

BadNews, el malware para Android que podría haber infectado 9 millones de terminales

El ecosistema Android vuelve a estar amenazado por la actividad de una campaña de malware que, en esta ocasión, combina una cuantiosa variedad de programas para infectar smartphones **a través descargas legítimas desde la tienda Google Play.**



La presencia de **BadNews**, que así se llama el ataque en cuestión, ya ha sido rastreada **en al menos 32 aplicaciones** como juegos, diccionarios y fondos de escritorio ofrecidos por cuatro cuentas de desarrolladores diferentes, según las indagaciones de [Lookout Mobile Security](#).

Sus autores han sido capaces de sortear los escudos de protección añadiendo una biblioteca de software malicioso en aplicaciones cuya publicación en Google Play ya había sido autorizada con anterioridad.

De este modo, conseguían engañar a los usuarios que confiaban en que [Bouncer](#), el servicio cloud implementado por Google para bloquear apps, ya habría revisado todos los programas ofrecidos.

Pero, en realidad, el sistema no pueden detectar comportamientos maliciosos porque éstos no han sucedido todavía: la infección de dichas aplicaciones se produce a posteriori. ¿Cómo? La técnica empleada por los ciberdelincuentes no está muy clara, pero se cree que los desarrolladores legítimos fueron engañados para añadir la librería maliciosa a su código base.

Una vez disponibles en la tienda y habiendo sido seleccionadas por los usuarios, las apps que contienen BadNews son capaces de conectarse a un servidor pirata durante horas y **transmitir piezas de información sensible, incluyendo el número de teléfono y el número de serie del dispositivo.** El servidor de comando y control también ordena la **instalación de AlphaSMS, un troyano para el envío de mensajes de texto a servicios Premium.**

Este malware también ha sido diseñado para mostrar noticias falsas con el objetivo de amasar más dinero y promocionar otras aplicaciones.

Los estragos están siendo considerables, sobre todo si se tiene en cuenta que **las aplicaciones afectadas han sido descargadas entre 2 millones y 9 millones de veces.** Los expertos recomiendan a los programadores de aplicaciones móviles que tengan especial cuidado con las librerías de terceros que incluyen en sus proyectos para evitar casos como éste.