Guía de Seguridad para usuarios de smartphones

INTRODUCCIÓN

Con el pasar de los años, los teléfonos móviles han experimentado una intensa evolución que ha llevado a utilizar desde gigantescos equipos hasta los actuales smartphones, dispositivos que poseen características similares a las de una computadora portátil. Estos teléfonos inteligentes permiten hacer cada vez más tareas como conectarse a Internet y compartir en redes sociales, navegar en la web, revisar el correo electrónico, y realizar trámites bancarios en línea, entre otros.

Sumado a lo anterior, los usuarios almacenan cada vez más información personal y sensible que además de estar expuesta al robo físico del dispositivo, puede resultar valiosa para los ciberdelincuentes que buscan obtener ganancias ilícitas utilizando códigos maliciosos u otras amenazas. Pese a que no todos los sistemas operativos del mercado móvil son igual de atacados por códigos maliciosos, existen varias recomendaciones generales que aplican a todo tipo de casos, dispositivos (smartphones, tablets o similares) y usuarios.

En base a todo lo anteriormente mencionado, ¿cuáles son las principales amenazas que afectan a los dispositivos móviles? ¿Qué medidas puede adoptar el usuario para mitigar el impacto de este tipo de ataques y peligros? La presente guía busca responder ambos interrogantes para que las personas puedan hacer un uso seguro y consciente de estos dispositivos móviles.

SISTEMAS OPERATIVOS MÓVILES

Al igual que con las computadoras en donde existen varios sistemas operativos, los teléfonos inteligentes también necesitan de uno. Actualmente existen diversas opciones dentro del mercado entre los que se destacan: Android, Symbian, Windows Mobile, Windows Phone, iOS (iPhone), BlackBerry; entre otros.

Sistema operativo móvil desarrollado por Google lanzado en 2007. Su capacidad de funcionar en distintos dispositivos y la gran cantidad de aplicaciones que están disponibles para éste lo hace una de las opciones más utilizadas y a la vez más atacada por los ciberdelincuentes.

Sistema operativo desarrollado por Research In Motion (RIM) para sus smartphones BlackBerry. Su primera aparición fue en 1999 a través de un dispositivo busca-personas. La principal diferencia de este sistema operativo con respecto a la competencia es que su nicho de mercado y fortaleza es el segmento corporativo.

Creado por Microsoft en el año 2000, este sistema operativo sigue siendo utilizado en algunos teléfonos inteligentes pese a que su desarrollo culminó con la versión 6.5.3 para dar paso Windows Phone, la siguiente apuesta de la empresa.

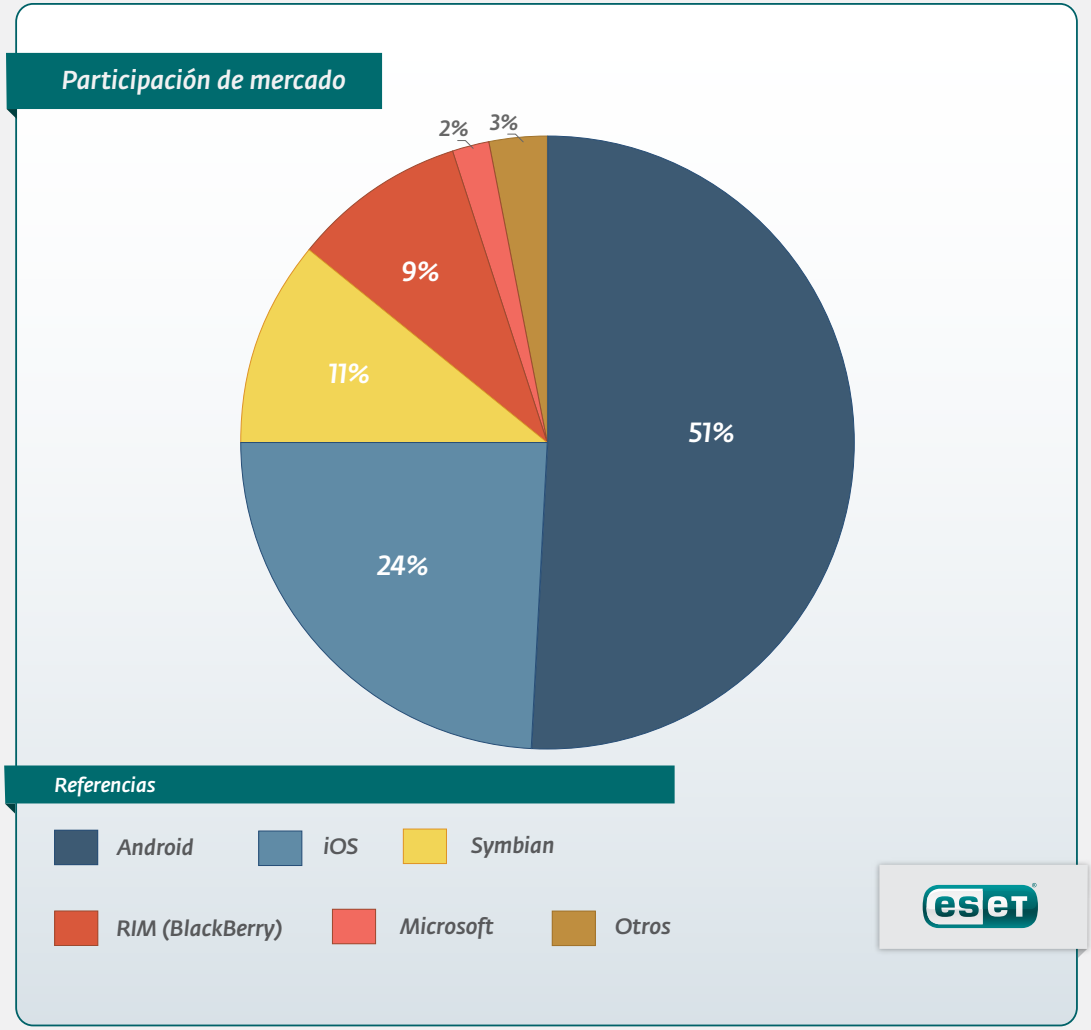
Lanzado por primera vez en la década de los 80 bajo el nombre de EPOC16, Symbian es el sistema operativo móvil más antiguo del mercado. Tras ser adquirido por Nokia en 2008, su popularidad creció entre los usuarios de smartphones. Actualmente es desarrollado y mantenido por Accenture.

