VEILLE TECHNOLOGIQUE LES FAILLES DE SECURITE SUR ANDROID

Coulibaly

HEWLETT-PACKARD Cpe.corp

Veille Technologique

La veille technologique consiste à s'informer régulièrement sur les avancées technologiques. Mon sujet choisi était les failles de sécurité sur androïde et Google.

Nous allons voir que peu de gens savent qu'androïde à subit différente faille au cours de sa vie et nous allons voir les principales dont : rowhammer, dirtycow, etc.

Nous allons aussi voir si androïde de Google et plus sécurisé que Ios de Apple.

Les différentes sources que j'ai utilisé lors de cette étude sont : Wikipédia, Wikileaks, Numerama, Airdroide, Quarooter et bien d'autre.

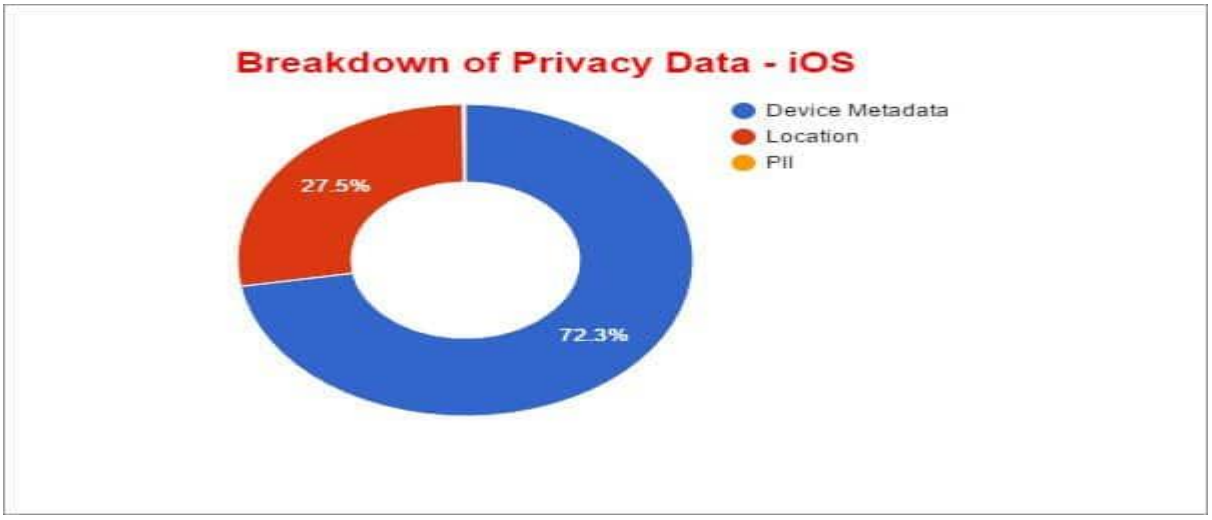
La faille de androïde la plus récente selon wikileaks est que certains espion américain de la CIA se sert de ses failles de sécurité. Mais Google retorque cette hypothèse bien sur cela dans le but de ne pas affoler ses internautes.Selon Heather Adkins, porte-parole de Google sur les dossiers sécurité et confidentialité, explique que l'entreprise « *est sûre que les mises à jour de sécurité et les protections à la fois dans Chrome et sur Android immunisent déjà les utilisateurs des vulnérabilités révélées.* »

