée cesse, mais le plaignant n'aura pas de regard sur la réalité de la surveillance. Cette procédure ressemble à celle mise en place en France par la loi Renseignement avec la #CNCTR et, pour les mêmes raisons, ne présente pas suffisamment de garanties de recours pour les citoyens.
Le projet de Privacy Shield, préparé et imposé dans la précipitation par la Commission européenne et le département du Commerce américain, ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. Les gouvernements européens et les autorités de protection des données doivent donc absolument refuser cet accord, et travailler à une réglementation qui protège réellement les droits fondamentaux. Les nécessités d'accord juridique pour les entreprises ayant fait de l'exploitation des données personnelles leur modèle économique ne peuvent servir de justification à une braderie sordide de la vie privée de dizaines de millions d'internautes européens.
Article original de La Quadrature du Net

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : un « bouclier » troué à refuser ! – Global Security Mag Online

---

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

Le Privacy Shield (« bouclier de protection des données personnelles »), un accord politique censé encadrer l'utilisation des données personnelles des citoyens Européens par les entreprises sur le sol américain, a été validé par les Etats membres, vendredi 8 juillet.

Pour la première fois, les Etats-Unis ont donné à l'Union européenne l'assurance écrite que l'accès des autorités aux données personnelles serait soumis à des limitations claires, des garde-fous et des mécanismes de contrôle, tout en écartant la surveillance de masse indiscriminée des données des Européens » s'est réjoui la commission dans un communiqué.

Le Privacy Shield est censé remplacer le Safe Harbor, un accord similaire qui a été invalidé par la Cour de justice de l'Union européenne (CJUE), qui a notamment cité le peu de cas que faisaient les agences de renseignement américaines des données personnelles des citoyens européens stockées sur le sol américain.
Les entreprises du numérique, placées dans une situation juridiquement inconfortable depuis l'annulation du Safe Harbor, ont salué cette étape supplémentaire sur le chemin de l'adoption définitive. « Même si les négociations n'ont pas été faciles, nous félicitons la commission et le ministère du commerce américain pour leur travail de restauration de la confiance dans les transferts des données entre l'UE et les Etats-Unis », a dit John Higgins, le directeur général de DigitalEurope, un lobby rassemblant notamment Google, Apple, Microsoft et IBM, qui dit aussi espérer que grâce au Privacy Shield « l'Europe puisse à nouveau se concentrer sur la manière dont les flux de données peuvent jouer un rôle dans la croissance économique ».

DE NOMBREUX OBSTACLES DEMEURENT

L'accord, entre la commission et les Etats-Unis, doit encore être validé par le collège des commissaires européens, avant son adoption définitive qui devrait intervenir le 12 juillet prochain, après des mois d'âpres négociations. Ce n'est pas la fin du débat autour de cet accord contesté.
L'accord n'a pas fait consensus auprès des Etats membres, les diplomates représentant plusieurs pays – l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters – se sont abstenus. Un moyen d'« exprimer leur méfiance vis-à-vis du texte » anticipait, jeudi lors d'une conférence, David Martinon, ambassadeur français pour la cyberdiplomatie et l'économie numérique, cité par le site Silicon.fr.
Par ailleurs, cet accord, sera très certainement contesté devant les tribunaux après son adoption. Max Schrems, l'Autrichien tombeur du prédécesseur du Privacy Shield, pourrait attaquer l'accord devant les juridictions européennes.
Dans le même ton, La Quadrature du Net, association française de défense des libertés numériques, a dénoncé un accord qui « ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. »
Article original de Martin Untinsinger

Réagissez à cet article

Original de l’article mis en page : Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté

L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté

Les Etats membres de lUE ont donné leur feu vert au «Privacy Shield», qui vient remplacer laccord «Safe Harbor» invalidé en octobre par la justice européenne.

Le «Privacy Shield» est sur la rampe de lancement. La Commission européenne l'a annoncé ce vendredi matin : le nouvel accord-cadre sur les transferts de données personnelles depuis le Vieux Continent vers les Etats-Unis a reçu le feu vert des Etats membres de l'Union, moins quatre abstentions (l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters). Il devrait être adopté formellement par la Commission mardi prochain. Ce «bouclier de confidentialité» vient ainsi succéder à l'accord dit «Safe Harbor» (ou «sphère de sécurité»), invalidé il y a neuf mois par la justice européenne.

