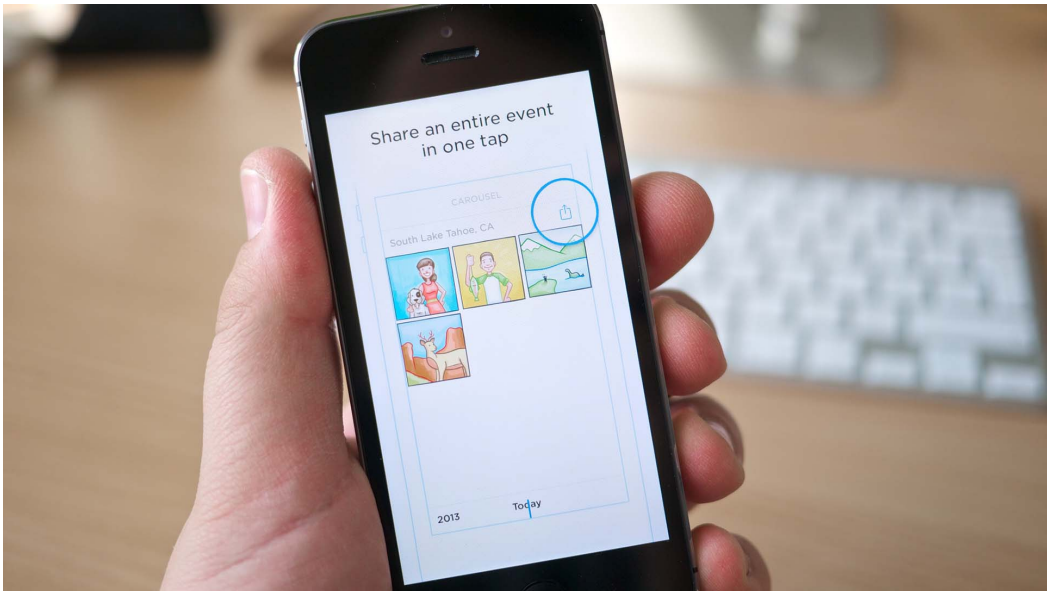
68 millions de comptes Dropbox piratés



68 millions de comptes Dropbox piratés

Quatre ans avoir avoir été victime d'un piratage et avoir su qu'il avait donné accès à une liste d'adresses e-mail, Dropbox a décidé il y a quelques jours de réinitialiser les mots de passe. Mais ce n'est qu'aujourd'hui que l'on en découvre l'ampleur.

La semaine dernière, Dropbox annonçait la réinitialisation de mots de passe d'utilisateurs inscrits depuis au moins 2012, en expliquant avoir été informé du fait qu'une base de données piratée à l'époque circulait, dans laquelle des adresses e-mails et des mots de passe hashés figurent. Dropbox avait prévenu dès 2012 qu'il avait été victime d'un tel piratage dû au vol d'un mot de passe d'un employé, et que les adresses e-mails obtenues avaient été utilisées pour envoyer des spams.

DROPBOX A MIS QUATRE ANS À RÉAGIR

Rien ne permet de penser que des mots de passe ont pu être déchiffrés. En revanche si vous utilisez le même mot de passe sur Dropbox que sur d'autres services en ligne, et si ces services ont eux-aussi été piratés, il est possible d'accéder à votre Dropbox en utilisant le mot de passe obtenu ailleurs. En 2012, le service en ligne avait d'ailleurs indiqué que des accès frauduleux avaient été faits par cette méthode, neutralisée lorsque l'on active la validation en deux étapes.

Dès lors, on ne comprend pas pourquoi Dropbox a attendu quatre ans (!) avant de réinitialiser les mots de passe.

Ce piratage dont la base de données resurgit après plusieurs années est le dernier en date d'une série similaire, qui fait penser qu'il pourrait s'agir du même groupe, ou de mêmes failles ont pu être exploitées à l'époque. Ainsi ces derniers mois on a appris la diffusion de 171 millions de mots de passe VK (le Facebook russe),427 millions de comptes Myspace,167 millions de mots de passe LinkedIn ou encore 32 millions de mots de passe Twitter.

Article original de Guillaume Champeau

Réagissez à cet article

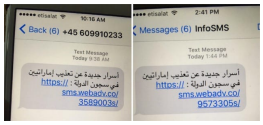
Original de l'article mis en page : Une base de 68 millions de comptes Dropbox circule chez les pirates — Tech — Numerama

Le malware Pegasus exploite 3 failles 0 day sur iPhone

	Le malware Pegasus exploite 3 failles 0 day sur iPhone

Les trois failles corrigées par Apple dans iOS 9.3.5 (ainsi que dans la dernière bêta d'iOS 10 livrée, contre toute attente, vendredi dernier) sont redoutables. Elles ont été exploitées par NSO Group, une société israélienne dont le fonds de commerce n'est autre que l'espionnage de journalistes et de militants. Le site Motherboard raconte la découverte de l'affaire qui relève du thriller…

Ce 10 août, Ahmed Mansoor, un militant des droits de l'homme dans les Émirats Arabes Unis, reçoit sur son iPhone un message lui proposant d'en savoir plus sur de *«nouveaux secrets sur la torture dans les prisons d'État »*. Un lien accompagnait ce message, qu'il s'est bien gardé de lancer.



