Seguridad informática en el sistema operativo Android y los riesgos presentes en internet

Camelo Pinzón, Javier Camilo
javiercamelo@ingenieros.com
Universidad Piloto de Colombia

Abstract—In recent years the evolution of the technology presents to the innovators and the big companies a race against time, almost to the point that consumers do not reach to know the latest products from the market because they develop new technologies and IT new products, which bring with them new vulnerabilities in relation to information security.

Keywords—Android, security, mobile devices, Trojan.

Resumen—En los últimos años la evolución de la tecnología presenta a los innovadores y a las grandes compañías una carrera contra el tiempo, casi al punto que los consumidores no alcanzan a conocer los últimos productos del mercado porque se presentan nuevas tecnologías y con esto nuevos productos, los cuales traen consigo nuevas vulnerabilidades en relación con la seguridad de la información.

Índice de Términos—Android, botnet, cibercrimen, ciberseguridad, seguridad de la información, sistema operativo, smartphones, tecnología, Troyano, vulnerabilidades.

I. Introducción

El incremento de la tecnología celular y el número de usuarios que acceden a estos productos cada día es mayor, lo que permite que existan riesgos a la hora de interactuar con esta innovación tecnológica, llegando al punto en que los cibercriminales generan cada vez más códigos maliciosos para vulnerar los sistemas operativos.

Android de Google, es considerado como el Sistema Operativo para Smartphones más utilizado, fig.1. Además, en el mercado la tendencia de tasa de uso es cada vez mayor, por lo que permite explicar el incremento y fortalecimiento de diversas amenazas informáticas que afectan este sistema operativo.

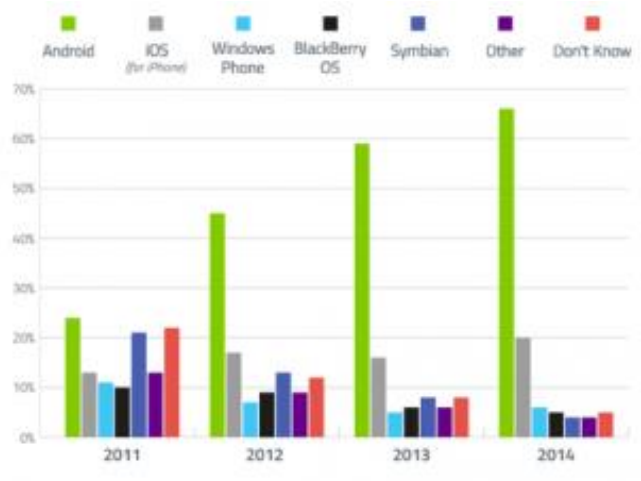

Figura 1 Preferencia de usuarios en sistema operativo para Smartphones [2].

La gráfica refleja el incremento de usuarios en el sistema operativo Android. Imagen: Global Web Index.

Adicionalmente, desde del año 2013 el software malicioso empezó a tener gran relevancia en electrodomésticos que cuentan con conexión a internet.

II. Cibercrimen en Android

Las amenazas informáticas como códigos maliciosos continúan siendo una de las principales causas de robo de información y pérdida de privacidad. La cantidad de detecciones, familias y variantes para detectar códigos maliciosos diseñados para Android, continúan creciendo rápidamente. Este incremento se explica básicamente por la rápida evolución tecnológica que han experimentado los dispositivos móviles y la información que es posible almacenar y procesar con ellos. También se ha notado una evolución técnica de ciertos códigos maliciosos como son los botnets; zombis manipulados por un usuario o atacante y el malware, diseñado para plataformas de 64 bits que también se ha vuelto

más complejo últimamente.

Algunos datos alarmantes sobre ciberseguridad en móviles, concretamente sobre Android, que representa el 80% del mercado (datos recogidos por G Data):

- ✓ 4500 malware nuevos generados diariamente.
- ✓ El Malware para Android subió un 600% en 2014
- ✓ 1,5 millones de incidentes de ciberseguridad relacionados con Android, 30% más que en 2013.

En este sentido, se ha detectado que los cibercriminales concentran su mayor atención en los sistemas operativos móviles que en los sistemas de los equipos como desktops o laptops. Esto se debe a que por medio de los smartphones, los delincuentes pueden obtener bastante información ya sea con estrategias fraudalentas o simplemente con ingeniería social.

III. Principales ataques y amenazas en el sistema operativo Android

Según una encuesta realizada por Kaspersky lab. y la Interpol [3], uno de cada 5 dispositivos basados en sistemas operativos Android es atacado por software malicioso. Los programas maliciosos más populares son los troyanos SMS, en donde se valen de mecanismos para infectar los dispositivos y poder capturar la información de transacciones electrónicas, por lo cual los atacantes pueden hacer transferencias de dinero a cuentas anónimas sin que la persona se dé cuenta que ha sido atacado.

