Encore une faille 0-day sur Flash Player menaçant vos ordinateurs | Le Net Expert Informatique

Encore une faille 0-day sur Flash Player menaçant vos ordinateurs

Ces derniers mois, Flash Player a subi les foudres de grands noms de l'informatique suite à de nombreuses vulnérabilités découvertes en plus des innombrables précédentes corrigées auparavant. Déjà alors, certaines institutions comme Facebook réclamaient l'abandon du plug-in Flash alors cet aveu issu de la société de développement Adobe ne risque pas d'arranger le sort de son Flash Player.

Un rapport publié par la société Adobe a été publié mercredi et confirme la présence d'une faille critique au sein de la dernière version du Player mais aussi des précédentes. Celle-ci peut être employée « lors d'attaques limitées et ciblées ». Sont concernées les dernières versions,19.0.0.207 incluse mais également toutes les précédentes itérations sur Windows et Mac, Adobe Flash Player Extended Support Release pour l'intégralité des versions 18 ainsi que les versions pour Linux.

En plus des vulnérabilités 0-day employés par la Hacking Team, cette faille avait été décelée au cours de l'été par TrendMicro qui mettait alors au jour une attaque informatique de grande envergure orchestrée par le groupuscule Pawn Storm, pirates visant différents ministères des affaires étrangères à travers le monde ainsi que certains média.

Si cette attaque reposait principalement sur l'utilisation de malwares, des méthodes de phishing et exploitait une faille inhérente à Java (la première repérée depuis des années), le magazine spécialisé a par la suite découvert que les hackers s'appuyaient aussi sur une faille présente dans Flash Player.

Confirmée par Adobe, celui-ci a aussitôt assuré se mettre à l'élaboration d'un correctif. Initialement prévu pour une distribution au 16 octobre, ce patch devrait finalement être disponible vers le 19 du même mois. Reste que la plus sûre des solutions en attendant sa mise à jour consiste à désinstaller complètement le lecteur. Si la faille ne concerne pas directement la personne lambda mais principalement les hautes institutions, le principe d'action pourrait tout de même être repris par d'autres pirates et appliqués à une plus grande partie de la population. Prudence.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

http://www.phonandroid.com/flash-player-encore-faille-0-day-menacant-ordinateurs.html

Oups ! Uber dévoile les données personnelles de chauffeurs | Le Net Expert Informatique

Oups ! Uber dévoile les données personnelles d

Un bug permettait de voir les données personnelles d'autres chauffeurs Uber. La société assure que seuls 700 conducteurs US ont été affectés et que la faille a été corrigée en seulement 30 minutes.

Uber l'assure, ses services sont bons pour l'économie et créent de l'emploi – pas salarié cependant, les chauffeurs ne signant pas de contrat de travail avec la multinationale. En France, la société a dû faire face au mécontentement, et pas des taxis cette fois, mais des chauffeurs eux-mêmes. La faille de sécurité dont a été victime cette semaine le service devrait probablement moins affecter ces travailleurs que la diminution tarifaire imposée par Uber. La société a ainsi, accidentellement, divulgué les données personnelles de plusieurs centaines de chauffeurs.

Un bug de débutant, mais des conséquences mineures

Cette fuite de données est la conséquence d'un bug logiciel. Elle a abouti à la divulgation de l'identité de conducteurs Uber, dont leurs numéros de sécurité sociale, parmi d'autres données sensibles. En enregistrant des documents d'assurance auprès d'Uber, des chauffeurs ont constaté que s'affichaient les informations d'autres utilisateurs de la plateforme.

Mais pas de panique, assure la société américaine. Selon cette dernière, qui a notamment été interrogée par The Register, moins de 700 chauffeurs américains sont concernés par cet incident. Et par ailleurs, poursuit Uber, le bug a été corrigé dans les 30 minutes qui ont suivi sa découverte.

Selon Gawker, ce bug pourrait être lié à la sortie d'une nouvelle application : Uber Partner. Celle-ci permet aux conducteurs de gérer leurs comptes et de suivre leurs courses, mais aussi de transmettre des données pour l'enregistrement des nouveaux chauffeurs.

