La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

	La célèbre société de jeux pour enfants Vtech piratée : 5 millions de données clients exposées ?

La société Vtech, spécialisée dans les jeux ludo-éducatifs, a indiqué que la base de données de ses clients inscrits à son espace de téléchargement d'application, dont Explora Park en France, a été piratée.

Une technique d'injection de code SQL a été utilisée
On ne peut pas dire que Vtech ait été gâté pour Noël. Alors que les fêtes de fin d'année approchent à grands pas, la société spécialisée dans la vente de jouets et de jeux vidéo ludo-éducatifs a subi la plus grande cyberattaque de son histoire. Et le moins que l'on puisse dire, c'est que l'addition pourrait être salée avec près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants, tous inscrits à son service de téléchargement et de vente en ligne.

Près de 5 millions de données clients potentiellement tombées entre les mains de pirates, dont celles de 200 000 enfants…
Connu en France sous le nom d'Explora Park, cet espace permet de télécharger jeux, applications et autres e-books pour différentes consoles et tablettes de la marque dont notamment Storio et Mobigo. «
Un accès non autorisé à la base de données clients de notre espace d'apprentissage a eu lieu le 14 novembre. Dès que nous en avons eu connaissance, nous avons lancé une enquête et pris des mesures pour nous défendre contre de futures attaques », a indiqué Vtech dans un communiqué. « Notre base de données clients contient des informations de profils incluant des noms, mails, adresses, mots de passes chiffrés, réponses aux questions secrètes, adresses IP, adresses mails et historique de téléchargement. » En revanche, la société a précisé que la base de données piratée ne contenait aucune donnée et information bancaire.

Une attaque par injection de code SQL. Les conséquences de ce piratage pourraient être lourdes.
Si Vtech n'a pas officiellement indiqué le nombre de clients impacté par ce vol de données, il pourrait s'élever à plus de 4,8 millions, selon nos confrères de Motherboard qui avaient prévenu la société après avoir été contacté à ce sujet par des pirates la semaine dernière.
D'après eux, le piratage a été perpétré par le biais d'une attaque par injection de codes SQL. Une technique classique permettant d'insérer des commandes malveillantes dans les formulaires d'un site web dans le but de collecter de façon détournée des informations sensibles et/ou confidentielles pour ensuite obtenir un accès root aux bases de données serveurs et permettre un accès complet à ces dernières.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-piratage-vtech-5-millions-de-donnees-clients-exposees-63117.html
Par Dominique Filippone

Les solutions VPN touchées par une faille sur la

redirection de ports

Les solutions VPN touchées par une faille sur la redirection de ports

---

Suivre
nVpn.net @nVpnNet
Fixed a possibility to exploit a VPNs PF feature revealing a user’s real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy
01:07 – 27 Nov 2015
4 4 Retweets 2 2 j’aime

La société de sécurité Perfect Privacy a averti hier dans un billet de blog que bon nombre de solutions VPN étaient vulnérables à des attaques par redirection de port. De fait, un grand nombre d'utilisateurs pourraient voir leurs adresses IP réelles être dévoilées par des pirates utilisant les mêmes réseaux.

Les VPN, ou réseaux privés virtuels, sont conçus pour permettre laccès à des ordinateurs distants. Ils sont également souvent utilisés pour masquer les adresses IP dorigine. Mais il n'est finalement pas très compliqué d'obtenir quand même cette information, surtout quand les solutions existantes autorisent la redirection de port et qu'elles ne sont protégées contre des attaques utilisant cette fonctionnalité.

La faille « #VPN Fail »

Hier, la société Perfect Privacy a averti qu'un grand nombre de solutions VPN pouvaient révéler ces adresses IP si un pirate savait où chercher.

Pour que l'attaque fonctionne, il doit se trouver sur le même réseau virtuel que sa victime et connaître son adresse IP de sortie.

Comme l'indique The Hacker News, cette étape est assez simple puisqu'il suffit d'attirer l'utilisateur sur un site évidemment contrôlé par le pirate. Si la redirection de port est activée, le pirate pourra obtenir l'adresse IP réelle de la victime en l'amenant à ouvrir par exemple une image. À partir de là, il devient possible de rediriger le trafic vers un port là encore contrôlé par le pirate, d'où le nom de l'attaque.