Deux ans de négociation

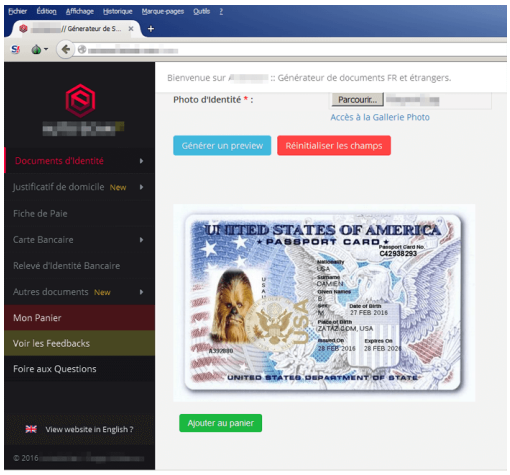
Mis en place en 2000, le Safe Harbor était censé garantir aux citoyens européens un niveau de protection suffisant de leurs données personnelles transférées sur le sol américain : les entreprises qui y adhéraient s'engageaient à respecter les normes de l'UE en la matière… via une certification annuelle qu'elles pouvaient s'autodécerner. Une «garantie» minimale qui a volé en éclats en 2013 avec les révélations d'Edward Snowden sur les pratiques de surveillance massive de la NSA, et notamment le programme Prism, qui permet à l'agence américaine d'accéder aux données stockées par les géants du Net.
Article original de Amaelle Guiton
Photo Dado Ruvic. Reuters

Réagissez à cet article

Original de l’article mis en page : Données personnelles : laccord entre lEurope et les Etats-Unis sur le point dêtre adopté – Libération

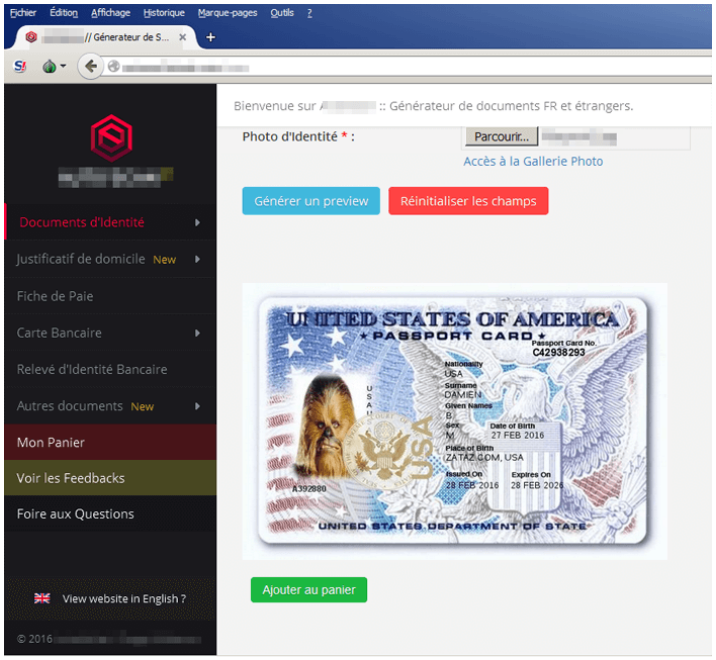
---

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.

Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

Microsoft stocke 200 Mo de données informatiques sous forme d’ADN

Microsoft stocke 200 Mo de données informatiques sous forme d’ADN

L'université de Washington a collaboré avec Microsoft pour écrire 200 Mo de données informatiques sur un bout d'ADN. Le but est d'optimiser au maximum l'espace de stockage et sa durabilité en allant vers un stockage biologique.