Utilizado sólo en dispositivos Apple como iPhone, iPod, iPad y Apple TV, este sistema operativo apareció en el mercado en 2007. En aquella época, logró revolucionar el mundo de los teléfonos inteligentes con interesantes características como una interfaz completamente táctil.

Sucesor de Windows Mobile cuya primera aparición fue en 2011. Con una interfaz gráfica renovada, este sistema operativo es incompatible con las aplicaciones desarrolladas para su antecesor.

PORCENTAJE MUNDIAL DE USO DE CADA SISTEMA OPERATIVO MÓVIL DURANTE EL CUARTO TRIMESTRE 2011

Como puede observarse en el gráfico anterior, el sistema operativo móvil con mayor tasa de participación del mercado es Android. Debido a la masividad y apertura del mismo, es posible observar que la mayoría de los códigos maliciosos mobile que se desarrollan en la actualidad están destinados para esta plataforma y sus usuarios. En el Laboratorio de Análisis de Malware ESET Latinoamérica se han detectado códigos maliciosos para Android capaces de sustraer información sensible de la víctima, rastrear a la misma a través del GPS, convertir el dispositivo móvil en parte de una botnet (red de equipos infectados), entre otras acciones maliciosas.



Fuente: Ventas mundiales de smartphones a usuarios finales por sistemas operativos 4Q11, Gartner.
Disponible en http://www.gartner.com/it/page.jsp?id=1924314.

RIESGOS ASOCIADOS AL USO DE ESTOS DISPOSITIVOS

En la actualidad existen diversos tipos de ataques y/o riesgos que puedan existir para los usuarios de smartphones: malware, phishing, fraudes y robo o pérdida del dispositivo. Cada uno de estos riesgos pueden perjudicar al usuario de diferentes maneras.

Por lo general, el éxito en la propagación de cualquier tipo de amenaza informática (exceptuando la pérdida del teléfono) radica principalmente en las estrategias de Ingeniería Social que el cibercriminal utilice. Para este tipo de dispositivos es común que se usen temáticas específicas para este segmento como troyanos que se expanden con la excusa de ser algún determinado juego mobile, o incluso se han llegado a reemplazar códigos QR legítimos por otros que no lo son, para dirigir al usuario a un sitio que descarga alguna clase de código malicioso.

Una vez que el ciberdelincuente ha escogido una temática, procede a expandir masivamente alguna amenaza.

EL MALWARE Y LOS SMARTPHONES

Aunque hace algunos años la problemática de los códigos maliciosos afectaba predominantemente a equipos estándar como PC de escritorio o portátiles, en la actualidad también representan un riesgo para los usuarios de smartphones.