En comparaison de la faille de sécurité du début d'année, la dernière semble mineure. Une base de données de 50.000 chauffeurs Uber avait en effet fuité sur GitHub. La société a été critiquée à plusieurs reprises pour ses pratiques en matière de sécurité et de confidentialité des données.

Pour redorer son blason et améliorer la sécurité de ses développements, Uber a créé cette année un poste de responsable de la sécurité informatique (RSSI) et embauché deux hackers renommés, Charlie Miller et Chris Valasek.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :
http://www.zdnet.fr/actualites/oups-uber-devoile-les-donnees-personnelles-de-chauffeurs-39826600.htm

Piratage de TV5 Monde: une facture très salée | Le Net Expert Informatique

	Piratage de TV5 Monde: une facture très salée

L'attaque subie par la chaîne francophone internationale en avril lui aura coûté plus d'une dizaine de millions d'euros. De quoi obliger TV5 à tailler dans son budget 2016.

« La sécurité informatique coûte cher, mais combien coûte l'absence de sécurité? », pourrait-on s'interroger, en paraphrasant Lincoln.

Chez TV5 Monde, on commence à avoir une idée du coût du piratage subi par la chaîne le 8 avril dernier: il dépassera largement la dizaine de millions d'euros.

Création d'une cellule de sécurité informatique

Précisément, ce piratage entraînera un surcoût de 4,8 millions d'euros cette année; de 2,4 millions d'euros l'an prochain; et pour les années suivantes 2 à 2,5 millions d'euros par an.

En pratique, la chaîne internationale a dû bien sûr investir pour renforcer la sécurité de ses réseaux. Un plan a été élaboré à partir des recommandations de l'ANSSI (Agence nationale de sécurité des systèmes d'information). Ce plan comprend notamment la création d'une cellule permanente dédié à la sécurité informatique qui n'existait pas auparavant. Une équipe de six nouveaux salariés est actuellement en cours de recrutement.

Sites web « sinistrés »

Mais ce n'est pas tout. La chaîne francophone fonctionne encore « en mode dégradé », indique son budget 2016. Interrogée, la chaîne n'a pas précisé ce que cela signifiait précisément. Mais le budget 2016 indique que de nombreuses missions (notamment la mise en ligne des émissions sur le site web), jusqu'à présent réalisées automatiquement, se font désormais manuellement, ce qui nécessite du personnel supplémentaire. « Les sites internet de la chaîne sont sinistrés », indique le budget.

Evidemment, de telles sommes sont significatives au regard du budget de la chaîne (110 millions d'euros). Des économies ont donc dû être recherchées sur d'autres postes. « Les budgets d'opérations (programmes, sous-titrage, marketing, communication) » ont été réduits. Notamment, « les budgets destinés aux acquisitions de programmes et au sous-titrage sont fortement affectés ».

La publicité sur internet « s'effondre »

Les malheurs de la chaîne ne s'arrêtent pas là. Le site web, dont l'audience déjà en chute libre depuis plusieurs années, a été inaccessible, puis ensuite rétabli avec un contenu réduit, ce qui accéléré la chute de l'audience. Au total, les visites ont chuté de 13% au premier semestre, et les vidéos vues de 15%. « La baisse significative des audiences numériques risque de s'accentuer dans les mois à venir », prévient le budget. Conséquence logique: « les recettes publicitaires sur le numérique s'effondrent ».

Rappelons que de nombreuses erreurs avaient été mises à jour après le piratage. Le site spécialisé Zataz a assuré avoir signalé à la chaîne publique une dizaine de failles depuis deux ans. Selon 01net.com, le réseau bureautique et le réseau de production télé de TV5 n'étaient pas totalement cloisonnés, ce qui a permis au piratage du premier de contaminer le second, entraînant un écran noir…

