Fuente:
El Pais

La compañía, que ahora recurre a fabricantes externos, podría asumir la fabricación de sus teléfonos para controlar mejor el ciclo de actualizaciones del sistema operativo

Cada vez se habla más de que Google podría lanzar este año un teléfono de fabricación propia, según han asegurado diferentes fuentes de la compañía a diarios como The Telegraph. No se trataría de un Nexus, fabricado por una empresa con la que se llega a un acuerdo. La idea sería lanzar un terminal diseñado y producido por la propia Google siguiendo los pasos de Apple con el iPhone. Este lanzamiento no es, por ahora, más que un rumor, pero la empresa lograría entre reforzar en ese dispositivo una de las principales debilidades de Android: la seguridad. Pues, entre otras cosas, controlaría mejor el ciclo de actualizaciones del sistema operativo.

El anuncio reciente de que la empresa Una ha lanzado un teléfono con una versión de Android que no deja instalar aplicaciones para salvaguardar la seguridad parece un buen ejemplo de que Google tiene un problema en ese aspecto. Con motivo del informe anual sobre seguridad que la empresa difundió el 16 de junio, en Panda Security daban un dato inquietante: unos 300 millones de usuarios de Android no estarían recibiendo parches de seguridad.

Serían sobre todo los que disponen de teléfonos con versiones del sistema anteriores a la 4.4. abandonados a su suerte. La fragmentación del sistema es una de las claves para que se produzcan estas amenazas. De hecho, inquietan las vulnerabilidades que han afectado a las versiones de Android desarrolladas por algunos fabricantes bastante relevantes. Un buen ejemplo es la que han sufrido recientemente terminales de LG, lo que ha llevado a la empresa coreana a habilitar una web de seguridad.

No es ni mucho menos el único caso. La empresa de seguridad G Data descubrió el año pasado 26 teléfonos con Android que venían con malware instalado de serie. No se trataba sólo de dispositivos de marcas poco conocidas, en la lista también aparecían teléfonos de empresas tan conocidas como Huawei, Lenovo o Xiaomi.

Para blindar la seguridad de Android, Google ha lanzado campañas para recompensar a los que logren encontrar vulnerabilidades en el sistema operativo. Además la nueva versión del sistema hace hincapié en la seguridad. Pero eso no parece suficiente para frenar los riesgos que pueden afectar a los usuarios.

El hecho de que Android sea un sistema más abierto que su gran rival, iOS de Apple, hace que sea mucho más sencillo que el usuario lo adapte a sus gustos, pero también es más fácil atacar su seguridad. Estos ataques pueden ir desde espiar a alguien descargando una aplicación en la propia tienda de Google hasta el robo de datos bancarios mediante un troyano.

Es cierto que servicios como Myspy permiten monitorizar la información de los iPhone, pero el hecho de que iOS sea una plataforma cerrada, una de los aspectos más polémicos que defendió Steve Jobs en su día, ha terminado siendo una ventaja en lo que a seguridad se refiere. De hecho, para que un dispositivo móvil de Apple llegue a ser tan vulnerable como un dispositivo Android es necesario alterar el sistema mediante Jailbreak.

Sólo así pueden instalarse aplicaciones fuera de la App Store que no han pasado por el filtro de Apple. Pero instalar una aplicación en Android saltándose los controles de Google en la Play Store es mucho más sencillo: basta con activar en el propio sistema la opción de instalar aplicaciones no firmadas. De hecho, empresas como Amazon invitan al usuario a que active esa función para poder instalar en cualquier teléfono su propia tienda de aplicaciones.

Existe un buen número de tiendas de apps para Android en las que se pueden encontrar aplicaciones que han sido rechazadas por Google. Muchos usuarios acuden a estas tiendas, o descargan aplicaciones sin firmar desde páginas web, sin conocer exactamente los riesgos a los que se exponen. Las aplicaciones que se distribuyen sin permiso de sus creadores pueden estar condimentadas con toda clase de amenazas.

Un caso que ilustró perfectamente este hecho fue el experimento que realizó el desarrollador Georgie Casey, que modificó una versión de la aplicación de teclado SwiftKey para que esta enviase a un servidor toda la información que se introducía con ella en el teléfono. Lo que incluye desde contraseñas a datos de cuentas bancarias.

Google podría acabar de un plumazo con el problema impidiendo que se instalen aplicaciones sin usar la Play Store y supervisar con mayor exhaustividad las que se venden en su tienda, aunque eso probablemente desataría el enfado de algunos usuarios y daría alas a que se intensifique el desarrollo de versiones alternativas de Android, como Cyanogen, un escenario que incluso podría poner en jaque el control del sistema por parte de Google.

Disponible en:
http://tecnologia.elpais.com/tecnologia/2016/06/29/actualidad/1467189614_484006.html#?ref=rss&format=simple&
[1]

Links
[1]
http://tecnologia.elpais.com/tecnologia/2016/06/29/actualidad/1467189614_484006.html#?ref=rss&format=sim