Les deux messages reçus par Mansoor — Cliquer pour agrandir

À la place, il a contacté un chercheur du Citizen Lab, un organisme de défense des droits numériques rattaché à l'université de Toronto. Aidé par Lookout, un spécialiste de la sécurité mobile, ils ont pu mettre au jour un mécanisme très élaboré de surveillance par iPhone interposé.
Si Mansoor avait touché le lien, il aurait provoqué le jailbreak de son iPhone et donné à NSO Group le plein contrôle de son smartphone. *« Un des logiciels de cyberespionnage parmi les plus sophistiqués que nous ayons jamais vus »*, expliquent les chercheurs.
NSO Group vient d'apparaitre sur les radars, mais cette entreprise très discrète (aucune présence sur internet) opère depuis 2010. Le malware qu'elle a mis au point, baptisé Pegasus, permet d'infecter un iPhone, d'intercepter et de voler les données et les communications. Une arme redoutable, qualifiée de *« fantôme »* par NSO pendant une de ses rares interventions publiques en 2013. Cette société vend Pegasus au plus offrant, notamment des gouvernements peu regardants sur les droits de l'homme.

Les données volées par Pegasus — Cliquer pour agrandir
NSO a visiblement pu pénétrer par effraction dans des iPhone depuis le modèle 5. Son malware est programmé avec des réglages qui remontent jusqu'à iOS 7.
Ces trois failles *zero day*, baptisées Trident par les chercheurs, ont été communiquées à Apple il y a dix jours. *« Nous avons été mis au courant de cette vulnérabilité et nous l'avons immédiatement corrigée avec iOS 9.3.5 »*, explique un porte-parole du constructeur. *« iOS reste toutefois le système d'exploitation mobile grand public le plus sécurisé disponible »*, rassure Dan Guido, patron de la société de sécurité informatique Trail Of Bits, qui travaille souvent avec la Pomme.
Il indique toutefois qu'il reste à améliorer le système de détection des vulnérabilités. Apple a annoncé début août un programme de chasse (rémunérée) aux failles.
Article original de Mickaël Bazoge

Réagissez à cet article

Original de l'article mis en page : Cyberspionnage : derrière les failles Trident d'iOS, le redoutable malware Pegasus | iGeneration

---

Pokémon Go inquiète l'armée française !

Pokémon Go inquiète l'armée française !

Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE

Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :

- *« sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;*
- *les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;*
- *ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »*

Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.

La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».

Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?

On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.

Article original de Omar Belkaab

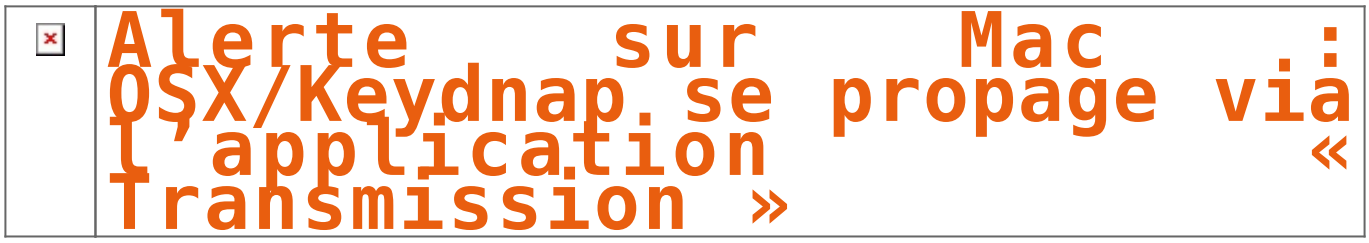
Réagissez à cet article

Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

Alerte sur Mac : OSX/Keydnap

se propage via l’application « Transmission »



Le mois dernier, les chercheurs d’ESET ont découvert un malware sur Mac OS X nommé OSX/Keydnap, qui exfiltre les mots de passe et clés stockés dans le gestionnaire de mots de passe « KeyChain » ; et qui crée une porte dérobée permanente.
Au moment de la découverte, notre Malware Researcher Marc-Etienne Léveillé expliquait que « 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 ».

Les équipes ESET viennent de découvrir que le malware OSX/Keydnap se distribue via une version compilée de l’application BitTorrent.

