La CNIL et l'Inria vont révéler les indiscrétions d'Android

La CNIL et l'Inria vont révéler les indiscrétions d'Android

CNIL va diffuser lundi une étude intéressante montée avec l'Inria. Elle visera à informer les utilisateurs de la masse de données personnelles passant dans les mains de leur smartphone et des applications installées. Une première campagne visait l'iPhone en avril 2013. Cette fois Android sera sur le grill.

Android, passoire ou blockhaus à données personnelles ?
Après une auscultation qui aura duré 3 ans, la CNIL va publier lundi une étude menée à bien avec l'Institut national de recherche en informatique et en automatique (Inria).
L'objet ? Révéler au grand jour les données qui sont enregistrées, stockées et diffusées par les smartphones. Alors que « plus de 30 millions de Français utilisent quotidiennement smartphones et tablettes (…) les utilisateurs savent très peu de choses sur ce qui se passe à l'intérieur de ces « boites noires » » affirment les deux entités dans un communiqué commun.

L'iPhone déjà épinglé en avril 2013
Ce projet de sensibilisation baptisé Mobilitics avait déjà fait l'objet d'une première vague de résultats en avril 2013, mais les attentions s'étaient alors concentrées sur les iPhone. Lors de cette campagne précédente, la CNIL et l'Inria avaient flairé 189 applications pour récolter 9 Go de données sur une période de trois mois. L'opération dénonçait par exemple le fait que trop d'applications et jeux aient pu obtenir l'identifiant unique de l'appareil (46 %) sa géolocalisation (33 % environ) ou avoir accès au carnet d'adresses (8 %) sans toujours pleinement justifier ces indiscrétions ou du moins informer l'utilisateur. Apple avait alors réagi en modifiant certains paramètres, notamment concernant l'accès à l'UDID

« De nombreux acteurs tiers sont destinataires de données, par l'intermédiaire d'outils d'analyse, de développement ou de monétisation présents dans les applications. Les analyses permettent d'identifier plusieurs acteurs recevant des informations récupérées par l'intermédiaire de cookies spécifiques aux applications. Les acteurs classiques du traçage en ligne sont déjà très présents au sein de certaines applications, mais les chiffres montrent également l'émergence d'acteurs nouveaux dédiés au mobile » remarquait alors la CNIL. Du coup, celle-ci réclamait des magasins d'application de nouveaux modes d'information « des utilisateurs et de recueil du consentement. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/91332-la-cnil-et-l-inria-vont-reveler-indiscretions-d-android.htm

Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigées contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (ROP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html

---

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Victime d’un piratage à l’envergure peu commune, Sony Pictures semble être plus que déterminé à mettre un terme à la diffusion de ses fichiers sur le Net. En effet, la filiale du groupe japonais orchestrerait elle-même plusieurs opérations de piratage afin d’empêcher le partage de documents sensibles…

L’information est révélée par le site Re/Code, qui évoque des sources « en connaissance directe du dossier ». Selon celles-ci, Sony Pictures s’appuierait sur les datacenters asiatiques d’Amazon utilisés pour fournir les services cloud du marchand afin de mener une attaque par déni de service sur les sites proposant de télécharger des données issues du récent piratage dont la compagnie a été victime. Et ce ne serait pas tout : le Japonais s’attèlerait également à décourager les curieux en diffusant des copies piégées des fichiers volés.
Rappelons que Sony Pictures a toutes les raisons de chercher à mettre un terme à ces fuites. Outre des films encore inédits, la centaine de To de données volées contenait aussi de nombreux documents personnels d’employés et d’acteurs, des rapports financiers, ou encore des accords confidentiels. Si la diffusion de ces informations a d’ores et déjà occasionné quelques grincements de dents, le Japonais se doit de limiter les dégâts, d’autant que tout ce butin numérique n’est pas encore disponible sur le Web. La méthode, toutefois, peut laisser perplexe.
Cependant, ce n’est pas la première fois qu’un poids lourd des médias combat le feu par le feu. En 2007, plusieurs firmes, dont Sony Pictures mais aussi Universal, EMI, Paramount ou encore Ubisoft avaient été pointées du doigt pour avoir eu recours aux services de MediaDefender, dont les tactiques anti-piratage étaient fort décriées. En effet, ce spécialiste de la défense des intérêts des producteurs de médias pratiquait déjà la diffusion de faux fichiers afin de rendre le piratage franchement laborieux – sans compter qu’il s’était particulièrement illustré par un litige avec The Pirate Bay, qui l’accusait, non sans preuve, d’avoir orchestré une attaque en bonne et due forme contre ses serveurs.