Actualmente, la mayoría de las familias de códigos maliciosos para Android y otras plataformas tienen como objetivo la suscripción a servicios SMS premium y el control del dispositivo. En menor cantidad, geolocalizar a la víctima a través del GPS o instalar más amenazas en el sistema. A continuación se pueden observar algunos acontecimientos y apariciones de familias de malware para dispositivos móviles:

2004

Symbian/Cabir

WinCE/Brador

Troyanos SMS

2007

Lanzamiento iPhone

iOS/iKee

Troyano Proxy para BlackBerry

2009

Primeros módulos de Zeus (Zitmo) y SpyEye (Spitmo) para mobile

2010

Aparece Zitmo para Symbian y BlackBerry

Lanzamiento de Android

5 familias de malware para Android

2011

Zitmo para Windows Mobile

Spitmo para Symbian, Android y BlackBerry

DroidDream: afectó más de 250.000 dispositivos Android

35 familias de malware para Android

2012

31 familias de malware para Android

Al menos 4 malware para Android distribuidos mediante Google Play

Nuevas variantes de Zitmo para Android y BlackBerry

iOS/Fidall: troyano para iPhone

OTROS RIESGOS EN LOS SMARTPHONES

SPAM

Al envío masivo de correo electrónico basura por parte de terceros, ahora se suman otros canales de comunicación propios de los teléfonos móviles como los mensajes de texto (SMS) y multimedia (MMS) con el fin de distribuir publicidad o en algunos casos propagar códigos maliciosos. Aunque el spam no necesariamente resulta peligroso para la integridad de la información, estadísticas indican que aproximadamente la mitad de los casos están relacionados al fraude, y en los otros representa una molestia o distracción para el usuario.

PHISHING

Técnica que consiste en obtener información personal o financiera del usuario haciéndole creer que quien solicita esos datos es un ente de confianza como un banco o una reconocida empresa. Generalmente el phishing llega como un correo electrónico en el que se asusta a la víctima con amenazas falsas para hacerla ingresar dicha información. En el mundo móvil esta amenaza también se puede propagar por mensaje de texto o incluso llamados telefónicos.

ROBO O EXTRAVÍO FÍSICO DEL DISPOSITIVO

En este tipo de situaciones el mayor problema no es la pérdida del dispositivo en sí y el perjuicio económico que ello acompaña, sino la imposibilidad de recuperar la información no respaldada que se tenga almacenada como también el mal uso que se le pueda hacer a la misma. Frente a un caso como este es necesario que el usuario contacte de inmediato a la empresa prestadora de servicios de telefonía móvil que tenga contratada. También, un software que permita la remoción de información de forma remota podría ser de gran ayuda para proteger la privacidad y confidencialidad de la información.

COMPRAS Y PAGO DE SERVICIOS DESDE UN SMARTPHONE

Una de las funciones más atractivas y utilizadas por los usuarios de estos dispositivos es la capacidad de comprar productos, contratar servicios y realizar transacciones bancarias en línea. Aunque esta característica indudablemente facilita la vida cotidiana de las personas, también puede transformarse en un problema grave si no se adoptan las medidas de seguridad necesarias. Ya se han reportado varios casos de códigos maliciosos móviles que roban información sensible de este tipo.

En este contexto, utilizar solo aplicaciones reconocidas, descargadas desde el sitio oficial del fabricante, y que se utilicen en un dispositivo protegido ante códigos maliciosos son las mejores prácticas para minimizar la probabilidad que se esté realizando un ataque que pueda afectar al usuario.

DESCARGA DE APLICACIONES

Como todo equipo informático de avanzada, es posible añadir a los dispositivos móviles nuevas funcionalidades y características instalando aplicaciones del fabricante y terceros. Sin embargo, esta posibilidad puede resultar muy peligrosa si se instalan aplicaciones desconocidas o no se adoptan los recaudos necesarios.

Gran cantidad de códigos maliciosos provienen a través de esta vía, problema que puede ser minimizado utilizando exclusivamente las tiendas o repositorios de aplicaciones oficiales de cada fabricante.

A continuación se detalla el nombre y la dirección de cada repositorio oficial:

Android: Google Play

https://play.google.com/store?hl=es

Windows Phone:
Windows Phone
Marketplace App World

http://windowsphone.com/es-AR/marketplace

Symbian: Ovi Store

https://store.ovi.com/?lang=es

BlackBerry: BlackBerry

http://appworld.blackberry.com/webstore/?&lang=es

iOS: App Store

Accesible a través de iTunes o directamente desde el smartphone

REDES INALÁMBRICAS Y BLUETOOTH

Las tecnologías de conexión inalámbrica permiten que el usuario pueda conectarse desde casi cualquier lugar a Internet como también compartir archivos con otras personas. Lo que a simple vista puede parecer algo muy útil también puede resultar bastante riesgoso en caso de no adoptar las medidas de seguridad necesarias. En todo momento se debe evitar utilizar conexiones inalámbricas (WiFi) públicas sin protección o clave. En caso de ser imposible, la recomendación es no realizar transacciones bancarias ni utilizar servicios que requieran de información sensible por ese medio. Además, el Bluetooth debe permanecer apagado si no se está utilizando para evitar la propagación de gusanos y el desgaste innecesario de batería.

