Android Malware

Fredy Cabrera

Universidad Católica: *"Nuestra Señora de la Asunción"*
Departamento de Electrónica e Informática
fdcz90@gmail.com

Resumen En este trabajo se presenta un análisis de las aplicaciones maliciosas-malwares-para la plataforma más difundida de los dispositivos móviles inteligentes: Android. Se hace un análisis básico de la arquitectura del Sistema Operativo. Se muestran los números que demuestran el crecimiento de los malwares en los últimos tiempos y se especifican los tipos de malwares existentes incluyendo la proporción de los mismos, sus formas de propagación. Se exponen las principales causas por las cuales Android es un sistema tan seductor para los atacantes y finalmente se presenta un breve tratamiento sobre las aplicaciones de seguridad que existen para el sistema en cuestión.

1. Introdución.

Los dispositivos móviles inteligentes se han ganado un lugar muy importante en la vida cotidiana, se han convertido en una herramienta necesaria para personas y empresas. Prueba de esto, constituye el notable aumento de las ventas de estos dispositivos en los últimos años y del gran número de empresas que han apostado en la producción para este mercado.
Android es el Sistema operativo de móviles más expandido en la actualidad, está basado en Linux y es de código abierto. La última propiedad permite a los fabricantes realizar pequeñas modificaciones para adaptarlos al hardware que producen y ponerlos en el mercado, esto es mucho más rentable que crear un nuevo sistema operativo desde cero y ponerlo a punto para la comercialización.
La gran aceptación de esta plataforma provocó que los maleantes informáticos hayan centrado su atención hacia la misma y que desde el 2010 hayan comenzado a atacar con software malicioso al mismo, esto principalmente para poder obtener ganancias económicas .
En los capítulos posteriores se realizará primeramente un tratamiento las características principales de este Sistema Operativo,historia ,arquitectura, dispositivos compatibles, el comportamiento en el mercado. Posteriormente se comienza con lo que se refiere al malware: el crecimiento de los últimos años, los tipos, las formas de instalación y a partir de éstas se darán los motivos de la gran cantidad de *malware* existente para este sistema operativo.

2. Android.

2.1. Breve Historia.

El pionero en el desarrollo de Android es **Andy Rubin** quien trabajó en firmas como Apple, WebTv y Danger Inc. En la última desarrolló un sistema operativo para móviles llamado DangerOS. Después de dejar esta empresa y lleno de muchas ideas en el 2003 formó un equipo con ingenieros amigos de empresas pasadas, la compañía se denominó Android Inc. Rubin se dedicó a buscar compañías inversionistas, exponiendo los beneficios de la plataforma basada en Linux que estaba desarrollando su equipo. Una de estas empresas fue **Google** quien compró Android en el año 2005, lo que presuponía la intención de Google de adentrarse en el mundo de los dispositivos móviles. Desde entonces han ocurrido diferentes acontecimientos que han logrado convertir a Android la plataforma para dispositivos móviles más popular.
En el año 2007 se estableció el Open HandSet Alliance, un consorcio de distintas empresas de software y hardware, incluyendo Google, cuyo principal objetivo es: "acelerar la innovación en los dispositivos móviles y ofrecer a los consumidores una rica, barata y mejor experiencia móvil".
El Android Open Source Project (AOSP) es el grupo encargado de desarrollar y mantener las compatibilidades de las distintas versiones de Android.

2.2. Arquitectura.

En base a [1] se dará a continuación una breve descripción de los componentes principales de este sistema operativo. Android se puede esquematizar en 4 niveles:

- El Kernel, es una versión del Kernel de Linux, modificada para adapatarlo a las capacidades de un dispositivo móvil, es decir para adaptarse a temas que refieren al consumo de energía y capacidad de cómputo. Aquí se encuentran todos los controladores del hardware disponible por el fabricante y sus interfaces para la capa superior. Una de las características más trascendentes es que este Kernel es multi-usuario, por lo tanto pueden estar corriendo aplicaciones de diferentes usuarios sin que "interfieran entre sí", esto permite establecer el sistema de seguridad que se conoce como *SandBox* o "Caja de Arena" , en donde cada aplicación es un usuario al cual se le asignan recursos y sin capacidad de salir de su "Caja". El comportamiento de cada aplicación en su caja es monitoreado por el sistema, pero éstas se pueden comunicar con un servicio de middleware que utiliza el sistema conocido como *IPC-Binder* (*InterProcess Communications*), que es otra de las modificaciones que se le ha agregado al Kernel original de Linux.
- Un middleware consistente en un conjunto de librerías escritas en C/C++, una versión optimizada de Java Virtual Machine conocida como Dalvik Virtual Machine DVM, y una librería central (*core libraries*) escrita en Java.

Esta es la capa que asegura que todas las aplicaciones pueden correr sin importar el hardware [1], las aplicaciones son entregadas en forma de códigos de bytes Dalvik, y el DVM se encarga de ejecutarla. Las librerías son utilizadas generalmente por los *frameworks* de aplicaciones, provee soporte para base de datos, programación 3D,etc.
Entonces cada aplicación se ejecuta como "un usuario" corriendo sobre su propio Dalvik Virtual Machine,

- Un *Framework* para las aplicaciones, esta capa provee diferentes servicios para las aplicaciones, la existencia de esta capa se debe la necesidad de controlar el acceso a la información. Esta capa facilita sustancialmente la tarea a los programadores de aplicaciones.
- Finalmente se encuentra la Capa de Aplicaciones, que contiene todas las aplicaciones que corren sobre el sistema.

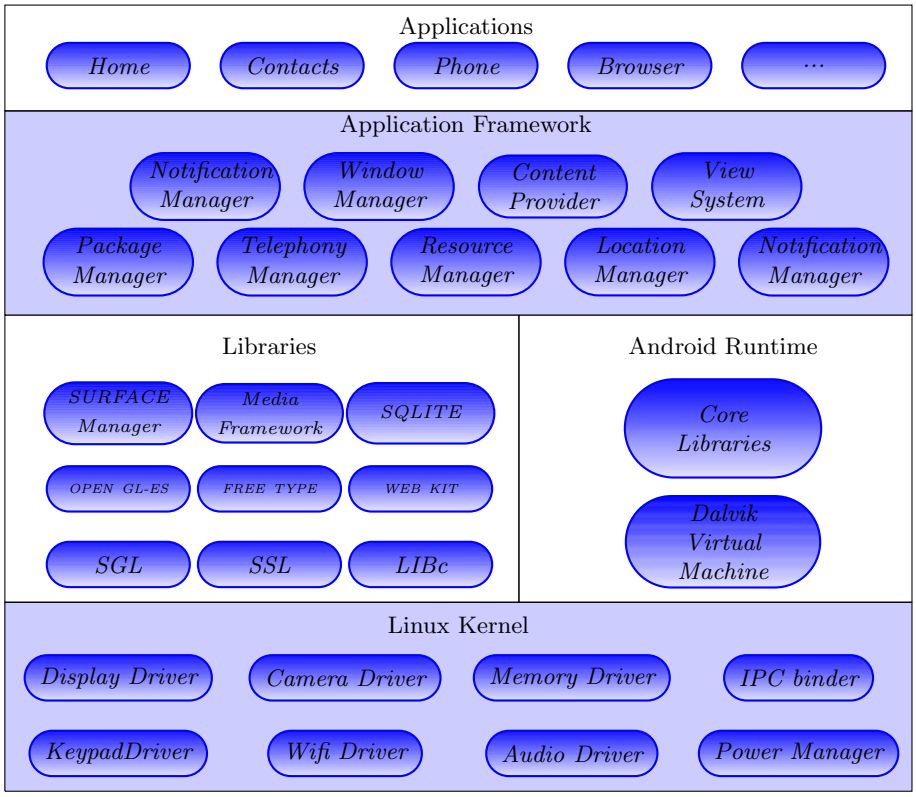

Figura 1. Arquitectura de Android.

[1] Tipo de procesador que posee el dispositivo

2.3. Dispositivos Compatibles.

Existen muchos dispositivos que corren Android, a continuación se darán una lista de ellos:

- SmartPhones.
- Tablets.
- Netbooks.
- Google TV.
- Vehículos.
- Dispositivos GPS.
- reproductores de multimedia.
- Impresoras.
- Teléfonos de hogar.
- Dispositivos de juego dedicados.

Como se ve la mayoría de estos son dispositivos móviles.

2.4. Mercado.

Android es el SO (sistema operativo) de dispositivos móviles inteligentes más difundido . Para tener una idea del comportamiento en el mercado se presenta en el cuadro 1 los números en ventas de las diversas plataformas disponibles , ésta fue extraída de [2], se dan los números para el segundo cuarto Q2 de los años 2011 y 2012, se ve que Android lidera las ventas totales con un 68 %, seguido por i-OS. Existen varias compañías que producen *hardware* con sistema operativo Android, pero es importante destacar que la empresa que lidera las ventas es Samsung, con el 44 % de las entregas de todas las entregas de aparatos con Android.
La cantidad total de entregas llega a una cantidad de 104 millones de unidades en el año 2012, este monto demuestra la penetración de mercado que tiene Android, doblando sus ventas del 2011.

Operating System	Q2 2012 Shipments	Q2 2012 Market Share	Q2 2011 Shipments	q2 2011 Market share	Year-over-Year Change
Android	104.8	68.1 %	50.8	46.9 %	106.5 %
iOs	26.0	16.9 %	20.4	18.8 %	27.5 %
BlacBerry Os	7.4	4.8 %	12.5	11.5 %	-40.9 %
Symbian	6.8	4.4 %	18.3	16.9 %	-62.9 %
Windows Phone 7/ Windows Mobile	5.4	3.5 %	2.5	2.3 %	115.3 %
Linux	3.5	2.3 %	3.3	3.0 %	6.3 %
Others	0.1	0.1 %	0.6	0.5 %	-80.0 %
Grand Total	154.0	100 %	108.3	100 %	42.2 %

Cuadro 1. SOs móviles y sus ventas. Unidades en millones.

2.5. Android-Market.

Otra característica importante que es accesible para Android es el Android-Market, que es una vía para que aplicaciones desarrollados por terceros puedan

ser accedidos e instalados por otros usuarios. Android-Market fue lanzado en octubre del 2008.
Para tener la posibilidad de lanzar una aplicación en Android-Market, el desarrollador debe registrarse abonando una cierta cantidad de dinero aproximadamente unos 25 USD. Posteriormente si su aplicación es descargada recibe el 70 % del precio de venta y Google se queda con el resto.
La utilización del Android-Market no es obligatoria, es decir los usuarios de Android pueden descargar las aplicaciones directamente de la página web del desarrollador o utilizar alguna otra tienda alternativa como: Verizon Amazon, Best Buy entre otros.