Mais revenons-en à l’affaire qui nous occupe. Pour l’heure, les spécialistes qui se penchent sur le cas de Sony Pictures sont unanimes : il s’agit d’une attaque sophistiquée, qui aurait sans l’ombre d’un doute fonctionné contre une vaste majorité de systèmes. Son origine, toutefois, demeure à confirmer. Bien que les regards se soient d’emblée tournés vers la Corée du Nord, et bien que les pirates aient explicitement demandé l’annulation du film The Interview, qui met en scène l’assassinat de Kim Jong-un par deux journalistes plutôt limités, le régime nie avoir avoir entrepris une quelconque action à l’encontre de Sony Pictures au-delà de ses sommations de renoncer au long-métrage. Une autre piste, de plus, a fait son apparition : une des salves de leaks (fuites) a été orchestrée depuis le très chic hôtel St. Regis, à Bangkok. De quoi s’interroger sur la véritable identité des curieusement vindicatifs Guardians of Peace.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesnumeriques.com/sony-pictures-mene-attaque-ddos-pour-mettre-terme-fuites-n37601.html
Par Johann Breton

Un « coffre-fort » en ligne pour le stockage des données

Un « coffre-fort » en ligne pour le stockage des données

L'Institut Hasso Plattner (HPI) de Potsdam (Brandebourg) et l'Imprimerie fédérale (Bundesdruckerei) ont convenu d'un partenariat de recherche. Dans le cadre d'un premier projet pilote, un « coffre-fort en ligne » sera développé et mis à la disposition du grand public, de l'administration et des entreprises. Ce système doit permettre à l'utilisateur de stocker et gérer ses données en toute sécurité.

Le HPI, centre de recherche sur les TIC créé et financé par le co-fondateur de l'entreprise SAP, apporte sa technologie « Cloud-RAID » [1]. Les techniques RAID, généralement appliquées aux disques durs, consistent à répartir les données sur plusieurs supports physiques distincts pour améliorer les performances, la sécurité ou la tolérance aux pannes du système. Cette architecture a été adaptée au cloud.

L'Imprimerie fédérale contribue au projet, quant à elle, avec sa plateforme « Trusted Service ». Celle-ci garantit l'identification fiable des utilisateurs du « coffre-fort en ligne » par un document d'identité. La solution, où les données ne doivent être visibles que par l'utilisateur concerné, doit être flexible et facile à utiliser. Plusieurs fournisseurs de cloud sont intégrés au projet, ce qui implique qu'aucun prestataire ne sera, seul, en possession de l'ensemble des données.

Le projet pilote court jusqu'en mars 2015. Afin d'intensifier les recherches en matière de la gestion de l'identité numérique, les deux partenaires prévoient la mise en place d'un laboratoire sur la sécurité au HPI.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.bulletins-electroniques.com/actualites/77364.htm

Cyber-sécurité : 10 tendances pour 2015

	**Cyber-sécurité : 10 tendances pour 2015**

L'année 2014 a été particulièrement chargée pour les professionnels de la sécurité informatique. A quoi s'attendre pour 2015 ? Le point avec Thierry Karsenti, directeur technique Europe de Check Point.

Pour l'année 2014, « nous nous attendions à une augmentation des tentatives d'ingénierie sociale, et l'avons bien constatée. Elles ont conduit à d'importantes fuites de données dans plusieurs enseignes bien connues. Les campagnes de logiciels malveillants ciblées se sont également intensifiées. Les attaques de « RAM scraping » et les attaques de rançonneurs ont fait les gros titres. Le nombre de problèmes de sécurité mobile a également continué d'augmenter, indique Thierry Karsenti. Le hic, ce sont les vulnérabilités massives qui ont été découvertes dans des composants informatiques établis, tels que Heartbleed et BadUSB, qui ont touché des dizaines de millions de sites web et d'appareils dans le monde entier. Personne n'y avait été préparé. 2015 verra-t-il les mêmes cyber-risques ?

1. **Les logiciels malveillants « zéro seconde »**

Plus d'un tiers des entreprises auraient téléchargé au moins un fichier infecté par des logiciels malveillants inconnus au cours de l'année dernière. Les auteurs de logiciels malveillants utilisent de plus en plus des outils spécialisés de masquage, afin que leurs attaques puissent contourner les mécanismes de détection des produits antimalwares et infiltrer les réseaux. Efficaces, les bots continueront d'être une technique d'attaque privilégiée, indique Thierry Karsenti.

2. **La mobilité**

Comme vecteurs d'attaque, les appareils mobiles offrent un accès direct à des actifs plus variés et plus précieux que tout autre moyen d'attaque individuel. « C'est également le maillon faible de la chaîne de sécurité, qui donne aux agresseurs un accès à des informations personnellement identifiables, des mots de passe, la messagerie professionnelle et personnelle, des documents professionnels, et l'accès aux réseaux et aux applications d'entreprise », précise le directeur technique.

