

Évolution du « Safe Harbor » vers le « UE-US Privacy Shield »



Évolution du
« Safe Harbor »
vers le « UE-
US Privacy
Shield »

La Commission européenne et les États-Unis ont convenu d'un nouveau cadre pour les transferts transatlantiques de données, l' « UE Privacy Shield », en lieu et place du « Safe Harbor ».

Le cadre était attendu depuis l'annulation du Safe Harbor par la Cour de justice de l'UE (CJUE) dans son arrêt du 6 octobre 2015, qui avait créé un vide juridique important en matière de transfert des données (voir notre article).

La Commission européenne et le groupe des CNIL européennes (G29) avaient, d'ailleurs, apporté une première réponse aux inquiétudes des entreprises confirmant que les clauses contractuelles types et les Binding Corporate Rules (BCR) restaient les solutions à privilégier pour assurer la conformité des transferts en cours, durant cette période de transition (voir notre brève).

Ce « bouclier de la confidentialité », présenté le 29 février dernier, aurait donc vocation à protéger les droits fondamentaux des Européens en cas de transfert des données aux États-Unis et à fournir des garanties aux entreprises qui font des affaires transatlantiques.

De nouvelles obligations pour les entreprises américaines

« La collaboration des deux partenaires de part et d'autre de l'Atlantique vise à ce que les données individuelles soient parfaitement protégées, sans renoncer pour autant aux possibilités qu'offre l'ère numérique », a déclaré Andrus Ansip, vice-président de la Commission européenne lors de la présentation publique du Privacy Shield. Et cette protection des données personnelles passerait d'abord par un encadrement des politiques des entreprises américaines en la matière. C'est en tout cas le souhait de la Commission. Le projet de « bouclier » prévoit que les entreprises américaines souhaitant importer des données personnelles provenant d'Europe devront s'engager, dans un code de bonne conduite, à respecter des conditions strictes quant à leurs traitements.

Le dispositif actuel du Privacy Shield prévoit aussi des mécanismes de surveillance afin de garantir le respect de ces obligations par les entreprises. Ces dernières seraient ainsi obligés de rendre public leurs engagements en la matière, qui restent pour le moment à définir, sous peine d'être sanctionnées par la Federal trade commission.

En cas de non-respect de ces engagements les citoyens européens pourraient déposer plainte contre les agissements des entreprises. Elles auront alors 45 jours maximum pour y répondre. Cependant, aucune sanction n'est prévue à ce jour si les délais sont dépassés. Pour que leurs plaintes soient traitées, les citoyens européens pourraient également s'adresser à leur CNIL nationale qui collaborera avec la Federal trade commission. L'instance américaine devra apporter une réponse dans les 90 jours. Enfin pour les cas non résolus, l'accord américano-européen prévoit le recours, en dernier ressort, à un tribunal d'arbitrage devant lequel les entreprises pourront être convoquées. La Commission précise que ce mécanisme de règlement extrajudiciaire des litiges sera accessible sans frais.

La surveillance des services de renseignements plus encadrée

Outre ces mécanismes de surveillance concernant les entreprises, l'exécutif européen a affirmé avoir obtenu de la part des américains un strict encadrement de l'accès des autorités publiques aux données personnelles.

« Pour la première fois, le gouvernement américain, par l'intermédiaire des services du directeur du renseignement national, a donné par écrit à l'UE l'assurance que tout accès des pouvoirs publics aux données à des fins de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, empêchant un accès généralisé aux données personnelles », s'est félicité Bruxelles dans un communiqué. Selon cet engagement pris par les américains, les citoyens européens disposeront d'un recours dans le domaine du renseignement national grâce à un mécanisme de médiation indépendant des services de sécurité nationaux. A ce jour, aucune précision n'a été donnée sur les conditions de nomination de ce médiateur ni aucune garantie concrète concernant son indépendance, ce que regrettent les détracteurs de ce texte.

Pour que les limitations de l'accès des pouvoirs publics soient respectés, le Privacy Shield prévoit un mécanisme de réexamen commun aux deux continents. En effet, la Commission européenne et la Federal trade commission, associés à des experts nationaux, pourraient contrôler chaque année le respect des engagements en s'appuyant sur toutes sources d'informations disponibles comme les rapports annuels de transparence des entreprises et ceux d'ONG spécialistes du respect de la vie privée. Côté européen, la Commission adressera un rapport public au Parlement européen et au Conseil, à la suite de ce réexamen.