Une réponse instantanée de l’équipe de transmission

Suite à l’alerte donnée par ESET, l’équipe de transmission a supprimé le fichier malveillant de leur serveur Web et a lancé une enquête pour identifier le problème. Au moment de la diffusion de la première alerte, il était impossible de préciser depuis combien de temps le fichier malveillant a été mis à disposition en téléchargement.

Selon les informations de la signature, l’application a été

signée le 28 août 2016, mais ne se serait répandue que le lendemain. Ainsi, les équipes ESET conseillent aux personnes qui ont téléchargé la transmission V2.92 entre le 28 et le 29 août 2016 de vérifier si leur système est compromis en testant la présence de l'un des fichiers ou répertoires suivant :

- /Applications/Transmission.app/Contents/Resources/-License.rtf
- /Volumes/Transmission/Transmission.app/Contents/-Resources/License.rtf
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/icloudsyncd
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/process.id
- $HOME/Library/LaunchAgents/com.apple.iCloud.sync.daemon.-plist
- /Library/Application Support/com.apple.iCloud.sync.-daemon/
- $HOME/Library/LaunchAgents/com.geticloud.icloud.photo.-plist

Si l'un d'eux est présent, cela signifie que l'application malveillante de « transmission » a été exécutée et que le malware Keydnap est probablement en cours d'exécution. Notez également que l'image malicieuse du disque se nomme Transmission 2.92.dmg tandis que l'original se nomme Transmission–2.92.dmg (trait d'union).

Article original de ESET

Pour protéger votre Mac, Denis JACOPINI recommande l'application suivante :

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

Privacy Shield adopté, nouveau fondement pour les transferts de données outre-atlantique

Privacy Shield adopté, nouveau fondement pour les transferts de données outre-atlantique

La Commission européenne a adopté mardi 12 juillet dernier le Privacy Shield. Ce nouvel accord remplace le Safe Harbor, et aura pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis adhérant à ce dispositif.

L'adoption de ce nouveau « bouclier de protection des données personnelles » est l'aboutissement d'un long processus, commencé dès 2014, avec la révélation par l'ancien agent de la CIA Edward Snowden de la surveillance de masse effectuée par les services de renseignements américains puis par le refus, sur ce motif, d'un citoyen autrichien de transférer ses données vers les Etats-Unis. La Cour de Justice de l'Union Européenne a ainsi dans une décision du 6 octobre 2015 déclaré invalide la décision de la Commission du 26 juillet 2000 constatant que les Etats-Unis assurent un niveau de protection adéquat aux données caractère personnel transférées. En effet la Cour a considéré que les Etats-Unis n'apportaient pas les garanties suffisantes pour protéger les données des citoyens Européens au motif que les pouvoirs des services de renseignements américains s'étendaient à toutes données exportées depuis l'Europe dès lors que l'intérêt de sécurité publique était en cause. La CJUE a considéré que ces intrusions étaient disproportionnées et heurtaient les principes de la Charte des droits fondamentaux de l'Union Européenne.
A la suite de cette décision, l'ensemble des transferts de données personnelles vers des entités situés aux Etats-Unis sur le fondement du Safe Harbor ont dû être suspendus et des solutions alternatives mises en place. Le Groupe de travail de l'article 29, qui est constitué des différents autorités de protection des données à caractère personnel au sein de l'UE (le G29), a assuré les organisations souhaitant poursuivre le transfert de données de l'UE vers les Etats-Unis qu'elles pouvaient se fonder sur les mécanismes alternatifs prévus par la directive de 1995 relative à la protection des données, telles que les clauses contractuelles types et les règles d'entreprise contraignantes (BCR).
En parallèle la Commission européenne et le gouvernement américain engageaient des discussions afin de trouver un nouvel accord sur le transfert des données personnelles des citoyens européens vers les Etats-Unis.
Le 2 février 2016, la Commission européenne et le gouvernement des États-Unis sont parvenus à un premier accord politique. La Commission a présenté le projet d'accord le 29 février 2016. Le groupe de travail « Article 29" a ensuite rendu un premier avis le 13 avril 2016 assez critique en particulier sur l'insuffisance des gardes fous accordés aux citoyens européens pour contrôler l'usage de leurs données.
Une résolution a été adoptée le 26 mai par le Parlement européen, et la Commission a clôturé la procédure d'adoption du nouvel accord le 12 juillet 2016 en adoptant une décision d'adéquation visant à reconnaitre au mécanisme « EU-U.S. Privacy Shield » un niveau de protection « essentiellement équivalent » aux exigences européennes. .

Le nouveau dispositif : Comment ça marche ?

Le Privacy Shield vise à permettre aux entreprises de transférer plus facilement vers les Etats Unis des données personnelles collectées dans l'Union européenne, tout en protégeant les droits des personnes concernées.