3. **Les systèmes de paiement mobile**

Le lancement d'Apple Pay avec l'iPhone 6 est susceptible de relancer l'adoption des systèmes de paiement mobiles par les consommateurs, ainsi que d'autres systèmes de paiement concurrents : "Tous ces systèmes n'ont pas été testés pour résister à de réelles menaces, ce qui pourrait signifier d'importantes chances de succès pour les agresseurs qui trouveront des vulnérabilités à exploiter ».

4. **Les failles dans l'open source**

Qu'il s'agisse de Heartbleed (voir l'interview de Patrick Duboys, fondateur d'Alice and Bob http://www.solutions-logiciels.com/actualites.php?actu=14573) ou de Shellshock (voir l'interview vidéo de Vincent Hinderer, expert en cyber-sécurité au Cert du groupe Lexsi http://www.solutions-logiciels.com/actualites.php?actu=15039), les vulnérabilités critiques des plates-formes open source communément utilisées (Windows, Linux, iOS) sont très prisées par les agresseurs car elles offrent d'énormes possibilités. Logiquement, ces derniers vont donc continuer de rechercher des failles pour essayer de les exploiter.

5. **Les attaques sur les infrastructures critiques**

Les systèmes Scada qui commandent les processus industriels devenant de plus en plus connectés, cela va étendre les vecteurs d'attaque qui ont déjà été exploités par des agents logiciels malveillants connus tels que Stuxnet. Près de 70% des entreprises d'infrastructures critiques interrogées par le Ponemon Institute ont subi des attaques au cours de l'année passée.

6. **Les objets connectés**

L'Internet des objets fournit aux criminels un réseau mieux connecté et plus efficace pour lancer des attaques. Les entreprises doivent se préparer à leur impact.

7. **Les réseaux définis par logiciel (SDN)**

La sécurité n'est pas intégrée au concept SDN, « et doit l'être », affirme Thierry Karsenti qui enchérit : « *Avec son adoption croissante dans les centres de données, nous nous attendons à voir des attaques ciblées qui tentent d'exploiter les contrôleurs centraux SDN pour prendre le contrôle des réseaux et contourner les protections réseau* ».

8. **L'unification des couches de sécurité**

Pour lui, les architectures de sécurité monocouche et les solutions isolées provenant de différents fournisseurs n'offrent plus une protection efficace pour les entreprises. Il affirme que de plus en plus de fournisseurs proposeront des protections unifiées issues de développements, de partenariats et d'acquisitions.

9. **Les protections en mode SaaS**

Thierry Karsenti prévoit « une utilisation croissante des solutions de sécurité sous forme de services pour fournir visibilité, contrôle, prévention des menaces et protection des données ». Cette augmentation se fera parallèlement à l'utilisation croissante des services de sécurité externalisés dans le Cloud public.

10. **L'évolution des analyses grâce au Big Data**

Le Big Data va apporter d'énormes possibilités à l'analyse des menaces pour identifier de nouveaux schémas d'attaque, selon l'éditeur. Les fournisseurs intégreront de plus en plus ces capacités analytiques à leurs solutions, et les entreprises devront également investir dans leurs propres systèmes d'analyse pour prendre les bonnes décisions en fonction du contexte et des menaces pesant sur leur activité. Le partage collaboratif de renseignements sur les menaces continuera de se développer, pour proposer des protections à jour qui répondent aux besoins spécifiques des utilisateurs finaux. Le directeur technique de Check Point ajoute que ces possibilités alimenteront à leur tour des solutions de sécurité unifiées capables de fournir automatiquement une protection contre les nouvelles menaces émergentes pour renforcer la sécurité des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.solutions-logiciels.com/actualites.php?actu=15189&titre=Cyber-securite-10-tendances-pour-2015 Par Juliette Paoli

Sony victime de hackers organisés et obstinés

Sony victime de hackers organisés et obstinés

Outre une société de sécurité mandatée par Sony, le FBI enquête lui aussi sur l'attaque informatique qui a visé récemment une filiale du groupe japonais, Sony Pictures. Et de premiers éléments ont été présentés par les enquêteurs au Sénat américain.

Ainsi comme les experts en sécurité de Mandiant, le FBI estime que l'attaque était inhabituelle et complexe à prévenir. Seules quelques entreprises auraient eu la capacité de bloquer la réalisation d'une telle attaque, estime l'agence fédérale.

Une attaque efficace sur 90% des entreprises

« Le malware qui a été utilisé aurait passé 90% des protections Internet qui sont déployées à l'heure actuelle dans le secteur privé et aurait probablement constitué un défi y compris pour un gouvernement fédéral » a déclaré le directeur adjoint de la division cybersécurité du FBI, Joe Demarest.

A l'occasion de cette audition devant un comité du Sénat, ce dernier a également précisé, selon The Hill, que l'attaqué était organisée et que son niveau de sophistication était extrêmement élevé. Quant à l'identité des auteurs, le FBI estime ne pas pouvoir la déterminer à ce stade, faute de preuves suffisantes.