Respecto a Latinoamérica, la encuesta concluyó que los principales países que han reportado un alto número de ataques dirigidos a dispositivos móviles son Brasil, México y Colombia.

Principales amenazas en Latinoamérica:

1. RiskTool: Generalmente es una herramienta adicional de un programa conocida comúnmente como “Crack / Keygen”, cuando se ejecuta por el usuario genera actividades malintencionadas que después pueden ser aprovechadas por los cibercriminales.

2. Trojan-SMS: Actual de la siguiente forma; el usuario descarga el malware en su equipo inadvertidamente, luego el Troyano envía un SMS a un número Premium sin el consentimiento del usuario, el SMS es transportado a través de la red de la compañía de telefonía prestadora del servicio SMS, posteriormente el código malicioso bloquea los mensajes de confirmación para finalmente permitir que el cibercriminal genere ganancias ilegales mediante el descuido de la victima

3. AdWare: Se ejecuta automáticamente y su objetivo es mostrar publicidad, también conocido como pop-up o ventana emergente, cuando la víctima realiza alguna actividad sobre la publicidad se ejecutan funciones maliciosas que anteriormente el cibercriminal ha configurado.

También, existen otras amenazas contra Android algunas comunes otras no, las cuales permiten a los cibercriminales sacar provecho y afectar a muchos usuarios.

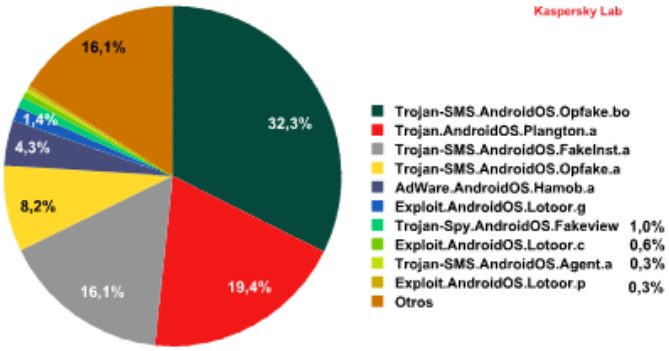

Figura 2 Amenazas más populares contra Android [4].

Existen medidas de seguridad y prevención las cuales ayudan a incrementar la seguridad y evitar riesgos:

- ✓ Instalar aplicaciones y software en

páginas oficiales.
- ✓ Actualización de aplicaciones y antivirus
- ✓ Utilizar contraseñas de usuario alfanuméricas.
- ✓ Cifrar datos y cifrar la memoria de los equipos.
- ✓ Realizar copias de seguridad.
- ✓ Evitar realizar transacciones financieras desde el dispositivo.
- ✓ Activar ubicación online de dispositivo para poder hacer borrado seguro en caso de pérdida o robo de equipo.

IV. Dispositivos electrónicos con Android

La evolución tecnológica se está evidenciando también en los dispositivos no tradicionales que utilizan Android como sistema operativo. En esta línea, se tienen productos como Smart TV, autos, casas inteligentes, sistemas inteligentes de iluminación, cámaras IP, cerradura digital, Google Glass, consolas, relojes, home appliance, entre otros. Lo anterior, plantea la posibilidad de que en un futuro se observen amenazas informáticas para equipos con conexión a internet que no sean directamente tablets o Smartphones y para lo cual los usuarios no tienen presente los riesgos y vulnerabilidades a los cuales estarán expuestos.

Esta probabilidad aumenta si se considera que el sistema operativo de estos aparatos es Android, aspecto que facilita técnicamente el desarrollo de códigos maliciosos y otras amenazas.

V. Preocupación de los usuarios por la privacidad en la nube

La privacidad en Internet no es un tema nuevo, el aumento de usuarios que manifiestan mostrarse preocupados por este tema ha aumentado en los últimos años. Esto empezó básicamente cuando varias infraestructuras informáticas comenzaron a ser migradas a la nube. En esta línea, la masificación del webmail, el almacenamiento en línea, entre otros, provocaron que una gran cantidad de usuarios guarden información personal y corporativa en Internet.

Es posible observar que en todas las regiones del mundo la tendencia indica un crecimiento en el almacenamiento de información en la nube; es decir, el uso de esta tecnología por parte de los usuarios va aumentando conforme pasa el tiempo.