Enfin, Arrêt sur images avait relevé que les mots de passe étaient affichés sur le mur. Filmés lors d'un reportage effectué dans les locaux par France 2 suite à l'attaque, ils avaient été donc été potentiellement vus par des centaines de milliers de téléspectateurs… Le mot de passe du compte YouTube était ainsi lemotdepassedeyoutube… TV5 avait admis « une bourde » et assuré que les mots de passe n'étaient pas affichés ainsi avant le piratage.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source : http://bfmbusiness.bfmtv.com/entreprise/piratage-de-tv5-monde-une-facture-tres-salee-922231.html
Par Jamal Henni

Surveillance : le spyware FinFisher détecté dans 32 pays | Le Net Expert Informatique

Le spyware FinFisher détecté dans 32 pays

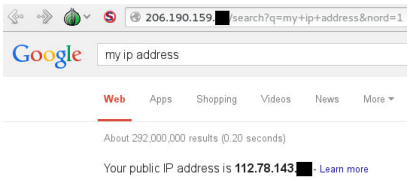
Malgré les mesures prises pour en dissimuler l'existence, le Citizen Lab a réussi à remonter à nouveau la trace du spyware FinFisher vendu aux autorités policières de nombreux états dans le monde, y compris dans des pays autoritaires.

Le business de l'espionnage des communications électroniques fonctionne toujours très bien. Alors que le piratage spectaculaire de la société Hacking Team n'a semble-t-il eu aucun effet notable sur ses relations commerciales avec les autorités qui exploitent ses services, son concurrent britannique FinFisher n'a visiblement lui non plus aucun problème à continuer ses activités, malgré la divulgation de ses codes sources et d'autres données internes en 2014.
Les gouvernements continuent de faire confiance à ces entreprises privées qui proposent ça et là des outils permettant de placer sur écoute des smartphones, d'accéder aux données d'un PC, de collecter toutes les touches frappées sur un clavier, d'activer discrètement des webcams, de géolocaliser des appareils, ou encore d'accéder au contenu de conversations en principe privées et chiffrées. Les intérêts pour la sécurité nationale priment sur les quelques questions éthiques que peuvent poser certaines méthodes, qui valent à ces firmes d'être placées sur une liste des « sociétés ennemis d'internet » par Reporters Sans Frontières.

Car les services qu'elles vendent ne sont pas achetés que par des démocraties bien sous tous rapports, malgré les restrictions à l'exportation qu'elles sont censées respecter.

Le laboratoire Citizen Lab a ainsi publié de nouvelles démonstrations de la présence des outils de Finfisher dans au moins 32 pays, dont plusieurs états peu recommandables du point de vue du respect des droits fondamentaux, comme la Malaisie, l'Arabie Saoudite, le Kazakhstan, l'Ethiopie, le Maroc ou le Bengladesh.
Déjà en 2012, le laboratoire avait prouvé que la suite d'outils d'espionnage Finfisher vendue à l'époque par la société britannique Gamma International (elle a depuis donné son indépendance à Finfisher GmbH, basée à Munich), était utilisée par au moins une quinzaine d'États dans le monde. Parmi eux figuraient déjà des pays autoritaires comme le Bahreïn, l'Ethiopie, l'Indonésie, le Turkménistan, ou les Emirats-Arabes Unies.
Comme Hacking Team, Finfisher assure qu'elle respecte l'arrangement de Wassenaar qui limite les possibilités d'exporter les outils de surveillance vers des pays autoritaires qui peuvent en faire un usage non conforme aux droits de l'homme, par exemple pour traquer des opposants politiques ou rechercher les sources de journalistes hostiles au régime. Mais la présence continue de ses outils sur des serveurs appartenant à des régimes dictatoriaux permet, au minimum, de douter de la véracité de telles affirmations.
Depuis les révélations de 2012, FinFisher a amélioré ses méthodes de dissimulation et systématiquement caché ses outils derrière des serveurs proxys, configurés pour paraître inoffensifs. Mais les chercheurs du Citizen Lab ont regorgé d'ingéniosité pour les trouver.
Depuis décembre 2014, l'organisation a scanné un maximum d'adresses IPv4 pour trouver des serveurs dont certaines caractéristiques correspondaient à ce qu'ils connaissaient de FinFisher. Ils ont trouvé 135 serveurs, dont la plupart étaient des serveurs proxys qui affichaient la page d'accueil de Google ou Yahoo. Ces serveurs là, qui servent uniquement de relais intermédiaire, n'avaient aucun intérêt puisqu'ils masquaient la géolocalisation des serveurs « maîtres » sur lesquels étaient installés les outils de FinFisher. Mais aux yeux de Google et Yahoo, c'est bien l'adresse IP du serveur maître qui communique.