Écrire 200 méga-octets de données informatiques sur de l'ADN de synthèse. C'est la prouesse réalisée par des scientifiques de l'université de Washington en collaboration avec Microsoft. Les informations inscrites sur les molécules contiennent la Déclaration universelle des droits de l'homme en plus de 100 langues, les 100 livres électroniques les plus téléchargés sur la bibliothèque Projet Gutenberg, une partie des bases de données de Crop Trust, un groupe consultatif international pour la recherche agricole et un clip musical du groupe américain Ok Go,
« *Nous utilisons l'ADN comme un espace de stockage de données numériques* », explique le professeur Luis Ceze dans une vidéo. « *La raison pour laquelle nous faisons cela est parce que l'ADN est très dense et que l'on peut mettre énormément d'informations dans un très petit volume* », ajoute-t-il.

LA TOTALITÉ DE L'INTERNET POURRAIT TENIR DANS UNE BOÎTE À CHAUSSURES
Il affirme également que la totalité de l'Internet pourrait tenir dans une boîte à chaussures grâce à ce procédé. L'autre motivation des scientifiques est aussi le fait que l'ADN peut être conservé très longtemps. « *Dans les bonnes conditions, il peut durer des milliers d'années tandis que les technologies de stockages ne tiennent que quelques décennies* ».

L'ADN est fait de différentes séquences de quatre molécules : l'adénine (A), la guanine (G), la cytosine (C) et la thymine (T).Les scientifiques ont réussi à encoder les données qu'ils voulaient stocker sur les quatre molécules de base de l'ADN synthétisé.
En analysant l'ADN, ils peuvent lire les informations et les rétablir à leur état original.
Les 200 Mo de documents sont enregistrés sur un bout d'ADN qui fait la taille de quelques grains de sucre. Celui-ci a été encapsulé pour éviter toute dégradation.
Les capacités de stockage de l'ADN sont énormes. Malheureusement, lire les données dessus prend beaucoup de temps – jusqu'à plusieurs heures. Aussi, ce procédé n'est pas prêt d'être démocratisé, d'autant plus qu'il coûte encore très cher. Mais cela serait apparemment en train de changer. « *La technologie pour lire l'ADN est en train de se développer rapidement et pourrait devenir suffisamment rapide et bon marché pour être commercialisée* », explique Luis Ceze à The Register.
Le scientifique pense que les premiers clients seront probablement les centres de données pour qui l'optimisation de l'espace de stockage est un enjeu permanent.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Microsoft stocke 200 Mo de données informatiques sous forme d'ADN – Sciences – Numerama

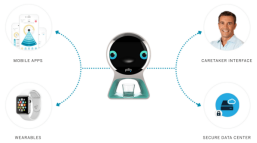
Pillo, un robot intelligent et connecté en guise de pilulier

Pillo, un robot intelligent et connecté en guise de pilulier

Pillo est un petit robot à placer dans le foyer, qui reconnait les membres de la famille pour distribuer à chacun les pilules dont ils ont besoin, et délivrer des conseils médicaux adaptés.

Pillo ne sera disponible qu'en 2017, toutefois, ce petit robot pilulier se dévoile déjà à l'occasion de son financement participatif sur IndieGogo. Un crowd-funding presque intégralement réussi ce lundi (près de 75 000 dollars levés) alors-même que le robot n'a été mis en ligne qu'il y a une semaine. Le petit pilulier aura réussi à convaincre des backers en très peu de temps.

Il a pour cela quelques arguments : le petit assistant domestique se propose d'être une interface afin de monitorer et gérer au quotidien la santé des foyers. Pillo distribue quotidiennement aux membres d'une famille les pilules qui lui sont nécessaires et pour cela le robot est équipé d'une technologie de détection des visages, afin de rendre le pilulier totalement autonome et faciliter nos quotidiens. Seulement, là où le robot convainc vraiment, c'est qu'en dehors de son rôle de distributeur, il parvient à trouver un vrai rôle en tant qu'objet .



En plus de surveiller votre consommation de médicaments et de vous demander d'en recommander quand il risque de vous en manquer, Pillo répond également à de nombreuses questions sur votre santé et les aliments que vous consommez et s'ambitionne comme une véritable interface pour les consultations à distance par exemple. Or, c'est là qu'on trouve la valeur ajoutée du Pillo face au pilulier de mamie ; le robot exécute une tâche essentielle chaque jour, mais en plus de répondre à un besoin, il introduit assez de composants et de possibilités pour s'ambitionner comme un véritable hub de la health tech à la maison.