Cette faille de sécurité, nommée « VPN Fail » par Perfect Privacy, a donné lieu à un avertissement lancé à de nombreux éditeurs. La plupart sont donc informés et le tir a été corrigé pour des solutions comme Private Internet Access, Ovpn.to et nVPN. Ce dernier est pour le moment le seul à avoir confirmé officiellement que cétait le cas, comme en atteste le tweet ci-dessous.

Perfect Privacy indique cependant que toutes les solutions n'ont pas été testées et que le nombre de produits vulnérables est donc sans doute important.

Clients VPN, systèmes dexploitation, BitTorrentLa faille pose évidemment un vrai problème de sécurité et de vie privée. Les VPN sont très utilisés dans les pays par exemple où la censure est importante, notamment parce qu'ils bloquent le repérage de la géolocalisation.

En conséquence, une faille qui laisserait apparaître la véritable adresse IP ne peut que briser tout l'intérêt de ces solutions et on peut espérer que des correctifs seront rapidement déployés.

La dangerosité de la faille est grande selon Perfect Privacy, puisqu'à cause de la nature même de la faille, on risque de la retrouver dans un très nombre de produits, dont les systèmes d'exploitation.

Elle peut également être utilisée pour piéger des internautes qui se serviraient de BitTorrent. La technique s'exploite d'ailleurs plus rapidement puisque le pirate n'a pas besoin d'amener l'utilisateur sur un site. Il doit simplement se trouver sur le même VPN et avoir activé la redirection de port.

nVpn.net @nVpnNet

Fixed a possibility to exploit a VPNs PF feature revealing a user's real IP https://goo.gl/KTxwza Thanks for early notice @perfectprivacy

01:07 – 27 Nov 2015

4 4 Retweets 2 2 j'aime

Rien à faire pour linstant du côté de lutilisateur

Dans tous les cas, la victime n'a pas besoin d'avoir l'option activée, et il n'y a donc rien qu'elle puisse faire de son côté. Tous les protocoles liés au VPN, comme OpenVPN et IPSec, sont également concernés. La seule solution est actuellement d'attendre, jusqu'à recevoir une notification de son fournisseur de solution VPN, si bien entendu ce dernier prend la peine de communiquer.

Réagissez à cet article

Source : http://www.nextinpact.com/news/97495-vpn-fail-solutions-vpn-touchees-par-faille-sur-redirection-ports.htm

Objets connectés : une moyenne de 5 failles par objet

Objets connectés : une moyenne de 5 failles par objet

9271 vulnérabilités majeures découvertes dans le firmware de 185 « objets de l'internet », principalement des routeurs, modems DSL/câble, téléphone IP, caméras de surveillance sous IP etc.

C'est le résultat brut de l'étude signée Andrei Costin et Aurélien Francillon d'Eurecom avec le concours d'Apostolis Zarras de l'Université de Bochum.
Réduire l'étude de ces trois chercheurs en quelques chiffres ne rend pas justice au travail effectué. En fait, son aspect le plus intéressant porte surtout sur l'automatisation et le travail à grande échelle de cette chasse au bug, grâce à la mise en place d'un environnement d'émulation.
La machine virtuelle est adaptée aux principaux systèmes et matériel du commerce, et les firmware chargés puis épluchés de manière dynamique les uns après les autres. Une sorte de « VM de torture » reproduisant au mieux l'environnement d'exécution.
Autre point important, cette recherche s'est limitée (sic) aux simples interfaces Web d'administration et de paramétrage qui sont en général intégrées dans le moindre des objets IoT. Et qui, pourrait-on ajouter, constituent le ventre mou de ces systèmes embarqués depuis des lustres. En d'autres mots, il n'est pas question ici des failles matériel, des trous Wifi/bluetooth/DECT, bref, de ce qui sort du volet « httpd » de ce travail. Il y a fort à parier que si l'analyse avait pu s'étendre à ces aspects, le nombre de défauts recensés aurait été probablement doublé.
Mais ce genre de tests est nettement moins susceptible de pouvoir être automatisé. Les armes de chasse sont classiques : Arachni, Zed Attack Proxy, w3af, ce qui n'interdit pas à tout chercheur souhaitant continuer ce travail d'y ajouter Metasploit ou Nessus.
L'environnement lui-même, Qemu, a été retenu en raison du nombre important de processeurs supportés : Arm, Mips, Mipsel, Axis Cris, bFLT, PowerPC, X86 et même Nios II d'Altera.
Certains cœurs échappent à ce crible, tels les processeurs spécifiques de Dlink ou un Risc 32 bits peu répandu, le Arctangent A5.
Plus de la moitié des objets utilisant un ARM ont été vulnérables à un Chroot et une attaque Web, entre 17 et 21 % pour les systèmes à base de MIPS, et un peu moins de 30 % pour les IoT avec moteur Mipsel.
Les vulnérabilités les plus fréquemment rencontrées sont : XSS (5000 sur les 9271 recensées), manipulation de fichiers (1129), exécution de commandes arbitraires (938), ajout de fichiers (513), divulgation de fichiers (461), injection SQL (442)…