Ce nouveau cadre international de protection des données doit encore être adopté par le collège des commissaires européens, après l'avis des autorités européennes chargées de la protection des données. En parallèle, les États-Unis vont devoir mettre en place ce nouvel instrument ainsi que les mécanismes de contrôle et de médiation. De nombreuses modifications ont encore le temps d'être apportées, surtout dans le contexte international des élections présidentielles américaines... [Lire la suite]



Réagissez à cet article

Source : [Direction juridique] L'actualité actuEL DJ : Du
« Safe Harbor » à l' « UE-US Privacy Shield »

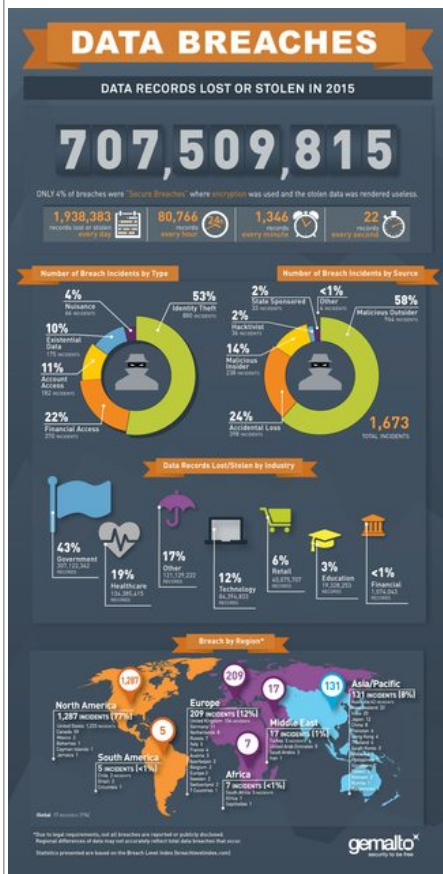
Cybercriminalité : les vols d'identité en forte hausse



Les vols d'identité ou d'informations personnelles ont été les attaques privilégiées en 2015. Elles supplantent ainsi les vols d'informations financières.

Le piratage de TV5 Monde, ou plus récemment le piratage de plusieurs millions de profils d'enfants et de comptes clients du fabricant de jouets VTech l'a bien montré : en 2015, les attaques informatiques de grande ampleur semblent plus nombreuses ou en tout cas plus visibles. Leur nombre a augmenté de 38%, indiquait récemment une étude de PricewaterhouseCoopers .

Selon une autre étude dévoilée ce lundi par Gemalto , il y a eu 1.673 brèches de sécurité ayant entraîné le vol ou la perte de plus de 700 millions de données en 2015. Les résultats du Breach Level Index 2015 de Gemalto n'augurent rien de bon : chaque heure, ce sont près de 80.766 données qui partent aux mains d'hackeurs malveillants. Aussi, l'impact de la faille de sécurité reste souvent difficile à évaluer : on compte ainsi 47% de brèches ouvertes où le nombre de données envolées était inconnu. Si les grandes fuites de l'histoire laissent entendre que souvent, le piratage vient de l'intérieur, en 2015, 58 % des fuites et pertes de données provenaient de l'extérieur.



Une affaire personnelle

On le savait, donc : les hackers ont été prolifiques l'année dernière. Ce que l'on savait moins, en revanche, c'est leur tendance à s'attaquer à une donnée bien plus banale en apparence, mais aussi bien plus précieuse qu'un compte en banque : « En 2014, les consommateurs peuvent avoir été concernés par des vols de numéros de cartes de crédit, mais il y a des protections intégrées pour limiter les risques », indique Jason Hart, Vice Président et directeur de la technologie pour la protection des données chez Gemalto, dans un communiqué. « En 2015, les criminels se sont concentrés sur des attaques à l'encontre d'informations personnelles et le vol d'identité, bien plus difficiles à contrer une fois qu'elles ont eu lieu ».

Ainsi, alors que les attaques visant des données financières ont baissé entre 2014 et 2015 – après un pic en 2013 –, les vols d'identité subissent une nette progression à plus de 300 millions de données volées. Et ces vols subissent une nette progression entre le premier et le deuxième semestre 2015. En fait, l'explosion du nombre de données compromises peut aussi s'expliquer par une démocratisation de l'enregistrement des informations personnelles par les sociétés. Difficile désormais d'accéder à un service en ligne sans créer de compte, s'identifier et donc dévoiler un peu de sa personne.