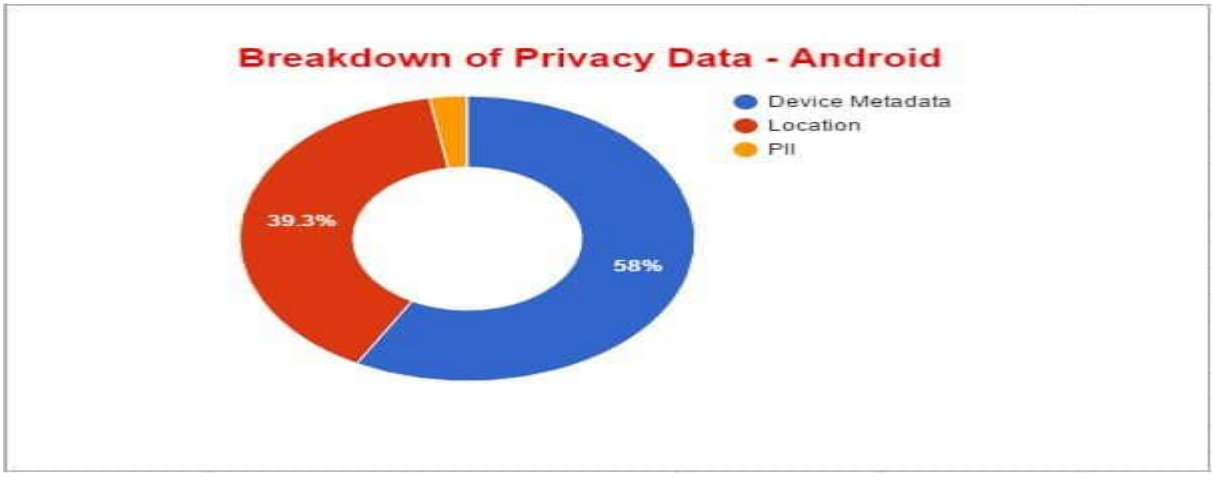
Du côté de Mountain View, Google aura mis un jour de plus à s'exprimer que son rival, mais pour finalement tenir un discours très proche. Dans un communiqué, initialement publié par Recode, Bien sûr, le géant conserve également une marge de manœuvre à l'instar d'Apple et précise que toutes nouvelles découvertes de brèches entraînera « *le déploiement de nouvelles protections* ».

Malheureusement pour les utilisateurs sous Android, les mises à jour de sécurité ne sont pas toujours déployées par les partenaires de Google. Et si Google parle de la mise à jour majeure effectuée, soit Android 7.1 qui a été rafraîchie en mars, elle ne concerne que 0,4 % des utilisateurs de smartphones Android.

Ensuite, Nous allons voir quelles sont les applications les plus sur chez androïde ou sur Apple. Selon une étude lancée par un certain Zscaler l'ios de apple n'est pas si sûr qu'il n'y parait. Les applications laissent, en effet, fuiter plus de données personnelles que les applis Android.

Toujours selon Zscaler ,les application de Apple laissent échapper plus de données que son confrère androïde. Comme est mentionnées sur ce graphe. 0,5% (sur 26 millions de transactions) pour iOS et 0,3% (sur 20 millions de transactions) pour l'OS de Google comme le révèle un test réalisé à partir du cloud.





Des chiffres qui restent toutefois assez faibles, en outre, la plupart des données en fuite ne sont pas des données pouvant être considérées comme sensibles. Les données en fuite sont classées en trois catégories : métadonnées de l'appareil, informations relatives à la localisation et données personnelles identifiables qui restent minoritaires. La plupart des fuites concernent donc les informations de l'appareil ou la localisation.
Sur iOS, seulement 0,2% des données en fuite sont des données privées comme l'adresse email ou le numéro de téléphone de l'utilisateur contre près de 3% sur Android. Dans les deux cas ça reste faible. 58% des fuites de données sur Android concernent les métadonnées de l'appareil (numéro IMEI, adresse Mac, version de l'OS) et 39,3% sont liées à l'emplacement de l'utilisateur et aux coordonnées GPS.

En revanche, là on ça devient inquiétant, c'est lorsqu'on constate que 50% des développeurs ne testent pas les failles de sécurité de leurs applications. Globalement, 4% des activités faites sur mobile par le biais des applications laissent échapper des données plus ou moins personnelles soit environ 200 000 sur les 45 millions de transactions effectuées. Notez qu'il y a deux ans, la CNIL avait conclu qu'Android exploitait moins vos données personnelles qu'iOS.

Nous allons maintenant voir la faille dite rowhammer publier dans un article de Quatoor en Octobre 2016 en effet un défaut dans le composants DRAM permet d'altérer le contenu de la mémoire d'un smartphone depuis une application classique.

La vulnérabilité Rowhammer exploite un problème de conception des composants de mémoire vive (DRAM). Il permet d'altérer les informations en en lisant d'autres de façon répétée.

Lors d'un accès répété à une cellule mémoire, des fluctuations de voltage peuvent survenir, lesquelles influent sur le contenu des cellules adjacentes. De quoi passer outre tout système de sécurité, afin de prendre le contrôle d'un ordinateur à l'aide d'un simple logiciel.