Le Privacy Shield est fondé sur les principes suivants:
• Des obligations strictes pour les entreprises qui traitent des données : dans le cadre du nouveau dispositif, le ministère américain du commerce procédera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes, afin de veiller à ce qu'elles observent les règles auxquelles elles ont souscrit. Les entreprises dont la pratique ne sera pas conforme aux nouvelles règles s'exposeront à des sanctions et à une radiation de la liste des entreprises adhérant au dispositif.
• Un accès des pouvoirs publics américains soumis à des conditions claires et à des obligations de transparence : les États-Unis ont donné à l'Union européenne l'assurance que l'accès des pouvoirs publics aux données à des fins d'ordre public et de sécurité nationale serait soumis à des limitations, à des conditions et à des mécanismes de surveillance bien définis. De même, tous les citoyens de l'Union bénéficieront pour la première fois de mécanismes de recours dans ce domaine. Les États-Unis ont exclu toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire dans le cadre du bouclier de protection des données UE-Etats-Unis. Le secrétaire d'État américain a instauré une possibilité de recours pour les Européens dans le domaine du renseignement national en créant un mécanisme de médiation au sein du département d'État ;
• Une protection effective des droits individuels : tout citoyen estimant que les données le concernant ont fait l'objet d'une utilisation abusive dans le cadre du Privacy Shield bénéficiera de plusieurs mécanismes accessibles et abordables de règlement des litiges. Lorsqu'un litige n'aura pas été réglé par l'un de ces moyens, un mécanisme d'arbitrage sera disponible, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouvert aux citoyens de l'UE passera par un médiateur indépendant des services de renseignement des États-Unis ;
• Un mécanisme de réexamen annuel conjoint : ce mécanisme permettra de contrôler le fonctionnement du Privacy Shield, et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale. Le réexamen sera mené par la Commission européenne et le ministère américain du commerce, lesquels y associeront des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données. La Commission s'appuiera sur toutes les autres sources d'information disponibles et adressera un rapport public au Parlement européen et au Conseil.

Le Privacy Shield reste donc un mécanisme souple, à l'instar du Safe Harbor sous-tendu par une nécessité d'auto-certification des entreprises américaines. Pour bénéficier de l'accord et faciliter les transferts de données personnelles entre l'Europe et les Etats Unis, les entreprises américaines adhérant au dispositif devront s'engager à respecter les obligations de protection des données du Privacy Shield.
La décision « Privacy Shield » entrera en vigueur à compter de sa notification à chacun des Etats membres de l'Union européenne et sera contraignante pour ceux-ci. L'applicabilité de ce cadre juridique aux entreprises concernées sera ensuite subordonnée à l'enregistrement de celles-ci auprès des autorités américaines en charge de la mise en œuvre du dispositif. Les entreprises américaines pourront obtenir la certification Privacy Shield à partir du 1er août 2016.
Si un des objectifs poursuivi par le Privacy Shield est d'exclure tout traitement massif des données européennes transatlantique la collecte massive de données pourra cependant être effectuée si elle est limitée à des objectifs de sécurité nationale prédéfinis : espionnage, terrorisme, armes de destruction massive, menaces sur la cyber-sécurité, sur les armées, ou menaces criminelles transnationales.

Un accord déjà critiqué

En dépit de son objectif d'amélioration de la protection des données personnelles, le nouveau cadre fait pourtant l'objet de nombreuses critiques.
Le G29 dans son avis d'avril 2016 avait notamment fait part de ses préoccupations sur un certain nombre de points manquants, incomplets ou peu clairs. Le G29 avait en particulier regretté l'absence de plusieurs principes tels que la limitation de la durée de conservation et l'interdiction des décisions automatisées. En ce qui concerne l'accès par les autorités publiques aux données, le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. Enfin, le G29 avait émis des doutes sur l'indépendance du médiateur (Ombudsperson) et sur le fait qu'il dispose de pouvoirs suffisants pour exercer son rôle efficacement et permettre d'obtenir un recours satisfaisant en cas de désaccord avec l'administration.
Il n'est pas certain que la nouvelle rédaction satisfasse pleinement le G29.
De même le 30 mai 2016, le contrôleur européen de la protection des données (EDPS en anglais), Giovanni Buttarelli, dans un Avis sur le Privacy Shield, demandait des améliorations « significatives » avant son adoption par la Commission européenne (CE). Selon l'Avis de l'EDPS: « La proposition de Privacy Shield est un pas dans la bonne direction, mais dans sa rédaction actuelle elle ne prend pas suffisamment en compte, de notre point de vue, toutes les garanties appropriées pour protéger les droits européens des individus à la vie privée et à la protection des données notamment en ce qui concerne le recours juridictionnel. Des améliorations significatives sont nécessaires dans l'hypothèse où la Commission européenne souhaiterait adopter une décision d'adéquation ».
Le G29 mène actuellement une analyse de la décision de la Commission et se réunira le 25 juillet 2016 afin de finaliser sa position.
Article original de DLA PIPER

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.L.I. (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 : Adoption du Privacy Shield par la Commission européenne : un nouveau fondement pour les transferts de données outre-atlantique, Partenaire – Les Echos Business

---

Des systèmes biométriques piratés à partir de vos photos Facebook

Des systèmes biométriques piratés à partir de vos photos Facebook

Des chercheurs découvrent comment pirater des systèmes biométriques grâce à Facebook. Les photographies sauvegardées dans les pages de Facebook peuvent permettre de vous espionner.