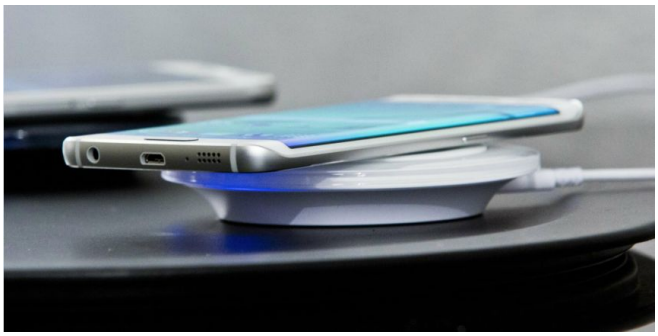
La confiance dans l'IoT, ça se mérite. Toutefois, précisent les trois chercheurs, il est des domaines où la sécurité est prise nettement plus au sérieux.
C'est notamment le cas de boîtier de télévision payante, par câble ou satellite. Probablement en raison des conséquences de pertes économiques directes qu'un défaut de sécurité provoquerait immédiatement, certainement aussi conséquemment aux multiples hacks qui, depuis plus de 20 ans, ont conduit ces intégrateurs à s'engager dans une course au blindage antipirates.
Comme quoi, c'est pas la sécurité qui manque, dans le domaine de l'Internet des Objets, c'est la menace financière.

Réagissez à cet article
Source : http://www.cnis-mag.com/iot-une-moyenne-de-5-failles-par-objet.html

Samsung Galaxy S6 et S6 Edge : sans le savoir, vous êtes (peut-être) sur écoute

Samsung Galaxy S6 et S6 Edge : sans le savoir, vous êtes (peut-être) sur écoute

Voilà une information qui ne devrait pas ravir les utilisateurs de smartphones de la marque Samsung. Une équipe de chercheurs en sécurité informatique vient d'annoncer avoir découvert une faille permettant d'écouter les conversations téléphoniques émises depuis les Galaxy S6 et S6 Edge.



En vrai, c'est plutôt une bonne nouvelle ! Explications.
Rassurez-vous, les ingénieurs de Samsung sont déjà sur le coup pour corriger la faille de sécurité;
On a du mal à y croire, et pourtant une équipe de chercheurs en sécurité informatique a découvert l'existence d'une faille permettant d'écouter les conversations téléphoniques des possesseurs de smartphones de la marque Samsung.
Le problème a été révélé par deux experts Daniel Komaromy et Nico Goldelors lors du Mobile Pwn20wn de PacSec à Tokyo, un concours de hackeurs « gentils » pour tester la sécurité des produits high-tech.
Il s'agit d'une attaque de type « Man in the Middle ». En langage informatique, l'attaque dites de « l'homme du milieu » est une technique qui consiste pour un hackeur à s'interposer entre vous et votre destinataire dans le but d'intercepter les échanges qui ont lieu.
Pour ce faire, toutefois, cela nécessite d'installer une station d'écoute à proximité du smartphone espionné. Ce qui est loin d'être à la portée de tous, évidemment.