Ses concepteurs ont promis que le produit serait commercialisé, peu importe la réussite de la campagne IndieGogo qui comme souvent sert d'opération publicitaire pour une startup. Le robot était disponible à partir de 256 $ sur la plateforme et sera commercialisé plus de 600 $ en 2017, dans un premier temps uniquement aux USA.
Mieux vaudra en tout cas être sûr de sa fiabilité et de sa sécurité, pour accepter de reposer sur un robot connecté pour distribuer ses pilules au petit déjeuner…
Article original de Corentin Durand

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

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

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

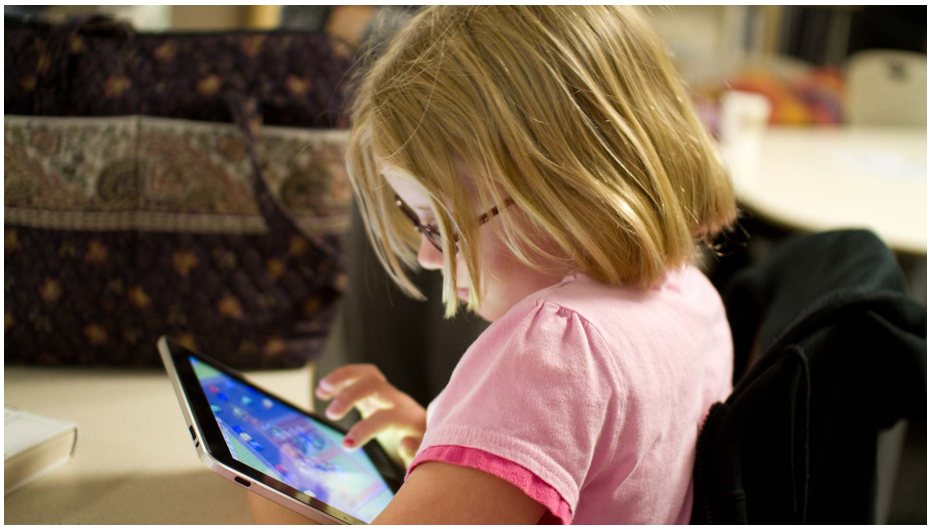
Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Pillo : un robot en guise de pilulier intelligent et connecté — Tech — Numerama

---

Attention aux ondes des tablettes et smartphones pour les enfants !



Attention aux ondes des tablettes et smartphones pour les enfants !

Un rapport publié par l'agence de la sécurité sanitaire met en garde les parents sur l'exposition des enfants aux ondes. Elle recommande un usage modéré et encadré des technologies sans fil. Elle suggère aussi une révision de la réglementation.

Attention aux technologies sans fil ! Telle est la mise en garde que vient de formuler l'agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) ce vendredi, dans un rapport portant sur le sujet hautement sensible de l'exposition aux radiofréquences et à la santé des enfants. Dans celui-ci, elle note « des effets possibles sur les fonctions cognitives et le bien-être » et recommande de limiter et d'encadrer l'usage de ces technologies.

Dans le cadre de ce travail, ce sont les enfants de moins de six ans qui ont fait l'objet d'un suivi particulier. L'Anses avait été saisie par les pouvoirs publics afin de vérifier si les dispositions réglementaires à propos des appareils radioélectriques destinés aux plus jeunes sont suffisamment protectrices en matière de santé et de sécurité. Il ressort que « les enfants pouvaient être plus exposés que les adultes » du fait de leurs spécificités morphologiques et anatomiques.

C'est ce que détaille à France Info Olivier Merckel, chargé de l'évaluation des risques. « Les enfants sont plus exposés que les adultes aux champs électromagnétiques : l'épaisseur du crâne chez les enfants est plus petite que chez les adultes donc on a une exposition globale plus importante ». En outre, les « caractéristiques de certains de leurs tissus » contribuent à cette vulnérabilité accrue. Il faut donc redoubler de vigilance quant à l'exposition des petits.
Le problème, c'est la généralisation des équipements de transmissions sans fil dans leur environnement. « Les données disponibles sur l'exposition montrent une forte expansion de l'usage des nouvelles technologies sans-fil, notamment chez les très jeunes enfants », relève le rapport. Il y a le smartphone, il y a la tablette, il y a les objets connectés, il y a le babyphone, il y a les jouets radiocommandés… et beaucoup d'autres appareils dédiés à la surveillance du petit ou à l'occuper.

