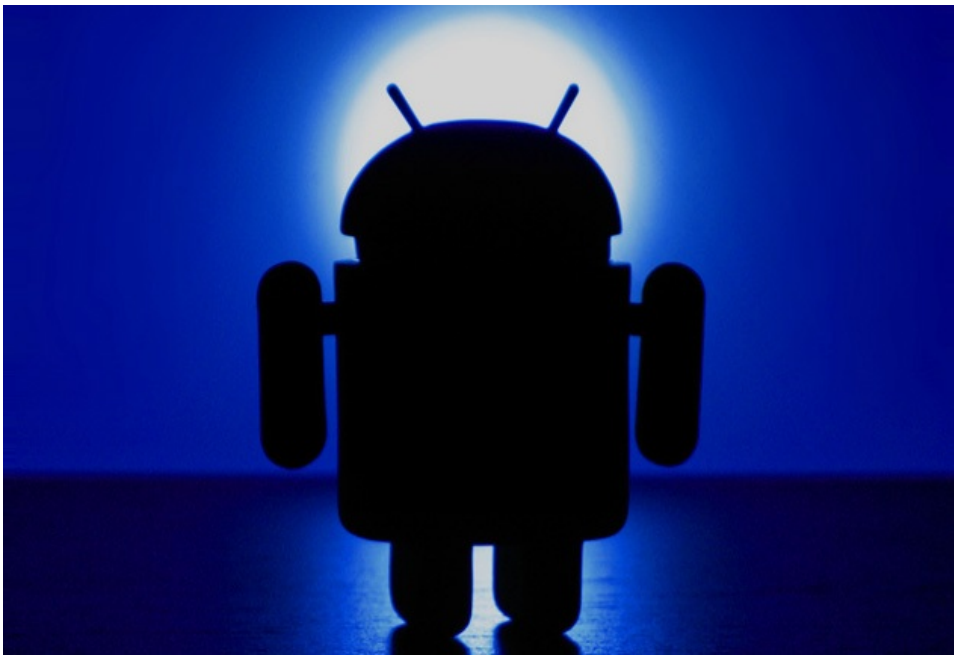
LES ESPIONS RECYCLENT ANDROID

LE 31 JANVIER 2012 ***PIERRE LEIBOVICI***

Android est le système d'exploitation mobile le plus vendu au monde. Mais aussi celui qui comporte le plus de failles de sécurité. Heureusement, l'Agence nationale de sécurité (NSA) américaine vient d'en publier une version améliorée. Et open source. Une louable attention qui soulève des soupçons.



Son nom : SE Android, pour Security Enhanced (Sécurité Renforcée) Android. Sa mission : "*identifier et résoudre les graves failles dans la sécurité d'Android*". Le tout, estampillé NSA, pour **National security agency**, les services de renseignement américains en charge de l'espionnage des télécommunications étrangères, mais également de la sécurisation des télécommunications gouvernementales américaines.

Pour faire simple, SE Android limite les dommages que pourrait entraîner une application malveillante sur les données du téléphone. Car des applications malveillantes, l'Android Market – équivalent de l'App Store d'Apple – en a hébergé beaucoup. Si certaines laissaient peser la menace d'**appels indésirables** et surtaxés, d'autres permettaient d'**activer à distance le micro** du téléphone ou encore de lire le contenu des SMS de l'utilisateur.

Chaque jour, il se vend pas moins de **700 000 téléphones** fonctionnant sous Android dans le monde. Dont on peut penser que quelques-uns sont achetés par les membres des ministères et agences gouvernementales états-uniennes. Soucieuse de remplir sa mission de sécurisation des télécommunications gouvernementales, la NSA a donc publié début janvier la première mouture de SE Android. Une extension qui n'est en fait pas si nouvelle : elle est basée sur SE Linux, un autre module de sécurité développé par la NSA spécialement pour Linux, le célèbre système d'exploitation open source.

Open source, le code de SE Android l'est aussi. Il est donc **accessible** à tous les développeurs amateurs ou professionnels qui veulent "*l'auditer*", comme on dit dans le milieu. De quoi dissiper toute inquiétude quant aux intentions réelles de la NSA. En théorie.

Entrée par la porte de derrière

Car la NSA ne se contente pas de sécuriser les télécommunications du gouvernement américain, elle exerce également une mission de renseignement électromagnétique. Aussi appelé interception des télécommunications. D'ailleurs, son site Internet **donne le ton** :

Nous recueillons l'information que les adversaires des Etats-Unis souhaitent garder secrète.