Capter les conversations, sans que l'utilisateur ne le sache

Tous les téléphones mobiles, et plus généralement tous les appareils de communication mobile, fonctionnent en réalité avec deux systèmes d'exploitation qui tournent l'un à côté de l'autre. Le premier, tout le monde le connaît : il se nomme Android, iOS, Windows Phone ou BlackBerry. L'autre est moins connu : il se trouve sur une puce électronique située dans la base du téléphone, qui permet de gérer les appels vocaux émis depuis le smartphone (appelé baseband).
Lorsque le téléphone est connecté à un réseau (mobile ou internet), la station d'écoute installée préalablement envoie un petit logiciel (un firmware, en langage informatique) qui permet de pirater cette puce électronique. Les communications peuvent alors être captées par un hackeur, à distance, sans que l'utilisateur ne puisse s'en apercevoir.

Une autre faille découverte sur l'appli Chrome Android

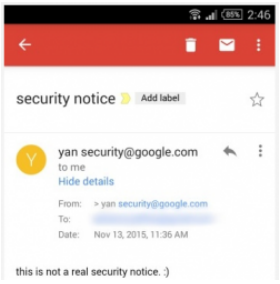
Rassurez-vous, les ingénieurs de Samsung sont déjà sur le coup pour corriger la faille ! Les deux chercheurs en sécurité informatique n'ont pas dévoilé publiquement l'ensemble de la procédure, pour éviter toute tentation. Un rapport détaillé a été remis à Samsung.
À l'instar de Google, le géant coréen propose désormais des mises à jour de sécurité mensuelles : la prochaine est disponible dans les prochains jours.
Lors du même événement, une autre faille a été décelée concernant cette fois le navigateur Chrome sous Android. Grâce à cette faille, il serait possible d'installer une application sur n'importe quel appareil Android, et sans que l'utilisateur ne puisse s'en apercevoir.

Source :
http://www.metronews.fr/high-tech/samsung-galaxy-s6-et-s6edge-sans-le-savoir-vous-etes-peut-etre-sur-ecoute/moks!xGbp39O9FvRQ/

Google corrige le bug de tromperie d’identité Gmail

Google corrige le bug de tromperie d’identité Gmail

Après avoir alerté Google fin octobre de l’existence d’un bug dans l’app Gmail pour terminaux Android permettant de changer l’adresse de l’expéditeur d’un message, la société vient finalement de le corriger.



C’est un bug plutôt gênant que la chercheuse indépendante en sécurité Yan Zhu avait découvert dans l’app Gmail pour Android. A savoir la possibilité de changer l’adresse d’expéditeur d’un message pouvant permettre ainsi de tromper le destinataire sur l’identité de la personne qui le lui a envoyé. Utilisé à mauvais escient, ce bug pouvait jusqu’alors être utilisé à des fins malveillantes en particulier dans le cadre d’opérations de phishing. Après avoir alerté fin octobre les équipes de sécurité de Google, la société est finalement en train de résoudre le problème : « Nous avons apprécié le rapport de la chercheuse et nous corrigeons le problème qu’elle a trouvé dans l’app Gmail pour Android », a indiqué la firme de Mountain View.
« Notre relation rapprochée avec la communauté des chercheurs en sécurité nous aide à garder les utilisateurs à l’abri ». Dans les colonnes de nos confrères de Motherboard, la chercheuse en sécurité Yan Zhu n’a en tout cas pas manqué de faire remonter sa consternation quant au temps de réponse de Google pour résoudre la situation : « Je ne veux pas dénigrer le travail de l’équipe de Google en matière de sécurité qui est difficile et qui doit sans doute être inondée de faux rapports », a indiqué Yan Zhu. « Cependant, le processus de rapport de bug légitime a été beaucoup plus frustrant que ce à quoi je m’attendais. » Article de Dominique Filippone

---

Denis JACOPINI est #Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous
Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://www.lemondeinformatique.fr/actualites/lire-google-corrige-le-bug-de-tromperie-d-identite-gmail-63009.html

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1 | Le Net Expert Informatique

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1

Le 7 novembre, soit samedi dernier, une énorme panne a cloué les avions au sol pendant plusieurs heures à l'aéroport d'Orly. Une panne provoquée par une panne informatique d'une des tours de contrôle qui scrute les données météo. Après plusieurs heures, le trafic a repris et l'histoire aurait pu s'arrêter là. Mais le Canard Enchaîné a révélé la vraie nature de cet incident.

