Asociación de Internautas

Android objetivo de casi todos los virus para móviles

El 99% de los virus para móviles se han dirigido a Android en 2012, recibiendo casi todos los ataques específicos de malware del año, así como botnets y espionaje móvil. Los programas maliciosos con mayor difusión en los móviles inteligentes son: troyanos SMS, módulos publicitarios y exploits para obtener derechos de root en el dispositivo móvil.

Juan Rico - Nación Red.- El estudio lo ha llevado a cabo Kaspersky Lab, centrándose en el malware de smartphones durante el año 2012.

Por su parte, Google, ha implementado el módulo Google Bouncer, que efectúa el análisis de las aplicaciones de Google Play. Ha sido su forma para intentar evitar esta tendencia de la dirección del ataque hacia su sistema operativo móvil. Aún así, no se ha conseguido cambios evidentes en el promedio de incidentes.

Dos programas maliciosos han sido los más destacables en cuanto a su incidencia. El primero, el programa malicioso Dougalek que provocó una de las grandes fugas de información personal en usuarios de dispositivos móviles.

El segundo, la aplicación Find and Call encontrada en la tienda virtual de Apple y en la de Android. Al descargar e instalar el programa, el usuario veía una solicitud de registro que pedía el correo electrónico y el número de teléfono que, tras ser proporcionados, eran enviados a un servidor remoto que utilizaba los números robados para enviar mensajes spam .

En el apartado de las botnets , destacar que el primer descubrimiento de este tipo fue a principios de año, y más en concreto, la botnet IRC para Android llamada Foncy. Funcionaba junto con el troyano SMS del mismo nombre tomando el control del smartphone y ejecutando cualquier acción que le indicara su creador.

En china, los creadores de virus lograron también crear una botnet con entre 10.000 a 30.000 dispositivos activos. La base era el backdoor RootSmart y los delincuentes informáticos la propagaron al empaquetarla en un programa legítimo y ponerla en el sitio de una popular tienda china extraoficial de aplicaciones para Android.

La infección permitió a los ciberdelincuentes asiáticos convertir en beneficio económico la red creada con los teléfonos infectados. Eligieron para este fin un método popular entre este grupo de delincuentes: enviar SMS de pago a números cortos.

En 2012 se usaron nuevos programas maliciosos para sistemas operativos diferentes a Android en ataques contra blancos específicos. Un buen ejemplo de estos ataques son los lanzados mediante ZitMo y SpitMo (Zeus- y SpyEye-in-the-Mobile), catalogados como troyanos bancarios. Nuevas versiones de ZitMo y SpitMo aparecían con regularidad, tanto para Android como para otros sistemas operativos.

Los escritores de virus siguen usando los mismos métodos de camuflaje que hace dos años. O bien

los disfrazan de certificados de seguridad , o bien los hacen pasar como software para proteger smartphones. En 2012 también aparecieron nuevas versiones de ZitMo para Blackberry.

La cantidad de programas maliciosos se ha incrementado de forma notablemente, como anticipó Kaspersky a principio de año. A parte de todas las amenazas, también merece la pena destacar la creciente cantidad de aplicaciones comerciales de monitorización, que a veces son difíciles de diferenciar de los programas maliciosos.
