Publicado en el 13/02/2014

Panda Security identifica nuevas amenazas de SMS Premium detectadas en Google Play

Panda Security, The Cloud Security Company, ha identificado aplicaciones de Google Play que suscriben a SMS Premium sin permiso. La compañía ha encontrado una nueva amenaza que ha infectado al menos a 300.000 usuarios, aunque esta cifra podría llegar a cuadriplicarse y acercase a 1.200.000 descargas.

"Peinados Fáciles", "Dietas para Reducir el Abdomen", "Rutinas Ejercicios para el Gym" y "Cupcakes Recetas" son, entre otras, aplicaciones maliciosas que se pueden descargar desde Google Play de una manera fácil y accesible.

Si cogemos como ejemplo "Dietas para Reducir el Abdomen", una vez instalada la aplicación, el usuario pasa por una serie de pantallas hasta aceptar los términos y condiciones del servicio, en ese momento suceden dos cosas diferentes: por un lado, el usuario verá una serie de recomendaciones para reducir su abdomen. Y por otro, y sin conocimiento del usuario, la aplicación buscará el número de teléfono del dispositivo, irá a una página web y lo registrará a un servicio de SMS Premium. Pero, ¿cómo se hacen los estafadores con el número de teléfono móvil? El número es "robado" desde una de las aplicaciones para móvil más populares del mundo: WhatsApp. Una vez que abres WhatsApp por primera vez, la aplicación solicita el número de teléfono móvil y lo guarda como parte de los datos para la sincronización de la cuenta.

Según datos de Google Play, esta aplicación tiene entre 50.000 y 100.000 descargas. El resto de aplicaciones mencionadas infectan de la misma manera, por lo que si añadimos las descargas de las cuatro aplicaciones, podemos decir que existen entre 300.000 y 1.200.000 descargas de todas ellas.

"La realidad es que están cobrando mucho dinero por este tipo de servicios premium, si hacemos una estimación conservadora de 20 € pagados por cada terminal, estamos hablando de una estafa enorme que podría estar entre los 6 y los 24 millones de euros", afirma Luis Corrons, Director Técnico de PandaLabs.

¿Cómo proteger los móviles?

Independientemente de la solución de seguridad que se utilice, el usuario debe leer siempre los permisos necesarios que se muestran antes de instalar cada aplicación. Si entre ellos se encuentran los relativos a la conexión a Internet y a permitir a la app que lea los SMS cuando no es realmente necesario, el usuario no debe proceder a la instalación.

Gracias a la solución Panda Mobile Security 1.1 y a su funcionalidad “Auditor de privacidad”, cualquier aplicación con permisos para comportarse de esta forma peligrosa será clasificada dentro de la categoría de “Cuesta dinero” y podrá ser eliminada desde allí.

“No todas las aplicaciones que estén dentro de esta categoría son maliciosas. No obstante, lo cierto es que cualquier aplicación con permisos suficientes como para comportarse de la forma aquí descrita estará en esta clasificación. Eso sí, si ves una aplicación que hayas instalado y no debería tener dichos permisos elimínala directamente“, explica Luis Corrons.

Además, estas aplicaciones maliciosas están diseñadas para atacar a usuarios españoles, puesto que los términos de servicio los ofrece una empresa española y, además, mencionan a compañías telefónicas españolas como Movistar, Yoigo, Orange y Vodafone. Por tanto, la cantidad que se le cobre al usuario dependerá de la compañía que éste tenga.

“Estas aplicaciones podrían permanecer en Google Play durante algún tiempo, ya que de hecho el usuario acepta los términos de servicio, por lo que hasta cierto punto tienen una defensa legal. En cualquier caso, no la suficiente defensa como para evitar que la solución Panda Mobile Security las detecte y elimine”, añade Corrons.

Más información, en el Blog de PandaLabs.

Datos de contacto:
Panda Security

Nota de prensa publicada en:

Categorías: Ciberseguridad