La falta de concientización en Seguridad de la Información, continúa siendo uno de los principales obstáculos al momento de proteger correctamente un sistema informático y la privacidad del usuario. Por lo mismo, saber qué tipos de amenazas puede comprometer la seguridad en Internet, es fundamental. Por ejemplo, un gran número de usuarios con dispositivos móviles y en su mayoría con sistema operativo Android sincronizan la información para poder ser almacenada en la nube, como lo son fotografías, correo, contactos, sin tener presente la confiabilidad de utilizar esta tecnología sabiendo que la información pasara a ser administrada por un tercero. Por esta razón, es muy indispensable ser cuidadosos al momento de compartir información en la nube.

A continuación se encuentran algunas recomendaciones cuando se realizan copias de seguridad en la nube:

- ✓ Cuando se trata de información personal y confidencial, siempre cifrar la información utilizando programas para cifrar y usar contraseñas seguras.
- ✓ No toda la información se puede compartir en la nube, para esto se debe tener claro cuál es la información que puede ser alojada en la nube, por tal motivo se debe clasificar la información.
- ✓ Se puede pagar el servicio de la nube, ayuda a que el operador aplique mejores políticas de seguridad a la información.
- ✓ Contar con un sistema operativo confiable, dado que el problema de inseguridad puede ser originado en el sistema operativo del equipo y no en la infraestructura de la nube.

VI. ¿Será posible la privacidad en internet?

Las amenazas informáticas y los sistemas de protección evolucionan constantemente. Por lo mismo, la privacidad en Internet sí es posible, pero en la medida en que el usuario se concientice y adopte las medidas necesarias para mitigar los riesgos a los cuales está expuesto por convivir con la tecnología y sus avances en el mundo.

Recomendaciones para reducir los riesgos en internet:

- ✓ Utilizar contraseñas con una longitud de más de ocho dígitos, utilizando palabras, números y símbolos.
- ✓ Instalar una solución antivirus con capacidad de detección proactiva, para minimizar el riesgo de infección por parte de códigos maliciosos.
- ✓ No utilizar computadoras públicas para acceder a servicios que requieran de información sensible, como bancos, tiendas en línea, correos o redes sociales.
- ✓ Si se está accediendo desde un dispositivo personal, pero utilizando una conexión Wi-Fi pública, tomar en consideración utilizar páginas cifradas con HTTPS.

VII. Panorama en Colombia

Colombia, es uno de los mercados más atractivos para los cibercriminales en Latinoamérica. Entre los ataques mayormente identificados se encuentra el phishing y ataques de malware, enfocados principalmente en el sector financiero y para lo cual este sector debe destinar grandes cantidades de recursos para afrontar los nuevos incidentes provocados por los criminales.

Actualmente, en el país se están creando esquemas para poder judicializar a las personas que de alguna manera u otra, sacan provecho de toda la tecnología que se está manejando actualmente por los usuarios. Para esto se deben contar con buenas prácticas y sistemas que permitan proteger a las personas de la mejor manera, esto es y representa un reto muy importante en la sociedad.

Amenazas presentes en Colombia:

- ✓ Pérdida o robo de equipos.
- ✓ RiskTool, Trojan, Virus o Malware, Botnets, Spam.
- ✓ Suplantación de identidad o Spoofing.
- ✓ Acceso a datos confidenciales; conversaciones, imágenes, vídeos.
- ✓ Acceso a páginas poco confiables.

VIII. Conclusiones

El desarrollo y la evolución de las tecnologías ayudan a mejorar cada vez nuestra calidad de vida; sin embargo, también trae sus complicaciones al estar expuestos a diferentes riesgos. Entre tanto no se haga un buen uso de la información y se lleve un manejo adecuado, no será posible contar con una buena práctica en seguridad informática.

Como principal medida para proteger la información se debe empezar por las redes sociales, limitando permisos y datos personales. También, hay que proteger los celulares que cuentan con conexión a internet, revisando los permisos que se manejan en estos y que las aplicaciones que se descargan sean de una fuente segura y confiable.

En equipos portátiles se debe asegurar antivirus y sus respectivas actualizaciones periódicas. Además, es posible vincular a toda esta información una buena alternativa como lo es cifrar datos, esto ayuda a que no todos los usuarios puedan tener acceso a esta información cifrada.

Todos los usuarios deben tener conciencia de la seguridad informática y empezar a demandar seguridad en sus datos personales y velar siempre por tener confidencialidad en su vida personal.

El robo de identidad y todo tipo de delitos atizando las tecnologías, se ha convertido en una dura realidad. Para evitar ser una víctima, es necesario proteger cuidadosamente la información personal, supervisar las cuentas y el historial financiero, y actuar rápidamente ante cualquier

indicio de uso indebido de su identidad.

Pero sobre todo es necesario concientizarse de los riesgos e instruirse en prácticas prudentes. Muchas son las razones lógicas, pero una de las que más preocupa, es la seguridad de los menores y que desde luego aprendan también a hacer un uso responsable tanto de teléfonos móviles, como de tabletas como de cualquiera otra de las tecnologías de comunicación que cada vez a una edad más temprana comienzan a utilizar.