Une équipe composée de chercheurs de l'Université libre d'Amsterdam et de l'Université de Californie vient de mettre au point l'application Drammer. Cette dernière permet d'exploiter l'effet Rowhammer pour prendre le contrôle de smartphones Android. L'application ne dispose pas de permissions particulières, mais permet toutefois de modifier l'espace mémoire réservé normalement au système.

Source : Silicon.fr

Il y a aussi un article que j'ai pu observer parlant de la faille androïde dite « dirtycow ». Elle est présente depuis 2007 dans le noyau Linux et elle a été récemment corrigée. Reste à diffuser le patch, notamment sur Android.

La faille est colmatée, mais le correctif doit encore être distribué. Pour Android, il faudra attendre le patch du mois de novembre… et espérer que les constructeurs, comme les opérateurs, s'organiseront pour accélérer la diffusion.

Toujours en Octobre 2016 des chercheurs d'une université néerlandaise ont annoncé avoir réussi à trouver une méthode permettant de mettre à mal la plupart des terminaux Android et ce sans qu'aucune faille logicielle ne soit réellement exploitée. Ceci pourrait ainsi ouvrir la porte à un boom des attaques par RAM processeur selon les chercheurs, pourraient permettre d'exécuter à distance sur un terminal mobile une application malveillante et ce sans avoir besoin de privilèges root ou de permission.

Baptisée « Drammer », cette forme d'attaque pourrait causer d'importants dégâts surtout si elle est combinée avec l'exploitation d'autres failles présentes dans le système Android. Malheureusement pour Google, la solution à se problème n'a toujours pas été régler.

J'ai trouvé un de Novembre 2016 prétendant que Google est plus sécurisé qu'Ios. Pour le directeur de la sécurité au sein de l'OS de Google, Adrian Ludwig, ça ne fait aucun doute. La plateforme mobile au petit robot vert est désormais aussi sûre que sa rivale grâce aux efforts déployés par le géant américain et cette tendance devrait encore s'améliorer dans l'avenir.

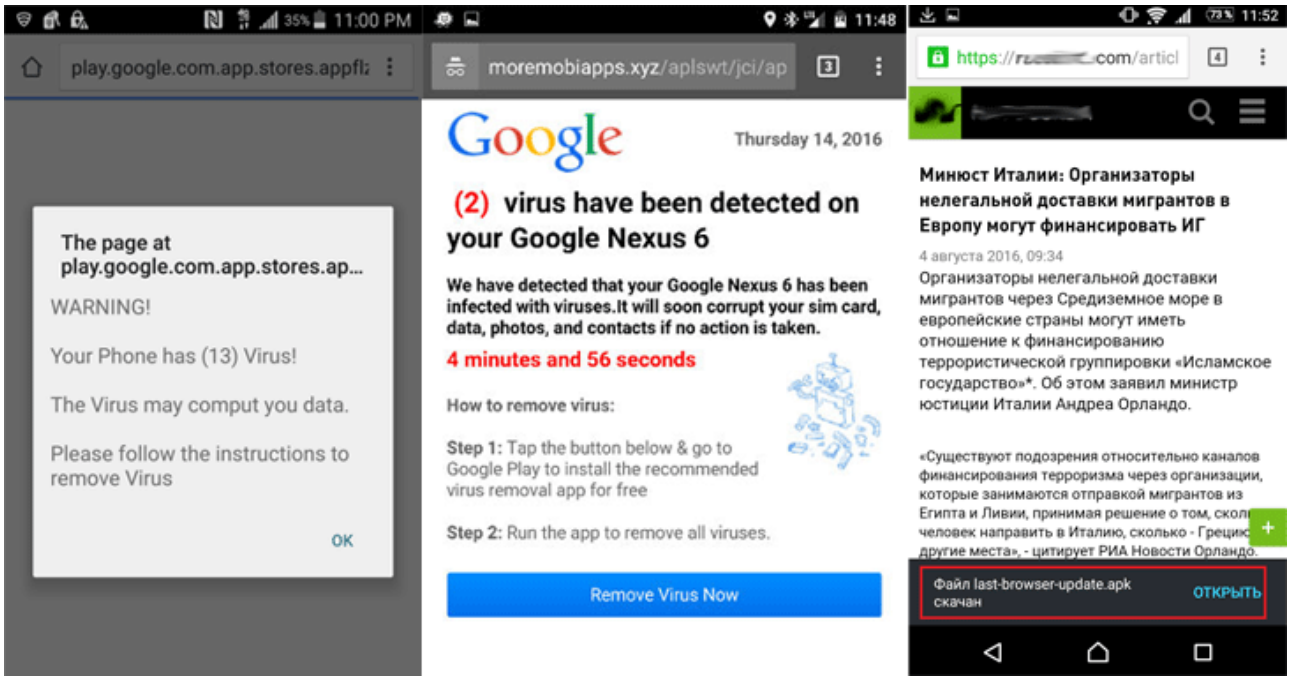
Comme l'a rappelé Adrian Ludwig, afin d'assurer la sécurité de son OS, Google scanne chaque jour pas moins de 400 millions de smartphones et 6 milliards d'applications. D'après lui, seulement 1% des smartphones Android sont infectés par des malwares et Google ne cesse de travailler à réduire ce pourcentage. Tous les mois, le géant américain propose des correctifs de sécurité pour les appareils tournant sous son OS.

