Android ¿Tentación para los ciberdelincuentes?

Jaraba Herazo, Henry Arley
hjarabah@gmail.com
Universidad Piloto de Colombia

***Resumen*—** El contenido de este documento explica como los ciberdelincuentes pueden perpetuar grandes daños sobre los dispositivos con sistema operativo ANDROID, dentro del entorno personal o en una organización empresarial, aspecto que facilita técnicamente el desarrollo de códigos maliciosos y otras amenazas. Se abordan las VULNERABILIDADES representativas de este sistema operativo en función de las amenazas recurrentes que los hackers efectúan, teniendo en cuenta que la evolución de la tecnología apunta a construir nuevos productos, basados en una plataforma operativa, y por ende, repercute en la confidencialidad, integridad y disponibilidad de los datos que las personas comprometen al interactuar con estos dispositivos, los cuales brindan o facilitan la realización del flujo de trabajo dentro de una empresa o conjunto de empresas.

Índice de Términos*—*AMENAZA-APP-MALWARE- MDM –RIESGO- BYOD-ROOT-ROM.

***Abstract*—** The content of this document explains how cybercriminals can perpetuate great harm on ANDROID OS devices within the personal environment or a business organization, something that technically facilitates the development of malicious code and other threats. The representative VULNERABILITIES of this operating system according to the appellants made threats that hackers are addressed, taking into account the evolution of technology aims to build new products based on an operational platform, and thus affects the confidentiality, integrity and availability of data that people undertake to interact with these devices, which provide or facilitate the completion of the workflow within a company or group of companies.

I. INTRODUCCIÓN

De acuerdo a la fuerte creciente e implementación de dispositivos móviles en el marco de las actividades empresariales, las empresas de seguridad han visto la imperativa necesidad de optar por medidas, técnicas e implementaciones que busquen proteger la información que almacenan los usuarios en un equipo ANDROID.

ANDROID es una moderna plataforma móvil construida para ser totalmente libre. Las APP (aplicaciones) hacen uso de hardware y software avanzado, así como de los datos locales y servidores, expuestos a través de la plataforma para traer innovación y valor a los consumidores. Fue diseñado para *desarrolladores*, por tal motivo, trae un pro y una contra, el *pro* es que los desarrolladores pueden trabajar fácilmente con él y aportar nuevas APP para el consumo general de los usuarios, la *contra* es que un atacante puede aprovechar las VULNERABILIDADES y propagar AMENAZAS por medio de apps con códigos dañinos en el *PLAY STORE (Tienda de aplicaciones de google).*

El uso de dispositivos móviles como herramientas de trabajo ha impulsado a las empresas a instaurar políticas como BYOD *(traiga su propio dispositivo)* y MDM *(Mobile Device Management)*. Esto implica crear un plan de gestión de seguridad en los dispositivos, pero en paralelo, trae problemas que se pueden convertir en grandes dolores de cabeza debido a una inadecuada gestión y carencia de

conocimiento por parte del área de tecnología encargado de monitorear o controlar los equipos en ciertos entornos de red.

Es necesario que las empresas y usuarios conozcan todos los riesgos a los que se encuentran sumergidos mediante el uso cotidiano de los dispositivos ANDROID, manteniendo una concienciación de seguridad.

II. HISTORIA DE MALWARE EN ANDROID

El código malicioso para dispositivos móviles, frecuentemente ha sido visto como un mito debido a las limitaciones de *hardware y software* que poseen. Sin embargo, la historia ha puesto en evidencia que los dispositivos móviles también son VULNERABLES a este tipo de AMENAZA.

En septiembre de 2008, el grupo de investigación de seguridad *Blitz Force Massada,* perteneciente a la Universidad de Ciencia y Tecnología Electrónica de China *(UESTC)* anunció por primera vez distintos ataques sobre el sistema operativo descrito. Se detectaron más de 30 ataques ejecutados, entre los cuales hallaron 11 aplicaciones maliciosas clasificadas en los cuatro módulos siguientes:

- *Android/CallAccepter.A12: Permite que el teléfono acepte todas las llamadas entrantes.*
- *Android/Radiocutter.A13: Apaga la radio, previniendo las llamadas salientes / entrantes.*
- *Android/SilentMutter.A14: Finaliza todas las llamadas.*
- *Android/StiffWeather.A15: Reúne información sensible y la envía al atacante.*

Tras haber analizado estas pruebas de concepto, se pudo establecer que su propósito no era hacer daños, sino de demostrar que este sistema operativo era vulnerable a código malicioso, al igual que cualquier sistema operativo.

