Cómo te vigilan los móviles Android sin que tú lo sepas | Tecnología | EL PAÍS

Un usuario compra un móvil Android nuevo. Da igual la marca. Abre la caja, pulsa el botón de encendido, el móvil se conecta a Internet y, sin hacer nada más, acaba de iniciar la máquina más sofisticada de vigilancia sobre sus rutinas.

No importa ya si se descarga Facebook, activa su cuenta de Google o da todos los permisos a una *app* rara de linterna o antivirus. Antes de cualquier acción, su móvil nuevo ha empezado a compartir detalles de su vida. El *software* que viene preinstalado de serie es el recurso más perfecto de ese móvil para saber su actividad futura: dónde está, qué se descarga, qué mensajes manda, qué archivos de música tiene.

"Las *apps* preinstaladas son la manifestación de otro fenómeno: acuerdos entre actores (fabricantes, comerciantes de datos, operadoras, anunciantes) para dar, en principio, valor añadido pero también para fines comerciales. El elemento de gravedad lo aporta la escala: hablamos de cientos o miles de millones de teléfonos Android", dice Juan Tapiador, profesor de la Universidad Carlos III y uno de los autores, junto a Narseo Vallina-Rodríguez, de IMDEA Networks y el ICSI (Universidad de Berkeley), de la investigación que revela este submundo. Los móviles Android representan más del 80% del mercado global.

El elemento de gravedad lo aporta la escala: hablamos de cientos o miles de millones de teléfonos Android

Juan Tapiador, profesor

El nuevo estudio internacional dirigido por los dos académicos españoles revela la profundidad del abismo. Ninguno de los hallazgos por sí mismo es radicalmente nuevo: es conocido que

los móviles juegan sobre la línea roja de los permisos a la hora de recopilar y compartir datos. La novedad de la función de las *apps* preinstaladas está en su extensión, falta de transparencia y posición privilegiada dentro del móvil: han analizado 1.742 móviles de 214 fabricantes en 130 países.

"Hasta ahora las investigaciones sobre los riesgos de privacidad en móviles se habían centrado en *apps* que están listadas en Google Play o en muestras de *malware*", dice Vallina. Ahora han analizado lo que los móviles traen de serie y parece fuera de control. Debido a la complejidad del ecosistema, las garantías de privacidad de la plataforma Android pueden estar en cuestión.

El artículo, que se publicará oficialmente el 1 de abril y al que EL PAÍS ha tenido acceso, ha sido ya aceptado por una de las principales conferencias de ciberseguridad y privacidad del mundo, el IEEE Symposium on Security & Privacy de California.

Nuestra información personal se manda a una amplia red de destinos, que cambia según el móvil, y algunos son controvertidos: a servidores del fabricante del móvil, a las empresas habitualmente acusadas de espiar en nuestras vidas —Facebook, Google— y a un oscuro mundo que va de corporaciones a *start-ups* que reúnen la información personal de cada cual, la empaquetan con un identificador que se vincula a nuestro nombre y la venden a quien pague bien.

Nuestra información personal se manda a una amplia red de destinos, algunos controvertidos

Nadie antes se había asomado a este abismo para hacer una una investigación de este calado. Los investigadores crearon la *app* Firmware Scanner, que recogía el *software* preinstalado de los usuarios voluntarios que se la descargaron. Para el estudio han analizado más de 1.700 dispositivos, pero disponen de más de ocho mil. El código abierto del sistema operativo

Android permite que cualquier fabricante tenga su versión, junto con sus *apps* preinstaladas. Un móvil puede tener más de 100 *apps* preinstaladas y otros cientos de librerías, que son servicios de terceros incluidos en su código, muchos de ellos especializadas en vigilancia del usuario y publicidad.

En total, un panorama internacional de cientos de miles de aplicaciones con funciones comunes, dudosas, desconocidas, peligrosas o potencialmente delictivas. Esta casi perfecta definición del término caos llevó a los investigadores a más de un año de exploración. El resultado es solo una primera mirada al precipicio de la vigilancia masiva de nuestros móviles Android sin conocimiento del usuario.

Más de un fabricante

Un móvil Android no es producto solo de su fabricante. La afirmación es sorprendente, pero en la cadena de producción participan varias empresas: el chip es de una marca, las actualizaciones del sistema operativo pueden estar subcontratadas, las operadoras de telefonía o grandes comercios que venden móviles añaden su propio *software*. Los actores que participan en la fabricación de un móvil van mucho más allá del nombre que pone en la caja. El control definitivo de todo el *software* que se coloca ahí y que tiene acceso privilegiado a los datos del usuario es indeterminable.