Bien évidemment, les constructeurs et opérateurs à jouer vraiment le jeu se comptent sur les doigts d'une main et beaucoup d'efforts sont encore à faire dans ce domaine. Mais d'après Ludwig, la plateforme est déjà sûre et il imagine mal qu'un jour une faille puisse être exploitée en masse au sein d'Android. D'après lui, les utilisateurs sont tellement nombreux qu'il est presque impossible pour un hacker de cibler tout le

monde en même temps. A titre d'exemple, Ludwig cite la faille Stage right découverte en 2015 Il précise qu'en dépit des risques pour la vie privée de l'utilisateur et du fait que pratiquement tous les smartphones du parc étaient vulnérables, celle-ci n'a encore jamais été exploitée

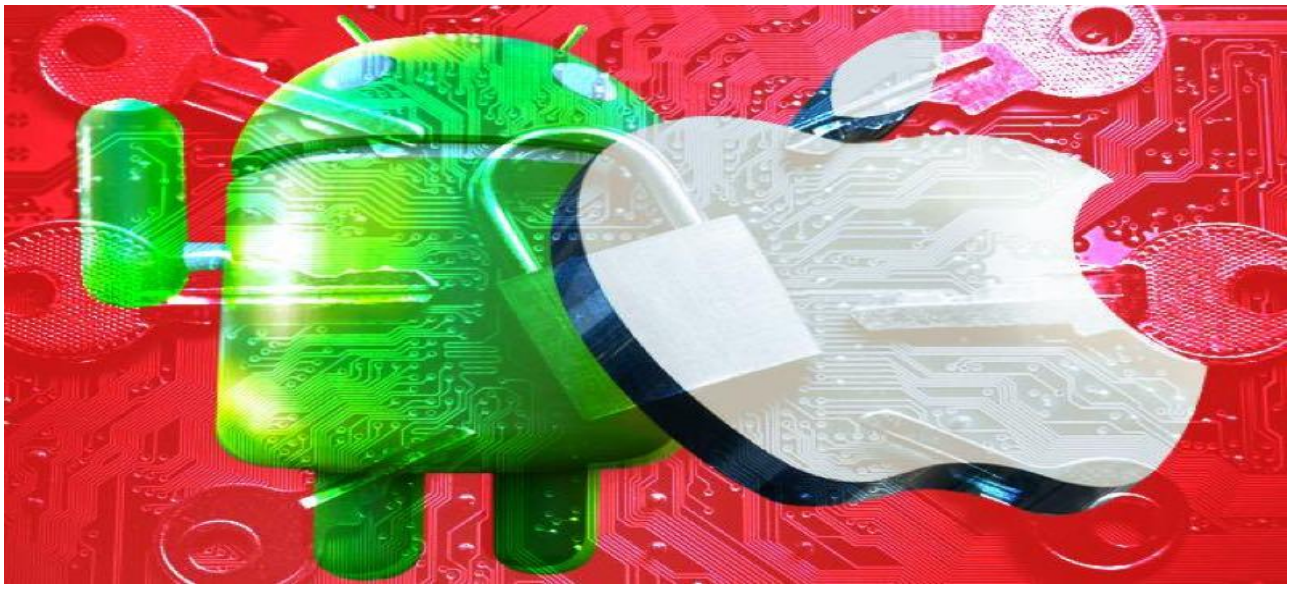
J'ai trouvé un article de the register parlant des failles chez chrome et sur androïde datant de 2016 qui a été découvert par des chercheur de Kaspersky. Elle concerne plus précisément l'installation d'APK. Les chercheurs expliquent le fonctionnement. Les hackers inondent de pub les smartphones infectés et prennent le contrôle du terminal à l'aide de trojans. Cela ne peut fonctionner que si le terminal autorise l'installation d'APK via des sources inconnues. Si cela est votre cas, il est conseillé d'enlever l'option, du moins pour le moment. Le temps que Google ne déploie un correctif de sécurité. Ce n'est pas fini. D'après Kaspersky, il semblerait que 380.000 smartphones Android soient infectés en ce moment. La firme mettra à jour Chrome d'ici le mois prochain afin de palier au problème. Puisque dans ce cas présent, c'est le navigateur internet de la firme qui est la porte d'entrée. Cette année est décidément bien remplie pour le petit robot vert qui semble être rempli de failles en tout genre. Ainsi, on se souvient de Quadrooter, la faille de son noyau Linux. Tandis que de son côté, iOS a été victime également de NSO Group. Rappelons que Google propose de rémunérer la découverte de faille de sécurité concernant ses services. Pour conclure, c'est un excellent moyen de se prémunir des failles de sécurité. Malheureusement cela ne suffit pas toujours.