Des liens avec la Corée du Nord ont été évoqués depuis le début de l'affaire, mais non confirmés. Les autorités du pays ont depuis démenti être à l'origine de cette cyberattaque, après avoir entretenu le flou au départ.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/sony-victime-de-hackers-organises-et-obstines-39811145.htm

Un autre programme secret de la NSA cible les réseaux GSM mondiaux

	Un autre programme secret de la NSA cible les réseaux GSM mondiaux

Des documents livrés par Edward Snowden évoquent un programme d'espionnage secret de la NSA. Appelé Auroragold, il cible les membres du GSMA pour recueillir des informations confidentielles sur les failles et les systèmes de cryptage, exploitées ensuite pour s'infiltrer dans les réseaux mobiles.

Selon des informations contenues dans des documents livrés par l'ex-consultant Edward Snowden, la NSA a lancé une campagne secrète pour intercepter les communications internes d'opérateurs et d'acteurs du secteur de la téléphonie mobile dans le but d'infiltrer leurs réseaux partout dans le monde. Dans un article publié samedi par le site The Intercept, qui a également mis en ligne les documents concernés, l'Agence nationale de sécurité américaine a mené, dans le cadre d'un programme appelé Auroragold, des opérations encore jamais rendues publiques.
Deux unités – Wireless Portfolio Management Office et Target Technology Trends Center – mises sur pied par la NSA, ont été chargées de surveiller de près les membres de la GSM Association, espionnant plus de 1200 adresses emails. L'objectif était d'intercepter dans les entreprises visées des messages internes et de recueillir des informations sur les failles de sécurité des réseaux et le cryptage des communications.
Les derniers documents indiquent qu'en mai 2012, sur les 985 réseaux de téléphonie mobile mondiaux, la NSA avait récolté des informations techniques sur 70 % d'entre eux. Mis à part les pays de quelques opérateurs ciblés – Libye, Chine et Iran – le document fourni par l'ancien consultant de l'agence américaine, toujours réfugié en Russie, ne contient aucun nom d'entreprises. Ces opérations d'espionnage ont permis à la NSA de récupérer des documents IR.21 utilisés par les membres de la GSMA pour signaler des failles de sécurité dans leurs réseaux. Les IR21 contiennent également des détails sur les solutions de cryptage utilisées par les opérateurs mobiles. D'après les documents d'Edward Snowden, la NSA, qui n'a pas répondu à une demande de commentaire, s'est servie de ces informations pour contourner le cryptage des communications.

Espionnage tous azimuts
Depuis juin 2013, de nombreux rapports et articles basés sur les documents fournis par Edward Snowden montrent l'étendu des opérations d'espionnage menées par la NSA sur Internet et les réseaux télécoms à travers le monde. Ils ont aussi permis de savoir que la NSA avait piraté les courriels de dirigeants de pays alliés des États-Unis et de découvrir qu'elle avait infiltré les réseaux et les systèmes d'entreprises étrangères, comme c'est le cas du constructeur chinois Huawei. L'an dernier, divers articles parus dans ProPublica, The Guardian et The New York Times, ont révélé que, pendant plusieurs années, la NSA s'était employée à affaiblir les normes de sécurité pour faciliter les opérations d'espionnage à grande échelle du gouvernement américain. Par exemple, des articles publiés en septembre 2013 par le Guardian et le NYT indiquent, sur la base des documents de Snowden, que la NSA a créé sa propre version du standard Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), un générateur de nombres aléatoires utilisé en cryptographie. Cette norme, approuvée pour un usage mondial en 2006, contiendrait une porte dérobée permettant à la NSA de s'introduire dans les systèmes de communications. Dès 2007, certains spécialistes et l'éditeur lui-même, RSA Security, recommandaient de désactiver par défaut le Dual_EC_DRBG. Des documents divulgués par Edward Snowden l'an dernier ont également apporté la preuve que la NSA pouvait espionner le trafic GSM chiffré avec l'algorithme A5/1.

Fin novembre, Symantec et Kaspersky Labs ont révélé l'existence d'un malware baptisé Regin, probablement développé par les États-Unis. Actif depuis au moins six ans, Regin cible les réseaux cellulaires GSM pour espionner les gouvernements, les infrastructures des opérateurs de téléphonie mobile, des instituts de recherche, des entreprises et des particuliers. En plus de ces opérations secrètes, la NSA espionne collectivement les conversations téléphoniques des citoyens américains. Le mois dernier, le directeur de la NSA, Michael Rogers a déclaré que l'agence ne prévoyait pas de réviser son programme de collecte : un projet de loi déposé devant le Sénat pour encadrer cette collecte n'a pas abouti.
Glenn Greenwald et Laura Poitras, les deux éditeurs et fondateurs du site The Intercept, ont déjà aidé Edward Snowden à diffuser ses documents par le biais de différents médias.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-un-autre-programme-secret-de-la-nsa-cible-les-reseaux-gsm-mondiaux-59530.html
Par Jean Elyan / IDG News Service