L'hebdomadaire revient en effet sur cette panne. Selon lui, elle concernait le système Decor (qui fourni les données météo) tournant sous… Windows 3.1. Un OS sorti en 1992, tout de même. C'est à cause d'une défaillance de ce système que des milliers de passagers se sont retrouvés bloqués. Dans le Canard, un ingénieur de l'aéroport donne d'ailleurs son avis sur la situation :

Samedi matin, le trafic n'était pas vraiment dense. Mais imaginez, pendant la COP21, le ballet des chefs d'Etat perturbé à cause d'un logiciel informatique qui date de la préhistoire. De quoi aura-t-on l'air ?

C'est vrai que l'histoire est tout de même étonnante, voire pathétique. Mais comme l'affirme l'hebdomadaire, le ministre des transports prévoit de renouveler le parc informatique de l'aéroport à partir de 2017.

Source :
http://www.journaldugeek.com/2015/11/12/une-grosse-panne-a-laeroport-dorly-provoquee-par-un-systeme-tournant-sous-windows-3-1/

Une faille dans un composant expose des milliers d’applications Java | Le Net Expert Informatique

Une faille dans un composant expose des milliers d’applications Java

Découverte il y a 9 mois, une vulnérabilité non corrigée dans le composant Apache Commons Collections expose les serveurs d'applications Java à un sérieux risque d'exécution de code à distance.

La dernière faille critique Java en date a été découverte dans la bibliothèque Apache Commons qui regroupe un ensemble de composants Java dont la maintenance est assurée par l'Apache Software Foundation. La bibliothèque est utilisée par défaut dans plusieurs serveurs d'applications Java et dans des produits comme Oracle WebLogic, IBM WebSphere, JBoss, Jenkins et OpenNMS.

La vulnérabilité, précisément localisée dans le composant Collections d'Apache Commons, résulte directement de la désérialisation des objets Java. Dans les langages de programmation, la sérialisation désigne le processus de conversion des données en format binaire. Cette conversion permet le stockage des données dans un fichier ou dans la mémoire, ou leur envoi sur le réseau. La désérialisation est le processus inverse.

La vulnérabilité, signalée par les chercheurs Chris Frohoff et Gabriel Lawrence en janvier 2015 pendant une conférence sur la sécurité, n'a pas suscité beaucoup d'attention. Sans doute que la plupart des gens estiment que la responsabilité de la prévention des attaques exploitant le processus de désérialisation incombe aux développeurs d'applications Java et non aux créateurs de la bibliothèque.

« Je ne pense pas qu'il faut incriminer la bibliothèque, même si elle peut certainement être améliorée », a déclaré par courriel Carsten Eiram, responsable de la recherche dans l'entreprise de sécurité Risk Based Security.

« En définitive, une entrée non fiable ne devrait jamais être désérialisée aveuglément. Les développeurs devraient comprendre comment fonctionne une bibliothèque et valider chaque entrée au lieu de lui faire confiance ou espérer qu'elle effectue à leur place ce travail de sécurisation ».

Un correctif bientôt disponible

Vendredi dernier, la faille est revenue dans l'actualité : les chercheurs de l'entreprise de sécurité FoxGLove ont livré des exploits proof-of-concept pour WebLogic, WebSphere, JBoss, Jenkins et OpenNMS basés sur la vulnérabilité. Mardi, Oracle a publié un avis de sécurité comportant des instructions d'atténuation temporaires pour WebLogic Server en attendant le correctif permanent que l'éditeur est en train de mettre au point. Les développeurs d'Apache Commons Collections ont également commencé à travailler sur un correctif.

Apache Commons Collections contient une classe InvokerTransformer. La faille utilise la sérialisation Java et une méthode d'appel dynamique dite de réflexion sur la classe InvokerTransformer pour exécuter du code distant. Un attaquant pourrait fabriquer un objet sérialisé avec un contenu malveillant pour qu'il soit exécuté au moment de sa désérialisation par une application Java avec l'aide de la bibliothèque Apache Commons. « Prises séparément, la classe InvokerTransformer et la sérialisation ne sont pas en cause, mais dès qu'elles sont combinées, la question de sécurité apparaît », a déclaré Joshua Corman, CTO de Sonatype, une entreprise d'automatisation de la chaîne d'approvisionnement des logiciels qui aide les développeurs à suivre et à gérer les composants qu'ils utilisent dans leurs applications.