J'ai trouvé un article toujours datant de novembre 2016,parlant d'une vulnérabilité déjà exploitée sur Chrome, et a permis à des hackers d'installer discrètement des chevaux de Troie sur les smartphones des victimes. Google était déjà au courant de l'existence de cette faille. Elle a été découverte par Mikhail Kuzin et Nikita Buchka, des chercheurs au sein du cabinet de sécurité Kaspersky. Jusqu'à présent, il est question de plus de 300 000 smartphones Android infectés. Concrètement, cette attaque se traduit par l'apparition de publicités vérolées. L'hacker commencera d'abord par faire apparaître une « fausse » publicité qui vous dira que votre appareil est infecté et que vous devez télécharger une application d'urgence. Cette publicité va donc télécharger l'application sans même avoir besoin de votre accord. D'après certaines sources, plusieurs de ces publicités auraient été observées sur des sites d'actualité russes. Il est important de rappeler qu'il faut éviter de télécharger des applications en dehors du Play Store dans le cas d'Android. Google pourrait corriger cette vulnérabilité et ce malware dans la prochaine version de son navigateur prévue semble-t-il, pour début décembre.



Voici un article de novembre 2017 Google a récemment déployé un système de double-authentification sur ses montres connectées Android Wear. Dans une période où les failles et les vulnérabilités sont de plus en plus nombreuses sur les objets high-techs, c'est une nouvelle bienvenue. La double authentification permet une double sécurité sur un appareil. Le système reste simple, en plus votre identifiant habituel, vous recevez un mot de passe valable pour un temps limité sur votre smartphone ou votre ordinateur.
Google est actuellement en train de déployer la nouvelle fonctionnalité. Seule une partie des utilisateurs ont pour l'instant accès à la double authentification. Le reste se fera au fil des semaines à venir.

Selon un article publié en 2017 Android a des années de retard sur iOS sur le terrain de la sécurité.C'est l'un des gros débats qui fait rage entre les fans d'Android et d'iOS. Lequel est le plus sécurisé ? Aujourd'hui, un expert en sécurité livre un avis sans équivoque : Android a des années de retour sur iOS sur ce terrain. En effet selon un cryptographe Matthew Green



ce sont les choix faits par Google qui posent problème en termes de sécurité sur Android. Le géant américain aurait commis l'erreur d'aborder le smartphone comme un PC. Si en terme d'architecture on en est très proche, ce n'est absolument pas le cas en termes d'usages.