Juniper Networks présente ses

prédictions réseau, cloud et sécurité pour l’année 2015

Juniper Networks présente ses prédictions réseau, cloud et sécurité pour l’année 2015

Bientôt, nous allons atteindre et même dépasser la barre des 5 milliards d'utilisateurs connectés. Il y a trente ans, l'innovation était un concept à sens unique, une démarche clairement orientée entreprises, où les consommateurs passaient au second plan. Depuis, les choses ont changé. Alors que près de la moitié de la population mondiale est connectée à Internet, les consommateurs ont désormais leur mot à dire et exigent des applications et services innovants pour la qualité de leur vie, à leur rythme et à leurs conditions.

L'environnent de l'entreprise est contraint d'évoluer au rythme des innovations, chaque année, plus nombreuses. Bruno Durand, vice-président TCC, EMEA, chez Juniper Networks a analysé les tendances 2015 dans les réseaux, le cloud et la sécurité. Il partage aujourd'hui ses conclusions avec vous.

Réseaux intelligents : La diffusion de contenu sème la confusion chez les câblo-opérateurs
Si la tendance est au numérique depuis plusieurs années, l'industrie du câble n'a pour ainsi dire pas évolué. Mais 2015 sera l'année du changement. Avec l'avènement et l'essor de la diffusion de contenu en streaming, les abonnés, qui se tournent vers différents fournisseurs de contenu comme Netflix, commencent à demander de nouveaux services à leurs câblo-opérateurs. Selon le rapport « U.S. Digital Video Benchmark » publié cette année par Adobe, le nombre des consommateurs de contenu en streaming a augmenté de près de 400 % depuis l'an dernier. Cette tendance devrait se poursuivre, et pour rester dans la course et gérer l'augmentation du trafic IP, les câblo-opérateurs devraient miser sur les réseaux virtualisés en 2015. Même si la transition durera plusieurs années, ils vont d'ores et déjà examiner les possibilités qui s'offrent à eux et commencer à lancer des appels d'offres pour trouver des fournisseurs partageant leur vision.

Le trading hypercontextuel (HCT) supplante le trading à haute fréquence
Passé de 7 milliards de dollars en 2008 à 1,4 milliard de dollars en 2013, le trading à haute fréquence est sur le déclin. Il représente à l'heure actuelle moins de 50 % des volumes d'activité des marchés financiers, contre 70 % en 2008. Le trading HCT (hypercontextuel) constitue le nouveau mouvement de dérèglement du marché. Il repose sur l'assimilation en temps réel des fils d'actualités classiques (Bloomberg, Thomson-Reuters, AP, CNN) et des flux des réseaux sociaux (Twitter, Facebook, LinkedIn, Blogs, etc.) en vue d'exploiter les informations du marché et d'acquérir un avantage concurrentiel en termes de transactions boursières. Le tout est piloté par des analyses permettant le chargement, le traitement et l'extraction rapides des données dans le but de tirer parti des discontinuités du marché. Le trading HCT relève de l'informatique distribuée et de la performance. La latence est le principal enjeu et ne constitue plus un facteur de différenciation. Un système extrêmement intelligent s'impose. Les entreprises et leur environnement informatique vont devoir pré-assimiler plusieurs centaines de flux d'informations en temps réel, ce qui nécessitera une programmation et un équipement réseau extrêmement pointus.

Big Data et réseaux : un bien ou un mal ?
Face à l'« Internet des objets », dont les tentacules (les terminaux) continuent de se déployer dans nos vies, les données générées vont être beaucoup plus nombreuses. Ainsi une simple connexion entre un téléphone et un système de sécurité résidentiel produira des données qu'il faudra bien stocker quelque part. En 2015, il s'agira à la fois d'analyser ces données, de les interpréter via une infrastructure réseau appropriée et de les sécuriser au moyen de technologies dédiées. Les entreprises et opérateurs de télécommunications revoyant leurs méthodes de développement de réseaux pour gérer la déferlante de données, la demande de spécialistes des données va atteindre des niveaux record.

Cloud : Des clouds privés d'un nouveau genre vont apparaître
Les entreprises hors de la sphère informatique habituelle exploiteront le cloud autrement pour proposer leurs produits et services. L'essor des paiements mobiles, la multiplication des équipements connectés et les questions de sécurité qui en découlent vont transformer les marchés verticaux de manière radicale. À l'instar de Nike, autrefois spécialisé dans les vêtements de sport et désormais marque lifestyle connectée avec ses dispositifs de suivi, ou de Starbucks, devenu un grand adepte des paiements mobiles et de la diffusion de contenu, nombre d'entreprises vont créer des clouds privés pour répondre aux exigences de leurs clients. Si le cloud, comme toute nouvelle technologie, était au départ l'apanage des chefs de file du secteur des hautes technologies (sites web, services financiers), les entreprises du monde entier et de tous horizons – par exemple, les compagnies pétrolières et gazières comme Hess – vont, elles aussi, pouvoir s'y mettre. En 2015, la création de clouds permettra de se démarquer dans tous les secteurs.