Por último, teniendo en cuenta las tendencias tecnológicas, es necesario preparar y asegurar que el uso de internet sea seguro. **En una primera instancia, es la propia persona quien decide qué información publicar y cuál no**, por lo tanto, también puede aumentar o disminuir el nivel de su privacidad en Internet. Adicionalmente, el mejor consejo es el uso de un software actualizado, disponer de un buen antivirus y no visitar portales webs de poca reputación.

REFERENCIAS

[1] Damián García (2014, Junio). Las estadísticas de la plataforma Android abanderan el comienzo de un interesante Google I/O 2014 (Online), disponible en: http://www.xatakandroid.com/mercado/las-estadisticas-de-la-plataforma-android-abanderan-el-comienzo-de-un-interesante-google-i-o-2014

[2] Salvador Vega. (2014, Junio). Apple en problemas: Dos tercios de los usuarios móviles prefieren Android (Online), disponible en: http://www.merca20.com/apple-en-problemas-dos-tercios-de-los-usuarios-moviles-prefieren-android/?pgnc=1

[3] Informe Kaspersky Lab e INTERPOL. (2014, Octubre). 1 de cada 5 usuarios de Android experimenta ciberataques (Online), disponible en: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/informe-kaspersky-lab-e-interpol-1-de-cada-5-?ClickID=ans0popknv9s95ato0rryoavwkryl9rassvs

[4] La Tercera. (2014, Octubre). ¿Sabes qué información de tu smartphone está disponible en la nube? (Online), disponible en: http://www.latercera.com/noticia/tendencias/2014/10/659-602449-9-sabes-que-informacion-de-tu-smartphone-esta-disponible-en-la-nube.shtml

[5] Denís Máslennikov. (2013, Mayo). Evolución de los programas maliciosos para dispositivos móviles Parte 6 (Online), disponible en: http://www.viruslist.com/sp/analysis?pubid=207271207

[6] Patricia Cravero. (2013, Noviembre). La privacidad en Internet, preocupación y desafío para 2014 (Online), disponible en: http://www.lavoz.com.ar/ciudadanos/la-privacidad-en-internet-preocupacion-y-desafio-para-2014

[7] André Goujon. (2013, Noviembre). Tendencias 2014: la privacidad en Internet sí es posible, pero… (Online), disponible en: http://www.welivesecurity.com/la-es/2013/11/27/tendencias-2014-privacidad-internet-posible-pero-primera-parte/

[8] André Goujon. (2013, Agosto). México y Perú son los países de Latinoamérica más afectados por malware de 64 bits (Online), disponible en: http://blogs.eset-la.com/laboratorio/2013/08/07/mexico-peru-paises-latinoamerica-afectados-malware-64-bits/

[9] Mauleón Ocampo. (2013, Agosto). Descubre los peligros del Whatsapp (Online), disponible en: http://www.farodevigo.es/vida-y-estilo/tecnologia/2013/08/09/expertos-alertan-aumento-delitos-internet/858574.html

[10] Gurú Móvil. (2013, Noviembre). Aumenta el riesgo de ataque cibernético para 2014 (Online), disponible en: http://gurumovil.com/2013/11/aumenta-el-riesgo-de-ataque-cibernetico-para-2014/

[11] Mateo Santos. (2013, Diciembre). Las tendencias de seguridad informática para 2014 (Online), disponible en: http://www.enter.co/especiales/enterprise/las-tendencias-de-seguridad-informatica-para-el-2014/

[12] Visionarios Tecnasa. (2013, Diciembre). 8 Tendencias de seguridad informática para el 2014 (Online), disponible en: http://www.visionariostecnasa.com/lo-que-debes-saber/8-tendencias-de-seguridad-informatica-para-el-2014#.UvMBa6OHeZQ

[13] Redacción IT Manager. (2013, Febrero). Amenazas Informáticas. Seguridad, el Reto (Online), disponible en: http://www.gerente.com/detarticulo.php?CodArticl=758

[14] Fernando Ariza. (2012, Diciembre). Cinco predicciones de seguridad informática para el 2013 (Online), disponible en: http://www.portafolio.co/negocios/cinco-predicciones-seguridad-informatica-el-2013

[15] Colprensa y Redacción de El País. (2012, Diciembre). En Colombia las cifras de delitos informáticos van en aumento (Online), disponible en: http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento

Javier Camilo Camelo Pinzón
Ingeniero Electrónico Universidad de San Buenaventura de Bogotá.
Aspirante a Especialista en Seguridad Informática Universidad Piloto de Colombia.
Web Master
Carvajal Tecnología y Servicios.