En effet, l'expert explique qu'un smartphone n'est pratiquement jamais éteint. Conséquence : les clés de chiffrement sont chargées en permanence dans la mémoire vive et elles n'en sont jamais expulsées. Et Google a choisi un chiffrement complet du disque, ce qui est très mauvais pour la sécurité.

De son côté, Apple a considérablement amélioré iOS depuis iOS 4 sur le terrain de la sécurité. La firme californienne a en effet intégré la fonction « data protection » qui chiffre toutes les données stockées sur le terminal. Mais Apple a choisi de ne pas chiffrer la totalité du disque.

La firme de Cupertino a fait le choix de chiffrer les fichiers eux mêmes. Ils sont donc tous protégés individuellement avec un clé unique par fichier, clé qui est cryptée elle aussi. Ainsi Apple propose un chiffrement sur plusieurs niveaux avec une protection complète, une protection jusqu'à l'authentification et une dernière protection. Il existe même une quatrième et ultime protection pour les applications qui ont besoin de créer de nouveaux fichiers. Matthew Green précise :

En donnant aux développeurs la possibilité de protéger individuellement les différents fichiers, Apple a permis de construire des applications qui peuvent fonctionner pendant que l'appareil est verrouillé, tout en fournissant une protection forte pour les fichiers contenant des données sensibles […] L'approche d'Apple n'est

pas parfait. Ce qu'il l'est, cependant, c'est un résultat évident d'un processus de longues et minutieuses réflexions.

Si Apple est donc encore très en avance, Matthew Green précise que Google est sur la bonne voie avec Android 7.0 Nougat qui introduit un système similaire à celui d'iOS. Mais cela intervient des années après Apple.

Source :01.net

Un article de novembre 2016 sur Super Mario Run qui est sans aucun doute le jeu mobile le plus attendu de cette fin d'année. Hélas pour les utilisateurs Android, Nintendo a décidé de ne sortir son jeu que sur iOS dans un premier temps. Jusqu'à maintenant silencieux, Shigeru Miyamoto, le papa de Mario, a fini par expliquer pourquoi il avait fait ce choix. Il serait question de sécurité.

C'est lors d'une interview donnée au site Mashable que le père de Nintendo, Shigeru Miyamoto a donné de nouvelles informations sur les prochaines aventures du plombier le plus célèbre du monde. Ainsi, il est revenu sur plusieurs éléments et notamment les raisons qui ont poussé Nintendo a lancer Super Mario Run en exclusivité sur iOS dans un premier temps.La sécurité est l'un des raisons pour lesquelles (Nintendo) a décidé de proposer son jeu sur iPhone et iOS en premier.

Selon le papa de Mario, Android manque de stabilité et surtout de sécurité. Et pour jouer à un jeu comme Super Mario Run, il faut que tout ce qui concerne le logiciel soit stable et sécurisé. Ce qui ne serait donc pas le cas d'Android selon Miyamoto.

D'ailleurs, Shigeru Miyamoto a précisé que le logiciel était « un atout de très grande valeur » que Nintendo voulait absolument sauvegarder. C'est pour cela d'ailleurs que l'entreprise aurait fait le choix de ne pas lancer un jeu disponible hors ligne.

Source : phone androide

Article de décembre 2016 sur un Archos pour androïde. L'affaire prend de l'ampleur et est à nouveau embarrassante pour les géants chinois de l'IT. En novembre dernier, la société Kryptonite alertait les utilisateurs de smartphones chinois sous Android vendus principalement aux Etats-Unis. Certains modèles bas de gamme contiendraient un programme chargé d'exfiltrer les données de l'utilisateur vers un serveur situé en Chine. Selon le KryptoWire, un peu plus de 700 millions de téléphones pourraient être affectés par cette faille de sécurité.

La société à l'origine du programme est une entreprise basée à Shangai connue sous le nom de Adups Technology. Elle est en charge du développement du firmware de plusieurs smartphones Android bas de gamme vendue sur les principaux sites de vente en ligne.

KryptoWire explique que le logiciel d'Adups (Adups FOTA) permettait également de détecter la présence de certains mots clefs dans les données collectées, de surveiller l'usage des applications sur le téléphone ou encore d'exécuter du code sur l'appareil en contournant les protections mises en place par Android. Le tout, sans que l'utilisateur n'en soit informé à aucun moment.