LES ENFANTS SONT PLUS EXPOSÉS QUE LES ADULTES
Or, on le devine aisément : plus la source émettrice est proche, plus l'intensité et la quantité du rayonnement sont élevées. En la matière, des appareils comme des smartphones ou des babyphones peuvent légitimement constituer une source d'inquiétude, car ils sont en général très près de la tête — que ce soit pour parler au téléphone ou bien pour entendre les bruits de bébé et s'assurer que tout va bien.

QUELS EFFETS POTENTIELS ?
L'Anses souligne toutefois que « les données actuelles ne permettent pas de conclure à l'existence ou non d'un effet des radiofréquences chez l'enfant sur le comportement, les fonctions auditives, les effets tératogènes et le développement, le système reproducteur, les effets cancérogènes, le système immunitaire, la toxicité systémique ». Des études plus approfondies seront sans doute nécessaires.
L'Anses mentionne toutefois deux cas où à un effet des radiofréquences est possible : les fonctions cognitives d'abord. « Les résultats montrant des effets aigus se basent sur des études expérimentales dont la méthodologie est bien maîtrisée », note le rapport. Un effet négatif sur le bien-être peut aussi être envisagé, même s'il « pourrait cependant être lié à l'usage du téléphone mobile plutôt qu'aux radiofréquences qu'ils émettent ». Bref ce serait plus ce serait la manière dont on s'en sert le problème.

UN USAGE RAISONNABLE
Est-ce que cela veut dire qu'il faut tenir les enfants loin de ces sources d'émission ? En clair, faut-il les priver de portable jusqu'à un âge avancé, retirer les jouets high tech et vérifier que la chambre n'est pas trop exposée ? Pour Olivier Merckel, il faut prendre quelques mesures, mais ne pas non plus exagérer. Les jeunes de moins de 13 ans peuvent passer « quelques appels, quelques SMS par jour » mais « certainement pas plusieurs heures ».
Un usage maitrisé. Tel est donc le conseil général donné par l'Anses à l'attention des parents. « L'Agence recommande aux parents d'inciter leurs enfants à un usage raisonnable du téléphone mobile, en évitant les communications nocturnes et en limitant la fréquence et la durée des appels ». Mais des actions doivent aussi être engagées du côté des pouvoirs publics, au niveau français ou européen.

UNE RÉGLEMENTATION À REVOIR
Pour l'Anses, il convient d'actionner plusieurs leviers, à commencer par l'obligation de soumettre l'ensemble des dispositifs radioélectriques, et notamment ceux destinés aux enfants, « aux mêmes obligations réglementaires en matière de contrôle des niveaux d'exposition et d'information du public que celles encadrant les téléphones mobiles ». L'agence demande aussi de reconsidérer les niveaux de référence visant à limiter l'exposition environnementale.
Les pouvoirs publics doivent également « réévaluer la pertinence du débit d'absorption spécifique (DAS) ». Il s'agit d'un indicateur utilisé pour l'établissement des valeurs limites d'exposition des personnes, à des fins de protection contre les effets sanitaires connus et avérés (effets thermiques) des radiofréquences. Il convient également de « développer un indicateur représentatif de l'exposition réelle des utilisateurs de téléphones mobiles », « quelles que soient les conditions d'utilisation ».