Les gouvernements très touchés

Toutes ces informations sont plus diverses, plus complètes. Les posséder c'est l'assurance d'avoir un moyen de pression sur la victime, voire de monnayer plus tard ce que l'on a subtilisé. Surtout quand il s'agit de données gouvernementales. Les attaques visant les institutions ont augmenté de 476 % entre 2014 et 2015 et 43 % des actes de cyberpiratage concernent ces organismes. Même si les gouvernements sont touchés, les hackers à l'origine des attaques sont rarement des activistes (2 %) ou encore des acteurs parrainés par l'Etat (2 %).

Il faut dire que les chiffres explosent notamment en raison d'attaques de forte ampleur à l'encontre des Etats-Unis et de la Turquie : 50 millions de données de citoyens turcs volées ou encore près de 78.8 millions d'informations, la plus grande attaque de l'année 2015, contre l'entreprise américaine d'assurance maladie, Anthem Insurance.

Cette dernière attaque démontre aussi que le secteur de la santé est de plus en plus visé : il représente 19 % des fichiers compromis et 23 % de toutes les attaques informatiques recensées. A l'opposé, le secteur financier s'en est plutôt bien sorti en 2015 : il représente 0.1 % des données piratées et 15 % des attaques totales. Tout comme le secteur de la distribution qui subit une forte chute (99 %) des vols de données recensés... [Lire la suite]



Réagissez à cet article

Source : *Cybercriminalité : les vols d'identité en forte hausse, High tech*

Les entreprises françaises particulièrement touchées par la Cybercriminalité



Le cabinet Pwc publie aujourd'hui une étude portant sur la fraude en entreprise. Stable dans le reste du monde, celle-ci a doublé en France avec pour principal moteur de croissance la cybercriminalité.

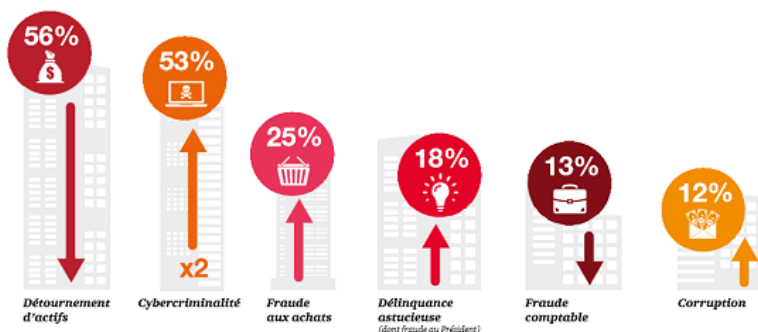
Les entreprises françaises ont-elles du souci à se faire ?

Selon une étude Pwc publiée aujourd'hui, la France se démarque du reste du monde à l'égard de la fraude visant les entreprises. Celle-ci toucherait en effet 68% des entreprises interrogées par Pwc, soit une hausse sensible par rapport à la dernière étude de 2014 où seuls 55% des entreprises déclaraient avoir été touchées par un acte de fraude.

Le principal moteur de cette croissance selon Pwc, la cybercriminalité qui a doublé au cours des deux dernières années et 53% des entreprises du panel interrogé expliquent avoir été victimes de cybercriminalité durant les deux dernières années, talonnant de près les détournements d'actifs qui conservent la première place du classement. Et la crainte que génère ce risque est également très présente pour les entreprises interrogées, 73% d'entre elles craignent de subir une cyberattaque dans les deux prochaines années. Pourtant, craindre une attaque ne signifie pas pour autant s'en prémunir efficacement « En dépit des risques de cybercriminalité constatés par la quasi-totalité des entreprises françaises, plus de la moitié d'entre elles n'ont pas encore de plans d'action opérationnels pour répondre à une cyberattaque » explique ainsi Jean-Louis Di Giovanni, associé PwC du Département Litiges et Investigations.

Classement des fraudes les plus fréquentes en France

2.