El resultado es un ecosistema descontrolado, donde nadie es capaz hoy de asumir la responsabilidad de lo que ocurra con nuestra información más íntima. Google creó la plataforma a partir de código libre, pero ahora es de todos. Y lo que es de todos no es de nadie: “El mundo Android es muy selvático, es como el *Far West,* especialmente en países con escasa regulación de protección de datos personales”, dice Tapiador.

“No hay ningún tipo de supervisión sobre lo que se importa y comercializa a nivel de *software* (y en gran medida de *hardware*) dentro de la Unión Europea”, dice Vallina. ¿El

resultado?, un caos donde cada versión de nuestros móviles Android conversa con su base desde el primer día, sin interrupción, para contarle qué hacemos. El problema no es solo eso que cuentan de nosotros, sino que el dueño del móvil no controla a qué da permisos.

El jardín cerrado de Google Play

Las empresas que reúnen datos de usuarios para, por ejemplo, crear perfiles para anunciantes ya tienen acceso a los datos del usuario a través de las *apps* normales de Google Play. ¿Qué interés tiene entonces un comerciante de datos en llegar a acuerdos con fabricantes para formar parte del *software* preinstalado?

Imaginemos que nuestros datos están dentro de una casa de varias plantas. Las *apps* de Google Play son ventanas que abrimos y cerramos: a veces dejamos salir los datos y a veces no. Depende de la vigilancia de cada usuario y los permisos que dé. Pero lo que no sabe ese usuario es que los móviles Android vienen con la puerta de la calle abierta de par en par. Da igual lo que haga con las ventanas.

El *software* preinstalado está ahí siempre, nos acompaña a todos lados y en todos los rincones del teléfono, y además no puede borrarse sin *rootear* el dispositivo —romper la protección que proporciona el sistema para hacer con él lo que quieras—, algo que no está al alcance de usuarios corrientes.

Ese usuario no sabe que los móviles Android vienen con la puerta de la calle abierta de par en par

Las *apps* que el usuario descarga de Google Play dan la opción de ver los permisos que pide: ¿permites a tu nuevo juego gratis acceder a tu micrófono? ¿Permites a tu nueva *app* acceder a tu ubicación para tener mejor productividad? Si nos parecen demasiados permisos, podemos borrarla. Las aplicaciones que supervisa Google tienen sus términos de

servicio y deben pedir un permiso explícito para ejecutar acciones.

El usuario, aunque no se fije o no tenga más remedio, es el responsable final de sus decisiones. Está dando permiso a que alguien acceda a sus contactos. Pero las *apps* preinstaladas ya están ahí. Viven por debajo de las *apps* indexadas en la *store*, sin permisos claros o, en muchos casos, con los mismos permisos que el sistema operativo. Es decir, todos. "Google Play es un jardín cerrado con sus policías, pero el 91% de las aplicaciones preinstaladas que hemos visto no están en Google Play", dice Tapiador. Fuera de Google Play nadie vigila con detalle qué acaba dentro de un móvil.

Dos problemas añadidos

El *software* preinstalado tiene otros dos problemas añadidos: uno, están junto al sistema operativo, que tiene acceso a todas las funciones de un móvil, y dos, esas *apps* se pueden actualizar y mutar.

El sistema operativo es el cerebro del móvil. Tiene acceso a todo siempre. No depende de que la *app* esté en marcha o de que el usuario pueda borrarla. Estará siempre ahí y, además, se actualiza. ¿Por qué son importantes las actualizaciones? Aquí va un ejemplo: un fabricante ha dado permiso a una empresa para que ponga en el móvil código para comprobar algo inocuo. Pero ese código puede actualizarse y, dos meses después o cuando la empresa sepa que el usuario vive en tal país y trabaja en tal lugar, mandar una actualización para hacer otras cosas. ¿Cuáles?, las que sea: grabar conversaciones, hacer fotos, mirar mensajes…

Las *apps* preinstaladas son fáciles de actualizar por su creador: si cambia el país o las intenciones de quien ha colocado ahí un sistema de rastreo, se le manda nuevo *software* con nuevas órdenes. El propietario de su móvil no puede impedirlo y ni siquiera se le piden permisos específicos: se

actualiza su sistema operativo.