D'autres composants Apache Commons vulnérables

Joshua Corman et Bruce Mayhew, un autre chercheur en sécurité de Sonatype, pensent que le problème ne concerne pas uniquement le composant Collections d'Apache Commons. Selon eux, d'autres composants Java pourraient poser un problème identique. « Je peux vous assurer qu'aujourd'hui, un tas de gens passent les composants les plus courants au peigne fin pour identifier d'autres classes sérialisables qui pourraient permettre l'exécution de commandes à distance », a déclaré Bruce Mayhew. « Et parmi eux, il y a des gens bien intentionnés, mais probablement aussi des gens mal intentionnés ». Si l'on en croit les discussions en cours sur la recherche de bogues, InvokerTransformer n'est sans doute pas la seule classe vulnérable de l'environnement Apache Commons Collections. Trois autres classes pourraient présenter le même problème. Les chercheurs de FoxGLove Security se sont intéressés de près à des projets de logiciels publics utilisables en « commons-collection » hébergés sur GitHub et ils ont identifié 1300 sources possibles. Et il faut aussi prendre en compte les milliers d'applications Java qui utilisent la bibliothèque dans les environnements d'entreprise.

Même s'il y a une forte probabilité que le problème dépasse le composant Collections, les développeurs devraient essayer de retirer les commons-collections du classpath ou de supprimer la classe InvokerTransformer du fichier jar concerné tant qu'il n'y a pas de correctif disponible pour la vulnérabilité. Mais tous ces changements doivent être appliqués avec précaution, car ils peuvent rendre les applications inopérantes.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-faille-dans-un-composant-expose-des-milliers-d-applications-java-62956.html

Par Lucian Constantin, IDG NS (adaptation Jean Elyan)

La NSA assure divulguer les vulnérabilités découvertes.

Avant ou après attaque ? | Le Net Expert Informatique

La NSA assure divulguer les vulnérabilités découvertes

L'agence de renseignement US assure communiquer aux éditeurs 91% des failles qu'elle découvre dans les logiciels. La NSA ne précise pas en revanche quand ces données sont transmises et si les failles ont été exploitées au préalable.

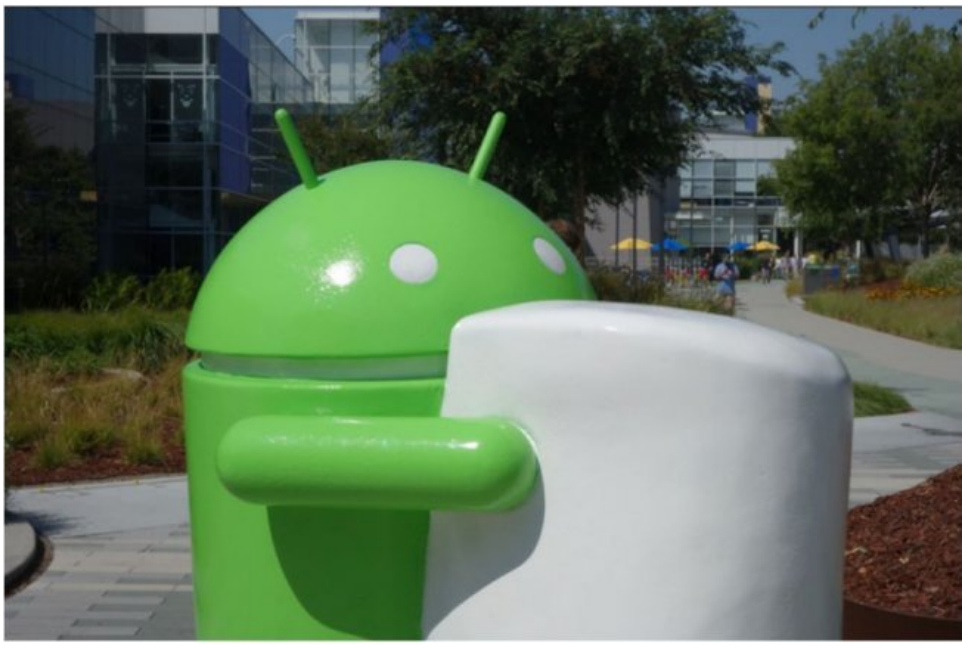
L'agence de renseignement américaine est une grande consommatrice de failles de sécurité. Celles-ci lui permettent en effet de récolter des informations. Mais la NSA, en ne dévoilant pas ces vulnérabilités, laisse aussi les entreprises US exposées à des attaques.
Après les révélations d'Edouard Snowden, ces pratiques ont été examinées. Pas sûr cependant qu'elles ne changent comme l'explique Reuters. Sur son site Internet, la NSA justifie sa démarche, estimant ainsi qu'il y « a des avantages légitimes et des inconvénients à la décision de divulguer les vulnérabilités ».