UN DÉBAT PERMANENT
La question des ondes et de leurs effets potentiels sur la santé a donné lieu à une littérature scientifique abondante. L'Anses elle-même publiait déjà en octobre 2013 un avis dans lequel elle notait à l'absence d'effets avérés sur la santé mais suggérait quand même de prendre des mesures de précaution, en particulier du côté des enfants et des utilisateurs intensifs. La publication avait toutefois fait l'objet de critiques dans la société civile, au sein d'associations spécialisées.
Deux ans auparavant, le centre international de recherche sur le cancer déclarait que les champs électromagnétiques de radiofréquence sont peut-être cancérogènes. Mais là encore, les conclusions avaient été discutées. Ainsi, des organisations professionnelles avaient estimé que le risque soulevé par les experts n'avait pas été clairement démontré par un lien évident de cause à effet et, que de ce fait, la poursuite des travaux scientifiques est indispensable.
Article original de Julien Lausson

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ondes : les enfants doivent moins utiliser les tablettes et smartphones

---

Le chiffrement des smartphones Android incassable ?

Le chiffrement des smartphones Android incassable ?

Un chercheur en sécurité décrit comment faire sauter la protection par chiffrement des données sur les smartphones Android équipés de puces Qualcomm.

Chiffrer l'ensemble de ses données sur un support de stockage est un bon moyen de les protéger en cas de perte ou vol du dit support. Néanmoins, il n'est pas infaillible. Particulièrement sur les smartphones Android équipés de processeurs Qualcomm. C'est ce que démontre le chercheur en sécurité Gal Beniamini. Dans un document très détaillé, il indique comment contourner les systèmes de protection. Et plus particulièrement, *« comment l'exécution du code TrustZone du noyau peut être utilisé pour briser efficacement le schéma de l'Encryption Full Disk d'Android »*, précise le chercheur.

Le Full Disk Encryption (FDE), la technique de chiffrement du disque d'Android, est proposé par Google depuis la version 5.0 de l'OS mobile. Il permet de générer des clés de chiffrement maître et esclave de 128 bits. La clé maître, également appelée DEK (pour Device Encryption Key) est protégée par chiffrement à partir du mot de passe, du code PIN ou du schéma de déverrouillage choisi par l'utilisateur. La DEK est stockée sur le smartphone (ou la tablette) dans un espace non chiffré de l'appareil, le *crypto footer*. Et c'est là que le problème survient. A cause d'une faille dans les processeurs de Qualcomm.

Utiliser une Trustlet

Pour comprendre pourquoi, il faut savoir que Android dispose, comme iOS, de mécanismes de temporisation et de blocage de l'appareil pour interdire les attaques par force brute (essais successifs de saisie des identifiants). Ces mécanismes sont liés au module KeyMaster qui s'exécute dans un environnement séparé de l'OS et considéré comme sécurisé, le Trusted Execution Environment (TEE). Le KeyMaster peut ainsi générer des clés de chiffrement sans les révéler au système d'exploitation. Une fois générées, ces clés sont à leur tour chiffrées et communiquées à l'OS. Quand ce dernier les sollicite, un bloc de données (le Blob, Binary Large OBject, un type de données qui permet l'intégration d'un pilote, souvent propriétaire, dans le code du noyau Linux) est fourni au KeyMaster sous forme d'une clé RSA de 2048 bits.

Mais le KeyMaster dépend de l'implémentation qu'en fait le fabricant sur son matériel. En l'occurrence, Qualcomm exploite bien le KeyMaster dans la TrustZone. Sauf que le TEE fourni par le constructeur, le QSEE (Qualcomm Secure ExecutionEnvironment), autorise des appliquettes (Trustlets) a s'exécuter dans cette zone sécurisée. Et, selon le chercheur, il est possible d'exécuter sa propre Trustlet dans la TrustZone en exploitant potentiellement une vulnérabilité Android. A partir de là, l'attaquant peut obtenir des privilèges administrateur et accéder au Blob qui contient les clés générées. Il ne reste alors plus qu'à lancer une attaque par force brute pour retrouver le code secret de l'utilisateur et disposer ainsi de la clé de déchiffrement du support de stockage.

Une correction difficile

Certes, la manœuvre n'est pas à la portée du premier venu. Et nécessite de disposer du terminal en main. Mais le déchiffrement d'un disque peut visiblement être exécuté par le fabricant des puces. Lequel peut avoir à se plier à une requête judiciaire comme on l'a vu avec Apple dans l'affaire de l'attentat de San Bernardino. Qui plus est, selon Qualcomm, le « bug » n'est pas facile à corriger. La correction demandera probablement une modification de l'architecture des processeurs. Lesquels équipent aujourd'hui une majorité de smartphones Android de la planète.