Esa información a veces es descomunal: características técnicas del teléfono, identificadores únicos, localización, contactos, mensajes o 'e-mails'

Juan Tapiador, profesor

"Algunas de esas *apps* llaman a casa pidiendo instrucciones y mandan información de dónde están instaladas. Esa información a veces es descomunal: informes extensos con características técnicas del teléfono, identificadores únicos, localización, contactos en la agenda, mensajes o *e-mails*. Todo eso lo recoge un servidor y toma una decisión de qué hacer con ese teléfono. Por ejemplo, según el país en el que se encuentre puede decidir instalar una *app* u otra, o promocionar unos anuncios u otros. Lo hemos averiguado analizando el código y comportamiento de las *apps*", dice Tapiador.

El servidor que recibe la información va desde el fabricante, una red social que vende publicidad, un desconocido comerciantes de datos o una oscura dirección IP que no se sabe a quién pertenece.

Un peligro es que esas oscuras *apps* preinstaladas usan los permisos personalizados (*custom permissions*) para exponer informacion a *apps* de la Play Store. Los permisos personalizados son una herramienta que Android ofrece a los desarrolladores de *software* para que las *apps* compartan datos entre ellas. Por ejemplo, si un operador o un servicio de banca tiene varias es admisible que puedan hablar entre ellas y compartirse datos. Pero a veces no es sencillo averiguar qué datos comparten algunas piezas de ese *software*.

Dentro de un móvil nuevo hay por ejemplo una *app* preinstalada que tiene acceso a cámara, contactos, o micrófono. Esa aplicación la ha programado un tipo que se llama Wang Sánchez y lleva un certificado con su clave pública y su firma. Aparentemente es legítima, pero nadie comprueba que el

certificado de Wang Sánchez sea real. Esa aplicación está siempre encendida, coge la localización, activa el micro y conserva las grabaciones. Pero no lo manda a ningún servidor porque la aplicación de Wang Sánchez no tiene permiso para enviar nada por Internet. Lo que sí hace es declarar un permiso personalizado que regula el acceso a esos datos: quien tenga ese permiso podrá obtenerlos.

Un día el propietario de ese móvil va a la Google Play Store y encuentra una *app* deportiva magnífica. ¿Qué permisos oficiales le piden? Solo acceder a Internet, que es perfectamente común entre *apps.* Y también pide el permiso personalizado de la aplicación de Wang Sánchez. Pero no se da cuenta porque estos permisos no se muestran al usuario. Así, lo primero que la *app* deportiva recién llegada dirá a la preinstalada es: "¿Ah, tú vives aquí? Dame acceso al micro y a la cámara". Era aparentemente una *app* sin riesgo, pero las complejidades del sistema de permisos hacen que puedan darse situaciones así.

Los autores de las 'apps'

Los autores de esas *apps* son uno de los grandes misterios de Android. La investigación ha encontrado un panorama similar a los bajos fondos de la *dark web:* hay por ejemplo *apps* firmadas por alguien que dice que es "Google" y no tiene pinta de serlo: "La atribución a los actores se ha hecho casi manualmente en función del vendedor en el que se encuentran, quienes las firman y si tienen por ejemplo alguna cadena que identifique a alguna librería o fabricante conocido (por ejemplo, Ironsource o Facebook)", dice Vallina. El resultado es que hay muchas que mandan información aceptable a fabricantes o grandes empresas, pero muchas otras se esconden detrás de nombres engañosos o falsos.

Esa información se vincula fácilmente a un número de teléfono o datos personas con nombres y apellidos, no números identificativos que anonimizan. El teléfono sabe quién es su propietario. La tarjeta SIM y docenas de *apps* vinculadas al *e-*

mail o a cuentas en redes sociales revelan fácilmente el origen de los datos.

Los Gobiernos y la industria conocen desde hace años este entramado. Las agencias federales de Estados Unidos piden sus móviles con sistemas operativos libres de este *software* preinstalado y adaptados a sus necesidades. ¿Y los ciudadanos?, que se espabilen. Sus datos no son tan secretos como los de un ministerio.

“Ejercer control regulatorio sobre todas las versiones posibles de Android del mercado es casi inmanejable. Requeriría un análisis muy extenso y costoso”, explica Vallina. Ese caos de ahí fuera permite que vivan en nuestros bolsillos unas máquinas sofisticadas de vigilancia masiva.

This content was originally published here.