Vue sous cet angle, la sortie d'un Android amélioré par la NSA a une autre teneur. En témoignent ces commentaires méfiants glanés sur les nombreux sites de fans du système d'exploitation :

Ces "petits mouchards indétectables" pointés du doigt, ce sont les "portes dérobées" (*backdoors* en anglais), un genre de **cheval de Troie** qui permet de prendre à distance le contrôle d'un système informatique. Et donc de récupérer les données d'un utilisateur à son insu. Le problème, comme l'indique un ingénieur de recherche en sécurité informatique qui n'a pas souhaité être cité, c'est *"[qu']il est très facile d'insérer une* backdoor *et de la noyer au milieu de milliers de lignes de code"*.

Des soupçons d'espionnage au moyen de chevaux de Troie, le gouvernement américain en a d'ailleurs connu beaucoup. En janvier 2007, **un scandale éclate** aux Etats-Unis lorsque la NSA admet avoir travaillé avec Microsoft à la sécurisation de Windows Vista. Deux ans plus tard, **la polémique rebondit** pour la même raison à propos de Windows 7, la dernière version du système d'exploitation le plus utilisé au monde. Enfin, en décembre 2010, les doutes sur les intentions des services gouvernementaux américains culminent avec l'affaire Open BSD. Gregory Perry, ingénieur informatique, **révèle** que son ancienne société, NETSEC, a introduit des portes dérobées dans le code d'Open BSD, un système d'exploitation libre comparable à Linux. Et qu'il remplissait-là son contrat avec le *Federal Bureau of Investigation* (FBI), le service de renseignement intérieur des Etats-Unis.

Cela dit, les nombreux experts en informatique interrogés par OWNI font part de leurs doutes sur d'éventuelles portes dérobées dans SE Android. Radoniaina Andriatsimandefitra, thésard à l'Ecole supérieure d'électricité de Rennes :

D'après mon premier examen du code de SE Android, rien n'indique la présence de backdoors mises en place dans le but d'intercepter les données du téléphone. De plus, un code disponible en open source est relu par un bon nombre de personnes ce qui augmente la possibilité de détection avant usage même du produit.
Cependant, même si une telle chose paraît improbable, elle n'est pas à exclure.

Même avis pour **Cédric Blancher**, chercheur au laboratoire en sécurité informatique d'EADS Innovation Works :

> ***L a NSA prendrait un risque énorme à laisser traîner une backdoor dans son code, considérant la probabilité non négligeable que celle-ci soit découverte un jour.***

L'argument open source revient sans cesse : parce que le code informatique de SE Android est vérifiable par quiconque souhaite mettre la main dans le cambouis, il semble peu probable que la NSA y ait inséré une porte dérobée. La densité du code de SE Android pourrait néanmoins réserver des surprises : *"On pourrait y découvrir un cheval de Troie dans seulement dix ans !"*, lance un ingénieur informatique.

Sous-traitance bon marché

En fait, l'intérêt de la NSA à rendre publique et libre d'accès une extension de sécurité pour Android se niche ailleurs. La licence libre est une nouvelle façon pour les services de renseignement américains d'imposer leurs propres standards de sécurité aux téléphones du monde entier. La pilule passe mieux que lors d'une annonce de collaboration NSA/Microsoft.

Mais l'open source a un autre avantage pour la NSA. Selon Radoniaina Andriatsimandefitra :

> ***En agissant de la sorte, elle s'offre la possibilité de déléguer une partie du développement et de la maintenance à des développeurs issus de la communauté libre.***

Un code de sécurité maintenu et enrichi gratuitement par une communauté de fans, que rêver de mieux pour la NSA ? Pas sûr, cela dit, que l'agence de sécurité rende la pareille, d'après Cédric Blancher :

> ***Ils se serviront sans doute de SE Android comme socle à d'autres développement conservés en interne.***

Ces développeurs contribueront peut-être aussi aux avancées du **futur smartphone** destiné aux soldats de l'armée américaine. Qui, comme par hasard, tourne sous Android.

Photos par **Scarigamy (CC-bysa)** et **Solo (CC-byncsa)**

7-CIRCLES
le 31 janvier 2012 - 18:44 • SIGNALER UN ABUS - PERMALINK

Il est peu probable que la NSA ait introduit un «cheval de Troie» dans leur cession d'Android, un «cheval de Troie» a proprement parler est un programme externe au système d'exploitation qui se greffe sur ce dernier et là on parle de l'OS lui même, c'est une question de terminologie. En revanche ils peuvent laisser une faille de sécurité exploitée par une backdor, l'exploiter pendant quelques temps et le jour de sa découverte dire que tout code peut avoir des failles, ce qui est vrai… Mais a nouveau c'est peu probable ils sont plus fins que cela.
Pour info, les gouvernements ont déjà profité de la faille de sécurité IPv6 et VPN…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

7-CIRCLES
le 1 février 2012 - 19:39 • SIGNALER UN ABUS - PERMALINK

désolé pour les fautes d'orthographe, j'ai écrit du smartphone justement :). Remplacer "cession" ligne 1 par version et "backdor" par backdoor.