3. Malware y Android.

3.1. Concepto de Malware.

En inglés fusión de las palabras "*malicious + software*", software malicioso. Se podría definir malware como cualquier software que sin tener autorización del usuario o aprovechándose del desconocimiento (ignorancia) realiza acciones consideradas poco éticas.
Este concepto ya ha sido manejado durante décadas en el mundo de las PCs, pero con la popularidad de los dispositivos móviles no tardaron en aparecer malwares dirigidos para estos. El objetivo principal de los atacantes (desarrolladores de malware) es la obtención de información confidencial. Esta información puede ser utilizada para distintos objetivos:

- Comercialización: los gustos de los posibles clientes de algún producto o servicio constituyen una información muy valiosa; y esta información puede ser obtenida de manera no legal y vendida a las empresas para poder elaborar perfiles de consumidor, sin que el consumidor se entere que éste puede existir.
- Crear nuevos agujeros: generalmente la información es obtenida utilizando "agujeros" en algún sistema. Esta información puede ser utilizada para crear nuevos "agujeros" o para agrandar el existente.
- Fraudes Financieros: obtener contraseñas de cuentas bancarias u otros.
- Daños al sistema: utilizar la información para causar un daño al sistema del cual fue extraída la información.

Estos y muchos otros más son los objetivos que se persiguen.

3.2. Crecimiento de malware para móviles.

El crecimiento en el año 2012 de los malwares ha sido inmenso. Según [3] la base de datos de malwares para dispositivos móviles que posee McAfee Labs se comporta como se ve en la figura 2.

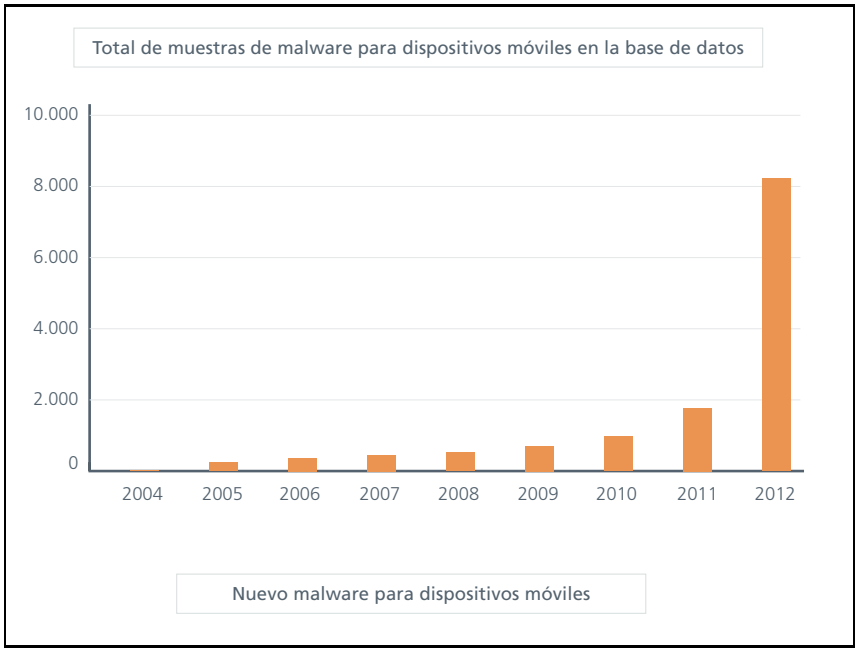

Figura 2. Cantidad de malwares para dispositivos móviles.Según [3]

Sin embargo [4] afirma haber pasado de 11138 muestras de malware en el 2010 a un total 28472 muestras en el 2011, con un crecimiento de un 155 % durante un año. Además en [3] se afirma que casi todos estos ejemplares son para Android y se presenta las cantidades en la figura 3

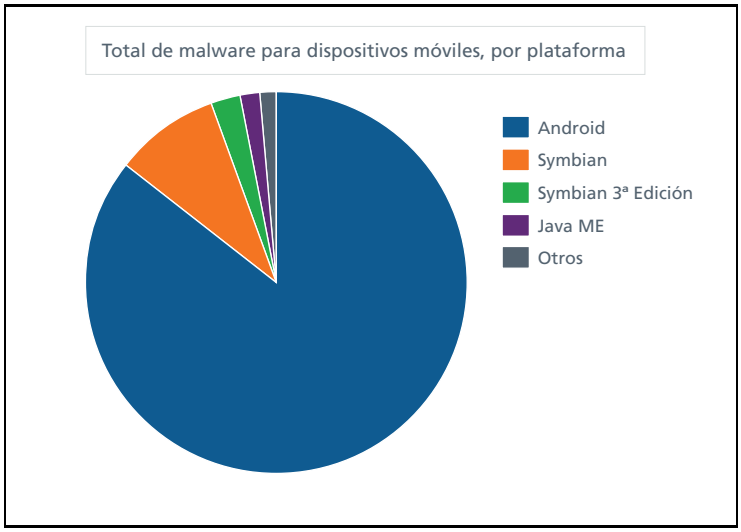

Figura 3. Sistemas operativos afectados por malware. Extraído de [3].

A partir de lo anterior se puede llegar a la conclusión de que Android es el más atacado en el mundo de los dispositivos móviles y a partir de aquí se hará referencia exclusivamente al malware sobre Android.

3.3. Tipos de Malware.

Se tienen diversas metodologías para obtener la información, esta metodología se especifica con el tipo de aplicación maliciosa:

1. *Spyware*: software espía, aplicación no autorizada que captura datos privados del sistema y es capaz de transmitir dichos datos a algún receptor. Este tipo de aplicación es el más común en las plataformas Android [4]. Generalmente se tienen tres funciones principales recoger información ya sea del sistema o de otras aplicaciones, la segunda es transmitir esta información, y la tercera es lograr seguir permaneciendo oculto. Los tipos de información o datos que se pueden recuperar se pueden dividir según [5] como : **datos en reposo** y **datos en tránsito**.
   Los **datos en reposo** se pueden dividir en:
   - Historiales de Comunicación:
     - SMS/MMS. Todos los SMS y MMS no borrados y los que fueron borrados pero continúan en la memoria flash pueden ser recuperados, incluyendo todos los metadatos relacionados con estos.
     - Historial de llamadas. Las llamadas realizadas también pueden ser accedidas, también con los respectivos metadatos, por ejemplo la posición de la celda donde se estuvo conectado al realizar la llamada.

- Mensajes de voz. Existen applicaciones de mensajes de voz, al igual que los SMS/MMS pueden ser recuperados.
- e-mail. Las aplicaciones de e-mail para Android generalmente suelen guardan el contenido de los *e-mail* en texto llano incluyendo las contraseñas utilizadas.
- Mensajes instantáneos y comunicaciones con empleados.

- Otros historiales:
  - Historial Web: incluyendo los URLs, cookies y las páginas en caché.
  - Historial de búsquedas de Google. incluyendo las palabras clave de búsqueda.
  - Historial de youtube. URL de videos vistos.
  - Historial de juegos e interacciones.
- Credenciales:
  - Nombres de Usuarios, contraseñas e información de dominio.
  - Puntos de Acceso Wi-fi, información y contraseñas.
  - Aplicaciones financieras.
- *Tracking*
  - Geo-localización. Datos del hardware GPS.
- Archivos:
  - Imágenes y videos. Capturados con las cámaras del teléfono.
  - Items de calendario.
  - Archivos corporativos que han sido almacenados en el móvil por conveniencia.

Los datos en tránsitos son :

- Contraseñas.
- Datos de Autenticación.
- Datos desplegados pero no almacenados en caché.

2. *SMS Trojans*: es el segundo tipo de malware que se presenta con mayor frecuencia, son aplicaciones que sin concesión de permisos del usuario envía mensajes de texto a números *Premium rate*, es decir números a los cuales por enviar mensajes cobra una monto mucho mayor que a un número normal. Generalmente estos números son anónimos y el usuario no puede recuperar su pérdida monetaria.
3. *Worms*: los famosos gusanos también están presentes, son aplicaciones que pueden autoreproducirse hasta llegar a saturar algún recurso del sistema. Generalmente tienen fin en sí mismo, es decir son diseñadas para dañar el sistema no para obtener otros beneficios a partir de este.
4. *SMS flooders*: envían mensajes de texto a un conjunto de números parte del directorio de números del usuario, son utilizados generalmente para hacer campañas publicitarias.

En la figura 4 se presenta el porcentaje de la cantidad de cada tipo de malware que se presenta sobre Android.

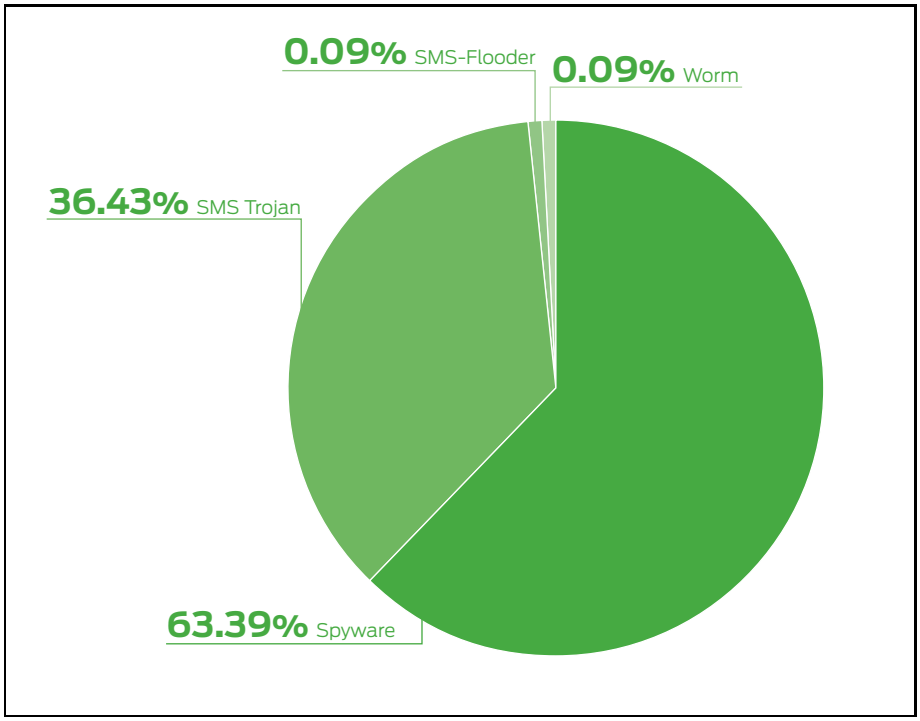

Figura 4. Porcentajes de tipos de malware. Extraído de [4].

3.4. Modos de instalación

En [6] se dan los tipos de instalación que se tienen:

- *Repackaging*: Una traducción directa al español sería re-empaquetamiento, es la técnica más utilizada para la instalación. Ya que todos tienen acceso a las tiendas de aplicaciones, cualquiera puede descargar una aplicación inicialmente benigna, una vez descargado el programa se puede aplicar técnicas de ingeniera inversa para poder des-ensamblar el programa, aquí es donde se le agrega el código malicioso generalmente sin quitar la funcionalidad principal de la aplicación origina, finalmente se re-ensambla el programa y se coloca nuevamente en el mercado de aplicaciones. Posteriormente usuarios inocentes descargan estas aplicaciones infectadas convirtiéndose en víctimas. Es innegable el rol beneficioso que tienen los mercados de aplicaciones, pero aquí tenemos un ejemplo claro de un punto negativo en su contra. Aproximadamente 86 % de las muestran que se utilizaron en [6] utilizan este tipo de técnica.
- Ataques de Actualización: en vez de albergar completamente la carga maliciosa en la aplicación, este es descargado en tiempo de ejecución cuando en rutinas de actualización de la aplicación. Este tipo de instalación es muy difícil de detectar.

- *Drive-by Download*: se inducen a los usuarios a realizar "descargas" que son presentadas como muy beneficiosas, pero cuya verdadera finalidad es introducir dentro del sistema las rutinas maliciosas.
- *Otros*: los métodos de ingeniería social y otros son incluidos dentro de este.

3.5. Cronología de Malware.

Se presentará una cronología de los malware más destacados basado en el trabajo realizado en [7] y complementado con [8] [2].

- **Enero 2010**. Aparece la primera aplicación de Phising[3] en el Android-Market , el usuario "Droid09" pretendía ser un cliente bancario para poder obtener las credenciales de inicio de sesión.
- **Marzo 2010**. Bot[4] para Android que afectaba a los sistemas Windows. La empresa Vodafone estaba enviando sin saberlo, sus dispositivos estaban precargados con el bot. Cuando el usuario conectaba su teléfono por USB al ordenador el bot se ejecutaba e infectaba al ordenador.
- **Julio 2010**. Spyware GPS empaquetado en el juego "Tap Snake". Era un juego que consistía en controlar los movimiento de una serpiente evitando obstáculos; pero en realidad era un spyware que podía monitorear la ubicación de la víctima usando el hardware GPS, la aplicación venía con un par que era el "GPS spy" que se instalaba en la plataforma del atacante y podía recibir los datos que 'Tap Snake" levantaba en una web.
- **Agosto 2010**. Aparece el primer SMS troyan : "Fake Player".La aplicación fingía ser un reproductor de multimedia.
- **Noviembre 2010**. Experimento "Angry Birds". Los investigadores Jon Oberheide y ZachLanier mostraron un falla que puede ser utilizada de tal manera que una aplicación pueda descargar aplicaciones adicionales sin autorización de los usuarios.Para probar su tesis se valieron del juego "Angry Birds" .
- **Diciembre de 2010**. Android se convierte como objetivo principal de las aplicaciones maliciosas.
- **Enero / Febrero 2011**. "aDrD" y "pJapps" aparecen en China, son versiones re-empaquetadas de aplicaciones legítimas, recogían información personal y se suscribían automáticamente a servicios.
- **Marzo 2011**. "Myournet/DroidDream" se denomina de esta manera a un conjunto de aplicaciones que utilizan una falla del sistema que permite acceder al usuario "root", a partir de esto le permitía a las aplicaciones descargar otras aplicaciones y transmitir información sin necesidad de pedir permisos al usuario.
  Estas aplicaciones se pusieron en el Android Market y fueron descargados entre 50.000 y 250.000 veces.
  La única manera que los usuarios que sospechaban que estaban infectados

[2] Para más detalle véase las referencias
[3] Aplicación de web que trata de conseguir datos financieros
[4] robot informático capaz de ser autónomo y establecer redes botnets.

de deshacerse de la aplicación era resetear el teléfono. Esto obligó a Google lanzar una herramienta de seguridad que permitía eliminar los efectos de la infección Myournet / DroidDream. Google lo publicó en el Android Market, con instrucciones que indicaban que no era necesario descargar manualmente la aplicación. Sin embargo, sólo unos pocos días más tarde, una versión de la herramienta de seguridad de Android Market había sido re-empaquetada se encontraba en la tienda de terceros en China.

- **Abril 2011**. versión re-empaquetada de "Walk and Text". Esta era una aplicación muy popular, fue re-empaquetado y subido para la descarga en tiendas de terceros, la aplicación era gratuita y una vez instalada enviaba un mensaje de texto a todos los contactos del teléfono móvil que decía: " hey, acabo de descargar una aplicación pirata de la Internet, Walk and Text para Android. Soy estúpido y barato, costó sólo 1 dólar . No lo robes como lo hice yo!"
- **Mayo 2011**. AndroidAdsms y AndroidOSAdsmsA Destinado a los usuarios chinos. Un link es enviado por SMS anunciando ser un parche para el dispositivo. Una vez que el programa haya sido instalado comienza a enviar mensajes a números Premium.
- **Mayo 2011**. Google remueve un troyano del Android Market, llamado Zsone, con la habilidad de suscribir a sus usuarios a cuentas premium. Afectó a más de 10000 usuarios.
- **Mayo 2011**. Nuevas aplicaciones DroidDream fueron encontradas. Ya habían infectado a aproximadamente 120000 usuarios.

3.6. Causas.

De todo lo mencionado, surge una cuestión inevitable: las causas por las que se da este fenómeno. A continuación se dará los motivos por las cuales se dieron los aumentos desmedidos en las cantidades de malware sobre Android.

1. **Escencia de los móviles:** Los dispositivos móviles están conectados casi todo el tiempo a la red, mucho más de lo que estaría conectado una computadora personal, esto es lo que buscan la mayoría de las personas: estar conectados donde sea, a partir de esto el móvil se convierte inmediatamente en un dispositivo que contiene una alta cantidad de información personal.
2. **Popularidad:** Las tremendas cifras mencionadas en la sección 2.4 demuestran la aceptación que tiene Android. esto a la vez es un atractivo para los desarrolladores de estas aplicaciones maliciosas, aumentar esfuerzos para obtener mayores ganancias es un "negocio". No hay que ser un experto en negocios para darse cuenta de esto, los malwares que tienen metas propagandísticas cumplirían mejor sus objetivos, cuanto a más personas y más específicos sean los perfiles mercadotécnicos se llevarán a cabo ataques de propagandas más centrados.
   El "boom" de esto dispositivos está ocurriendo y todos, incluso los "oportunistas", quieren formar parte de esto. Lo mismo que ocurrió en su momento con el Sistema Operativo para PCs Windows está sucediendo con Android,

lo mismo pero a una velocidad mucho más alta.
La popularidad también empuja a las empresas a lanzar productos sin pasar por una revisión minuciosa de seguridad a lo que se refiere al software y al hardware mismo. Como se sabe cada fabricante toma el código fuente ofrecido por Google y le realiza las modificaciones para adaptarlo y optimizarlo al producto que está fabricando. Por la ferocidad del mercado actual los plazos de tiempo para realizar estas modificaciones son cada vez más cortos impidiendo los controles efectivos.
La popularidad desfavorece a la diversidad, la diversidad favorece a la seguridad, mientras más tipos de hardware y software existan es más difícil que se llegue a la "convergencia de ataque" que se está logrando en la actualidad.

3. **Políticas de distribución de aplicación:** Google lleva a cabo una política libre a lo que se refiere a a la distribuación de las aplicaciones.

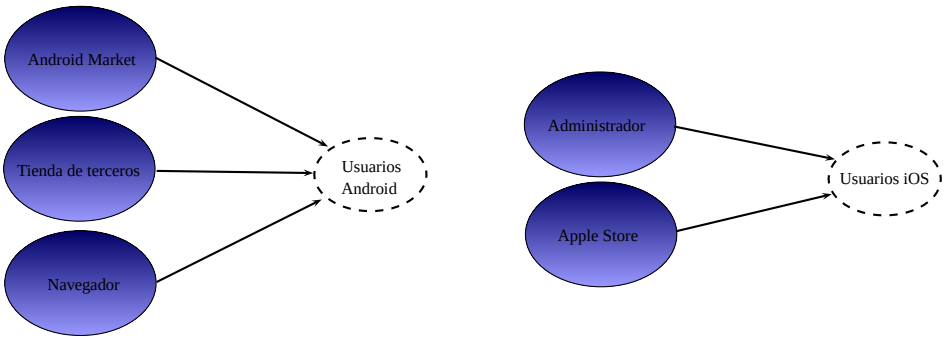

Figura 5. Esquema de distribución de aplicación de Android y iOS.

Esta libertad trae su lado negativo. En la figura 5 se presenta una comparación entre los usuarios de Android y de iOS. Mientras como se decía en la sección 2.5 Google permite que sus usuarios realicen descargas exclusivamente del Android-Market, sino también de otras tiendas alternativas y de la página web de los desarrolladores, en cambio iOS solo permite descargas del Apple Store o de algún Administrador de dispositivos móviles, este administrador requiere la previa aprobación de Apple. Como se ve Apple puede controlar mas de cerca las aplicaciones dirigidas a iOS, mientras que Google tiene control del Android-Market pero no de las otras fuentes de aplicación. En este sentido según [9] :"La tienda de Apple se controla más de cerca y, al menos por el momento, es más segura".
Aunque generalmente se den ciertas indicaciones de riesgos como las de la figura 6, generalmente el usuario se ve sugestionado por las capacidades que dice tener la aplicación.

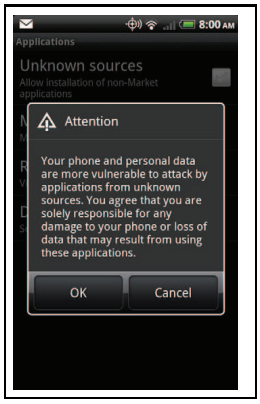

Figura 6. Alertas de precaución en Android. Extraído de [5].

4. **Modelo de Seguridad**: el modelo de seguridad de Android consiste esencialmente en la concesión de permisos en el momento de la instalación de la aplicación. Estos permisos son otorgados por el usuario final. Idealmente la aplicación en el momento de ejecución correría en su caja de arena (ver sección 2.2) sin poder utilizar recursos que no le son permitidos, más adelante se verá que esta restricción se puede eludir.

