Publicado en el 26/02/2014

Panda Security descubre un nuevo ataque masivo a usuarios de Android mediante publicidad maliciosa en Facebook

Panda Security, The Cloud Security Company, destapa un nuevo ataque masivo a usuarios de Android. En este caso se trata de una campaña muy elaborada que tiene su origen en Facebook, donde los ciberdelincuentes publican anuncios en los que se promocionan diferentes aplicaciones. Panda Security ha contactado ya con Facebook para advertir de esta campaña de publicidad maliciosa de la popular red social.

Aplicaciones que son troyanos

Cuando el usuario navega desde su móvil Android a través de Facebook encontrará en el muro de la red social diferentes mensajes bajo el título de "Publicación sugerida", donde se anuncian utilidades para WhatsApp del tipo: "¿Quieres saber cómo ver las conversaciones de tus amigos en WhatsApp? ¡Descúbrelo aquí! o "¿Quieres ocultar la conexión de WhatsApp? Descárgate ya la App para que la gente no te vea". Si la supuesta víctima pincha sobre alguno de estos anuncios, es redirigida directamente a una falsa versión de Google Play, la tienda de aplicaciones de Android. El usuario, creyendo que se encuentra en el sitio original, se descargará la aplicación de forma gratuita, que, en realidad, se trata de un troyano que le suscribirá a un servicio de SMS Premium sin su conocimiento.

"En esta ocasión los ciberdelincuentes explotan las opciones que Facebook ofrece en base a la publicidad contratada. En este caso se muestra únicamente a visitantes de Facebook españoles que acceden a la red social a través del navegador de su móvil Android. Hemos realizado pruebas con una misma cuenta desde PC, iPad, iPhone y Android y sólo se muestra la publicidad en el caso del sistema operativo de Google", afirma Luis Corrons, Director Técnico de PandaLabs en Panda Security.

El troyano monitoriza todos los mensajes de texto recibidos en el teléfono, y si el remitente es el número del servicio de SMS Premium lo interceptará y eliminará para que no quede rastro del mismo. Sin embargo esta técnica no funciona con la última versión de Android, la 4.4 (KitKat), así que los autores del troyano han ideado una ingeniosa táctica para salvar este obstáculo: al recibir el mensaje, el volumen del teléfono se silencia durante dos segundos y, a continuación, se marca como leído en la bandeja de entrada. La aplicación incluye un contador de SMS, así, cuando llega el primer mensaje del servicio SMS Premium, puede leerlo para obtener el PIN necesario, registrándolo en la página web correspondiente de confirmación para activar el servicio de mensajes de pago.

Un troyano que no quiere competencia

El troyano elimina, además, cualquier mensaje cuyo remitente sea el número 22365, otro número asociado a servicios de SMS Premium de una empresa aparentemente ajena a este ataque. Todo parece apuntar a que se trata de una medida para protegerse ante un determinado competidor: si un troyano tratara de registrarse se impedirá su acceso al mensaje. De este modo, no podrá acceder al PIN y activar el servicio.

Los ciberdelincuentes no sólo utilizan WhatsApp como reclamo, sino que utilizan la misma mecánica con cualquier temática que pueda resultar popular: “Vídeos impactantes”, “Trucos Candy Crush”, “Trucos Angry Birds”, etc.

Con la protección de Panda Mobile Security

Gracias a la solución Panda Mobile Security 1.1 y a su funcionalidad “Auditor de privacidad”, cualquier aplicación con estos perfiles peligrosos será clasificada dentro de la categoría de “Cuesta dinero” y podrá ser eliminada desde allí. No obstante, no todas estas aplicaciones que se encuentran en esta categoría son maliciosas. Sólo aquellas que tengan permisos suficientes como para comportarse de la forma anteriormente descrita integrarán esta clasificación. Si el usuario ha instalado una aplicación y no debería tener dichos permisos, deberá eliminarla directamente.

Más información en el Blog de PandaLabs

Datos de contacto:

Nota de prensa publicada en:

Categorías: Ciberseguridad