L'approche de la NSA est à remarquer, contrôler les capacités des applications à manipuler des éléments "sensibles" par le système d'exploitation est plus efficace que garantir la certification au niveau Android Market. Je ne pense pas que Google ait les moyens de faire une revue de code complète en profondeur de toutes les applications, ça couterait trop cher. L'idée de la NSA consiste a intervenir directement au niveau des autorisations applicatives de l'OS.
Avec AndroidSE, la NSA réitère sa contribution à la sécurité open source, après SELinux, qui a été intégré dans les distributions Redhat, Fedora et surement d'autres. Comme avec toute procédure de contrôle de droits applicatifs et utilisateur, il y a une contrainte supplémentaire pour les développeurs d'applications (complexité de fonctionnement accrue). L'utilisation d'AndroidSE risque de poser problème à l'ensemble des développeurs Android. Il ne suffit pas de "faire un don" à la communité open source pour que AndroidSE soit un succès, il faut aussi rallier la communauté des développeurs, c'est le pari de cette nouvelle version d'Android.

Marius C., Ingénieur ISEP promo 2003

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEIBOVICIPIERRE
le 1 février 2012 - 20:00 • SIGNALER UN ABUS - PERMALINK

1/ Effectivement, la question est terminologique, la NSA pourrait avoir volontairement inséré des failles dans le système pour ensuite les exploiter au moyen d'une backdoor. Merci pour cette remarque.

2/ Je suis d'accord avec vous quant à la faible probabilité de failles volontaires dans SE Android. Les experts que j'ai interrogés sont du

même avis. Mais les doutes subsisteront tant que le code n'aura pas été éprouvé et audité par différentes communautés de développeurs.

3/ Google a très certainement les moyens d'auditer le code de toutes les applications de l'Android Market, mais il est clair que cela demanderait un effort considérable. J'avais omis la question de la modification des autorisations applicatives avec SE Android pour des raisons de simplicité, mais vous avez tout à fait raison. Entre autres nouveautés, SE Android fait passer le contrôle d'accès des applications du téléphones d'un système DAC à un système MAC.

4/ Enfin, rallier à la cause de SE Android la communauté des développeurs est évidemment un objectif de la NSA. Cela avait marché pour SE Linux, dont on trouve l'essentiel des ajouts de sécurité dans le noyau Linux depuis plusieurs années. Mais cela n'est pas une raison pour omettre que la NSA voit aussi là un moyen de faire développer son produit "gratis".

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

7-CIRCLES
le 1 février 2012 - 20:37 • SIGNALER UN ABUS - PERMALINK

Merci d'avoir pris le temps de répondre, Owni est très agréable pour sa réactivité.
Par rapport à la conclusion du point 4/: si le projet est sous le contrôle de la communauté open source, ce n'est plus le projet de la NSA, il pourra évoluer sans contrôle de la NSA, à moins que, comme dans le cas d'Android où Google est le seul contributeur, la NSA soit le seul contributeur de SE Android, c'est à vérifier. Je le vois plus comme comme un "don" de "framework", que comme une aubaine à bas prix; la NSA paie plus de 30.000 employés, son budget est conséquent, ils pourraient subventionner sans problème le développement. Sauf que, dans ce cas, je pense que l'adhésion serait moins grande à son "Extension" d'Android (j'ai vérifié, certains modules sont remplacés mais la base reste Android Google). Cette ouverture peut être vue comme une stratégie de succès au près de la communauté Android.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BLACKHATFRANCE
le 4 février 2012 - 10:21 • SIGNALER UN ABUS - PERMALINK

Ce que le monsieur veut te dire, c'est que peut être un développeur aura une idée révolutionnaire pour réformer la sécurité du système actuel, que la NSA pourrait utiliser pour un de leurs futurs tools :/

C'est + de la recherche & développement, de l'investissement dans l'idée :/

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

SEVAN
le 31 janvier 2012 - 23:34 • SIGNALER UN ABUS - PERMALINK

"Android est le système d'exploitation mobile le plus utilisé au monde."