   Se analizará primeramente el caso de la concesión de permisos por parte del usuario. Según [9] existe una poca prolijidad por parte de los desarrolladores de aplicaciones, es decir las aplicaciones piden permisos excesivos, permisos que ni siquiera serán utilizados, esto hace engorroso al usuario distinguir las aplicaciones lícitas de las que tienen objetivos maliciosos. Este hecho se puede deber ,de acuerdo a [9], a:

   a) Falta de documentación sobre los métodos y de los permisos que necesitan los mismos.

   b) Problemas en las pruebas: las rutinas que son insertadas para depurar el software que se está desarrollando no son eliminadas de la versión final.

   c) Errores propagados en los foros: existen diferentes foros donde los desarrolladores comparten sus códigos, algunos de ellos con errores; como se realiza simplemente un proceso de "copiar y pegar" este error va propagándose en diferente aplicaciones.

   Para tener una idea de los permisos que piden los malwares y los que son requeridos por las aplicaciones benignas se presenta el resultado de [6] en las figuras 7 y 8. Por lo que se ve en las dos gráficas se desvían en lo permisos de menor uso, pero se ve que tienen un comportamiento similar aunque difieran en cantidad en la parte inferior de la gráfica, por lo que podemos decir que no es un buen parámetro fijarse simplemente en los permisos.

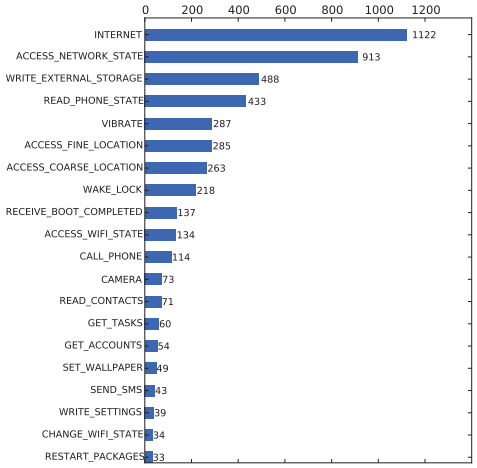

Figura 7. Lista de permisos requeridos por 1260 muestras Aplicaciones benignas. Extraído de [6].

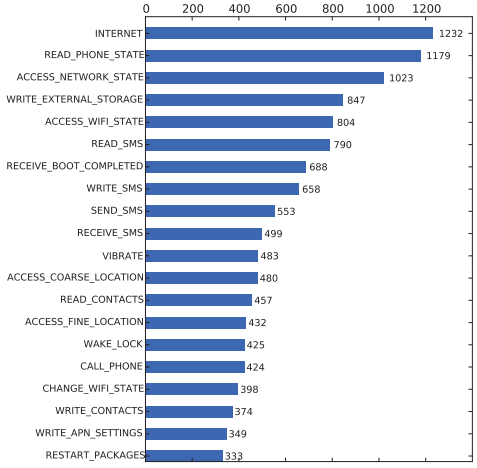

Figura 8. Lista de permisos requeridos por 1260 muestras de malware. Extraído de [6].

Además el sistema de de permisos puede ser burlada mediante un tipo de ataque que se conoce como "ataque de intensificación de privilegios" (Privilege Escalation Attack) y se basa en una falla del sistema de comunicación entre los procesos (ver sección 2.2). Se presentará la explicación que se hace

en [10]. En la figura 9 se presenta un esquema particular para poder explicar el ataque.

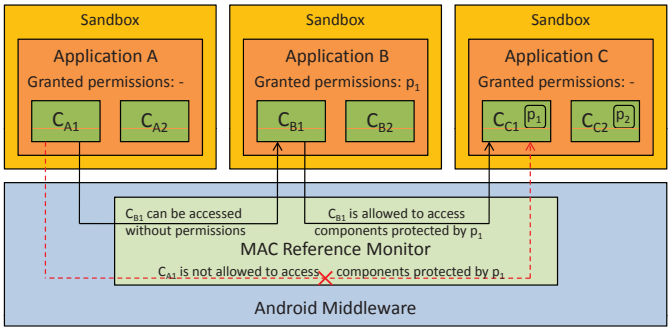

Figura 9. Esquema de ataque por intensificación de privilegios.Extraído de [**?**].

Se presentan 3 aplicaciones A_1,A_2 y A_3 cada una en su propia caja de arena, A_1 no tiene permisos para acceder a los datos protegidos por el permiso P_1, los datos protegidos por este permiso son los que van a ser procesados por A_3,otra aplicación A_2 recibió el permiso P_1 en el momento que fue instalado, pero esta aplicación no tiene ninguna restricción para que otra aplicación pueda comunicarse con ella, es decir A_1 podría acceder a los datos de A_3 comunicándose con A_2 que a su vez es el que accede a los datos y los proporciona a A_1. Esta simple propiedad de transitividad es muy peligrosa y de acuerdo a [6] es una de las más utilizadas por las aplicaciones maliciosas.

3.7. Software Anti-malware

Se han realizado varios estudios y se han propuesto soluciones ([12] y [13] son ejemplos de estos) para los ataques de intensificación de privilegios; también las empresas de seguridad están trabajando para dar a los usuarios una experiencia más segura, estas empresas ofrecen software que generalmente funcionan con un sistema de base de datos y no con el comportamiento en tiempo real.
Se presenta a continuación un análisis realizado en [14], en este se ha realizado una prueba del desempeño que tienen las actuales aplicaciones de seguridad desarrollados. Para ello juntaron un conjunto de muestras de malware y procedían a instalarlo (en un simulador), posteriormente realizaban el escaneo con diferentes aplicaciones, arrojando los resultados que son desplegados en la figura 10.