Para más información, se recomienda consultar la guía de seguridad en redes inalámbricas desarrollada por ESET Latinoamérica: *http://www.eset-la.com/centro-amenazas/redes-inalambricas.*

REDES SOCIALES

Las redes sociales permiten un nivel de interacción impensado antes de su invención, además han logrado un gran impacto y alcance en poco tiempo. De esta forma, sus características hacen que estos servicios sean muy apetecidos por los usuarios. Sin embargo, lo mismo ocurre con los cibercriminales quienes invierten tiempo y recursos en crear códigos maliciosos que se propaguen por esta vía. Por otro lado, una incorrecta configuración de la cuenta de la red social puede exponer información del usuario a terceros, facilitando el robo y suplantación de identidad.

Es recomendable analizar la configuración que ofrecen las redes sociales en estos dispositivos y, si la seguridad no es la óptima, evitar utilizarlas en redes WiFi públicas donde la privacidad de los datos no esté garantizada.

CONSEJOS PARA MITIGAR EL IMPACTO DE AMENAZAS EN DISPOSITIVOS MÓVILES

1

Implementar una solución de seguridad integral

La misma debe detectar proactivamente malware, filtrar mensajes no solicitados, revisar la correcta configuración del teléfono y ofrecer la posibilidad de borrar remotamente toda la información almacenada en caso de robo o extravío del dispositivo.

2

Instalar sólo aplicaciones provenientes de repositorios o tiendas oficiales

Utilizar software legítimo proveniente de fuentes y repositorios oficiales ayuda a minimizar la posibilidad de convertirse en una víctima de códigos maliciosos.

3

Actualizar el sistema operativo y las aplicaciones del smartphone

Al igual que con las computadoras, actualizar tanto el sistema operativo como los programas es necesario para obtener mejoras de seguridad y nuevas funcionalidades.

4

Establecer contraseña de bloqueo

Es recomendable que ésta posea más de cuatro caracteres.

5

Desactivar opciones no utilizadas como Bluetooth o GPS

De este modo, se evita la propagación de códigos maliciosos y el gasto innecesario de la batería.

6

Evitar utilizar redes inalámbricas públicas

De ser imprescindible, no utilizar servicios que requieran de información sensible como transacciones bancarias, compras, etc. Preferentemente se deben utilizar redes 3G.

7

Respaldar la información almacenada

Es recomendable realizar periódicamente copias de seguridad de la información almacenada en el dispositivo. También se debe evitar escribir información sensible como contraseñas en forma de recordatorios o mensajes de texto.

8

Configurar adecuadamente redes sociales

No compartir información de forma pública y limitar cantidad de amigos.

9

No seguir hipervínculos sospechosos de correos, mensajes o sitios web

Tampoco escanear cualquier código QR.

10

Ser cuidadoso con el dispositivo para evitar su robo o pérdida

No dejar el smartphone sin vigilar. Es recomendable utilizar la funcionalidad manos libres en lugares concurridos. Se deben utilizar redes 3G.

CONCLUSIÓN

La era de los dispositivos móviles llegó para quedarse. Las sociedades están acostumbrándose progresivamente y de forma cada vez más masiva a los beneficios que aporta un teléfono inteligente. Los usuarios tienen la posibilidad de estar conectados con la casa y oficina desde un mismo lugar, realizar trámites en línea en circunstancias en las que de otro modo sería imposible, o incorporar nuevas funcionalidades mediante la instalación de diversas aplicaciones.

Todas esas características son las que convirtieron a estos dispositivos móviles en tan deseables para las personas quienes buscan a través de los mismos facilitar aspectos de la vida cotidiana. Sin embargo, si el uso que se le da a los dispositivos móviles es el incorrecto y el usuario no se instruye acerca de las amena¬zas que existen ni adopta las medidas necesarias para resguardar su información, podría convertirse en una nueva víctima de ataques informáticos. En la actualidad, los ciberdelincuentes concentran gran parte de sus recursos en la creación de amenazas para este mercado que crece a pasos agigantados así como también sus riesgos.

Es por este motivo que los usuarios deben tomar conciencia de la información que transportan y utilizan en este tipo de dispositivos, y poner en práctica medidas de precaución para resguardarla con el fin de no sufrir ningún incidente de seguridad que podría ocasionar consecuencias indeseables.