PREMIÈRE ASTUCE :
« DIS-MOI MON ADRESSE IP »

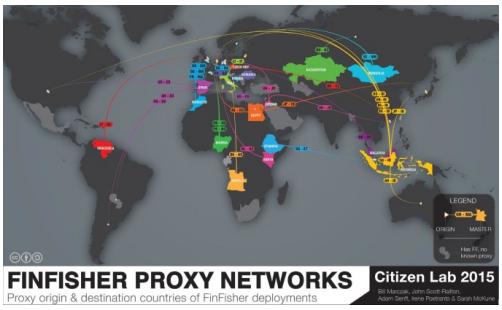


Lorsque Google était affiché, il suffisait d'exécuter la requête « my IP adress » (qui ne fonctionne pas avec Google France) pour que Google réponde au serveur maître, et que celui-ci renvoie la réponse au serveur relais, qui lui-même l'affichait à Citizen Lab. Ils ont ainsi pu trouver des adresses IP de serveurs maîtres installés dans différents pays, et découvrir leur géolocalisation.

DEUXIÈME ASTUCE :
« DIS-MOI QUEL TEMPS IL FAIT »

Sur Yahoo, la commande n'existe pas. Mais le service sait afficher la météo qui correspond au lieu qu'il associe à l'adresse IP de l'internaute. Les chercheurs ont donc demandé à Yahoo d'afficher la météo et découvert que, par exemple, un serveur qui était censément installé en Lituanie renvoyait la météo de Caracas, au Venezuela. Un pays où les journalistes sont régulièrement persécutés. Ca ne permettait pas d'obtenir en direct l'adresse IP, mais au moins de savoir où elle était attachée.

La carte des proxys :



Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source : http://www.numerama.com/tech/126760-surveillance-le-spyware-finfisher-detecte-dans-32-pays.html
Par Guillaume Champeau
Crédit photo de la une : Thibaut Démare

Une panne informatique bloque le contrôle des passagers dans les aéroports US | Le Net Expert Informatique

Une panne informatique bloque le contrôle des passagers dans les aéroports US

Avant-hier soir, plusieurs aéroports américains parmi les plus importants ont été victimes d'une panne informatique – probablement un problème de bases de données – bloquant le contrôle des passagers lors du débarquement et avant l'accès aux terminaux des portes d'embarquement.

Le système informatique du Department of Homeland Security, le service des douanes aux États-Unis, a connu une défaillance majeure dans plusieurs aéroports américains ce qui a entrainé des attentes et des retards pour certains passagers. CNBC rapporte que le système informatique en question est celui qui vérifie les noms des passagers aériens avec la liste des personnes soupçonnées de terrorisme par la Homeland Security. Dans ces circonstances, le personnel des douanes et de la protection des frontières est censé utiliser des méthodes alternatives pour le traitement des passagers dans les aéroports où les systèmes informatiques sont hors services.

Les médias sociaux ont commencé à remonter les problèmes hier soir vers 8 h (heure de la Côte Est des États-Unis) soit 2 h du matin en France. Jusqu'à présent, les alertes ont rapporté le problème à l'aéroport JFK de New York, Logan de Boston, San Francisco, Baltimore-Washington, Hartsfield Jackson d'Atlanta, Dallas-Fort Worth, Charlotte Douglas, et éventuellement d'autres aéroports.