% des fraudes déclarées par les entreprises au cours des 2 dernières années

À l'échelle mondiale, seuls 37% des entreprises sondées disposent d'un plan de réponse à incident entièrement opérationnel. Mais le risque se révèle également moins élevé à l'international, où seuls 32% des entreprises interrogées expliquent avoir été confrontées à une fraude ou une tentative de fraude orchestrée par des cybercriminels. L'étude menée par Pwc a porté sur plus de 6000 entreprises à travers le monde entre juillet et septembre 2015. La cybercriminalité est très certainement en hausse, malheureusement la méthodologie de Pwc ne précise pas exactement quels critères ont été retenus pour définir ce qui se cache derrière la notion de « victimes de la cybercriminalité ». Comme l'explique un porte-parole de la société : « Ce sont les entreprises qui ont répondu avec des profils parfois très différents. Il n'est donc pas exclu que le simple envoi d'un mail de phishing ait été comptabilisé comme un acte de cybercriminalité par certaines et pas par d'autres. » Le critère peut donc avoir interprété selon différentes variables par les entreprises interrogées... [Lire la suite]



Réagissez à cet article

Source : *Cybercriminalité : les entreprises françaises particulièrement touchées par la fraude – ZDNet*

Une incroyable bourde de Numericable dénoncée par la CNIL !



Une incroyable
bourde de
Numericable
dénoncée par la
CNIL !

Un abonné à Numericable a été suspecté à tort de pédopornographie, subi de multiples perquisitions et harcelé à tort par la Hadopi, parce que l'opérateur renvoyait par erreur son identité aux services de police et de gendarmerie qui l'interrogeaient.

Les faits sont assez graves pour que la CNIL décide de les rendre publics. Le gendarme de la vie privée a révélé mardi que l'opérateur Numericable était directement responsable du harcèlement administratif et judiciaire subi par un abonné, qui a été « *identifié 1 531 fois pour délit de contrefaçon, inculpé 7 fois* », et qui a « *fait l'objet de nombreuses perquisitions à son domicile et de plusieurs saisies de ses équipements informatiques* ».

L'homme n'avait pourtant rien à se reprocher. Mais lorsque Numericable recevait de l'Hadopi, de la police ou de la gendarmerie une demande d'identification d'un abonné à partir de son adresse IP avec date et d'heure d'utilisation, l'opérateur utilisait un logiciel maison, buggé.

« *Lorsque l'application ne parvenait pas à associer une adresse IP à une personne, elle ne générait pas de message d'erreur et renvoyait par défaut à un même abonné* », constate la CNIL. Plus concrètement, le logiciel associait l'adresse IP de la réquisition à l'adresse MAC de son client, unique pour chaque box Numericable. Mais lorsqu'il n'arrivait pas à trouver les informations, le logiciel utilisait alors l'adresse MAC 00:00:00:00:00:00, attribuée fictivement à plusieurs abonnés. Dont la victime du harcèlement.

Très énervée contre Numericable (mais sans doute moins que le malheureux client), elle note que « *ce problème n'a été identifié qu'avec l'insistance d'un service de police chargé d'une procédure pénale ouverte à l'encontre de l'abonné* ».

1531 DÉNONCIATIONS EN QUATRE MOIS



C'est alertée par l'ancienne présidente de la Hadopi, Marie-Françoise Marais, que la CNIL a décidé d'une mission de contrôle auprès de Numericable, et découvert le pot aux roses. « *Au vu des éléments du dossier, la formation restreinte de la CNIL a considéré que la société NC NUMERICABLE n'avait pas respecté son obligation légale de transmettre des données exactes aux autorités de poursuite, en vertu de l'article 6-4° de la loi Informatique et Libertés* », rapporte l'autorité administrative.

Selon le texte de la délibération (.pdf), le nom de l'abonné persécuté a été communiqué à 1531 reprises entre le 26 janvier et le 15 avril 2013, c'est-à-dire en l'espace de moins de quatre mois. Y compris, ce qui est plus que fâcheux, dans des affaires de pédophilie. C'est lorsque l'Hadopi a transmis le dossier de l'abonné ultra-multi-récidiviste à la justice que le parquet a constaté qu'il y avait visiblement un petit problème.

Le contrôle de la CNIL n'est toutefois intervenu que deux ans plus tard, le 15 avril 2015. Des contrôles complémentaires sur pièces ont été réalisés jusqu'à fin septembre 2015.