Les solutions SDN en 2015
Les réseaux SDN (Software-Defined Network) vont se multiplier, à mesure que le marché et la technologie gagnent en maturité et que de plus en plus d'entreprises prennent conscience de la valeur de ces solutions. Les entreprises françaises commencent à voir les avantages du SDN selon une étude publiée cette année par Juniper : automatisation accrue, sécurité renforcée et centralisation dans la gestion des ressources. Si, en théorie, ils peuvent faciliter la gestion des réseaux et réduire les coûts, qu'est-ce que les entreprises vont réellement en faire ? Le SDN (couplé aux analyses) procure l'agilité nécessaire pour fournir des services avant que les clients ne les réclament.

Sécurité : Le marché noir continue de gagner en maturité
Selon une étude réalisée par RAND Corporation et Juniper Networks, les marchés noirs de la cybercriminalité ont atteint un niveau de maturité significatif. Et, cette tendance devrait se poursuivre en 2015. Face à la vulnérabilité persistante des systèmes de point de vente et l'afflux de services cloud, les pirates motivés par l'argent ont de beaux jours devant eux.

De nouveaux outils de piratage et kits d'exploitation des vulnérabilités des systèmes informatiques devraient voir le jour. Par ailleurs, malgré les mesures de répression prises par les services de police à l'encontre des sites web frauduleux tels que Silk Road, de nouveaux marchés devraient se développer pour répondre à la forte demande d'enregistrements volés et autres biens illicites. Les principaux fournisseurs de cloud et sites marchands étant la cible d'attaques à grande échelle, le nombre de cartes bancaires et autres identifiants proposés à la vente sur le marché noir devrait demeurer significatif.

L'analyse des données s'étend à la sécurité
Face à la volonté permanente de fournir des renseignements mieux exploitables et de meilleure qualité sur les menaces, on peut s'attendre à une hausse de la demande de spécialistes des données dans le domaine de la sécurité (« Data Scientists »). Déjà fortement sollicités dans d'autres secteurs, les professionnels capables de fournir des données plus précises sur les menaces seront extrêmement recherchés. C'est en appliquant les meilleures pratiques de la science des données à la sécurité que les entreprises disposeront de renseignements fiables et utiles sur les pirates et leurs attaques, et parviendront à se démarquer.

Sécuriser l'Internet des objets
Face à la multiplication des équipements connectés à Internet, le nombre de pirates et d'attaques a de fortes chances d'augmenter. À l'ère de l'Internet des objets, les entreprises qui ne s'étaient jamais soucié de la sécurité de leurs logiciels ne vont plus pouvoir se voiler la face, sous peine de s'exposer à de lourdes conséquences. Les pirates capables de prendre le contrôle à distance d'équipements médicaux, de voitures, de thermostats et autres systèmes physiques représentent une menace de taille pour la société. Les sociétés qui développent ces technologies doivent désormais intégrer la sécurité dans leur processus et mettre au point des outils permettant de corriger rapidement les systèmes concernés. À défaut, les risques de piratage logiciel des environnements et systèmes physiques stratégiques seront bien plus nombreux.

Nette amélioration de la confidentialité des données des utilisateurs
La confidentialité des données jouera un rôle majeur dans le développement et l'adoption de nouveaux produits. Suite aux récentes révélations sur les programmes de surveillance à grande échelle des administrations et services de police, les individus sont nettement plus intransigeants sur la confidentialité de leurs données, et les sociétés l'ont bien compris. Apple a, par exemple, renforcé la sécurité de son nouvel iPhone et de son système d'exploitation en mettant au point un système de cryptage par défaut qui va jusqu'à lui interdire l'accès aux données en sa qualité d'éditeur. Résultat : il ne peut pas fournir d'informations sur ses clients à d'autres parties, comme l'administration, et les oblige ainsi à contacter directement l'utilisateur.

Outre la sécurité renforcée des produits grand public, les applications de communication respectueuses de la confidentialité vont commencer à se généraliser. Face à des utilisateurs soucieux de la protection de leurs données, les applications comme Wickr et Silent Circle vont gagner en popularité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Juniper-Networks-presente-ses,20141210,49338.html
par Juniper Networks

4 bonnes raisons d’aimer Google (par Phil Jeudy)

4 bonnes raisons d’aimer Google (par Phil Jeudy)

Oui, je sais. Je suis fou d'écrire ça. La mode est à l'anti-Googlisme. Partout, on veut se payer la tête de Google, son évasion fiscale, ses commercialisations de données personnelles, son lobbying Bruxellois, ses histoires de coeur, que sais-je.

