

## **La siguiente generación de ataques a dispositivos móviles**

El ritmo de innovación en los teléfonos móviles y otros dispositivos inalámbricos inteligentes se ha acelerado enormemente en los últimos años, adicionando características, velocidad y potencia de cómputo. Pero ahora los atacantes están empezando a superar a los chicos buenos en las plataformas móviles, con el desarrollo de novedosos y innovadores ataques, así como métodos para robar datos que rivalizan cualquier cosa vista en el escritorio, dicen los expertos.

Durante años se han realizado terribles predicciones por parte de los expertos de la industria acerca de la inminente oleada de malware para móviles; virus y troyanos que específicamente se centran en teléfonos inteligentes y PDAs, y que generan estragos en los dispositivos móviles. Pero nunca la gran onda de malware para móviles se materializó. Ha habido un virus para móviles aquí y allá, pero para la mayoría de los casos los atacantes han decidido renunciar a ese tipo de ataques, y en su lugar se han centrado en técnicas furtivas que les dan ilimitado - e inadvertido - control del dispositivo.

Troyanos bancarios dirigidos a plataformas como el iPhone y Windows Mobile han aparecido en los últimos meses, así como falsas aplicaciones de banca móvil que son ofrecidas en las tiendas de programas. Estas aplicaciones maliciosas tiene la apariencia de las aplicaciones bancarias legítimas generados por los grandes bancos internacionales, y están diseñadas para capturar las credenciales de los usuarios de banca en línea.

Este particular vector de ataque - la introducción de aplicaciones maliciosas o troyanos en las tiendas de aplicaciones móviles - tiene el potencial de convertirse en un problema muy grave, dicen los investigadores. Tyler Shields, un investigador de seguridad en Veracode que desarrolló un software espía como prueba de concepto para el BlackBerry a principios de este año, dijo que la forma en que están configuradas las tiendas aplicaciones y su relativa falta de garantías, las hacen blancos fáciles para los atacantes que buscan maximizar la eficacia y el alcance de sus aplicaciones maliciosas.

"Las tiendas de la aplicación, cómo todo, tienen cosas buenas y malas. Todo está en un lugar, eso es bueno. Pero lo negativo es que tienes un único punto de distribución en caso de amenazas potenciales", dijo Shields. "Si logro pasar una sola pared, puedo obtener una gran cantidad de

descargas muy rápidamente. ¿Cómo los usuarios pueden distinguir las aplicaciones peligrosas de las seguras en la tienda de aplicaciones?

Como parte de su investigación, Shileds utilizó las APIs de control oficiales proporcionadas por RIM, fabricante del BlackBerry, para desarrollar su aplicación llamada txsBBSPY. También firmó la aplicación utilizando las llaves proporcionados por RIM. Él no trató de colocarla en la tienda BlackBerry App World, simplemente porque los usuarios de BlackBerry pueden cargar aplicaciones desde cualquier lugar, por lo que no era necesario.

Pero es probable que no le hubiera costado trabajo realizarlo, tomando en cuenta los modelos de seguridad empleado por estas tiendas. Las empresas, como RIM, Apple y Google, que mantienen las tiendas de aplicaciones, no garantizan la seguridad o la calidad de ellas, por lo que los usuarios las descargan e instalan bajo su propio riesgo.

"Sin excepción, nadie piensa por un momento sobre lo que sucede tras bastidores en estas tiendas de aplicaciones", dijo Shields. "Los dueños de las tiendas reconocen que tiene que reforzar la seguridad, pero que no quieren frenar el número de aplicaciones que venden. Si lees la letra pequeña, la descarga queda bajo tu propio riesgo."

Shields, y otros investigadores y ejecutivos de seguridad de la industria dicen que el desarrollo de aplicaciones móviles maliciosas puede convertirse en el vector de ataque más popular y lucrativo para los cibercriminales en los próximos años. La convergencia de las poderosas plataformas de computación móvil, tales como el iPhone, Android y BlackBerry con la creciente popularidad de las tiendas de aplicaciones, y los teléfonos móviles como sistemas de pago, hace que estos ataques sean atractivos para los atacantes cualificados.

¿No existe un porcentaje que se aplique a los valiosos recursos que durante varias semanas o meses se pudieran destinar para elaborar un sofisticado esquema de robo de identidad u otro tipo de estafa con la esperanza de embolsar a unos cuantos cientos de víctimas, cuando se puede utilizar ese tiempo para desarrollar una banca móvil maliciosa o una aplicación de compras que podría atraer a decenas de miles de descargas en cuestión de días?

"Hay enfoques muy técnicos, como los ataques del sistema operativo, pero eso es mucho más difícil de hacer", dijo Shields. "Desde el punto de vista del atacante, es demasiado esfuerzo, cuando simplemente se puede dejar

caer en algo en la tienda de aplicaciones. Todo se reduce a los esfuerzos contra la recompensa. El enfoque del troyano spyware será el futuro de la delincuencia. ¿Por qué gastar el tiempo buscando en las cajas, cuando se puede hacer que los usuarios las entreguen por si mismos? Si a esto le añadimos troyanos personalizados y las investigaciones que he hecho, es para dar mucho miedo.

"Y, generalmente los mismos datos personales que se encuentran en un PC ahora están un teléfono móvil. Las personas ya tienen tarjetas de 32 GB y usan sus teléfonos como servidores de medios. Ya son importantes dispositivos de cómputo. Las personas sin muchos conocimientos técnicos se quedan boquiabiertas cuando se enteran de estas cosas. Se dan cuenta de que es posible en las PCs, pero aún no pueden imaginarse cómo lidiar con una situación así, si sus teléfonos son atacados ", dijo Shields.

Es un nuevo día para las amenazas móviles, y los atacantes tienen una gran ventaja.

Fecha: 17/05/2010

Fuente: threadpost.com