Le problème aurait été corrigé par Numericable en 2014, à la suite d'une demande d'information adressée par un service de police le 26 septembre 2014. L'opérateur a reconnu les faits, et échappé à une sanction financière en raison de sa promptitude à modifier le logiciel lorsqu'elle a eu connaissance de l'origine du problème. La CNIL a toutefois décidé d'adresser un avertissement public, en guise de peine infamante, devant appeler tous les opérateurs à la vigilance.

L'histoire ne dit pas si l'abonné en cause a porté plainte pour réparation du préjudice subi... [Lire la suite]



Réagissez à cet article

Source : Une incroyable bourde de Numericable dénoncée par la CNIL ! – Politique – Numerama

Piratage du capteur d'empreinte d'un téléphone

avec une simple imprimante à
jet d'encre



Piratage
d'un capteur
d'empreinte d'un
téléphone avec
une simple
imprimante à jet
d'encre

Les capteurs de biométrie sont sur le grill après une nouvelle tentative fructueuse de piratage sur des téléphones Samsung Galaxy S6 et Huawei Honor 7. L'iPhone 5s a pour sa part résisté.

La biométrie serait pour beaucoup l'avenir de la sécurité, surtout en situation de mobilité. Et bien ce sont les chercheurs de l'université du Michigan qui viennent de prouver qu'une imprimante à jet d'encre pouvait à elle seule permettre de pirater les systèmes de capture d'empreinte de téléphones Samsung et Huawei. Objectif : rentrer dans le téléphone. Une imprimante à jet d'encre basique certes, mais pour réaliser ce hack, ils ont toutefois du s'équiper d'encre et de papier spécifique.

Démonstration en vidéo du hack de capteur biométrique réalisé par l'université du Michigan. (Source : Université du Michigan)

En moins de 15 minutes, selon les chercheurs qui publient une vidéo à ce sujet, il est donc possible d'entrer par effraction dans un smartphone, à condition bien sûr de récupérer l'empreinte digitale du possesseur du téléphone. Ensuite, une impression en haute résolution sur un papier brillant et une encre spécifique permet de duper le module d'analyse d'empreinte des téléphones Samsung Galaxy S6 et Huawei Honor 7. Les chercheurs précisent par ailleurs que la tentative de hack sur un iPhone 5s s'est soldée par un échec.

Pas une première, mais très peu cher et facile à réaliser

Ce n'est pas la première fois que les capteurs d'empreinte digitale sont floués par des tentatives de piratage. Mais jusqu'alors les techniques utilisées reposaient sur de l'impression 3D et des moules spécifiques. Cette nouvelle méthode s'avère de fait bien moins onéreuse, et bien plus rapide. De quoi poser quelques questions quand on sait que Samsung (et d'autres) prévoient de proposer de l'authentification de paiement avec de la biométrie.

Il convient de noter toutefois que l'utilisation de la biométrie à tort et à travers fait l'objet de critiques depuis fort longtemps. Il s'agit de ne pas confondre authentification et identification d'une part, et surtout de ne pas l'utiliser pour de l'authentification forte... [Lire la suite]



Réagissez à cet article

Source : *Capteur d'empreinte : un piratage avec une simple imprimante à jet d'encre – ZDNet*

Comment une cyberattaque a mis des centrales ukrainiennes hors service



Comment une cyberattaque a mis des centrales ukrainiennes hors service ?

S'il reste encore des zones d'ombres, le doute n'est désormais plus permis : la panne électrique qui a touché l'Ukraine à Noël a bien été causée par une cyberattaque. C'est la première fois qu'un réseau électrique est mis hors service par une attaque informatique. Mais que les opérateurs d'importance critique soient prévenus : ce n'est sûrement pas la dernière.

Le rapport publié jeudi 3 mars par l'équipe de réponse d'urgence pour la sécurité informatique des systèmes de contrôle industriels (ICS-CERT) du département de la Sécurité intérieure des Etats-Unis (DHS) est sans appel : le blackout électrique qu'a connu une partie de l'Ukraine fin 2015 a bien été causé par des hackers. Il confirme ce faisant les conclusions avancées par le SANS ICS (un autre groupe d'experts en cybersécurité industrielle) début janvier, et entérine l'évènement comme étant la première attaque réussie sur un réseau électrique.

