NOTA TÉCNICA

Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios"

Autores: Julien Gamba (IMDEA Networks Institute), Mohammed Rashed (UC3M), Abbas Razaghpanah (Stony Brook University, USA), Juan Tapiador (UC3M) Narseo Vallina Rodriguez (IMDEA Networks Institute)

En esta nota técnica se realiza una aproximación al estudio titulado *An Analysis of Pre-installed Android Software* realizado por los grupos IAG del Instituto IMDEA Networks y COSEC de la Universidad Carlos III de Madrid sobre el análisis de aplicaciones (apps) preinstaladas en dispositivos que utilizan el sistema operativo Android.

El estudio será publicado en el próximo 41th IEEE Symposium on Security and Privacy, se puede encontrar https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf Por sus implicaciones con relación a la protección de datos de carácter personal y la privacidad de las personas, es de gran interés para la Agencia Española de Protección de Datos (AEPD) y para todos los posibles agentes involucrados en los tratamientos de datos personales que tienen lugar desde dispositivos móviles con el sistema operativo Android; tanto desde la concepción de productos y servicios digitales como durante todo el ciclo de vida de dichos productos y servicios, con relación a la aplicación de los principios de protección de datos desde el diseño y protección de datos por defecto.

La AEPD contribuye a la divulgación de este estudio al considerarlo de interés general para toda la comunidad implicada en el desarrollo y distribución de estos dispositivos servicios y productos de la economía digital. En definitiva, dicho estudio se espera que contribuya al establecimiento de garantías para la aplicación efectiva del derecho a la protección de datos de los interesados cuyos datos e informaciones personales puedan ser objeto de tratamiento.

Por otra parte, la AEPD espera contribuir con carácter general a la divulgación de trabajos de índole científica relacionados con los tratamientos de datos personales sobre los que se sustenta la economía digital con la finalidad de facilitar la aplicación de los principios generales del RGPD y facilitar la necesaria prevención para garantizar los derechos y libertades de las personas, colaborando con los responsables y profesionales de la tecnología a la implantación de

dichos principios, e impulsando al mismo tiempo la investigación científica en el ámbito de la protección de datos y la privacidad.

Las conclusiones que se establecen en el mismo corresponden únicamente a sus autores y son de carácter científico sin entrar en consideraciones jurídicas y sin perjuicio de posibles acciones que pudieran derivarse de los poderes y el marco de coherencia que establece el RGPD con relación a los posibles tratamientos de datos personales que pudieran existir en este entorno.

ANDROID

La versión *open source* de Android mantenida por Google, conocida como Android Open Source Project (AOSP), es adaptada por fabricantes de dispositivos inteligentes Android y operadores en la industria de telecomunicaciones con el fin de mejorar las prestaciones de sus productos y añadir funcionalidad que proporcione valor añadido y así diferenciarlos en el mercado.

Google ha desarrollado un programa que define los requisitos que el sistema operativo modificado debe cumplir para permanecer compatible con los servicios de Google [1] y manteniendo una lista pública de vendedores certificados [2].

Como resultado, actualmente todos los vendedores de dispositivos Android distribuyen sus propias versiones modificadas de Android en las que también incluyen software (apps) desarrollado por ellos mismos o por terceros, entre los que se encuentran operadores móviles, redes sociales o servicios de publicidad en Internet. Estas son las conocidas aplicaciones preinstaladas sobre las que el usuario medio no tiene los conocimientos para desinstalar o eliminar del dispositivo ni tampoco es posible verificar técnicamente la aplicación de los principios de protección de datos por defecto y desde el diseño.

En principio, Android implementa un sistema de permisos para permitir que el usuario controle directamente el acceso de las apps a recursos de sistema (v.g., GPS) y datos personales (v.g., lista de contactos) [7,8]. Android permite al usuario controlar el acceso a dichos recursos durante la instalación de las apps desde Google Play (o a través de la configuración del sistema una vez instaladas). Sin embargo, las apps preinstaladas se ejecutan con permisos privilegiados de sistema y sin posibilidad, en la mayoría de los casos, de ser desinstaladas del sistema de forma sencilla. Esto les asigna grandes privilegios de acceso a recursos protegidos para el software preinstalado, además de muchas limitaciones para que los usuarios puedan ejercer control sobre el mismo. Estos privilegios se extienden a librerías de terceros embebidas en las apps preinstaladas para fines publicitarios y de monitorización de usuarios.