Je visitais un entrepreneur Français de la Silicon Valley la semaine passée, et il me rappelait a priori des propos échangés il fut un temps : » C'est une boite de merde, Google, hein ?! ». Bon, alors j'ai dit ça, mais là, je vais dire autre chose.
Google souffre d'un problème lié au temps modernes : la technologie est de plus en plus complexe, et passe de moins en moins vis à vis du grand public, parce qu'il faut s'arracher les cheveux pour montrer des choses qui parfois ne peuvent pas se voir facilement, à l'écran ou sur du papier journal.
Et je pense que, à l'image d'une presse politique plus intéressée d'une façon générale par des ronds-de-jambe d'arrière cour que de rendre une image fidèle de la situation du pays, la presse spécialisée se complait à prendre son audience pour des ignares, et tout ceci fait que l'on n'explique jamais assez comment les nouvelles technologies rendent service à leurs utilisateurs. Parler de quincailleries, et du dernier iPhone 12 et du Samsung 28, ça, c'est facile, y a qu'à comparer des chiffres. Mais se creuser la tête pour comprendre ce que fait une startup dans le domaine du cloud computing comme Docker, non Madame, y a trop de travail.

Amis lecteurs, on ne vous explique pas assez comment ça marche, Internet. Et d'ailleurs des sociétés comme Google ne le font pas suffisamment bien, c'est fort possible. Une compagnie mondiale, équipée d'agents commerciaux dans tous les pays, n'est pas la meilleure quand il s'agit de s'adresser aux marchés locaux, loin des « product managers » qui se creusent la tête pour vous servir les produits de demain. Vous ne parlez qu'à des vendeurs de soupe, des marchands de pub.
Je viens de rencontrer une équipe de journalistes français en visite professionnelle à San Francisco pour se poser des questions sur la société de Mountain View, avec des bons éléments de réflexion en tête. Ça nous change. Et franchement ça m'inspire ces quelques petits rappels qui me paraissent importants à garder en tête…

1. Les services de Google sont gratuits.
Si vous utilisez l'application Gmail de messagerie de façon normale, et que vous ne stockez pas trop de fichiers, vous ne payez rien. Vous ne payez pas pour utiliser la carte Google sur votre smarphone, pas plus que les fichier en ligne de Google Drive. Les requêtes sur le moteur de recherche ? Gratuites. Utiliser Blogger pour publier des histoires sur Internet, on ne paye pas. Utiliser un outil de traduction, stocker un nombre raisonnable de photos sur Internet ? Idem. Bloquer son téléphone Android qu'on vient de vous voler ? Service gratuit. Derrière la grande utilisation d'informations que Google opère selon leurs conditions générale d'utilisation, de vente et de tutti quanti, pleins d'outils à votre disposition au prix de 0 la tête à toto.

2. Vos données personnelles servent à améliorer des outils mis à votre disposition d'une façon générale gratuitement.
Internautes, Internautesses, on vous ment, on vous spolie. Derrière beaucoup d'anti-Googler, il y a une Arlette qui sommeille. Et qui oublie de vous dire aussi que l'utilisation de vos données personnelles servent à Google à perfectionner les outils mis à votre disposition. Il n'y a pas que la publicité que l'on vous sert en priorité, il y a toutes ses passerelles entre les produits Google : entre une recherche faite sur un ordinateur qui est mémorisée lorsque vous passez sur le browser de votre téléphone (si vous utilisez Chrome, cela va de soi), pour vous délivrer des informations sur mesure avec Google Now qui cherche à vous simplifier la vie (à défaut de pouvoir bien l'organiser, il y a encore du travail). Lorsque vous travaillez sur votre outil de messagerie, Google travaille à vous apporter le sucre alors que vous allez chercher votre café sur Internet. La meilleures façon de protéger vos données ? Tenez les loin d'Internet, votre meilleur outil de sécurité, ce sont vos doigts.

3. Google vous protège, dites lui merci.
Quand on regarde de près le mode connecté d'aujourd'hui, avec tous ces téléphones portables, routeurs, modems, ordinateurs portables, et bientôt votre lunettes, vos T-shirt connectés, le web est une grande passoire trouée. Estimez vous heureux que les hackers soient encore une race à part, organisée mais minoritaires, et essentiellement à but politique. Le jour où ces anonymes vont s'organiser par district et se soulever collectivement, vous allez vite réaliser à quel point vos données les plus fragiles sont accessibles. Mêmes les photocopieurs s'y mettent, des milliards de photocopies stockées sur des mémoires installées sur ces matériels par leurs fabricants se baladent en ce moment sur Internet. Des entreprises plus grosses que Google se font attaquer par des cyber-criminels en permanence, et bien que la nouvelle n'arrive pas à vos oreilles, car tout est fait pour éviter le scandale, la réalité est bien là : devant la grande abime d'un web où rien n'est vraiment caché, nous sommes tous à poil. Et bien Google, avec ses mots de passes, ses serveurs sécurisés, ses procédures, c'est un peu de protection dans un monde de brutes.