	Product	Average Family Detection	
A	avast! Free Mobile Security		>90%
A	Dr.Web anti-virus Light		
A	F-Secure Mobile Security		
A	IKARUS mobile.security LITE		
A	Kaspersky Mobile Security		
A	Lookout Security & Antivirus		
B	McAfee Mobile Security		
B	MYAndroid Protection		
B	NQ Mobile Security		
A	Zoner AntiVirus Free		
A	AegisLab Antivirus Free		>65%
A	AVG Mobilation Anti-Virus Free		
A	Bitdefender Mobile Security		
B	BullGuard Mobile Security		
B	Comodo Mobile Security		
A	ESET Mobile Security		
A	Norton Mobile Security Lite		
A	Quick Heal Mobile Security		
A	Super Security		
B	Total Defense Mobile Security		
A	Trend Micro Mobile Security		
A	Vipre Mobile Security (BETA)		
A	Webroot SecureAnywhere		
B	BluePoint Security Free		>40%
B	G Data Mobilesecurity		
B	Kinetoo Malware Scan		
B	ALYac Android		>0%
B	Android Antivirus		
B	Android Defender Virus Shield		
B	Antivirus Free		
B	BlackBelt AntiVirus		
B	CMC Mobile Security		
B	Fastscan Anti-Virus Free		
B	GuardX Antivirus		
B	MobiShield Mobile Security		
B	MT Antivirus		
B	Privateer LITE		
B	Snap Secure		
B	TrustGo Mobile Security		
B	LabMSF Antivirus beta		0
B	MobileBot Antivirus		

Figura 10. Promedio de detección de malware. Extraído de [14].

4. Conclusiones

Los móviles inteligentes están conectados en todo instante a la red, almacenan una gran cantidad de información personal, financiera, corporativa; por lo que todo lo consista sobre el tema de seguridad es de vital imporatncia para una buena experiencia.
Android es el sistema operativo para móviles más utilizado en la actualidad, y como tal está en el centro de la mira de todos los atacantes cibernéticos. Como producto de esto es el masivo crecimiento de los malwares que son desarrollados para funcionar sobre esta plataforma.Los atacantes se aprovechan generalmente de las fallas del sistema, y en general se ha mostrado que el modelo de seguridad "orientado a permisos" mismo no provee una protección efectiva, por el mal manejo de los permisos que existe.
La libertad que propone Google para las descargas de aplicaciones de tiendas de terceros y de páginas web tienen su lado negativo, ya que Google no tiene control sobre los mismos y es utilizado como foco de propagación de malware
El afectado inmediato de los ataques es el usuario, en primera instancia pierde su privacidad se puede saber donde está , que está haciendo e inclusive qué va a hacer.Las pérdidas monetarias son otro aspecto a destacar entre las consecuencias negativas de estas aplicaciones maliciosas.
Las empresas de seguridad están reaccionando aunque lentamente ante esta situación, pero ya existen aplicaciones con buen desempeño frente a estos malwares.

Referencias

1. D. de Android, "What is Android?" 2012, disponible en: https://developer.android.com .
2. IDC, "International Data Corporation Worldwide Mobile Phone Tracker," Agosto 2012, disponible en: http://www.idc.com.
3. M. Labs, "Informe de Mcafee sobre amenazas: Primer trimestre de 2012." 2012.
4. J. Networks., "2011 Mobile Threats Report." Febrero 2012.
5. H. A., *Android Forensics. Investigation, Analysis and Mobile Security for Google Android.*, T. E. John McCash, Ed. Elsevier, 2011.
6. Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution." 2012.
7. R.Osorio and C.Ramirez, "Características y parámetros de la seguridad para los smartphones con sistema operativo android." Universidad Tecnológica de Pereira, Tech. Rep., 2011.
8. "One Year of Android Malware (Full List)," Agosto 2012, disponible en: http:// paulsparrows.wordpress.com/2011/08/11/one-year-ofandroid- malware-full-list/.
9. M. Labs, "Protección de dispositivos móviles: presente y futuro," 2011.
10. A. R. S. Lucas Davi, Alexandra Dmitrienko and M. Winandy, "Privilege Escalation Attacks on Android," Ruhr-University Bochum, Germany, Tech. Rep.
11. I. N. Xuetao Wei, Lorenzo Gomez and M. Faloutsos, "Malicious Android Applications in the Enterprise: What do they do and how do we fix it?" Department of Computer Science and Engineering, University of California, Riverside, Tech. Rep.
12. C. L. J. L. S. H. M. P. S.-J. C. Yeongung Park, ChoongHyun Lee, ""Rgbdroid: A Novel Response-Based Approach to Android Privilege Escalation Attacks"."
13. A. D. T. F. S. S. Bugiel, L. Davi, "XManDroid: A New Android Evolution to Mitigate Privilege Escalation Attacks," Technische Universitat Darmstadt, Germany, Tech. Rep., 2011.
14. "Test Report: Anti-Malware solutions for Android," AV-TEST The Independent IT-Security Institute, Tech. Rep., 2012.
15. P. Schulz, "Android Security-Common attack vectors." Rheinische Friedrich-Wilhelms-Universitat Bönn, Germany, Tech. Rep., 2012.