A priori, se pone de manifiesto la falta de trasparencia en el proceso por el cual una app está preinstalada en un dispositivo específico Android. La prensa generalista ha cuestionado a varios vendedores de dispositivos Android por

exhibir comportamientos abusivos, introducir vulnerabilidades, así como la existencia de acuerdos no trasparentes con grandes empresas de publicidad en Internet [3,4,5] con fabricantes y distribuidores de estos dispositivos, cuestión que en este momento podría estar ratificando este análisis.

La ausencia de un análisis académico y sistemático sobre los riesgos del software preinstalado en dispositivos Android ha motivado la ejecución de este estudio que viene a sentar las bases para la mejora de la calidad de estos productos y servicios que finalmente redundará en la confianza del usuario final en los mismos gracias a las garantías para su derecho a la protección de datos, es decir, protección de datos como factor de confianza del ciudadano en los servicios y productos de la economía digital.

OBJETO Y METODOLOGÍA DE LA INVESTIGACIÓN

Los esfuerzos del equipo de investigación representado por los autores se han centrado principalmente en arrojar luz sobre tres ejes de trabajo:

1. Identificar e investigar los agentes presentes en el software preinstalado en Android y que aprovechan el acceso privilegiado a recursos del sistema para la obtención de datos personales de usuarios a escala;
2. Revelar posibles acuerdos comerciales entre vendedores de dispositivos Android y terceros, incluyendo organizaciones especializadas en la monitorización y rastreo de usuarios y en proporcionar publicidad en Internet;
3. Detectar y analizar vulnerabilidades y otras prácticas opacas o cuestionables.

El estudio realizado cubre más de 82.000 apps preinstaladas en más de 1,700 dispositivos Android fabricados por 214 marcas. Las muestras se han obtenido, con consentimiento informado de los interesados, gracias a la voluntaria y desinteresada colaboración de usuarios Android distribuidos por todo el mundo. A continuación, las apps obtenidas han sido analizadas por el equipo de investigación usando técnicas avanzadas de análisis de software. Más del 91% de las apps analizadas no están publicadas en Google Play, incluyendo software desarrollado por grandes compañías.

Además, se ha analizado un cuarto punto:

4. Trasparencia en la información proporcionada a un usuario en el momento de iniciar su dispositivo móvil con relación a la instalación de apps y recogida de datos.

Para este último punto, se adquirieron seis nuevos dispositivos Android de proveedores populares directamente de un mayorista y se analizó la información proporcionada, así como los formularios de consentimiento y términos de uso mostrados desde el momento del encendido inicial del dispositivo y, por tanto, partiendo de la configuración de base del fabricante.

RESULTADOS

Los principales hallazgos del análisis académico se resumen en los siguientes puntos:

- Aparte de los permisos estándar definidos en Android y bajo control del usuario, se han identificado más de 4.845 permisos propietarios o personalizados por los vendedores ("custom permissions") expuestos por apps preinstaladas. Este tipo de permisos permite que apps publicadas en Google Play puedan eludir el modelo de permisos de Android para acceder a datos del usuario sin requerir su consentimiento a la hora de instalar una nueva app.
- Este esquema de permisos es utilizado por desarrolladores de dispositivos, operadores móviles, servicios de publicidad y monitorización de usuarios, proveedores de contenidos, redes sociales, servicios de comunicación, o consorcios industriales, entre otros muchos actores.
- En cuanto a los tipos de organizaciones responsables del desarrollo las apps preinstaladas se han identificado más de 1.200 compañías, así como la presencia de más de 11.000 librerías de terceros (SDKs) incluidas en la mismas [6]. Una parte significativa de las librerías están relacionadas con servicios de publicidad y monitorización online con fines comerciales. Este análisis revela la existencia de un complejo ecosistema de desarrolladores y acuerdos comerciales entre firmas para la monetización de los servicios móviles.
- Un análisis exhaustivo del comportamiento del 50% de las apps identificadas revela que una fracción importante de las mismas presentan comportamientos potencialmente maliciosos o no deseados. Por ejemplo, algunos servicios de monitorización de usuarios y analítica combinan telemetría de uso del dispositivo con otra información como la geolocalización del usuario, sus contactos, identidades, correos electrónicos e historial de llamadas. En particular, se han encontrado:
    - Muestras de malware conocido como Xynyin, SnowFox, Rootnit, Triada y Ztorg;
    - Troyanos genéricos que permiten la instalación silenciosa de software o toma de control remota del dispositivo (rooteado)
    - Software preinstalado que facilitaría prácticas potencialmente fraudulentas a través del envío de mensajes SMS a números premium, la promoción de apps para captar nuevos usuarios y la publicidad online.
- Con relación a la información suministrada durante la inicialización de un nuevo terminal, de los seis dispositivos Android estudiados, en tres de ellos no se encontró una política de privacidad salvo los términos de uso estándar de Android. Los tres restantes mostraron una política de

privacidad en la que se menciona la recopilación de datos para análisis, pero no se encontró información sobre si estos datos son recopilados por terceros y sobre los fines específicos.

CONCLUSIONES PRELIMINARES

Del estudio se deriva que el modelo *open source* de Android y los actuales modelos de monetización de los dispositivos y aplicaciones móviles habilitan que un gran número de actores puedan monitorizar y obtener información personal de los usuarios a nivel del sistema operativo a través de software preinstalado.

El usuario final desconoce la presencia de estos actores en sus terminales Android y las implicaciones que dichas prácticas tienen sobre la protección de su información personal.

La mera presencia de este software con privilegios de sistema operativo hace difícil su eliminación sin ser un usuario experto. Por otra parte, el número de permisos existentes dista mucho del número de permisos que podrían ser gestionados humanamente y ponen de manifiesto un déficit de transparencia de los aplicativos y del propio sistema operativo Android al mostrar únicamente al usuario una relación de permisos distinta de la real, limitando así su capacidad de decisión para gestionar su información personal y el ejercicio de su derecho a la protección de datos.

De dicho estudio se deducen también complejas relaciones comerciales entre dichos actores, que conforman el ecosistema de monetización en Android y la industria publicitaria online.

Finalmente, y con relación a la aplicación de los principios de protección de datos desde el diseño y protección de datos por defecto establecidos en el Reglamento General de Protección de Datos, es fundamental que desarrolladores y vendedores de dispositivos móviles conozcan está circunstancia y para que apliquen dichos principios en aras de ofrecer las máximas garantías de protección a sus usuarios.

REFERENCIAS BIBLIOGRÁFICAS

[1] Android Compatibility Program.
https://source.android.com/compatibility/overview
[2] Android Certificate Partners.
https://www.android.com/certified/
[3] "Facebook Gave Device Makers Deep Access to Data on Users and Friends". New York Times, 2018.
https://www.nytimes.com/interactive/2018/06/03/technology/facebookdevice-partners-users-friends-data.html.
[4] "Oneplus device root exploit: Backdoor in engineermode app for diagnostics mode". Now Secure. 2017.
https://www.nowsecure.com/blog/2017/11/14/oneplus-device-rootexploit-

backdoor-engineermode-app-diagnostics-mode/
[5] "App Traps: How Cheap Smartphones Siphon User Data in
Developing Countries". Wall Street Journal. 2018.
https://www.wsj.com/articles/app-traps-how-cheap-smartphones-helpthemselves-
to-user-data-1530788404.
[6] Abbas Razagpanah, et. al. ,"Apps, trackers, privacy, and regulators:
A global study of the mobile tracking ecosystem". In Proceedings of NDSS (2018).
[7] K.W. Au, et. al "Pscout: analyzing the android permission specification".
In Proceedings of the 2012 ACM Conference on Computer and Communications
Security (2012), ACM, pp. 217–228.
[8] Adrienne Porter-Felt, et al. "Android permissions demystified". In
Proceedings of the 18th ACM Conference on Computer and Communications
Security (2011), ACM, pp. 627–638