De nombreuses entreprises de haute technologie considèrent le système de reconnaissance faciale comme l'une des méthodes fiables pour être reconnu par votre ordinateur. J'utilise moi-même la reconnaissance biométrique digitale, rétinienne et du visage pour certaines de mes machines. C'est clairement un des moyens simples et fiables de vérification d'une identité. Cependant, des chercheurs prouvent que la biométrie peut se contourner, dans certains cas, avec une photo, de la colle…

Une nouvelle découverte vient de mettre à mal, cette fois, la reconnaissance faciale mise en place par Facebook. Comme je pouvais vous en parler en 2014, Facebook met en place une reconnaissance faciale que des commerçants Américains ont pu tester avec succès. Des chercheurs ont découvert que cette prouesse technologique n'est pas encore parfaite et sujette au piratage. Des pirates peuvent utiliser votre profil Facebook, et les photos sauvegarder.

Systèmes biométriques

Des étudiants de l'Université de Caroline du Nord ont expliqué lors de la conférence d'Usenix, à Austin, avoir découvert une nouvelle technique particulièrement exaspérante pour intercepter l'intégralité d'un visage, via Facebook. Le rendu 3D et certaines « lumières » peuvent permettre de cartographier votre visage en deux clics de souris. Les chercheurs ont présenté un système qui créé des modèles 3D du visage via les photos trouvées sur Facebook. Leur modèle 3D va réussir ensuite à tromper quatre systèmes de reconnaissance faciale… sur 5 testés : KeyLemon, Mobius, TrueKey, BioID, et 1D.

Pour leur étude, 20 cobayes volontaires ont participé à l'expérience. Leurs photos sont tirées d'espaces publiques comme Facebook, mais aussi LinkedIn et Google+. La modélisation des visages à partir de 27 images différentes va permettre de créer des modèles en 3D, avec des animations faciales : bouches, yeux… Les chercheurs ont reconstruit les visages via les bouts trouvés sur les différentes photographies.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Pirater des systèmes biométriques à partir de vos photos Facebook — Data Security BreachData Security Breach

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Le géant de l'informatique Hewlett-Packard s'associe avec 3M pour préinstaller sur ses prochains ordinateurs portables professionnels un filtre anti espion.

Quoi de plus courant que de croiser à la terrasse d'un café, dans le train ou dans un aéroport ces fiers commerciaux pressés de travailler, même dans un lieu non sécurisé. Autant dire que collecter des données privées, sensibles, en regardant juste l'écran de ces professionnels du « c'est quoi la sécurité informatique ? » est un jeu d'enfant.

Hewlett-Packard (HP), en partenariat avec 3M, se prépare à commercialiser des ordinateurs portables (Elitebook 1040 et Elitebook 840) dont les écrans seront équipés d'un filtre anti voyeur. Un filtre intégré directement dans la machine. Plus besoin d'utiliser une protection extérieure.

Une sécurité supplémentaire pour les utilisateurs, et un argument de vente loin d'être négligeable pour le constructeur. Selon Mike Nash, ancien chef de la division de sécurité de Microsoft et actuellement vice-président de Hewlett-Packard, il est possible de croiser, partout, des utilisateurs d'ordinateurs portables sans aucune protection écran. Bilan, les informations affichés à l'écran peuvent être lues, filmées, photographiées.

Le filtre pourra être activé et désactivé à loisir.

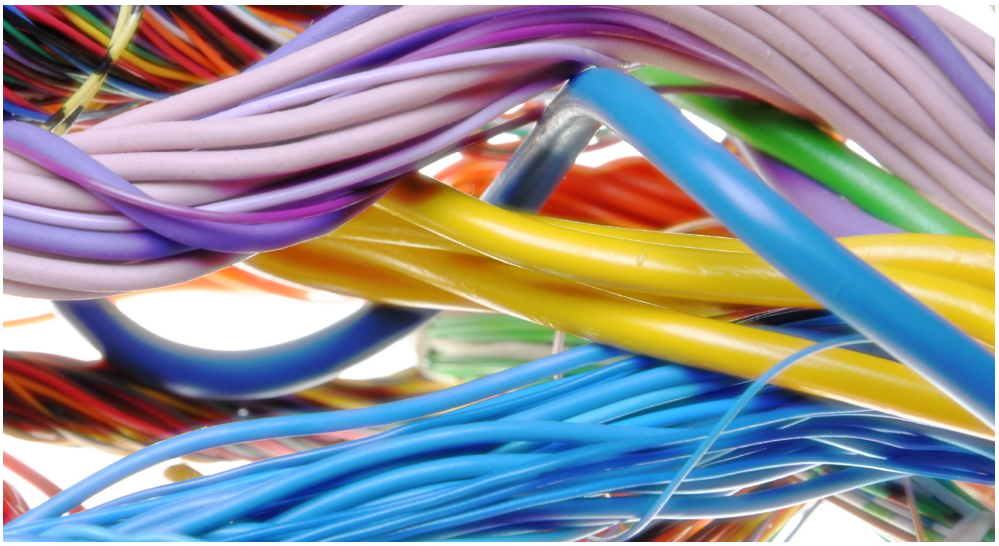
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Filtre anti espion sur les prochains Hewlett-Packard – Data Security BreachData Security Breach

---

La neutralité du Net triomphe en Europe



La neutralité du Net triomphe en Europe

En publiant ses lignes directrices sur la neutralité du net qui s'imposent à tous les régulateurs européens, le BEREC a donné pleinement satisfaction aux organisations qui plaidaient pour une obligation la plus ferme possible de respecter le principe par lequel Internet s'est développé.

Le BEREC, qui regroupe les différents régulateurs des communications électroniques en Europe (dont l'Arcep en France), a publié mardi ses lignes directrices très attendues, sur l'implémentation par les autorités nationales des règles de neutralité du net prévues par la régulation adoptée par le Parlement européen en fin d'année 2015.

Le cadre général laissait quelques zones d'ombre, que le BEREC est venu combler au bénéfice d'une consultation publique menée cet été, qui a vu la société civile se mobiliser massivement. Plus de 500 000 réponses ont été envoyées à l'organisation.

Beaucoup craignaient que le BEREC ne laisse quelques trous béants dans les règles imposées aux opérateurs, d'autant plus après le coup de pression donné par ces derniers au prétexte du passage à la 5G vers 2020. Orange avait même affirmé qu'il n'y aurait pas de 5G avec la neutralité du net, la prochaine génération de réseaux mobiles imposant d'attribuer des droits d'utilisation de certaines fréquences ou certains protocoles en fonction des applications.

Mais le **texte publié mardi** obtient un satisfecit d'une limpidité rarissime de la part du lobby de la société civile European Digital Rights (EDRi). « *L'Europe fait désormais office de créateur de standard mondial dans la défense d'un internet ouvert, concurrentiel et neutre* », se réjouit dans un communiqué Joe McNamee, le directeur exécutif de l'association, en félicitant le BEREC.
Thomas Lohninger, de l'organisation SaveTheInternet.eu créé pour faire pression sur le BEREC, parle même de « *triomphe pour le mouvement européen des droits numériques* », obtenu après « une très longue bataille, et avec le soutien d'un demi million de personnes ». Il assure qu'avec les lignes directrices publiées mardi, l'Europe affirme des « *principes qui font d'Internet une plateforme ouverte pour le changement, la liberté et la prospérité* ».

INTERDICTION DU ZERO-RATING

Les règles adoptées par le BEREC prévoient notamment de donner à l'Arcep et à ses homologues le pouvoir d'imposer des sanctions lorsque les FAI dégradent la qualité d'accès à des services, ou favorisent indûment un type de services par rapport à d'autres.
Elles interdisent aux opérateurs de créer des « services spécialisés » (proposés directement par les FAI, notamment via leurs box), qui ne respectent pas les règles de la neutralité du net, lorsqu'ils ont des équivalents en tant que services proposés normalement sur Internet, ou lorsqu'ils conduisent à minimiser la bande passante accordée à l'internet ouvert.
Aussi, les lignes directrices interdisent quasiment dans les faits la pratique du « zero rating », qui consiste pour un opérateur à ne pas bloquer ou facturer la bande passante consommée par une application spécifique (par exemple des forfaits qui incluent Facebook et YouTube mais pas Twitter et Dailymotion, ou qui permettent un accès illimité au cloud de l'opérateur mais pas à celui de Google ou Apple), ou par certains types d'applications. Ces pratiques contestées n'étaient pas interdites explicitement par le règlement européen. Elles ne le sont toujours pas formellement par le BEREC, mais les conditions fixées sont tellement strictes qu'il sera très difficile pour un opérateur de continuer à avoir recours au zero-rating.