Combien de temps la NSA garde-t-elle le secret ?

Et les arbitrages entre une divulgation rapide et la rétention de cette information « peut avoir des conséquences significatives ». En dévoilant une vulnérabilité, la NSA précise ainsi qu'elle renonce à la possibilité de collecter du renseignement crucial : attaque terroriste, vol de propriété intellectuelle ou découverte d'autres failles encore plus dangereuses.
Néanmoins, la NSA assure, « historiquement », avoir communiqué plus de 91% des vulnérabilités identifiées dans les produits soumis à son audit interne, développés ou utilisés aux Etats-Unis. Et les autres ? Il s'agit de failles déjà corrigées ou gardées secrètes pour des raisons de sécurité nationale, explique l'agence.
Mais comme le souligne Reuters, la question est plus de savoir quand les vulnérabilités sont communiquées aux éditeurs et ainsi corrigées. D'après un ancien officiel de la Maison-Blanche, il est raisonnable de penser que ces 91% de failles sont préalablement exploitées avant de faire l'objet d'une divulgation.
La NSA n'apporte aucun commentaire sur ce point. Mais la faille Heartbleed est une illustration de ces pratiques. La NSA aurait eu connaissance de cette faille critique et l'aurait exploitée pour ses opérations au moins deux ans avant qu'elle ne soit connue publiquement. L'agence de renseignement réfute cependant.

Source :
http://www.zdnet.fr/actualites/la-nsa-assure-divulguer-les-vulnerabilites-decouvertes-avant-ou-apres-attaque-39827840.htm

20 000 apps Android détournées dans les boutiques parallèles | Le Net Expert Informatique



20 000 apps Android détournées dans les boutiques parallèles

Sous l’apparence d’applications Android très utilisées comme WhatsApp ou Google Now, des copies malveillantes, proposées sur des boutiques aux critères de sélection moins stricts que Google Play, installent au coeur des terminaux mobiles des adwares extrêmement difficiles à déloger.

Des experts en sécurité de Lookout ont trouvé plus de 20 000 exemples d’apps Android compromises, dont certaines sont des copies d’applications figurant parmi les plus populaires comme Facebook, Google Now, SnapChat, Twitter ou WhatsApp. Elles contiennent du code malveillant et affichent agressivement des publicités sur les terminaux.

Par ailleurs, contrairement aux habituels adwares, ces apps sont installées de telle façon que les utilisateurs ne peuvent pas les supprimer. Elles noyautent les terminaux en accédant aux accès racines permettant de sortir des sandbox restreignant les manipulations et peuvent ainsi prendre le contrôle complet du terminal, de ses applications et de ses données.

Les apps compromises résident sur des boutiques parallèles à Play

Les utilisateurs qui téléchargent leurs apps de façon classique sur la boutique Google Play, ne sont normalement pas concernés car ces applications comportant un cheval de Troie sont principalement distribuées à travers d’autres boutiques d’apps en ligne. Cependant, certains utilisateurs passent par ce type de boutiques car elles proposent souvent des apps que Google Play n’autorise pas, relatives aux jeux en ligne ou pornographiques.

Les pays dans lesquels Lookout a détecté le plus grand nombre d’applications compromises sont les Etats-Unis, l’Allemagne, l’Iran, la Russie, l’Inde, la Jamaïque, le Soudan, le Brésil, le Mexique et l’Indonésie. Les chercheurs de la société spécialisée en sécurité mobile ont distingué trois familles d’apps qui noyautent automatiquement les terminaux à la racine, respectivement dénommées Shedun, Shuanet et ShiftyBug. Les pirates qui les exploitent repackagent les apps les plus populaires de Google Play et les installent sur des boutiques en ligne moins regardantes sur la sécurité. « Nous pensons que ce type d’adware intégrant des chevaux de Troie vont devenir de plus en plus sophistiqués avec le temps et qu’ils pourront mieux dissimuler leur présence sur le terminal », expliquent les chercheurs de Lookout dans un billet.