Un fonctionnaire du DHS a toutefois confirmé à NBC qu'un « pépin » dans les systèmes informatiques – surement un problème de bases de données – est à l'origine du problème à l'aéroport JFK. NBC, de son coté, cite des responsables gouvernementaux de haut niveau confirmant les problèmes, et précise que les fonctionnaires ne pouvaient pas indiquer quand le problème serait réglé.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lemondeinformatique.fr/actualites/lire-une-panne-informatique-bloque-le-controle-des-passagers-dans-les-aeroports-us-62672.html

---

Alerte de cyberattaques dans les avions | Le Net Expert Informatique

Alerte de cyberattaques dans les avions

L'Agence européenne de sécurité aérienne (AESA) estime que l'aviation est vulnérable et qu'il faut mettre en place des structures dédiées pour lutter contre cette nouvelle menace.

En mai dernier, lorsque le hacker Chris Roberts avait fait les gros titres avec son histoire de piratage d'un avion en plein vol, les compagnies aériennes ont rétorqué en cœur qu'une telle action serait totalement impossible. Elle estimaient que M. Roberts n'était qu'un vantard mythomane. Mais les instances de régulation commencent à voir les choses d'un œil différent, à commencer par celles de l'Union européenne.

Interrogé par l'association des journalistes de la presse aéronautique et spatiale (AJPAE), le directeur exécutif de l'Agence européenne de sécurité aérienne (AESA) Patrick Ky a souligné la vulnérabilité de l'aviation à un éventuel acte de piratage. « C'est un risque auquel il faut qu'on se prépare, l'aviation est vulnérable. Dire que l'aviation n'est pas sujette au cyber-risque, c'est se voiler la face », a-t-il déclaré. Selon le patron de l'agence, il faut mettre en place des « réseaux spécifiques » de spécialistes en cyberattaques pour « informer de la menace et des moyens de s'en prévenir ».

L'AESA fait appel à un hacker

M. Ky a affirmé avoir pu lui-même constater les capacités d'un hacker à pénétrer le réseau de communication d'une compagnie aérienne. « J'ai fait appel à un hacker qui a la particularité d'avoir également une licence de pilote commercial, a-t-il expliqué auprès des Echos. En moins de 5 minutes, il est parvenu à rentrer dans le réseau Acars ». Acars (Aircraft Communication Addressing and Reporting System) est un système de communication et de surveillance par radio basé sur l'échange de messages entre un avion et une station au sol. Il intervient dans la gestion du trafic aérien et permet de s'assurer du bon fonctionnement des équipements de l'aéronef. Mais le hacker ne s'est pas arrêté là. « Il ne lui a fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait », ajoute Patrick Ky.

En décembre dernier, cinq grandes organisations internationales de l'aviation (OACI, ACI, CANSO, IATA et ICCAIA) avaient adopté une feuille de route commune pour harmoniser leurs mesures respectives en matière de cybermenaces, et souligné que « la sécurité et la sûreté du système aéronautique mondial » étaient « potentiellement vulnérables aux attaques de pirates informatiques et autres cybercriminels ».

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://hightech.bfmtv.com/internet/l-europe-sonne-l-alerte-sur-le-risque-de-cyberattaques-dans-les-avions-920964.html
Par Gilbert Kallenborn

Il s'implante une puce NFC dans la main pour pirater des

smartphones Android | Le Net Expert Informatique

Glissée sous la peau, la puce NFC devient invisible après que la plaie a cicatrisé. DRPhoto:	**Il s'implante une puce NFC dans la main pour pirater des smartphones Android**

Les pirates ne reculent devant rien pour hacker des téléphones mobiles. Dernière expérience en date : s'implanter une puce NFC dans la main. Rien que ça.

Seth Wahle est un ingénieur pour une société spécialisée dans les technologies sans fil, APA Wireless. A ses heures perdues, ce hacker teste la sécurité de ce type de dispositif. Et ne fait pas dans la demi-mesure : il est parvenu à s'implanter une puce NFC sous la peau de la main, à la jonction entre le pouce et l'index de sa main gauche. De la sorte, il est capable de hacker des smartphones Android rien qu'en les effleurant avec sa paume.

Comment a-t-il fait ?