Article original de Guillaume Champeau

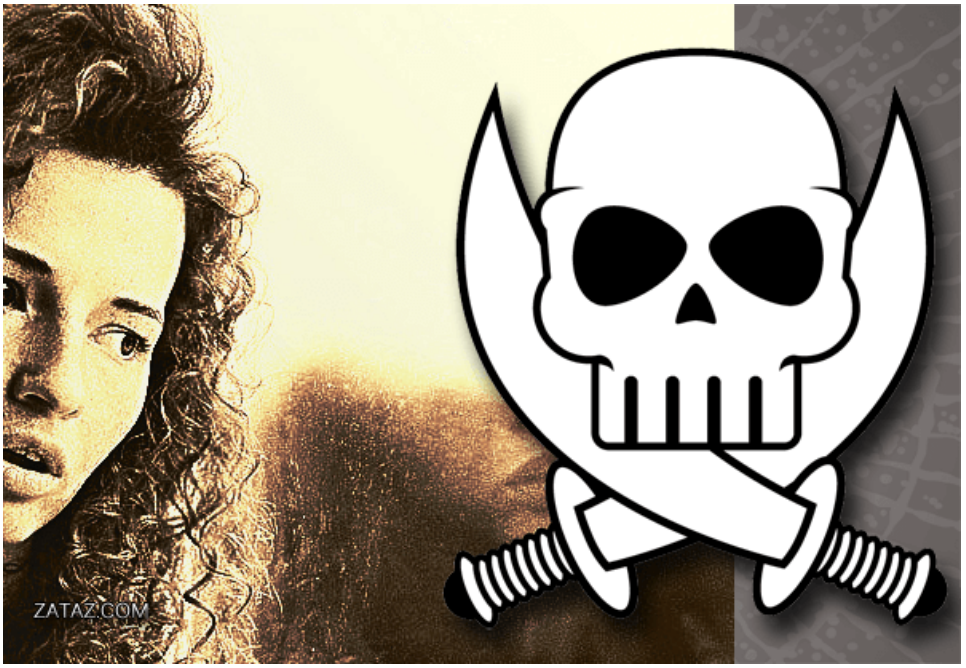
Réagissez à cet article

Original de l'article mis en page : Un « triomphe » pour la neutralité du Net en Europe — Politique — Numerama

---

Des sites de rencontres touchés par des attaques

dites de leurre venant du réseau TOR



Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR

Les chercheurs mettent en garde contre une augmentation d'attaques par leurre visant les sites de rencontres venant du réseau TOR.
Les attaques par leurre sont montées via un site de rencontres concurrent pour détourner les utilisateurs d'un site victime vers celui de l'attaquant. La plupart de ces attaques ciblent de multiples services de rencontres et diffusent des spams à un grand nombre d'utilisateurs, en les invitant à rejoindre d'autres sites, probablement tous contrôlés par le même pirate. La motivation de l'instigateur de ces attaques semble donc claire, écarter les utilisateurs d'un site victime et les attirer vers le sien.
Les chercheurs d'Imperva ont récemment assisté à une augmentation des pirates utilisant le réseau TOR pour dissimuler leur identité et mener à bien ce type d'attaques.
Les attaques par leurre venant du réseau Tor se caractérisent par des messages en provenance de clients Tor à un taux relativement faible (mais régulier), de 1 à 3 demandes chaque jour, probablement pour passer sous le radar des mécanismes de limite de vitesse et éviter les contrôles de détection automatique des navigateurs. Malgré le taux très faible des demandes qu'Imperva a pu observer, il est probable que le nombre total de celles-ci soit beaucoup plus élevé, avec seulement quelques demandes exposées dans l'aperçu du trafic utilisateurs Tor.
Il faut également prendre en compte le déficit d'image que représente ces attaques menées par les centaines de faux profils très attractifs qui harcèlent les utilisateurs du site victime et qui abaissent la crédibilité de celui-ci.
Selon Itsik Mantin, directeur de la recherche de sécurité à Imperva : « ***Ces attaques ont le potentiel de perturber considérablement le business des opérateurs de site de rencontres. En utilisant le réseau TOR les attaquants sont capables de cacher leur emplacement réel et leurs identités, ce qui les rends encore plus difficiles à détecter et à bloquer*** ».
Afin de se protéger contre les attaques par leurre, il est recommandé aux sites de rencontre de surveiller de près les faux comptes et de fermer tout ce qui pourrait être considéré comme illégitime. Il est également conseillé de monitorer l'ensemble du trafic TOR et de bloquer toute activité suspecte.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Quelque soit l'e-mail reçu, ceci nous prouve une fois de plus qu'il est nécessaire de décupler notre vigilance. Sachez que le protocole d'envoi des e-mails, le fameux SMTP, se base sur la norme RFC 821 qui date de 1982. Ceci dit, vous comprendrez mieux si je vous dis que ce protocole ne prévoyait pas les dérives d'usages que nous connaissons aujourd'hui.
De nos jours, cette faille, exploitée à outrance par les pirates informatiques, autorise sans aucune difficulté l'usurpation d'identité. Avec les technologies d'aujourd'hui, n'importe qui peut se faire passer pour n'importe qui, et rien ne vous empêche de vous faire passer pour Larry Page ou Serguei Brin (les fondateurs de Google en 1998) en créant une adresse e-mail de type larry.page@gmail.com ou serguei.brin@gmail.com pour peu que ces adresses e-mail ne soient pas prises. Pire, vous pouvez recevoir un e-mail indiquant le vrai nom et la vraie adresse e-mail de votre meilleur ami alors que vous répondre à une adresse e-mail légèrement différente, celle du pirate usurpant l'identité de votre ami…
De qui peut-on encore se fier ?
Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 : ZATAZ Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR – ZATAZ

Devez-vous changer votre mot de passe DropBox ?