Uno de los principales tipos de MALWARE que atacan a los sistemas operativos de manera común, es el *spyware*, que consiste en recopilar la mayor cantidad de información privada de un usuario sin que este se percate. Y por supuesto, el sistema de *Google* no iba a ser la excepción de evitar este tipo de malware, tanto así, que en noviembre de 2009, *Retina -X Studios* anunció al mundo el primer software espía profesional para el sistema operativo ANDROID, llamado *Mobile Spy*, esta aplicación podía controlar dispositivos de manera silenciosa a través del navegador web, llamadas, mensajes de texto, fotos, videos, ubicaciones GPS y direcciones URL.

Un par de meses después, en enero de 2010, el *First Tech Credit Union* y otras entidades financieras como el *Travis Credit Union*, *Royal Bank of Canada, City Bank de Texas,* y *Valley Credit Union* reportaron la existencia de posibles aplicaciones fraudulentas en el *Android Market*. Eran aplicaciones de banca móvil dirigidas a bancos, que tenían el objetivo de recopilar información personal de los clientes por medio del acceso a sus cuentas bancarias, y basados en esta información, realizaban actos fraudulentos.

En los años 2010 y 2011, tras la llegada de los equipos *Motorola Droid y el Google Nexus One*, la plataforma ANDROID se hizo más atractiva para los *criminales cibernéticos,* ya que en esta época hubo un notorio crecimiento del *spyware, phishing* y *rootkits*. Se presentaron grandes vulnerabilidades en el *Android Market*, una de ellas, se producía al descargar e instalar aplicaciones publicadas en la tienda de aplicaciones, tales como *Angry Birds Bonus Levels*, juego que al ser descargado, instalaba de manera silenciosa aplicaciones como *Fake Contact Stealer, Fake Location Tracker* y *Fake Toll Fraud,* que no eran dañinas, pero si generaban incomodidades con sus anuncios. También se resalta el uso de *Backdoor*, *este troyano de puerta trasera* era utilizado para realizar espionaje a los

usuarios que gestionaban un SMS, y su objetivo final era realizar el envío de mensajes SMS a otros celulares sin que el usuario del celular infectado se percatara.

En los últimos años, se han incorporado *Trojanos* con diferentes formas de presentación, una de ellas, es el SMS, se evidencia a través del envío de SMS aleatorios a la lista de contactos almacenados que contiene el móvil contagiado. También se disfraza en los *Wallpapers* que se instalan en el equipo, los cuales exponen una imagen infectada con un tipo de malware, que al instante en que el usuario reinicie el equipo, el malware ejecuta una serie de comandos en el *Shell (Software con interfaz gráfica que ofrece interacción entre usuario y sistema operativo)* obteniendo el control del equipo por vía remota.

A pesar de que este sistema operativo es reciente, ha dejado al descubierto muchas VULNERABILIDADES que se consideraban seguras al momento de ser anunciado su lanzamiento. Junto con estas debilidades, casi que en paralelo, se han efectuado AMENAZAS que han ocasionado un gran impacto ante el gigante de *Google*.

Es clave que en este documento se especifiquen medios y técnicas empleadas en otros sistemas operativos, que han minimizado los RIESGOS e IMPACTOS de sus respectivas plataformas a lo largo de la historia. Basado en estos medios y técnicas, se puede sacar provecho y aplicar estrategias con el fin de aumentar los niveles de seguridad en ANDROID; aunque nunca van a ser del todo seguros, pero al menos brindarán un mejor seguimiento y control para los usuarios de este sistema operativo.

III. ¿CÓMO SERÍA UNA BUENA GESTIÓN DE LA SEGURIDAD A NIVEL EMPRESARIAL?

De acuerdo al notorio incremento de AMENAZAS enfocadas a aprovechar las VULNERABILIDADES presentes en los sistemas ANDROID, es un hecho que los dispositivos con el sistema operativo de *Google* requieren de una óptima gestión basada en buenas prácticas. Dichas prácticas, no se encuentran reguladas bajo un estándar, sin embargo, se pueden ir construyendo de acuerdo a la historia, presente y futuro que va de la mano del avance tecnológico en los sistemas operativos de los móviles. Al seguir unas buenas prácticas, se mitigan los riesgos ante los eventuales ataques de los CIBERDELINCUENTES, quienes con su creatividad y buen conocimiento de las herramientas, devastan los sistemas de seguridad que incorporan los desarrolladores de *Google*.

Para realizar una adecuada gestión de seguridad, es necesario conocer los medios, integrantes y activos que participan bajo el contexto empresarial. Dentro de esta arquitectura, se encuentran los usuarios, equipos, *Apps*, documentos y activos de la empresa. Partiendo de esta información, se empiezan a desarrollar etapas que trabajan de manera cíclica dentro del contexto de la gestión de la seguridad informática, debido a que siempre va a existir un alto nivel de RIESGO.