Le magazine américain Forbes explique qu'il a trouvé une puce NFC que l'on peut implanter sans danger sous la peau d'un être humain. Dotée de seulement 888 bytes de mémoire, elle est encapsulée dans un petit récipient en verre vendu sur un site chinois et qui est usuellement utilisé pour implanter des puces RFID dans le bétail pour le marquer. Pour la somme de 40 dollars (35 dollars), il a ensuite trouvé une personne qui a accepté de lui injecter la puce sous la peau à l'aide d'une seringue spéciale. Ne restait plus ensuite qu'à attendre que la plaie créée cicatrise.

Un simple contact téléphone-main et un programme s'installe discrètement

Avec ce dispositif, Seth Wahle affirme qu'il est désormais capable de hacker n'importe quel smartphone Android doté de la technologie NFC (communication proche par simple contact). Il lui suffit de mettre le téléphone brièvement en contact avec la paume de sa main pour que celui-ci ne se rende sur une page web piratée qui va déclencher le téléchargement d'un petit programme. Et ce, sans alerter les systèmes de sécurité du smartphone.

Une fois celui-ci installé et actif, il est capable de récupérer n'importe quelles données du mobile et même de prendre des photos. Son système n'est pas encore optimal (il perd assez vite la connexion avec le téléphone piraté, notamment quand ce dernier est verrouillé ou redémarré) mais génère déjà de nombreuses questions et craintes pour le futur. Seth Wahle, qui a montré sa performance aux journalistes de Forbes, s'apprête à la présenter plus en détail lors d'une importante conférence de hackers qui se tiendra à Miami du 15 au 17 mai prochain. Nul doute que son intervention sera très suivie…

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.metronews.fr/high-tech/pour-pirater-des-smartphones-android-il-s-implante-une-puce-nfc-dans-la-main/modD!v2YdgmEKKTEuE/

Les PME pourraient être victimes de la remise en cause du Safe Harbor | Le Net Expert Informatique

Les PME pourraient être victimes de la remise en cause du Safe Harbor

Les réactions ont été nombreuses, suite à la décision de la Cour européenne de Justice de remettre en cause l'accord de Safe Harbor entre les Etats-Unis et l'Europe. La France, par exemple, s'en est félicitée. Mais les conséquences restent incertaines. La remise en cause du Safe Harbor, en soi, ne constitue pas une révolution. Cet accord ne faisait que faciliter les transferts de données entre Europe et Etats-Unis : les sociétés américaines pouvaient collecter et exploiter ces données en échange d'une certification annuelle obtenue auprès des autorités américaines. Près de 5.000 entreprises fonctionnaient sous ce régime.

Mais ce n'est pas le seul moyen d'acheminer des données des deux côtés de l'Atlantique. Les entreprises américaines et européennes peuvent signer, entre elles, des clauses contractuelles standards. Elles peuvent aussi obtenir le consentement des utilisateurs, mais ce cas ne fonctionne que pour les entreprises s'adressant aux particuliers, pas aux professionnels. Enfin, elles peuvent demander une autorisation à la Cnil.

D'autres plaintes ?

Ces autres possibilités dressent en tout cas, en négatif, le portrait des probables « victimes » de ce nouveau flou : les petites et moyennes entreprises, européennes ou américaines, qui n'ont pas de service juridique fourni en interne pour pouvoir signer des clauses contractuelles ou s'occuper de la question rapidement. « Nous sommes inquiets. Pas forcément pour nous, car tous nos échanges sont régis par des contrats, mais pour les petites entreprises, qui n'ont pas de service juridique ou d'avocats pour s'occuper de ces sujets », confirmait il y a quelques jours Stephen Deadman, directeur adjoint de la vie privée chez Facebook, de passage à Paris.