La liste des fabricants qui auraient installé ce logiciel ne cesse de s'allonger. Outre le groupe américain Blu (120.000 smartphones concernés), le New York Times relève qu'Adups compte ZTE ou Huawei parmi ses clients. Mais selon Trustlook, d'autres fabricants de renom utiliseraient Adups dont le français Archos ainsi que le chinois Lenovo qui exploite également la marque Moto (ex-Motorola). Le nom des modèles concernés n'a pas été divulguée. Ces deux fabricants n'ont pas encore réagi à ces révélations. Adups de son côté assure que la dernière version de son logiciel ne collecte plus de données personnelles. Interrogé par le New York Times à ce sujet, les porte-paroles d'Adups nient toute collusion avec les services secrets chinois et expliquent que la faute incombe à « une société privée ayant fait une erreur. » Adups explique avoir réalisé ce firmware pour répondre à une commande d'une entreprise chinoise qui souhaitait exploiter ces données afin de connaitre le profil de ses

utilisateurs et améliorer le support technique. Le nom de l'entreprise à l'origine de cette demande n'a pas été révélé. Ce logiciel n'était pas censé sortir du marché chinois, précise également Adups.

Rappelons que Huawei et ZTE ont nié ces allégations. Mais se contentent d'une communication très policée sans vraies informations. Huawei affirme qu'aucun de ses smartphones n'inclut le firmware en question. Et si tel était le cas, il s'agirait de terminaux issus de de fournisseurs non autorisés. Donc la possibilité existe. ZTE dit à peu près la même chose ajoutant qu'il n'a jamais eu l'intention d'utiliser ce firmware.

Qui dit vrai ? Une chose est sûre, cette affaire ne risque d'améliorer la perception des industriels chinois aux Etats-Unis. Rappelons que les accusations d'espionnage ont poussé les autorités à blacklister les équipements réseaux de Huawei du territoire américain...

Article du 3 janvier 2017 sur le correctif de sécurité d'Android pour le smarphone LG.

LG devance Google sur la publication du bulletin des failles corrigéesSouvent, les constructeurs tiers ont du mal à suivre le rythme de Google, notamment dû au fait qu'ils ont des gammes bien plus larges. Aujourd'hui, les choses sont un peu différentes puisque c'est LG qui publie le changelog (le détail des modifications apportées) du correctif de sécurité de janvier avant même que Google ne l'ait publié.

Dénommé SMR-JAN-2017, celui-ci corrige plusieurs failles pouvant permettre une élévation des privilèges (et donc, permettre à une application de s'arroger des droits administrateurs), ainsi qu'une faille critique relative aux appareils équipés de puces MediaTek. Elle permet de dérober les données personnelles via l'application MTKLogger, pouvant transmettre des informations sans le consentement de l'utilisateur.Google pourrait cependant déployer le correctif avant LG

Néanmoins, si c'est LG qui est le premier à publier le bulletin de sécurité (le lien vers la page du site d'Android n'étant d'ailleurs pas active pour le moment), ce pourrait quand même être Google qui sera le premier à déployer le correctif mensuel sur les

Nexus et Pixel. En effet, LG n’a pas encore annoncé de date de déploiement, du fait des différents modèles et opérateurs qui sont concernés sûrement. Il se pourrait donc bien que Google ait donc déjà distribué le correctif de sécurité d’ici là.Bien que LG n’ait donc pas encore commencé le déploiement de ce correctif de sécurité, on ne peut que se réjouir de sa réactivité. En effet, rien que dans les dernières semaines de 2016, on a pu assister à la confirmation qu’un spyware chinois était présent sur des millions de smartphones, ce qui a poussé la marque Blu à arrêter temporairement la commercialisation de ses produits pour retirer le logiciel, et Huawei et ZTE à communiquer dessus.

En conclusion je pense qu’il y a encore beaucoup trop de faille liée à la sécurité sur Google et Android. En bien que Google fasse tous sont possible pour limité la fuite de données personnelle de ses clients beaucoup trop de chercheur ou d’hacker parviennent à contourner ses failles. De plus la sécurité de Ios et beaucoup plus élevé que Android depuis quelque années en effet comme est mentionnées dans les articles Android est une aubaine pour les hacker expérimenter .