4. Google s'améliore. Dites aussi merci.
Je suis, par la force des choses, un « tout-Google ». Je dispose d'un matériel qui ne permet pas d'utiliser simplement des licenses de Microsoft, je me suis déjà fait voler un ordinateur (et perdu au passage des années-photos), et j'utilise les services au quotidien de produits poussés par quelques 50.000 et quelques employés. Google Voice reconnait mon anglais quoique polishé, l'accent est toujours bien là. Les outils de traduction sont encore plus simples à utiliser. Les outils de messagerie demande du temps d'adaptation, les résultats des requêtes sont de plus en plus visuels et agréables à consulter… L'impression générale est là : les outils marchent de mieux en mieux, et en plus de ça quelques acquisitions comme Waze pour le GPS, l'Uber embarqué dans la cartographie, le design, tout ça va dans le bon sens. Les outils de Google sur mobile vont à contre-pied de l'univers surfait des applications mobiles qu'on vous vend à gogo, tel le marchand de poisson pas frais de la BD d'Astérix, et c'est la bonne direction pour les années à venir : de la simplicité, pas de surf sur des écrans jamais assez grands… de l'interactif, du conversationnel. Quoi de plus normal sur un téléphone portable ! Faites dont l'expérience vous-mêmes, parlez lui donc, à votre smartphone, vous verrez bien.

Les problèmes de fonds restent entiers, tant d'un point de vue fiscal que légal, mais tout ce micmac reste bien éloigné des problèmes qu'un utilisateur de base comme moi peut avoir au quotidien.
Alors, verser un peu de rose et une petite dose de bonnes nouvelles dans un monde bleu et froid plein d'effroi, ça n'a jamais fait de mal.

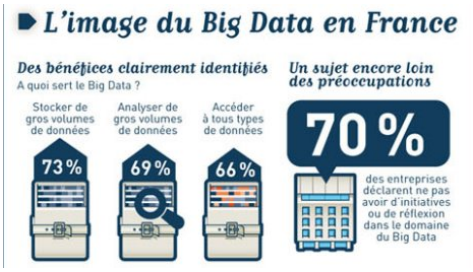
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.huffingtonpost.fr/phil-jeudy/avantages-google_b_6292352.html
par Phil Jeudy

Comment stocker ses données en toute sécurité

Comment stocker ses données en toute sécurité

L'actualité du piratage et du vol de grandes bases de données, de fichiers de clients, est hélas toujours très riche et risque de ne pas se tarir, au contraire (voir par exemple, cette très instructive « dataviz » des plus grandes bases de données piratées et la très riche collecte d'informations de La Quadrature du Net sur le « privacy nightmare », le cauchemar du respect de la vie privée).



Dernier en date, Domino's Pizza, qui s'est vu dérober une base de 600 000 noms, prénoms, adresses postales, numéros de téléphone, courriels et parfois codes d'entrée d'immeuble. Ou Sony, comme le rapporte Courrier International et l'a raconté Rue89, qui s'est fait pirater des dizaines de milliers de documents…

Grosses données, grosses responsabilités
Dans une interview pour l'édition américaine du Huffington Post, Sandy Pentland, spécialiste des Big Data, ces énormes masses de données que collectent opérateurs et services web (cf. « Big Data, vers l'ingénierie sociale ? »), rappelle une règle de sécurité assez simple à l'intention des entreprises. Les organisations doivent apprendre qu'elles ne peuvent stocker leurs données à un seul et unique endroit.

Capture d'écran de l'interview (HuffingtonPost.com)

Elles doivent les organiser par répartition, en séparant chaque type de données, en utilisant différents systèmes informatiques et différentes techniques de chiffrement. Avec la collecte des Big Data, viennent de grandes responsabilités pour éviter les « Big brèches », les « gros dommages », c'est-à-dire les risques de piratage informatique majeur. La restauration de la confiance du public après les révélations d'Edward Snowden est à ce prix.

Comme l'explique Sandy Pentland :
« Les ressources informatiques et humaines doivent toujours être redondantes et fragmentées afin d'éviter que des acteurs centraux trop puissants, qui peuvent être corrompus, ne puissent passer outre les précautions de sécurité standards. »

Il y a encore des progrès à faire ! Notamment et avant tout chez les fournisseurs de service de fichiers clients et de bases de données, qui souvent proposent des solutions bien trop centralisées…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://rue89.nouvelobs.com/2014/12/09/repetez-apres-dois-stocker-toutes-donnees-meme-endroit-256466
par Hubert Guillaud