Imagen 1. Arquitectura de gestión de la seguridad en Android

Fuente: Elaboración propia a partir de los recursos que contempla la política BYOD

A. Primera etapa

Es necesario contar con una visualización de todo el entorno informático móvil, ya que así se pueden clasificar los distintos recursos involucrados, obteniendo la gestión de usuarios, terminales, aplicaciones, documentos y los gastos asociados. A cada recurso identificado se le debe estimar un nivel de seguridad, de acuerdo a su nivel de criticidad.

B. Segunda etapa

Efectuar la integración con servicios de directorio corporativo, por ejemplo, integrar cuentas de acceso, correos electrónicos y diversos mecanismos de comunicación existentes. Lo más complicado e importante de esta integración, es hacerla de manera automática, en donde la configuración sea propagada a todos los equipos ANDROID que estén dentro del entorno de red de la empresa, ya que de esta forma, se evitaría que los usuarios tengan que realizar configuraciones que requieran de un alto grado de conocimiento técnico. Mediante esta integración de servicios de comunicación, se configura el *Wi-fi*, correo electrónico, *VPNs*, *apps* y gestión de certificados. Por último, se realiza la personalización de equipos corporativos.

C. Tercera etapa

Esta etapa va más dirigida a las aplicaciones del sistema operativo que residen en el móvil. Se debe realizar un listado total de las aplicaciones permitidas, negadas y requeridas en la red. Adicionalmente, dependiendo de las aplicaciones halladas en el móvil, deben generarse distribuciones, instalaciones y bloqueos de aplicaciones. Aquí, es donde entra en rigor, una navegación web segura y filtrada, definiendo restricciones en la red, por ejemplo, no entrar a redes sociales como *Facebook*, ni sistemas multimedia como *Youtube;* todo esto para evitar un alto consumo del ancho de banda y el ingreso de virus en la red. Al tener una buena gestión e integración entre la red de la empresa y el dispositivo, es requerido que los documentos compartidos sean protegidos mediante técnicas de cifrado.

D. Cuarta etapa.

Para finalizar una buena gestión, se deben analizar en detalle los periféricos que poseen los móviles, administrar sus puertos, cámaras y medios de almacenamiento. Adicionalmente, toca construir sistemas que localicen un dispositivo ANDROID *sospechoso* dentro de la red, con miras de aplicarle un seguimiento, bloqueo, borrado remoto y selectivo de sus respectivas aplicaciones que contengan código malicioso. Para culminar esta etapa, se recomienda descargar una aplicación MDM del *Play Store*, que en lo posible, permita almacenar eventos y acciones en un motor de reglas, con el propósito de detectar anomalías en el sistema operativo de los dispositivos.

IV. USAR ANDROID CON SEGURIDAD A NIVEL PERSONAL

Con el transcurrir de los días ANDROID se hace más conocido, no sólo a nivel de usuarios comunes, sino también en organizaciones que fomentan a sus empleados el uso de *Smartphone* o *Tablet* para desarrollar actividades empresariales.

Es obvio, que la información de una empresa representa su activo más importante. Y por lo tanto, muchas organizaciones restringen el uso de esta plataforma móvil ANDROID para evitar que ocurran grandes pérdidas. Sin embargo, se pueden poner en práctica una serie de útiles consejos que ahorraran futuros inconvenientes a los usuarios que operen sobre esta plataforma.

A. Primer consejo.

El primer consejo, es crear un *patrón de bloqueo de pantalla mediante un pin, patrón, contraseña* y en los versiones superiores *(Ice Cream Sandwich*,

Jelly Bean y Kit Kat) agregar la opción de desbloqueo facial o por reconocimiento de voz.

B. *Segundo consejo*

Otro consejo fundamental, es instalar una aplicación MDM que permita detectar *Malware* y evitar su ejecución, fortaleciendo la seguridad ante los posibles ataques de virus que se desencadenen. Dentro de las características más relevantes de un MDM, se distinguen la realización de un escaneo para el análisis de seguridad, administración del sistema, *Navegación Web segura* y diversas opciones para realizar un respaldo de datos. También genera un listado de los permisos adquiridos por las apps instaladas dentro del móvil. Una buena sugerencia, seria instalar la APP llamada *TrustGo*, líder en valoración según el ranking que soportan diversas organizaciones dedicadas a la seguridad informática.

Imagen 2. Sistema MGM

Fuente: Elaboración propia a partir de la captura de pantalla de un móvil con sistema operativo Android

C. *Tercer consejo*

Una valiosa capa de seguridad, es instalar aplicaciones que garanticen la *confidencialidad* e *integridad* de los datos que suministran los usuarios al emplear aplicaciones empresariales. Herramientas ideales para lograr esta medida, serian *SecureAuth* y *PhoneFactor*.

