Malware móvil se desplaza hacia el fraude por SMS

Como el negocio de malware móvil evoluciona, un número significativo de criminales se han asentado en las aplicaciones que secretamente sus víctimas cobran por los servicios de texto de alta calidad, según muestra un estudio reciente.

Ciberdelincuencia asociado con los virus móviles es una empresa relativamente joven, por lo que los modelos de negocio están todavía en evolución. Sin embargo, en su informe anual sobre el Estado de Mobile Security, Lookout encontró que el fraude SMS, conocido como fraude telefónico, ha crecido en forma sostenida desde julio de 2011.

El nuevo nombre en el fraude se ha convertido en la principal amenaza a nivel mundial en el primer trimestre de este año, lo que representa el 62 por ciento de todas las amenazas basadas en aplicaciones al final de la primera mitad del año. Antes de fraude telefónico, el software espía era la mayor amenaza en los teléfonos móviles.

Desde el descubrimiento del virus de móvil por primera vez en 2004, los delincuentes han estado experimentando con una variedad de modelos de este tipo de negocio.

"Cuando miramos hacia atrás en los últimos 12 meses, hay una indicación muy grande, que ciertos tipos de desarrolladores de malware han encontrado un modelo de negocio que funciona para ellos", dijo Derek Halliday, un investigador de seguridad en Lookout. ***"Y estos indicadores incluyen un exceso de un determinado tipo de familia de malware que nos referimos como el fraude telefónico"***.

Ese modelo de negocio se ha vuelto popular sobre todo en Europa del Este y Rusia, donde la regulación de los servicios

de primera calidad es débil y las tiendas de aplicaciones móviles no son monitoreadas de cerca. De hecho esas regiones, junto con Ucrania y China, constituían la mayoría de las infecciones de nuevos malware , según el informe. En los EE.UU., la tasa de infección fue de menos de 1 por ciento.

En los EE.UU., la mayor amenaza proviene de usuarios que hacen clic en enlaces maliciosos enviados por mensaje de texto o que se encuentran en un sitio web móvil. Los criminales cibernéticos que utilizan este tipo de ataques suelen ser personas que buscan tener información personal que puede ser utilizada en el robo de identidad.

Sobre la base de la actividad de sus propios clientes, Lookout predice cuatro de cada diez usuarios de telefonía móvil de Estados Unidos hará clic en un vínculo inseguro este año.

En un informe separado sobre las amenazas de seguridad en Internet, Symantec encontró que más de tres de cada 10 usuarios de telefonía móvil recibirá un mensaje de texto de un desconocido pidiendo que hagan clic en un vínculo incrustado o marcar un número desconocido.

Symantec también encontró en 2011 que dos tercios de los adultos en los 24 países que realiza un seguimiento en Europa, América del Norte, América del Sur, Asia y el Medio Oriente hace uso de los dispositivos móviles para acceder a la Web. Al mismo tiempo, el número de vulnerabilidades en los dispositivos se ha duplicado desde 2010.

En general, la mayoría de usuarios móviles no son conscientes de los riesgos de seguridad cada vez más con sus dispositivos. Dos de cada tres usuarios no utilizan ningún tipo de seguridad, y el 44% no son conscientes de que la tecnología de protección existe, dijo Symantec.

Delincuencia informática Global del año pasado, incluyendo los dispositivos móviles y los ordenadores personales, los consumidores de costos $ 110 mil millones, mientras que el

número de víctimas alcanzó 556 millones, dijo Symantec.