UNE SÉRIE D'ATTAQUES SOIGNEUSEMENT PLANIFIÉES

Les intrusions dans le réseau de trois opérateurs énergétiques ont impacté environ 225 000 clients. Bien que le service ait repris quelques jours plus tard, il reste encore limité, même à l'heure actuelle. D'après les témoins interrogés par l'ICS-CERT, les attaques auraient été coordonnées de telle manière qu'elles se sont produites à 30 minutes d'intervalle sur chaque réseau, touchant des installations centrales et régionales. L'opération a très probablement nécessité une longue reconnaissance et étude des victimes.

Lors de l'attaque, plusieurs individus ont pris l'accès des systèmes grâce à des outils de contrôle à distance, soit au niveau de l'OS, soit au niveau des systèmes ICS, le tout via des accès VPN (réseau privé virtuel) dont ils avaient précédemment obtenu les codes d'accès. Une fois l'attaque effectuée, le malware KillDisk a été utilisé pour effacer les fichiers compromis et corrompre les secteurs de démarrage des machines ou les firmwares des équipements pour les rendre inopérants. Les attaquants auraient également surchargé les centres d'appels des énergéticiens pour les empêcher de réagir immédiatement à l'évènement. De plus, trois autres organisations en charge d'infrastructures critiques ont aussi été pénétrées, mais sans impact direct sur leurs opérations.

DES ZONES D'OMBRES PERSISTENT

Malgré ces nouvelles informations, le rôle exact qu'a joué le malware BlackEnergy dans l'attaque n'est toujours pas connu. Ce malware, connu du milieu de la cybersécurité depuis 2007, a été retrouvé sur trois des systèmes impactés. Originellement présenté comme la potentielle arme du crime, il est possible qu'il n'ait en fait été utilisé que pour obtenir des codes d'accès. Il est aussi bon de noter que le rapport de l'ICS-CERT se base uniquement sur les témoignages du personnel IT de six organisations ukrainiennes qui ont été directement témoins des événements, et pas sur une analyse technique du code ou du matériel impliqué dans l'incident.

Ces considérations mises à part, le fait que différents groupes d'experts soient d'accord sur l'origine cybercriminelle de la panne constitue une ultime (et sinistre) mise en garde à l'égard des opérateurs d'importance vitale (OIV). Car ces incidents ne font malheureusement que commencer. ... [Lire la suite]

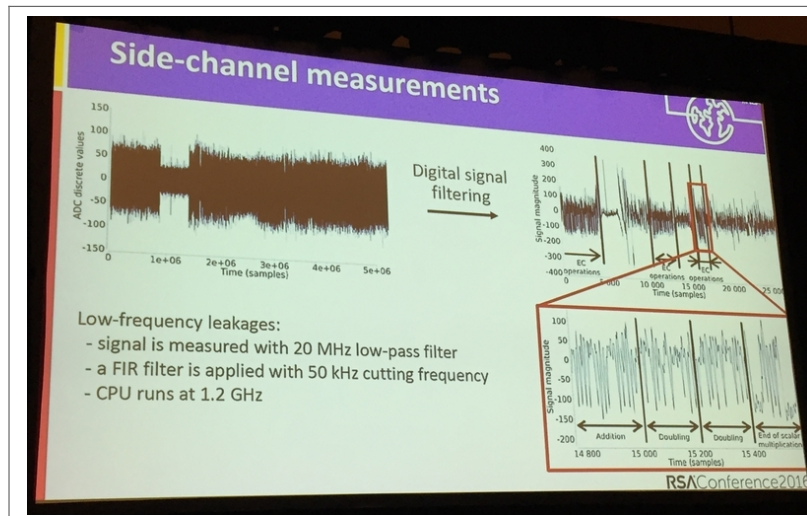


Réagissez à cet article

Source : *Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service*

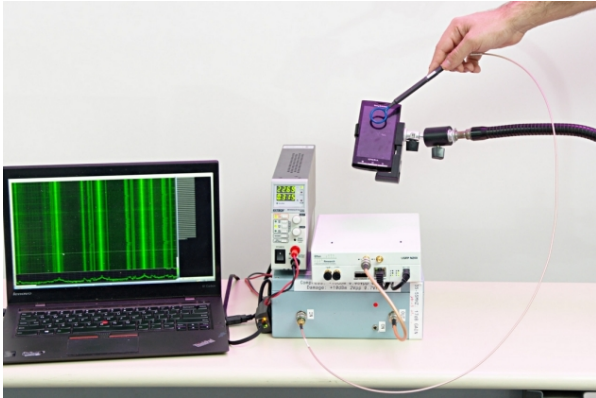
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites

électromagnétiques



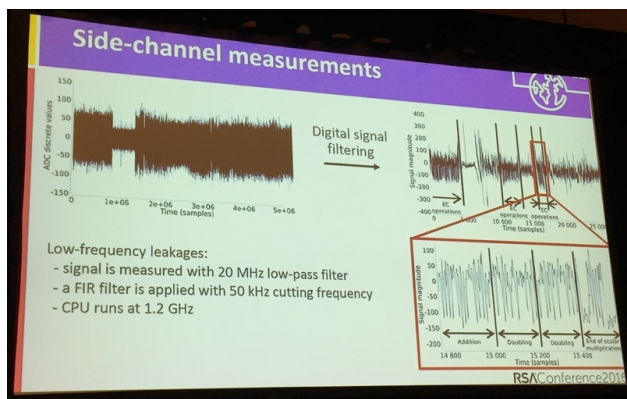
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques

Des chercheurs arrivent à extraire des clés de chiffrement privées en captant les signaux involontaires des circuits imprimés. Parmi les applications vulnérables figurent OpenSSL et les porte-monnaie Bitcoin.



Les smartphones d'aujourd'hui embarquent de plus en plus procédés cryptographiques pour sécuriser tout un tas d'échanges et de transactions. L'équipement matériel, toutefois, n'est pas forcément à la hauteur des enjeux. Deux équipes de chercheurs viennent de présenter concomitamment des attaques non invasives qui s'appuient sur les émanations électromagnétiques des terminaux mobiles pour récupérer des clés privées de signatures électroniques. Elles permettraient, par exemple, de pirater des porte-monnaie Bitcoin, des transactions Apple Pay ou des connexions sécurisées par OpenSSL.

La première équipe est française et regroupe quatre chercheurs issus d'Orange Labs, HP Labs, NTT et l'université de Rennes. Le 3 mars, à l'occasion de la conférence RSA 2016, ils ont montré comment extraire d'un téléphone Android des clés privées basées sur les algorithmes de courbes elliptiques (Elliptic Curve Digital Signature Algorithm, ECDSA). Leur étude se limite à une librairie cryptographique spécifique, à savoir Bouncy Castle 1.5. Quand celle-ci réalise les calculs mathématiques liés à la signature d'un message, les circuits intégrés du téléphone émettent des ondes électromagnétiques à basse fréquence (50 kHz).



Le traitement du signal révèle les opérations mathématiques (« addition », « doubling »)

Les chercheurs captent ce signal au moyen d'une antenne appliquée sur le téléphone et arrivent, par traitement de signal, à reconnaître les différentes opérations de ce calcul. Cette information est suffisante pour récupérer in fine la clé secrète. La librairie vulnérable a, depuis, été modifiée de telle manière que l'on ne puisse plus reconnaître les opérations (version 1.51). Néanmoins, une attaque concrète aurait pu être, selon les chercheurs, de cibler les porte-monnaie Bitcoin car ils s'appuient sur Bouncing Castel.

Ainsi, un attaquant aurait pu piéger le lecteur NFC d'un commerce qui accepte les Bitcoins et, ainsi, récupérer les adresses Bitcoin des clients. Ce qui lui permettrait alors d'en disposer comme bon lui semble. « On pourrait également imaginer des attaques à plus longue distance, à condition de disposer d'un équipement de captation suffisamment puissant, comme peuvent en avoir les agences gouvernementales », nous explique Mehdi Tibouchi, l'un des quatre chercheurs français, à l'issue de leur présentation.

Des attaques low-cost

La seconde équipe qui a planché sur ce type d'attaques est israélienne et regroupe cinq chercheurs issus de l'université de Tel Aviv et de l'université d'Adelaide (Australie). Leur attaque cible également les signatures basées sur les courbes elliptiques ECDSA, mais son domaine d'application est nettement plus large.