D. *Cuarto consejo*

Entre las sugerencias más importantes, se resalta el uso de una APP llamada *Android Device Policy*, la cual se encarga de suministrar una efectiva administración de *acceso* del dispositivo, ya sea en el entorno personal o en el entorno organizacional.

E. *Quinto consejo*

Para el manejo de *mails*, es indispensable manejarlos con mucha precaución y preservar la *disponibilidad* de su información, para lograr esto, es necesario utilizar un gestor de *mails* que opere con diferentes cuentas de correo de manera segura, una aplicación recomendable para la gestión de *mails* sería *TouchDown*.

F. *Sexto consejo*

Algo valioso, es mantener actualizado el sistema operativo ANDROID con las últimas actualizaciones que pública *Google* en el *Play Store*, de esta manera se reducen las VULNERABILIDADES detectadas en el área de calidad de Google. Un concepto muy útil para realizar las actualizaciones, es el que representa el *ROOT* (usuario Administrador con máximos privilegios en ANDROID), con este perfil se puede acceder a administrar las aplicaciones de bajo nivel, por un lado trae beneficios, como lo es instalar aplicaciones que no son posibles con el usuario por defecto, administrar de manera privilegiada los recursos del dispositivo, crear e instalar un *ROM* (Sistema operativo) personalizado con mejoras incorporadas, y lo más atractivo, es que ofrece una fuerte interacción *Hardware/Software* para sacar el máximo provecho del *performance* del dispositivo. Sin embargo, trae grandes peligros, como lo son el débil acceso a los códigos fuentes, inadecuada personalización del sistema operativo, afectación en los componentes electrónicos, perdida de garantía por parte del fabricante, y el más importante, daño

irreversible del *hardware* debido a una mala manipulación.

V. CONCLUSIONES

Ahora que *Google* domina con gran superioridad el segmento móvil a nivel mundial, y que seguramente seguirá abarcándolo durante muchos años, es necesario ir implementando la conciencia de seguridad dentro del uso habitual de los dispositivos que emplean su respectivo sistema operativo. Es sorprendente ver como esta plataforma esté monopolizando 81% del mercado global, manteniéndose en un gran crecimiento del 51.3% respecto al año 2013, aunque algo que es mucho más sorprendente, valga la redundancia, es la versatilidad con la que se adapta dentro de varios dispositivos. Se puede encontrar en relojes inteligentes llamados *Smartwach*, televisores con *Google TV*, consolas de videojuegos, computadores, entre otros, en fin, las posibilidades parecen ser infinitas.

Así igual de infinitas, son las amenazas de *malware* a la que están expuestas las personas que usan un dispositivo con este sistema operativo, las cuales no solo los emplean a nivel personal, sino que cada vez más con el paso del tiempo se requiere como una gran necesidad para el desarrollo de tareas en el entorno empresarial. Las empresas deben encargarse de implementar una buena gestión de la seguridad en los sistemas ANDROID, recurriendo a implementar políticas como BYOD y MDM, garantizando seguridad y respaldo en la tranquilidad de sus empleados al usar sus móviles como recursos de trabajo.

Finalmente, la seguridad debe instaurarse en dos partes claves, en el entorno empresarial, y el entorno personal, siendo este último el que representa mayor impacto, ya que la educación *"viene de casa"*. Por tal razón, los usuarios deben conocer, implementar y en lo posible, ir ampliando los consejos de seguridad descritos en el contenido de este documento, para prevenir los ataques que siempre van a efectuar los *ciberdelincuentes*. Gracias a estas mejores prácticas, se reduce el riesgo de ocasionar un gran impacto negativo sobre los dispositivos ANDROID.

VI. REFERENCIAS

[1] Carlos A. Castillo. (2014, Enero) "Android Malware Past, Present, and Future" [Online]. Disponible: http://www.mcafee.com/us/resources/white-papers/wp-android-malware-past-present-future.pdf

[2] Android Open Source Project. (2014, Febrero) "Android Security Overview" [Online]. Disponible: http://source.android.com/devices/tech/security/

[3] Developer Android. (2013, Diciembre) "Security Tips" [Online] Disponible: http://developer.android.com/training/articles/security-tips.html

[4] Android Authority. (2014, Enero) "Top 15 antivirus and anti-malware apps for Android" [Online]. Disponible: http://www.androidauthority.com/10-best-antivirus-apps-for-android-269696/

Autor

Henry Arley Jaraba Herazo
Ingeniero de Sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia
2014