Le cabinet d'avocats Bryan Cave, de son côté, a déjà reçu plusieurs dizaines de clients inquiets ces jours-ci. « C'est d'autant plus inquiétant que les entreprises françaises ont moins l'habitude, par rapport aux entreprises anglo-saxonnes notamment, de travailler avec des conseillers juridiques, affirme l'avocat Joseph Smallhoover, de Bryan Cave, qui conseille plusieurs sociétés américaines et européennes. Et ce sont ces mêmes PME qui sont le plus créatrices d'emplois. » Et ce n'est sans doute pas fini. « En affirmant que les Etats-Unis n'ont pas un niveau de protection suffisant, la Cour européenne de Justice ouvre aussi la voie à des attaques contre les clauses contractuelles », poursuit Joseph Smallhoover. C'est pour cette raison que les responsables politiques appellent, eux, depuis plusieurs jours, à fournir un nouveau cadre aux transferts de données. La ministre de la Justice Christiane Taubira a estimé vendredi qu'il fallait « aller vite parce qu'on ne peut pas prendre le risque ni d'un vide juridique, ni d'un manque de protection, ni d'un manque de garanties par rapport à la circulation des informations. » Les négociations entre Europe et Etats-Unis pourraient bien s'accélérer.

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lesechos.fr/tech-medias/hightech/021393249999-les-pme-pourraient-etre-victimes-de-la-remise-en-cause-du-safe-harbor-1164083.php
Par Nicolas RAULINE

Attaque par phishing simulée au PMU : 120 employés piégés | Le Net Expert Informatique

	Attaque par phishing simulée au PMU : 120 employés piégés

La pièce jointe que l'on ouvre et qui diffuse un virus dans toute l'entreprise demeure le vecteur principal des attaques informatiques. Le PMU a testé les réactions de ses collaborateurs en mai dernier en leur envoyant un email de ce type conçu par ses soins. 22% ont cliqué dans la pièce jointe.

Le hack, c'est trop facile. Environ 120 collaborateurs du PMU se sont laissés piéger par un faux email leur proposant de gagner un iPad. Ils ont cliqué dans le lien présent dans l'email et donné leurs coordonnées.

6% ont donné leurs coordonnées

C'est le résultat d'un test mené en vraie grandeur par le PMU en mai dernier pour mesurer la résistance à une attaque par phishing de ses collaborateurs. Résultat : 22% des salariés ont ouvert la pièce jointe associée à un faux email d'invitation à participer à un jeu pour gagner un iPad.

Et 6% – soit environ 120 personnes – ont cliqué sur le lien présent à l'intérieur et donné leurs coordonnées pour gagner le lot. La pièce jointe affichait un faux message destiné à effrayer durant quelques minutes ceux qui l'avaient ouverte en leur faisant croire que leur PC est en danger et va être vidé.

Le test a été réalisé de façon anonyme, par un prestataire externe, en revanche, on sait que ce sont des personnes de tous les services qui ont cliqué dans l'email.

L'attaque contre TV5 monde

La DRH a donné le feu vert à l'opération car le test a été réalisé juste après les incidents de TV5 Monde qui avait vu la chaîne être bloquée durant une journée à la suite d'une attaque informatique.

Le résultat est à la fois inquiétant et rassurant. Inquiétant car test est intervenu après que le PMU ait procédé à deux ou trois campagnes de sensibilisation au phishing, en expliquant aux collaborateurs qu'il ne faut pas cliquer sur les liens présents dans les emailings. Rassurant, car le fait que le PMU communique de tels résultats permet de sensibiliser l'ensemble des entreprises à ce type de risques.

Le phishing est banal

Le phishing est une attaque informatique qui consiste à envoyer des emails imitant ceux de sociétés reconnues – banques, organismes sociaux – afin de recueillir les coordonnées bancaires des personnes ciblées.

Les attaques qui propagent des virus informatiques dans les entreprises – appelées APT (Advanced Persistent Threat) – passent majoritairement par l'ouverture de pièces jointes qui diffusent ensuite un code informatique malveillant entre les machines du réseau de l'entreprise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.larevuedudigital.com/2015/10/03/simulation-dune-attaque-par-phishing-120-employes-du-pmu-pieges/

Décryptage du Safe Harbor | Le Net Expert Informatique

Décryptage du Safe Harbor

La Cour de justice de l'Union européenne (CJUE) a rendu la semaine dernière une décision historique en invalidant le « Safe Harbor ». Cet accord, concocté par le Département du Commerce des États-Unis, approuvé par la Commission européenne, légalise le transfert de données personnelles de citoyens européens vers les États-Unis. Amazon, Facebook et les autres géants américains du Net pouvaient donc librement exporter nos données et les exploiter à leur guise à des fins publicitaires. Son invalidation va changer la donne, et les défenseurs du respect de la vie privée, parmi lesquels l'UFC-Que Choisir, s'en réjouissent.