Source :
http://www.lemondeinformatique.fr/actualites/lire-20-000-apps-android-detournees-dans-les-boutiques-paralleles-62898.html
Article de Lucian Constantin / IDG News Service (adapté par Maryse Gros)

Une vulnérabilité dans les Cartes bancaires connue et

exploitée discrètement | Le Net Expert Informatique

Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement

Des chercheurs viennent de publier un rapport d'étude sur l'exploitation concrète mais discrète d'une vulnérabilité affectant les cartes EMV et connue depuis plus de 5 ans.

Combien de cas réellement constatés ? Combien de cas non constatés ? C'est la question que soulève l'étude que viennent de publier Houda Ferrradi, Rémi Géraud, David Naccache et Assia tria, de l'Ecole normale supérieure et du CEA-TEC Paca.

Dans celle-ci, les quatre chercheurs se penchent des cartes bancaires EMV modifiées pour permettre leur utilisation sans en connaître le code PIN, en toute discrétion, grâce à deux puces câbles l'une sur l'autre, sur la puce d'origine : « la première puce est clipsée sur une carte authentique volée. La seconde puce joue le rôle d'intermédiaire et communique directement avec le terminal de point de vente. L'ensemble est intégré au corps en plastique d'une autre carte également volée ».

Le concept est connu depuis début 2010. C'est le chercheur Steven J. Murdoch, de l'université de Cambridge qui avait levé le voile sur une vulnérabilité potentiellement grave des cartes bancaires à puces dites EMV. Une faille qui « permet à un fraudeur d'utiliser une carte de paiement à puce volée pour régler un achat, via un terminal de paiement électronique non modifié, sans connaître le code PIN du porteur légitime de la carte bancaire ». Ainsi, un dispositif électronique intercepte et modifie les communications entre la carte à puce et le terminal de paiement électronique. Lorsque celui-ci demande à la carte de vérifier le code PIN saisi par l'utilisateur, le dispositif du pirate intercepte la requête et se charge, à la place de la carte, de répondre au TPE que le code a été vérifié et confirmé. Voilà ce que décrivait alors, par le menu, le chercheur britannique dans un rapport d'étude préliminaire.

Lors d'un entretien téléphonique avec LeMagIT, Steven J. Murdoch évoquait alors l'ampleur de la menace : « le reçu indique que la transaction a été autorisée par code PIN », du moins était-ce le cas lors de ses tests au Royaume-Uni, pour des transactions de type offline comme online – à savoir, avec ou sans connexion aux serveurs de contrôle des transactions. Un détail lourd de conséquences : même armé d'une déclaration de perte ou de vol, comment le porteur légitime de la carte pourra-t-il dégager sa responsabilité face à un banquier qui ne manquera pas de lui rappeler qu'il est responsable de la confidentialité de son code PIN ? Pour Steven J. Murdoch, le risque était notamment que « d'autres aient découvert la faille avant nous ».

La lecture du rapport des quatre chercheurs français nous apprend qu'environ 40 modifications frauduleuses de cartes, exploitant la vulnérabilité dévoilée par Murdoch, ont été découvertes en 2011 : « en mai 2011, le GIE Cartes Bancaires a relevé qu'une dizaine de cartes EMC, volées en France quelques mois plus tôt, étaient utilisées en Belgique. Une enquête de police a été ouverte ». Le montant de la fraude liée à cette opération : un peu moins de 600 000 € sur plus de 7 000 transactions.

Début 2010, sans surprise, le GIE Cartes Bancaires minimisait toutefois la menace, estimant qu'elle « nécessitait des équipements qui ne sont pas très discrets ». Certes, la carte frauduleuse présente une puce d'apparence plus épaisse que la normale. Mais au moins dans le cas de cette fraude ayant fait l'objet d'une enquête, cela n'a pas éveillé de soupçons.

Source :
http://www.lemagit.fr/actualites/4500256061/Cartes-bancaires-une-vulnerabilite-connue-exploitee-discretement
par Valéry Marchive