Ainsi, ces chercheurs ont réussi à extraire des clés privées sur les librairies OpenSSL et CoreBitcoin sur iOS, qui sont toujours vulnérables à l'heure actuelle. Ils ont également réussi des extractions partielles de clés privées avec la librairie CommonCrypto d'iOS et la version Android d'OpenSSL. Toutefois, CommonCrypto – qui est notamment utilisé par Apple Pay – n'est pas vulnérable au-delà de la version iOS 9 car Apple a intégré des « mécanismes de défense » contre ce type d'attaques.

Selon les chercheurs israéliens, les fuites de signaux peuvent être captées de façon électromagnétique par une petite antenne, ou de manière électrique par une petite résistance intégrée au niveau du câble de chargement USB (prix : quelques dollars). Dans les deux cas, le signal est envoyé dans l'entrée d'une carte son Creative Track Pre Sound, ce qui permet de le numériser et de l'amplifier (prix : 50 dollars). Au final, la mise en œuvre de l'attaque est donc de faible coût. Les chercheurs ont réalisé leurs tests avec un iPhone 3GS et un Sony-Ericsson Xperia x10 ... [Lire la suite]



Réagissez à cet article

Source : *On peut pirater les smartphones iOS ou Android à cause de leurs fuites électromagnétiques*

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?

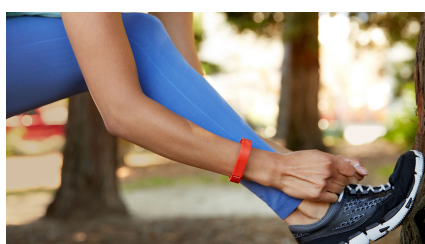


Comment
contrer les
nouvelles
menaces en
Cybersecurité
contre le
système
d'information
?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

Les accessoires connectés sont en plein boom



Les accessoires connectés sont en plein boom

En plein essor, le marché des accessoires connectés a enregistré des chiffres records lors de l'année 2015.

Vous avez sûrement dû remarquer de plus en plus de personnes munies de montres ou de bracelets connectés... Peut-être en avez-vous une vous-même. Parfois critiqués pour leur esthétique peu flatteuse, les bracelets et montres high-tech ont quand même connu un gros succès l'année précédente, comme le suggèrent les chiffres publiés par l'International Data Corporation (IDC) (<http://www.idc.com/getdoc.jsp?containerId=prUS41037416>).

En 2015, le marché des wearables a explosé. Plus de 78 millions d'accessoires ont été vendus, soit une augmentation de 171 % par rapport à l'an passé. « L'augmentation des ventes d'accessoires connectés signifie que le marché n'est pas uniquement destiné aux technophiles. Ces accessoires sont très bien accueillis par le grand public », fait remarquer Ramon Llamas, analyste à l'IDC.

LE PALMARÈS

Mais alors quel constructeur est le grand gagnant ?

Fitbit a terminé l'année 2015 de la même façon qu'il l'a commencée, en pôle position avec plus de 21 millions de bracelets connectés vendus, soit une augmentation de 93 % par rapport aux ventes effectuées l'année précédente. Fitbit est suivi par le chinois Xiaomi à l'origine du petit bracelet connecté low cost Mi Band.



Le constructeur chinois a vendu 12 millions d'objets, ce qui représente plus de 15 % du marché. Xiaomi est suivi de près par Apple qui occupe la troisième place du podium. La marque à la pomme a vendu plus de 11 millions d'Apple Watch, ce qui représente 14,9 % de parts dans le marché des accessoires connectés et jusqu'à 50 % pour le seul marché des montres connectées. Suivent ensuite Samsung et Garmin plus loin dans le classement.



Apple, qui est devancé par d'autres fabricants dans le classement général, est toutefois le grand gagnant de l'année passée. Même si l'entreprise de Tim Cook se trouve être troisième du classement, les prix de vente ne sont pas les mêmes d'une société à l'autre. Apple a vendu onze millions d'Apple Watch à 400 euros l'unité. Alors que Xiaomi, qui a écoulé 12 millions de bracelets connectés Mi Band, le vend à 15 dollars l'unité,... [Lire la suite]



Réagissez à cet article

IT Forum Sénégal 2016 : Interview de Mohamadou Diallo : Directeur de publication de CIO-MAG



IT Forum Sénégal
2016 : Interview de
Mohamadou Diallo :
Directeur de
publication de CIO-
MAG

18 et 19 février 2016, IT Forum Sénégal 2016 : Mohamadou Diallo : Directeur de publication de CIO-MAG interviewé



Réagissez à cet article