Le Safe Harbor en deux mots

Europe et États-Unis ont une vision différente de la protection des données personnelles des citoyens. Leurs politiques respectives en la matière sont donc divergentes. L'Europe interdit notamment le transfert des données personnelles vers des pays qui offrent un niveau de protection inférieur au sien (1). Pour ne pas priver les entreprises américaines de cet « or numérique » en provenance de l'Europe, le Département du Commerce des États-Unis (l'équivalent d'un ministère du Commerce) a concocté un cadre juridique qui légalise le transfert de données personnelles : le Safe Harbor, aussi appelé Sphère de sécurité. Les entreprises qui souhaitent en profiter doivent garantir certaines conditions (information des consommateurs sur l'exploitation de leurs données, droit de rectification, sécurité des données, etc.) et obtenir une certification. 4 000 entreprises américaines en sont titulaires, parmi lesquelles Microsoft, Amazon, Google ou encore Facebook.

De quelles données parle-t-on ?

Les données personnelles sont au centre de la plupart des modèles économiques des entreprises du Net. Vos achats, les messages que vous publiez sur les réseaux sociaux, vos habitudes de navigation sur Internet, les mots que vous saisissez dans les moteurs de recherche, ou bien encore les livres et les films que vous achetez en ligne sont autant d'indicateurs qui permettent de définir finement des profils de consommation et de vous envoyer des publicités ciblées, donc efficaces, donc vendues à prix d'or.

Quels sont les fondements de la décision de la CJUE ?

Tout est parti d'une plainte de Maximillian Schrems, un citoyen autrichien, auprès de l'autorité irlandaise de contrôle, l'Office of the Data Protection Commissioner, l'équivalent de notre Cnil (2). Maximillian Schrems utilise Facebook et sait qu'en vertu du Safe Harbor, ses données sont traitées aux États-Unis. Mais les révélations d'Edward Snowden, en 2013, sur la surveillance opérée par la NSA (National Security Agency) prouvent que le pays n'offre pas un niveau de protection suffisant des données. Or le Safe Harbor engage les États-Unis à fournir un niveau de protection au moins équivalent à celui de l'Europe.

La CJUE s'est prononcée sur deux points. D'abord, elle a confirmé qu'une autorité nationale (la Cnil et les autres) a le droit d'enquêter lorsqu'elle est saisie par un citoyen sur le sujet, et ce malgré l'existence du Safe Harbor. Ensuite, elle estime que la Commission européenne a eu tort d'accepter cet accord sans vérifier que les États-Unis n'interdisaient pas les opérations de surveillance généralisée (comme celles de la NSA). Du coup, 15 ans après son entrée en application, la justice suspend le Safe Harbor. Une décision historique.

Cette décision va-t-elle changer quelque chose ?

À court terme, les entreprises du Safe Harbor se retrouvent dans un trou juridique. Elles doivent subitement gérer une situation passée de légale à illégale du jour au lendemain. Les grandes entreprises disposent des armes suffisantes pour poursuivre leurs activités à coup de bras de fer juridiques. Mais quid des entreprises plus modestes ?

À moyen terme, l'Europe réaffirme son attachement à la protection des données personnelles. Cette décision de la CJUE pèsera sans doute dans les discussions sur le projet de Règlement européen sur les données personnelles. Ce texte, actuellement au stade des négociations tripartites entre le Parlement, le Conseil et la Commission, constituera à l'avenir le socle de la politique européenne en matière de protection de la vie privée.

(1) Directive 95/46/CE sur la protection des données personnelles.
(2) Commission nationale de l'informatique et des libertés.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.quechoisir.org/telecom-multimedia/internet/actualite-donnees-personnelles-decryptage-du-safe-harbor
Par Camille Gruhier