Malware en dispositivos móviles

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autor:
Pablo Ramos
Especialista de Awareness & Research

Fecha:
Marzo 2012

Índice

Introducción

El uso de dispositivos móviles se encuentra en aumento desde hace años y, con la aparición de los smartphones, las capacidades de estas terminales han crecido de manera exponencial. Según el estudios de IDC, en el primer trimestre del 2011 se vendieron **371.8 millones de unidades**, lo que significa un crecimiento de un 20% respecto al mismo período del 2010 (310.5 millones). En lo que respecta a la región de Latinoamérica, la relación entre la cantidad de **smartphones** y los dispositivos móviles tradicionales ya no es tan amplia, y por ello ha aumentado la cantidad de conexiones a redes 3G.

Este cambio permite a los usuarios contar con una conexión a Internet las 24 horas del día, como así también que transporten con ellos una gran cantidad de información en sus bolsillos, que años atrás no solían hacer.

Todas las virtudes que ofrecen estas plataformas también traen aparejados ciertos riesgos, no solo relacionados con los códigos maliciosos, sino también al robo de información o la pérdida del equipo.

Las amenazas existentes para las distintas plataformas móviles incluyen malware, ataques de phishing, scams y fuga de información. Por lo general, siempre se hace uso de técnicas de **Ingeniería Socia**l para engañar a los usuarios y consumar el ataque.

Muchos usuarios desconocen que las plataformas móviles son utilizadas por los desarrolladores de códigos maliciosos para enviar enlaces dañinos que redirigen al usuario a la descarga de malware, y es debido a ello que caen víctimas de los engaños.

La falta de conocimiento acerca de las amenazas para dispositivos móviles, expone a los usuarios a la pérdida de su información o la infección de su smartphone.

Plataformas móviles

Una particularidad del mundo de los dispositivos móviles es la diversidad de plataformas existentes que están a disposición de los usuarios. A diferencia del mercado de escritorio, donde aún Windows posee amplia mayoría del mercado, al momento de adquirir un teléfono inteligente, los usuarios tienen diversidad de opciones para elegir.

El mercado se encuentra dividido principalmente entre 5 sistemas operativos distintos: **Android**, **Symbian**, **Windows Mobile**, **iOS**, y **RIM**. Cada una de estas plataformas cuenta con distintas características en lo que respecta a sus funcionalidades, distribución de aplicaciones y modelo de seguridad. La presente distribución del mercado ha llevado a los desarrolladores de códigos maliciosos a focalizarse en las plataformas líderes llegando así a una mayor cantidad de víctimas. Según la información publicada a mediados del 2011 por la consultora Gartner, el mercado de los dispositivos móviles es liderado por **Android** con el 43% del total, seguido por **Symbian** (22%), **iOS** (18%), **RIM** (12%) y **Windows Phone** en la quinta posición con el 2%:

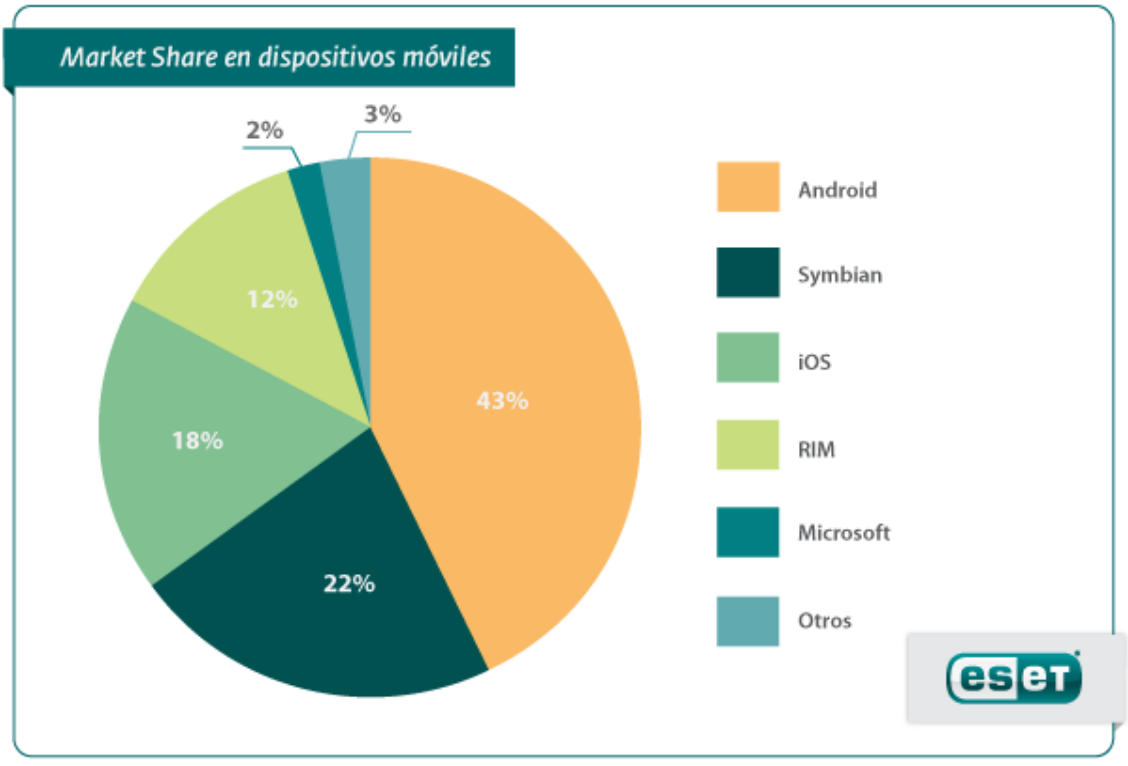

Imagen 1 - Market Share de smartphone

Cada una de las plataformas presenta distintas funcionalidades al usuario, en lo que respecta a su utilidad y la manera de distribuir sus aplicaciones. Estas características son utilizadas por los

desarrolladores de códigos maliciosos con el afán de vulnerar la seguridad del usuario e infectar su equipo, ya sea para el robo de información o cualquier otra actividad maliciosa. Muchas de las amenazas encontradas en la actualidad buscan el acceso a información personal del usuario, sin que el mismo sea consciente de ello.

Android

La **plataforma móvil de Google** se encuentra en el mercado desde septiembre del 2008 y a partir de ese momento ha tenido un crecimiento importante, llegando hoy en día a ser la plataforma móvil líder en teléfonos inteligentes. Como consecuencia, en la actualidad, es una de las plataformas para la cual **más códigos maliciosos están apareciendo**, explotando ciertas características presentes en la arquitectura del sistema y sus repositorios de aplicaciones. 2011 fue el año que más amenazas presentó para esta plataforma.

El desarrollo de este sistema operativo está centrado en un núcleo basado en Linux para los servicios base. El mismo, trabaja sobre capas de abstracción entre el hardware y el software. Por sobre la capa que ofrece el *kernel* (núcleo) del sistema, se encuentran librerías desarrolladas en C/C++ que permiten el manejo de gráficos y otras funcionalidades, como las bases de datos **SQLite**. También se encuentra el **Runtime de Android** formado por un conjunto de bibliotecas base desarrolladas en Java y en dónde por cada aplicación que se encuentre se ejecuta un proceso separado dentro de la **máquina virtual de Dalvik**.

En conjunto con los permisos necesarios para la ejecución de una aplicación, que se declaran en el **AndroidManifest.xml**, Android asigna un User ID y un Group ID distinto a cada una de ellas. De esta manera cada proceso se ejecuta de manera aislada ofreciendo un modelo de seguridad compacto y eficiente.

Por lo general, el método de propagación de amenazas para esta plataforma suele ser a través de cuentas de desarrolladores falsas que publican aplicaciones maliciosas en el **Android Market** o a través de repositorios de aplicaciones no oficiales.

Desde mediados del 2010 se ha incrementado la cantidad de amenazas existentes para **Android** en dónde han aparecido diferentes códigos maliciosos como Geinimi, DroidDream y Raden. Estos troyanos se encontraban ocultos dentro de videojuegos, ocultando su verdadera identidad y comportamiento.

En el caso puntal de Raden, troyano SMS detectado por ESET Mobile Security como *Android/Raden*, la amenaza se encontraba oculta en juegos (como el conocido buscaminas) en dónde al iniciarse el mismo se ejecutaba la función (**startNewGame()**) y luego de configurar todos los parámetros se realizaba el llamado a la función **sendSMS()** que se encarga de enviar un mensaje de texto para suscribir al usuario a un servicio de mensajes premium:

Imagen 2 - Inicio de Juego

De esta manera, la función **sendSMS()** envía un mensaje de texto al número **1066185829** con el contenido **921X2**, suscribiendo al equipo infectado a un servicio de mensajes premium. Para ocultar su comportamiento, esta amenaza captura los mensajes de respuesta del servicio de mensajes y evita su notificación al usuario para evitar ser detectado.

Otras amenazas como las mencionadas anteriormente permiten la recepción de comandos remotos haciendo que el dispositivo se convierta en un equipo zombi perteneciente a una **botnet**. En estos casos, el *botmaster* puede efectuar comandos para acceder a información personal del usuario o instalar otros códigos maliciosos en el equipo.

Android es una plataforma relativamente nueva. No obstante, ha sido víctima de códigos maliciosos innovadores y avanzados que utilizan las funcionalidades del sistema operativo de **Google** para beneficio de los desarrolladores de códigos maliciosos.

A lo largo del 2011 el Laboratorio de Análisis e Investigación de ESET Latinoamérica analizó 41 familias de códigos maliciosos de las cuales 15 eran troyanos SMS. Esto posiciona a los troyanos SMS como una de las técnicas más utilizadas por los desarrolladores de malware. Además, **el 65% de las amenazas aparec en los últimos cinco meses**, destacando la tendencia identificada por el Laboratorio de ESET para el 2012. Además, se detectaron falsas soluciones de

seguridad, que engañaban al usuario bajo la promesa de proteger el smartphone cuando en realidad robaban información personal.

Asimismo, otras conclusiones de este análisis que realizó el Laboratorio de ESET Latinoamérica son:

- El 30% de las amenazas estuvieron disponibles para su descarga en el Android Market.
- El 37% son troyanos SMS.
- El 60% de los códigos maliciosos tiene alguna característica de botnets, es decir, algún tipo de control remoto sobre el dispositivo.

Symbian

Presente en el mercado desde hace más de una década, Symbian ha sido por mucho tiempo una de las plataformas móviles de mayor uso a nivel mundial. A lo largo de su historia, y con la evolución de su sistema operativo, surgieron distintas amenazas que intentaron burlar el modelo de seguridad.

Symbian centra su arquitectura de seguridad en dos conceptos conocidos como *data caging* y *capabilities*, en donde cada aplicación solo cuenta con acceso a sus recursos o determinadas áreas del sistema de archivos. De esta manera se evita que una aplicación pueda acceder al directorio privado de otra o a los datos.

Existen distintos tipos de accesos dentro del sistema de archivos, con funciones específicas:

- **/resources**: Se permite la escritura en el momento de la instalación de una aplicación, la lectura de su contenido no se encuentra restringida. Contiene los íconos de las aplicaciones, mapas de bits, etc.
- **/sys**: Almacena los archivos binarios, los registros de instalación y los certificados de administradores (*root*). Su escritura está permitida durante la instalación de las aplicaciones y la lectura solo para *backups*.
- **/private**: Sección privada designada para cada aplicación en donde se puede almacenar la información privada.
- **/all the rest**: Documentos compartidos que pueden ser accedidos por todas las aplicaciones y servicios del sistema como por ejemplo fotografías, música y documentos.

Las aplicaciones para esta plataforma cuentan con una firma digital que garantiza su veracidad. Existen distintos tipos de certificados para aplicaciones, según los recursos a los que solicita acceso. Dicho certificado puede ser falsificado por algunas amenazas, y esta es una de las maneras utilizadas para engañar al usuario e infectar su dispositivo.

Los códigos maliciosos para Symbian pueden propagarse en archivos con extensión *SIS* o también ser desarrollados en Java. Esto se debe a que la plataforma soporta cualquiera de los dos formatos. Dichas amenazas cuentan con capacidades que van desde el envío de mensajes de texto a números Premium, hasta el robo de credenciales bancarias.

En ese contexto, los troyanos bancarios para plataformas móviles han evolucionado con el pasar de los años, y una de las amenazas para Symbian fue **Zitmo**, un troyano que convertía el dispositivo en parte de una *botnet* dedicada al robo de credenciales bancarias. Zitmo significa "*Zeus In The Mobile*" y es una variante del popular *crimepack* Zeus, para dispositivos móviles. La propagación de este troyano es a través de mensajes de texto a través de los cuales simula ser un certificado que le permite al usuario acceder a información de la banca electrónica.

El número de la posible víctima es obtenido a través de una computadora infectada con Zeus, que como parte del engaño invita al usuario a ingresar la información de su celular: marca y modelo y plataforma del mismo. Con esta información el atacante envía un mensaje que contiene el enlace a la descarga de **Zitmo** según los datos ingresados por el usuario. Cuando el usuario selecciona el enlace, descarga lo que supone ser una actualización de seguridad pero no es más ni menos que el troyano:

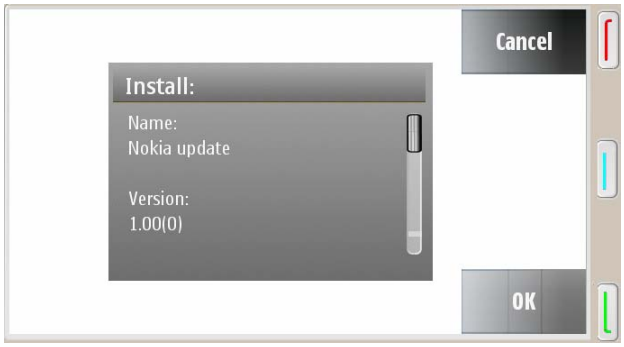

Imagen 3 - Zitmo, supuesta actualización

Entre las características más importantes de Zitmo se destaca que una vez que un equipo ha sido infectado, éste puede ser administrado de manera remota y envía la información a un número de teléfono almacenado como *Admin*.

Los comandos interpretados por este código malicioso permiten especificar qué información será redirigida al atacante, desactivar o activar la captura de mensajes y modificar la lista de contactos. Estos son los principales comandos conocidos:

- BLOCK ON: Ignorar todos los comandos
- BLOCK OFF: habilitar los comandos remotos
- SET ADMIN: cambiar el número del C&C (Centro de Control)
- SENDER ADD: agregar un contacto

- SENDER REM: eliminar un contacto
- SET SENDER: actualizar un contacto

En la siguiente imagen, podemos ver cómo se observan estos comandos en el código de la amenaza:

```
.text:0000E570 ; ---------------------------------------------------------------------------
.text:0000E574 off_E574        DCD dword_2B040         ; DATA XREF: sub_DA4C+44↑r
.text:0000E578 off_E578        DCD aOn                 ; DATA XREF: sub_DA4C+124↑r
.text:0000E578                                         ; "ON"
.text:0000E57C off_E57C        DCD aOff                ; DATA XREF: sub_DA4C+178↑r
.text:0000E57C                                         ; "OFF"
.text:0000E580 off_E580        DCD aBlockOn            ; DATA XREF: sub_DA4C+1CC↑r
.text:0000E580                                         ; "BLOCK ON"
.text:0000E584 off_E584        DCD aBlockOff           ; DATA XREF: sub_DA4C+220↑r
.text:0000E584                                         ; "BLOCK OFF"
.text:0000E588 off_E588        DCD aSetAdmin_0         ; DATA XREF: sub_DA4C+278↑r
.text:0000E588                                         ; "SET ADMIN"
.text:0000E58C off_E58C        DCD aAddSender          ; DATA XREF: sub_DA4C+300↑r
.text:0000E58C                                         ; "ADD SENDER"
.text:0000E590 off_E590        DCD aAddSenderAll       ; DATA XREF: sub_DA4C+33C↑r
.text:0000E590                                         ; "ADD SENDER ALL"
.text:0000E594 off_E594        DCD asc_2B0C8           ; DATA XREF: sub_DA4C+394↑r
```

Imagen 4 - Algunos comandos de Zitmo

Todas las actividades realizadas por esta amenaza se efectúan en segundo plano, evitando que el usuario se dé cuenta que está infectado. Zitmo es una amenaza que funciona en conjunto entre un código malicioso para computadoras y uno para dispositivos móviles logrando el robo de información confidencial del usuario para acceder a sus cuentas bancarias. Existen variantes de esta amenaza para otras plataformas móviles como por ejemplo Android, Windows Mobile y Blackberry. .

Windows Mobile

Microsoft cuenta con su plataforma para dispositivos móviles desde hace algunos años. En sus primeras versiones conocidas como Pocket PC hasta en las más actuales se han introducido distintos cambios en lo que respecta a arquitectura, funcionalidades y seguridad.

En relación a su modelo de seguridad, Windows Mobile utiliza una combinación de políticas de seguridad, roles y certificados para gestionar la ejecución de aplicaciones en el sistema. En otras palabras, la estructura es muy similar a la del sistema operativo Windows para computadoras de escritorio o notebook.

Las políticas de seguridad dan la opción de configurar si una aplicación o instalación se puede ejecutar o debe ser bloqueada, permitiendo solo la instalación y ejecución de aplicaciones firmadas, o caso contrario, preguntarle al usuario antes de efectuar cualquier acción.

En lo que respecta a permisos de ejecución de aplicaciones, existen tres niveles:

- Con privilegios
- Normal
- Bloqueado

Una aplicación que se ejecute con privilegios podrá realizar cambios a nivel de configuración, lo que podría resultar dañino para el sistema ya que cuenta con permisos de acceso completo a archivos del sistema.

Las aplicaciones en Windows Mobile suelen ejecutarse en modo normal ya que de esta manera se restringe la llamada a ciertas API. Cuando una aplicación se ejecuta con este nivel de permisos puede leer pero no escribir en zonas protegidas del registro, archivos del sistema y el directorio \Windows\System.

En lo que respecta a amenazas para esta plataforma, a lo largo de su evolución ha sido objetivo de códigos maliciosos como PMCryptic.exe, detectado por ESET Mobile Security como una variante de *Win32/Agent.ILERAWK*. Esta amenaza, busca copiarse en las tarjetas de memoria y realizar llamadas a números premium, comportamiento similar al ya explicado para otras plataformas. Una vez que se ejecuta este código malicioso, se crean una serie de carpetas en el sistema en donde se alojan los diferentes archivos que son ocultados para evitar ser encontrados en caso de análisis.

Esta amenaza, crea los siguientes archivos en el sistema:

- [TARJETA SD]\2577\autorun.exe
- [TARJETA SD]\2577\[5 CARACTERES ALEATORIOS].exe
- [TARJETA SD]\[NOMBRE DE CARPETA ALEATORIO].exe
- [TARJETA SD]\[NOMBRE DE CARPETA ALEATORIO]\[5 CARACTERES ALEATORIOS].exe
- [TARJETA SD]\[5 CARACTERES ALEATORIOS].exe
- %Windir%\2577\autorun.exe
- %Windir%\2577\[5 CARACTERES ALEATORIOS].exe
- %Windir%\[NOMBRE DE CARPETA ALEATORIO].exe
- %Windir%\[NOMBRE DE CARPETA ALEATORIO]\[5 CARACTERES ALEATORIOS].exe
- %Windir%\[5 CARACTERES ALEATORIOS].exe
- %Windir%\windows.exe
- windows.exe
- system.exe

En la siguiente imagen pueden observarse algunos de estos archivos creados por el malware:

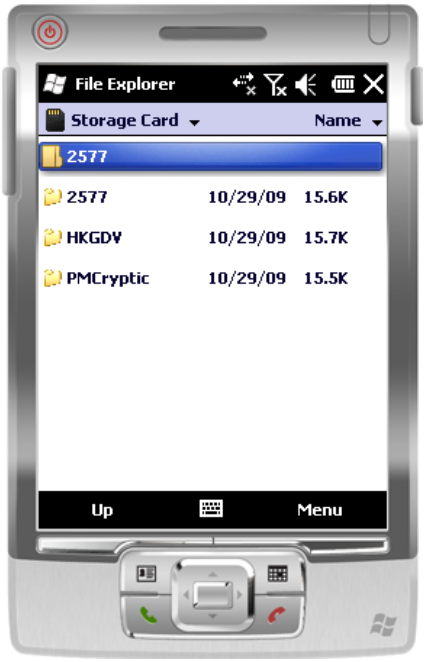

Imagen 5 - PMCryptic.exe archivos creados

iOS

Apple cuenta con iOS, su sistema operativo para plataformas móviles; que incluye al **iPhone**, **iPad** e **iPod**. Actualmente, la última versión de disponible es iOS 5.0.1 desarrollado íntegramente en el lenguaje Objetive-C, C y C++.

Este sistema operativo fue publicado en el 2007 durante la **MacWorld Conference & Expo** en conjunto con el **iPhone**. Desde ese entonces, se han publicado nuevas actualizaciones que incluyeron, entre otras cosas, la posibilidad de ejecutar procesos de forma simultánea (*multitasking*).
En lo que respecta al modelo de seguridad del sistema operativo y las aplicaciones disponibles para esta plataforma, Apple analiza cada una de las aplicaciones antes de que se encuentren disponibles en el Apple Store.

Imagen 6 - iOS 4.3.x

Una de las mayores fallas de seguridad en lo que respecta a los dispositivos con iOS se concreta cuando el usuario realiza el *Jailbreak* del dispositivo. Este proceso brinda la posibilidad de instalar aplicaciones por medios alternativos que no son la propia **Apple Store**. Durante el proceso de liberación para poder instalar aplicaciones no oficiales, se vulnera la seguridad del dispositivo y se lo deja expuesto a amenazas. El *Jailbreak* no es un código malicioso en sí, pero explota vulnerabilidades de iOS para poder ganar privilegios y modificar la configuración del sistema, permitiendo así sobrepasar el modelo de seguridad e instalar aplicaciones.

Entre los códigos maliciosos para la plataforma móvil de Apple, el gusano IKEE, explotó una vulnerabilidad del protocolo de comunicación SSH en teléfonos a los cuales se les había realizado el Jailbreak, cuya cuenta del usuario root tenían la misma contraseña: "airplane".

Una vez que un equipo es infectado con este gusano, el mismo realizaba un escaneo de las direcciones IP de la red 3G y dejaba una copia de sí mismo en todos los dispositivos a los cuales se había realizado el Jailbreak.

L a primera versión de este código malicioso, detectada como IKEE.A fue desarrollada por un adolescente australiano llamado Ashley Town. El gusano modificaba el fondo de pantalla de los dispositivos infectados.

La segunda versión de esta amenaza, denominada IKEE.B o *duh*, se propagó por Europa y utilizó la misma vulnerabilidad de SSH e incluía la conexión a un centro de control (C&C) desde dónde podían recibir comandos. Esta versión del gusano convirtió a los iPhone infectados en zombis de una red botnet.

BlackBerry

Diseñado y creado por Research In Motion (RIM), una compañía canadiense, Blackberry se encuentra en el mercado desde 1999 y es una de las plataformas preferidas por el sector empresarial. Esta preferencia se debe principalmente a que contiene soporte nativo para correo electrónico corporativo a través de MIDP (Mobile Information Device Profile),funcionalidad que permite interacción con Microsoft Exchange, Lotus Dominio o Novell.

Para el desarrollo de aplicaciones para estos dispositivos se encuentran a disposición las API de esta plataforma. A modo de seguridad para la utilización de ciertas funcionalidades, las mismas deben estar firmadas digitalmente.

El núcleo del sistema operativo está basado en C++, aunque el desarrollo de las aplicaciones se realiza en Java.

Imagen 7 – BlackBerry OS 6.0

En lo que respecta a códigos maliciosos para esta plataforma, también se encuentra el caso de Zitmo, que fue presentado anteriormente para Symbian. Esta amenaza que trabaja en conjunto con un código malicioso para computadoras, envía un mensaje de texto y redirige al usuario a la descarga de este troyano.

Zitmo modifica el comportamiento del equipo analizando los mensajes de texto entrante y saliente para ocultar los comandos enviados por el atacante evitando así que el usuario note que su equipo ha sido infectado. Asimismo tampoco aparece en el listado de aplicaciones instaladas para no levantar sospechas.

Robo de información bancaria en dispositivos móviles

Como se mencionó anteriormente, el robo de información bancaria es uno de los objetivos de los cibercriminales. Es por ello que la existencia de *crimepack*, como **Zeus** o **SpyEye**, además de contar módulos de infección para los equipos de escritorio, posee herramientas para vulnerar la seguridad de los dispositivos móviles.

Estos crimepacks han incluido dentro de sus funcionalidades distintas variantes para dispositivos móviles, afectando a Symbian, Blackberry, Windows Mobile y recientemente Android.

El mecanismo de propagación de estos ataques se inicia con la infección de la computadora utilizada por el usuario. Una vez que un equipo es comprometido, comienza a formar parte de una red de computadoras zombis que responde a las órdenes del Botmaster.

Al ingresar a la banca electrónica desde un equipo infectado se presenta ante el usuario una página falsa en dónde se solicita la información correspondiente a su dispositivo móvil, incluyendo el número de teléfono, marca, modelo y sistema operativo. Luego le envía un mensaje de texto que contiene un enlace para descargar la supuesta aplicación de seguridad. Cuando el usuario instala este código malicioso, sus mensajes son enviados al atacante.

El objetivo final de este tipo de ataque es vulnerar los sistemas de doble autenticación que presentan algunas entidades financieras, con la intención de lograr un acceso íntegro a las cuentas del usuario.

Diez consejos para usuarios móviles

Las técnicas de propagación más comunes entre las plataformas móviles incluyen desde el envío de mensajes de texto con un enlace malicioso, hasta la inyección de código en una aplicación oficial para efectuar el robo de información o convertir al dispositivo en parte de una botnet. Es por ello que para a los usuarios móviles, es aconsejable tener en cuenta las siguientes buenas prácticas, para estar protegidos ante códigos maliciosos y otras amenazas informáticas:

1. **Activar el acceso al dispositivo mediante PIN**. Si la terminal lo permite, establecer una contraseña para el desbloqueo de la misma. De esta forma se impide su uso por parte de terceros, así como el acceso a los datos almacenados en caso de pérdida o robo.

2. **Realizar 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.

3. **Activar 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.

4. **Asegurarse siempre que los equipos a los que es conectado el dispositivo estén limpios** y no transmitirán archivos infectados al móvil.

5. **No insertar en el dispositivo tarjetas de memoria** sin haber comprobado antes que están libres de archivos infectados con algún tipo de malware.

6. **Descargar software sólo desde sitios de confianza** o desde las tiendas oficiales (como por ejemplo Apple Store, Ovi de Nokia, Android Market, etc.) y que siempre estén certificadas por los fabricantes.

7. **No acceder a enlaces facilitados a través de mensajes** SMS/MMS no solicitados y que impliquen la descarga de contenidos en el equipo.

8. **Desconectarse siempre de los servicios web** que requieran contraseña antes de cerrar el navegador web.

9. **Instalar un software antivirus**, como ESET Mobile Security, que le permita la detección de amenazas en el teléfono, de forma que impida la ejecución y transmisión hacia otros equipos.

10. **Agendar el número IMEI** (Identidad Internacional de Equipo Móvil) de su teléfono. Este número, único para cada dispositivo móvil en todo el mundo, permite a las operadoras desactivar el teléfono en caso de robo, incluso si se le cambia la tarjeta SIM. Para ver el código, marque *#06#. El teléfono devolverá el código IMEI.

Conclusión

En Latinoamérica, el uso de smartphones se encuentra en aumento. Los usuarios están utilizando sus dispositivos para acceder a su información, las redes sociales y sus cuentas bancarias. Esta amplia utilización de tecnologías móviles, ha derivado en una mayor creación y elaboración de códigos maliciosos para cada una de las plataformas.

Teniendo en cuenta que uno de cada cinco usuarios no protege su smartphone con una solución de seguridad, se abre una brecha muy importante que podría terminar en la fuga de información tanto a nivel hogareño como empresarial.