Néanmoins, le chercheur reste optimiste. *« J'espère qu'en jetant la lumière sur le sujet, cette recherche va motiver les équipementiers et Google à se réunir pour penser à une solution plus robuste pour le FDE*, écrit-il. *[…] Je crois qu'un effort concentré des deux côtés peut aider à rendre la prochaine génération d'appareils Android vraiment « inviolable ». »*

Article original de Christophe Lagane

Original de l'article mis en page : Le chiffrement des smartphones Android n'est pas incassable

---

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X

(ESET)

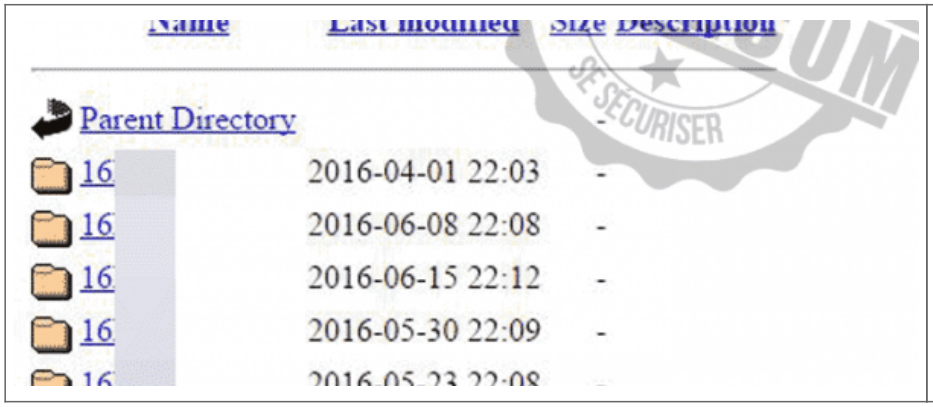
Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Fuite de données colmatée pour l'Université de Bordeaux



Fuite de données colmatée pour l'Université de Bordeaux

Un problème informatique à l'université de Bordeaux donnait accès à plus de 15 000 dossiers d'étudiants. La CNIL est intervenue à la suite du protocole d'alerte de ZATAZ pour faire colmater une fuite de données que personne n'avait vue.

Tout a débuté voilà quelques semaines. Benjamin postule sur la plateforme APOFLUX de l'Université de Bordeaux. Rapidement, APOFLUX permet de déposer ses vœux pour rejoindre un cursus, une formation. Comme l'indique le site, APOFLUX est un outil de dépôt de vœux « ***Il ne s'agit en aucun cas de votre inscription administrative définitive à l'Université de Bordeaux***« . Bref, un espace ou les étudiants déposent des dizaines d'informations allant du simple au très sensible. « ***En cherchant une information sur mon dossier,*** m'expliquait alors Benjamin, ***je me suis rendu compte d'un – truc – plutôt moche***« . Et je trouve que le terme moche est très poli. Via un espace web non protégé baptisé « Dépôt », n'importe quel internaute avait accès à l'ensemble des dossiers des étudiants postulants. Chaque espace de stockage offrait à la lecture des curieux, de maladroits de la souris ou de violeurs d'intimité numérique, les relevés de notes, lettres de motivations, CV… ainsi qu'à l'ensemble des candidatures passées par APOFLUX. Le lien avait beau être en HTTPS, le S voulant dire que les connexions entre l'internaute et le serveur était chiffré, cela ne protégeait pas pour autant les informations sauvegardées.

Fuite de données colmatée, étudiant dans le silence

J'ai saisi la CNIL, qui au passage est d'une efficacité redoutable dès que je leur communique une alerte. Le problème a été colmaté en quelques heures. Pour le moment, l'université n'a pas contacté les étudiants concernés par cette fuite d'information. Espérons qu'aucun malveillant ne soit passé par là avant l'alerte de ZATAZ. Impossible de savoir depuis quand ces « portes ouvertes » étaient accessibles sur la toile.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Fuite de données colmatée pour l'Université de Bordeaux – ZATAZ