Devez-vous changer votre mot de passe DropBox ?

On vous demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que devez-vous faire ?
L'entité propose de faire des sauvegardes de ses fichiers dans le Cloud, le fameux nuage. Bref, des disques durs hors de chez vous, hors de votre entreprise, sur lesquels vous déposez vos données afin d'y accéder partout dans le monde, et peu importe le support : Ordinateur, smartphone…
Depuis quelques heures, une vague de courriels aux couleurs de DropBox vous indique « ***On me demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que dois-je faire ?***« , si les plus paranoïaques ont jeté la missive de peur d'être nez-à-nez avec un phishing, je me suis penché sur le sujet, histoire de m'assurer que l'alerte valait la peine d'être lancée. Je vais être rapide avec le sujet, oui, il s'agit bien d'un courriel officiel de la firme US.

Lors de votre prochaine visite sur dropbox.com, vous serez peut-être invité à créer un nouveau mot de passe. Une modification « ***à titre préventif à certains utilisateurs*** » souligne Dropbox. Les utilisateurs concernés répondent aux critères suivants : ils ont créé un compte Dropbox avant mi-2012 et ils n'ont pas modifié leur mot de passe depuis mi-2012. Vous commencez à comprendre le problème ? Comme je vous le révélais la semaine dernière, des espaces web comme Leakedsource, le site qui met en danger votre vie privée, sont capable de fournir aux pirates une aide précieuse. Comment ? En diffusant les informations collectées dans des bases de données piratées.

Que dois-je faire ?
Si, quand vous accédez à dropbox.com, vous êtes invité à créer un nouveau mot de passe, suivez les instructions sur la page qui s'affiche. Une procédure de modification des mots de passe qui n'a rien d'un hasard. Les équipes en charge de la sécurité de DropBox effectuent une veille permanente des nouvelles menaces pour leurs utilisateurs. Et comme vous l'a révélé ZATAZ, Leaked Source et compagnie fournissent à qui va payer les logins et mots de passe d'utilisateurs qui utilisent toujours le même sésame d'accès, peu importe les sites utilisés. Bref, des clients Adobe, Linkedin … ont peut-être exploité le même mot de passe pour DropBox.
Bilan, les pirates peuvent se servir comme ce fût le cas, par exemple, pour ma révélation concernant le créateur des jeux Vidéo Rush et GarryMod ou encore de ce garde du corps de Poutine et Nicolas Sarkozy. Les informaticiens de Dropbox ont identifié « ***d'anciennes informations d'identification Dropbox (combinaisons d'adresses e-mail et de mots de passe chiffrés) qui auraient été dérobées en 2012. Nos recherches donnent à penser que ces informations d'identification sont liées à un incident de sécurité que nous avions signalé à cette époque***. » termine DropBox.
A titre de précaution, Dropbox demande à l'ensemble de ses utilisateurs qui n'ont pas modifié leur mot de passe depuis mi-2012 de le faire lors de leur prochaine connexion.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Comme tout e-mail reçu, la prudence est de rigueur. Avant de valider l'authenticité d'un e-mail envoyé par une firme telle que Dropbox, nous avons dû analyser l'entête de l'e-mail reçu et comparer les données techniques de celles répertoriées dans les bases de données connues.
J'imagine que vous n'aurez pas le courage d'apprendre à le faire vous même ni que vous trouverez l'intérêt de consacrer du temps pour ça.
Comme chaque mise à jour demandée par un éditeur ou un constructeur, comme tout changement de mot de passe recommandé par une firme, nous vous conseillons de le faire en allant directement sur le site concerné.
Dans le cas de « Dropbox », nous vous recommandons de rechercher « dropbox.com » dans google ou de taper « dropbox.com » dans votre barre d'adresse et de vous identifier. Vous serez ainsi sur le site officiel et en sécurité pour réaliser la procédure demandée.

Attention
Vous ne serez en sécurité que si votre ordinateur n'est pas déjà infecté. En effet, taper un nouveau mot de passe si votre ordinateur est déjà infecté par un programme espion revient à communiquer au voleur une copie de vos nouvelles clés. Taper l'ancien mot de passe revient aussi à donner au voleur la clé permettant peut-être d'ouvrir d'autres portes !!!

Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 : ZATAZ Changez votre mot de passe DropBox – ZATAZ