Ça sera probablement bientôt le cas car Android est en forte croissance, mais il me semble que Symbian est toujours devant :

http://www.allaboutsymbian.com/images/news/chartfixed.png

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEIBOVICIPIERRE
le 1 février 2012 - 11:04 • SIGNALER UN ABUS - PERMALINK

"Vendu" a remplacé "utilisé", merci de votre vigilance ! Un récent audit de l'agence Gartner prévoit que Symbian ne devrait plus représenter que 5% des ventes d'OS mobiles en 2012.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

FAND
le 1 février 2012 - 10:10 • SIGNALER UN ABUS - PERMALINK

Article intéressant même si l'information n'est pas très fraiche, néanmoins l'introduction m'a interpellée.

"Android est le système d'exploitation mobile le plus utilisé au monde. Mais aussi celui qui comporte le plus de failles de sécurité."

Vous avez des sources ? Un audit de sécurité, une comparaison, des chiffres qui mettent en relation les différents OS mobile ? Je ne me rappelle pas avoir lu quelque part que Android était plus truffé de diverses failles qu'iOS, que BlackberryOS, Windows Phone ou Bada.
Corrigez-moi si je me trompe, mais la seule actualité qui pourrait étayer cette affirmation se rapporte à l'absence (ou la trop faible) régulation de l'Android Market, mais il y a eu plus d'histoire d'application polémique (cf Juif ou pas juif) que de véritable malware. En revanche je vous le concède, la forte utilisation de ce système risque de donner le même effet que Windows, cette à dire une prolifération de virus pour l'OS le plus utilisé, c'est inévitable.

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEIBOVICIPIERRE
le 1 février 2012 - 10:57 • SIGNALER UN ABUS - PERMALINK

"Information pas très fraîche", cela dit, la première version du code de SE Android a été publiée il y a moins d'un mois. Ci-dessus, vous trouvez plutôt une analyse de l'intérêt nouveau de la NSA pour la sécurisation des mobiles que l'annonce de sortie d'un produit.

L'affirmation selon laquelle Android est l'OS mobile qui comporte le plus de failles de sécurité est, en effet, contestable car elle ne s'appuie pas sur une étude comparative complète recensant toutes les failles de sécurité découvertes pour tous les OS mobiles sur une période donnée. Les seules études connues à ce sujet proviennent d'entreprises de cybersécurité, dont l'objectivité peut-être mise en doute.

Exemple avec l'éditeur de logiciels Kapersky et son édition 2012 "Cyberthreat Forecast" :
"In terms of mobile threats in 2012, Kaspersky Lab expects to see Google Android continue to be the target of choice for the mobile malware market as well as an increase in the numbers of attacks that exploit vulnerabilities."

L'Android Market est effectivement bien moins régulé que les autres marchés d'applications des OS mobiles. Et cela n'a pas donné lieu qu'à des applications "polémiques" comme "Juif ou pas juif" [qu'on a aussi trouvée sur l'AppStore avant que la polémique n'éclate d'ailleurs]. Beaucoup d'applications malicieuses (qui comportent des malwares) ont en effet été détectées. Pour la petite histoire, Symantec affirme avoir décelé la plus grave infection dure à des apps malicieuses pas plus tard qu'hier…
(http://www.mobilemag.com/2012/01/30/biggest-android-malware-infection-ever-says-symantec/)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

REGUEN
le 1 février 2012 - 17:43 • SIGNALER UN ABUS - PERMALINK

Ou simplement Android est le système sur lequel il est le plus rentable de faire peur vu que c'est le plus à même d'accueillir des antivirus envahissant. Ecouter sans discernement leur discours est au mieux dangereux. L'Android Market a un taux de retrait d'applications de plus de 30% quand l'AppStore (avec son si efficace contrôle a priori) retire également A POSTERIORI près d'un quart de son catalogue, si je me rappelle bien.

Bon article, mais si on pouvait éviter les fausses évidences distillées par les éditeurs de sécurité…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LEIBOVICIPIERRE
le 1 février 2012 - 18:22 • SIGNALER UN ABUS - PERMALINK

Il me semble avoir bien indiqué sur le commentaire précédent que les "fausses évidences distillées par les éditeurs de sécurité" étaient à prendre avec des pincettes : "l'objectivité [des entreprises de cybersécurité qui pubient ces études] peut-être mise en doute."

Le business de la cybersécurité reste en tout cas un sujet très intéressant, comme vous le notez. D'autant plus depuis que les mobiles sont considérés comme de nouvelles cibles commerciales par ces fabricants…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

REGUEN
le 1 février 2012 - 18:33 • SIGNALER UN ABUS - PERMALINK

Nuancer le propos dans l'article même aurait été plus utile qu'en commentaire, amha. Enfin bon…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE