**PRESS RELEASE**
**NOTA DE PRENSA**

Madrid, España, Enero 29, 2020

# AEPD y CNIL otorgan sus premios de protección de datos a un equipo en el que participan investigadores de IMDEA Networks

## El artículo galardonado es “Un análisis del software de Android preinstalado” de Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador y Narseo Vallina-Rodriguez

**El artículo “Un análisis del software de Android preinstalado” de Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador y Narseo Vallina-Rodriguez, ha recibido este mes dos prestigiosos premios: uno de la Agencia Española de Protección de Datos (AEPD) y otro de la CNIL (Autoridad de Protección de Datos de Francia) e Inria. El estudio tiene un enorme impacto social en tanto que revela los problemas de privacidad y seguridad asociados con el software preinstalado en dispositivos Android y su cadena de suministro.**

El 28 de enero, la AEPD eligió el Senado como escenario para otorgar el galardón “Investigación en protección de datos personales Emilio Aced” a este equipo de investigadores procedentes de IMDEA Networks Institute (institución promovida por la Comunidad de Madrid), la Universidad Carlos III de Madrid, el International Computer Science Institute (ICSI) en Berkeley (EEUU) y Stony Brook University de Nueva York (EEUU). La agencia falló el 18 de diciembre de 2019 los ‘Premios de Protección de Datos 2019’, que reconocen los trabajos que promueven en mayor medida el conocimiento, la investigación y la difusión del derecho fundamental a la protección de datos. En la ceremonia de entrega se presentó, asimismo, la campaña de la AEPD “Por todo lo que hay detrás”.

Unos días antes, el 22 de enero, los científicos recibieron el CNIL-Inria Privacy Award por el mismo *paper* en la conferencia internacional CPDP 2020 - Data Protection and Artificial Intelligence celebrada en Bruselas. Julien Gamba presentó en ella este estudio que, además, ha sido aceptado para publicación en el IEEE Symposium on Security and Privacy 2020 (EEUU). Un artículo muy profundo, ya que abarca más de 82.000 *apps* preinstaladas en más de 1.700 dispositivos fabricados por 214 marcas. De la investigación se desprende que muchas de las aplicaciones preinstaladas facilitan el acceso privilegiado a datos y recursos del sistema sin posibilidad de que un usuario medio pueda desinstalarlas.

“Nuestros resultados muestran hasta qué punto la cadena de suministro de dispositivos Android es opaca para los usuarios y poco entendida por los investigadores. La gran mayoría de las aplicaciones preinstaladas no son públicas, lo que hace que sean difíciles de recopilar y analizar: esto es en parte porque han escapado al escrutinio de la comunidad científica durante mucho tiempo. Se nos ocurrió una solución innovadora para reunir un gran conjunto de datos de aplicaciones preinstaladas y detectamos que había una gran cantidad de empresas involucradas en la creación de dispositivos Android, incluidas aquellas con modelos empresariales orientados a datos, que podrían poner la privacidad y la seguridad de los usuarios en riesgo”, explica Gamba, estudiante de doctorado en IMDEA Networks e investigador principal del estudio.

**Principales resultados**

Aparte de los permisos estándar definidos en Android y que pueden ser controlados por el usuario, los investigadores han identificado más de 4.845 permisos propietarios o personalizados por los intervinientes en la fabricación y distribución de los terminales. 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 al instalar una nueva app.

En cuanto a las apps preinstaladas en los dispositivos, se han identificado más de 1.200 desarrolladores tras el software preinstalado, así como la presencia de más de 11.000 librerías de terceros (SDKs) incluidas en la mismas. Una parte significativa de las librerías están relacionadas con servicios de publicidad y monitorización online con fines comerciales. Estas apps preinstaladas se ejecutan con permisos privilegiados y sin posibilidad, en la mayoría de los casos, de ser desinstaladas del sistema. Un análisis exhaustivo del comportamiento del 50% de las apps identificadas revela que muchas de ellas presentan comportamientos potencialmente peligrosos o no deseados.

En relación con la información ofrecida al iniciar un nuevo terminal, se pone de manifiesto un déficit de transparencia de las apps y del propio sistema operativo Android al mostrar al usuario una relación de permisos distinta de la real, limitando su capacidad de decisión para gestionar su información personal.

Según Gamba, “el verdadero desafío es identificar con certeza a las partes interesadas de la cadena de suministro”. Aunque este estudio ha permitido arrojar algo de luz sobre este ecosistema y destapar a muchas partes interesadas de la cadena de suministro, “todavía hay muchas maneras de evitar la detección”. “Actualmente estamos trabajando para mejorar las herramientas de vanguardia con el fin de diseñar formas de descubrir la presencia de todos estos interesados y finalmente pintar una imagen completa de la cadena de suministro de Android”, expone el investigador de IMDEA Networks.

**Fuente(s):** IMDEA Networks Institute

**–END–**

Translated to English:
/news/2020/aepd-and-cnil-award-their-data-protection-priz-team-including-rearchers
Fuente original:
/noticias/2020/aepd-cnil-otorgan-sus-premios-proteccion-datos-un-equipo-que-participan

## Quiénes somos

**IMDEA Networks Institute** es un instituto de **investigación en redes de computación y comunicación**, cuyo equipo multinacional trabaja en ciencia fundamental y tecnología de vanguardia. Como instituto en crecimiento y de habla inglesa, con sede en Madrid, España, IMDEA Networks ofrece una oportunidad única a científicos pioneros que aspiran a desarrollar sus ideas. IMDEA Networks se ha establecido a nivel internacional a la cabeza del **desarrollo de los principios y tecnologías de red del futuro.** Nuestro **equipo** de investigadores de acreditada reputación diseña hoy las redes del mañana.

***Algunas palabras clave que nos definen****: 5G, Big Data, blockchains (cadena de bloques) y registros distribuidos, cloud computing (computación en la nube), redes de distribución de contenidos, analítica de datos, redes energéticamente eficientes, computación en la niebla y en el borde, posicionamiento en interiores, Internet de las Cosas (IoT), aprendizaje de máquinas, redes de ondas milimétricas, computación móvil, economía de red, medición de red, seguridad de red, sistemas en red, protocolos y algoritmos de red, virtualización de red (redes definidas por software – SDN y virtualización de funciones de red – NFV), privacidad, redes sociales, redes submarinas, redes vehiculares, redes inalámbricas y más...*


IMDEA Networks Institute +34 91 481 6210

28918 Leganés (Madrid) Spain mediarelations.networks@imdea.org

Avda. del Mar Mediterráneo, 22 www.networks.imdea.org

Twitter: @IMDEA_Networks | LinkedIn | Facebook | Instagram | Flickr | YouTube