Durante el 2011, se ha detectado un incremento en los códigos maliciosos que, sin autorización del usuario, reenvían su información hacia distintas direcciones URL, como en el caso de *Android/Lightdd.A*, o *Android/Spy.Geinimi.A*. De esta manera, se está marcando una tendencia en el robo de información y el control de los dispositivos móviles de manera remota.

Además, las nuevas variantes de ZITMO y SPITMO demuestran que los desarrolladores de códigos maliciosos están orientando sus amenazas para vulnerar los sistemas de seguridad y acceder de esta manera a la información que los usuarios poseen en sus dispositivos móviles. Sobre un total de nueve variantes de estas amenazas, cinco de ellas vieron la luz durante el 2011.

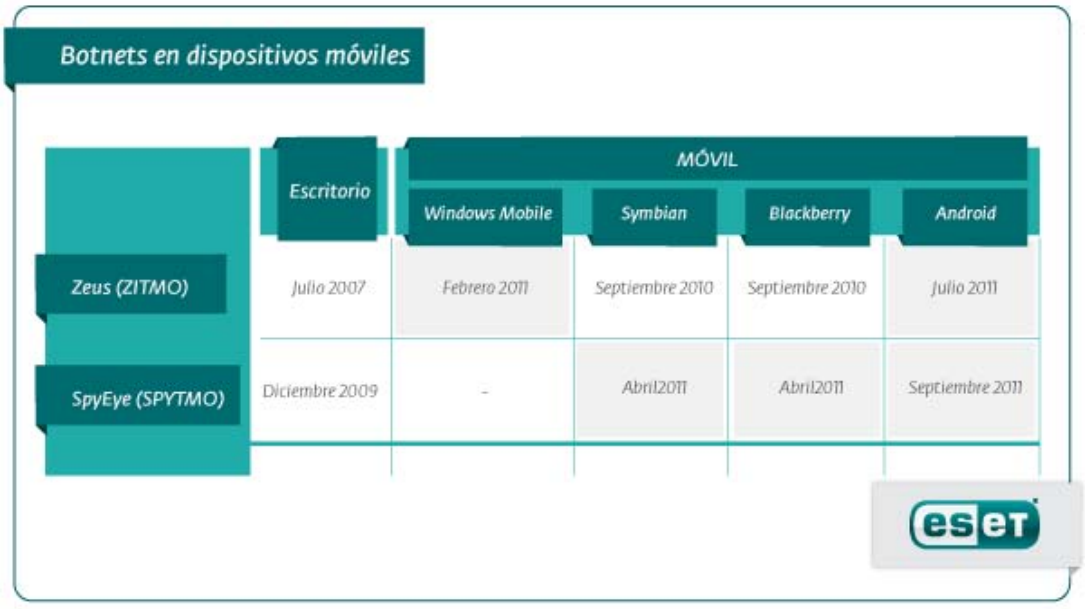

Imagen 8 – Surgimiento de Zeus y SpyEye para equipos de escritorio y móviles

Con la aparición de nuevos usuarios, nuevas aplicaciones y la posibilidad de acceder a sitios como el home banking desde los dispositivos móviles, los desarrolladores de malware están dirigiendo sus ataques a estas plataformas. Algunos de los motivos que justifican esta tendencia son la concentración de información en un solo lugar, la creencia de que no existen amenazas para smartphones y la falta de utilización de una solución de seguridad en los dispositivos.

Según datos de ESET Latinoamérica, más del 80% de los usuarios no cuenta con una solución de seguridad en su dispositivo móvil. Es así como al no proteger su smartphone no solo expone su información a la infección con un código malicioso sino que también, en caso de pérdida o robo del equipo, no puede eliminar la información contenida en él dando lugar a la fuga de información personal o empresarial. En conjunto, todos estos hechos representan una gran brecha en la seguridad, dado que una vez que un equipo se encuentra infectado podría ser conectado a una red hogareña o empresarial propagando la amenaza.

Como se ha observado a lo largo del artículo cada una de las plataformas presenta características que son explotadas por los atacantes ya sea través de códigos maliciosos o Ingeniería Social. Sin importar cuál es la plataforma, el objetivo es acceder a la información del usuario y así poder obtener algún beneficio ya sea a través del robo de credenciales de acceso, envío de mensajes de texto a números *premium*, generación de tráfico en Internet y pago por clic.