UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Seguridad para smartphones con sistema operativo Android orientado a prevenir la infección por malware y mantener la seguridad de la información del usuario

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Germán Iván Rueda Tlazalo

DIRECTORA DE TESIS

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2019

Índice

Agradecimientos

El presente trabajo está dedicado a:

Mis padres: Ma. Isabel Tlazalo Barrera, mamá gracias por todo tu tiempo y paciencia desde aquel momento en que inició mi educación básica ya que desde el pre-escolar tuviste la dedicación para enseñarme y explicarme las cosas que en su momento fueron nuevas para mí. Tu dedicación y cariño fueron la base para que pudiera pasar por los siguientes niveles en mi educación y hoy día llegase el momento de estar a punto de concluir un ciclo de mi educación superior.

Arturo Rueda Albino, papá gracias por haberme apoyado dándome la posibilidad y las facilidades de haber terminado la carrera, agradezco el esfuerzo que realizaste para darme las comodidades que sé, tú no tuviste cuando pasaste por la educación universitaria y hasta el día de hoy me sigas apoyando en diversas situaciones, otra cosa que agradezco es que siempre has estado presente en momentos importantes y actividades que han significado mucho para mí.

Papás son lo más importante que tengo y los amo, cualquier cosa que pueda hacer para retribuirles lo mucho que me han dado sin duda es poco para lo que se merecen.

Mis abuelitos: Arturo Rueda López, Isabel Albino de la Luz, José Tlazalo Zayas y Ma. Isabel Barrera; abuelitos a pesar de que tres de ustedes ya no están entre nosotros físicamente para mí su presencia está presente cada día de mi vida, por los consejos y muy buenos momentos que pasé a su lado, ustedes fueron un gran impulso para lograr superar ciertas situaciones difíciles que acontecieron a lo largo de mi formación como profesionista y gracias a eso es que puedo presentar este trabajo con el fin de cerrar este ciclo de mi formación universitaria. Además, gracias a ustedes tengo a unos excelentes padres.

Mis tíos: Sergio, Julio, Felipe, Pimi, Alejandro, Fernando, Elizabeth, Genoveva, Maximino, Armando y Catalina. Gracias a todos ustedes por estar presentes y brindarme su apoyo en diversos aspectos de mi vida, ustedes han aportado en mi formación desde el momento en que convivo con ustedes

en el día a día, así como cuando se acercaron a darme algún consejo y alentarme para aplicarme en mis estudios.

Mis primos, a todos ustedes también les agradezco por ser parte de mi vida y aportar a ella con las experiencias que hemos pasado y que han significado aprendizajes. Quiero hacer una mención para Isabel, Diana y Gabi; ustedes que están iniciando su formación universitaria en la máxima casa de estudios, la UNAM, pongan su mayor empeño para concluir de la mejor forma posible y así aprovechen el sacrificio que mi tía Cata hace por ustedes.

Mis amigos, con quienes he tenido el honor de convivir desde el ámbito escolar hasta el laboral sin duda han presentado experiencias, aprendizajes que han contribuido y a forma a la persona que soy. Para Led y Gerardo, el tener la oportunidad de vivir situaciones con ustedes a lo largo de nuestro paso por la Facultad sin duda hizo muy ameno todo ese tiempo y estrés al que nos enfrentamos.

Mi asesora de tesis la M. en ciencias, la ingeniera Ma. Jaquelina López Barrientos, gracias por haberme aceptado como su tesista, así por el tiempo que dedicó en guiar mi trabajo hasta este momento en que por fin se tiene concluido.

Por último y no menos importante sino por el contrario, a la Universidad Nacional Autónoma de México que me abrió sus puertas desde que inició mi formación en el CCH oriente y ahí fue donde definí y me decidí por una ingeniería la cual cursé en la H. Facultad de Ingeniería que me brindó la oportunidad de ocupar un lugar en sus instalaciones para formarme como ingeniero en computación y así poder aportar al mundo laboral de mi México con los conocimientos que en ella obtuve.

Introducción

SEGURIDAD PARA SMARTPHONES CON SISTEMA OPERATIVO ANDROID ORIENTADO A PREVENIR LA INFECCION POR MALWARE Y MANTENER LA SEGURIDAD DE LA INFORMACION DEL USUARIO

En los teléfonos móviles ha habido una evolución muy notable en cuanto a sus funcionalidades en los últimos años, ya que hoy en día van más allá de mantener comunicadas a las personas mediante voz o mensajes de texto. El avance tecnológico ha permitido que estos dispositivos disminuyan su peso y tamaño, además de incorporar funciones tales como: agenda electrónica, fotografía y video digital, video llamadas, GPS, reproducción de música, correo electrónico, entre otras.

La integración de todas estas funciones en el teléfono móvil se logra mediante una plataforma, que es capaz de gestionar los módulos de hardware y software con el fin de llevar a cabo actividades semejantes a las de una computadora personal, es así como nace el término de teléfono inteligente o smartphone.

Entre los sistemas operativos móviles empleados por los smartphones están: Android (de google), iOS (de Apple), Windows Phone (de Microsoft), BlackBerryOS (de BlackBerry), Bada (de Samsung), Symbian (de Nokia), Firefox (de Mozilla), webOS (de HP) y Ubuntu Touch (de Ubuntu).

De acuerdo con el estudio de la consultora Gartner en noviembre de 2013, los tres principales sistemas operativos móviles con mayor presencia en el mercado internacional son: Android en primer lugar con el 81.9%, seguido por iOS con 12.1% y en tercer lugar Windows Phone con 3.6%.

Por otra parte la firma Kantar Worldpanel publicó a principios de 2014 un estudio en el cual Android terminó el 2013 dominando los mercados de Europa, China, Estados Unidos de América y América latina. Por ejemplo en Europa mantiene un 68.6% del mercado, mientras que Apple le sigue con 18.5% y en tercer lugar está Windows Phone con 10.3% (los países considerados fueron: Reino Unido, Alemania, Francia, Italia y España). Mientras que en América Latina (los países que participaron en el estudio fueron Argentina, Brasil y México) el comportamiento fue de la siguiente forma: Android abarcó un 83.5%, seguido de Windows Phone con el 4.9%, iOS con 4.3%, Black Berry con el 2.8%, mientras que el 4.5% restante lo abarcaron “otros” sistemas operativos.

Como se puede apreciar por parte de ambos estudios, el sistema operativo líder en el mercado de los smartphones es Android, seguido de iOS y Windows Phone. Esto implica que poseen un gran

número de usuarios que operan sus datos personales por medio de los smartphones para diversos fines, este es uno de los principales incentivos por lo cual los creadores del malware hayan decidido ampliar su rango de acción a estos dispositivos, debido a que su uso se ha generalizado y el mercado está en continua expansión.

Algunos objetivos de los creadores de software malicioso son:

Nombres de usuario y contraseñas: La obtención de estos valores permitirá suplantar la identidad de la persona a la que le han sido sustraído los datos, además de permitir al atacante tener acceso a las cuentas de los diferentes servicios que utilice la víctima.

Datos de formularios: Los formularios más deseados por los atacantes podrían ser los relativos a compras online, debido a que los datos pueden traducirse en beneficios económicos, como son los referentes a las tarjetas de crédito.

Datos y documentos privados: Aparte de los datos personales específicos, también se tiene gran interés en la obtención de documentos que solo están disponibles en círculos cerrados. Concretamente, el atacante podría enfocarse en fotografías, correos electrónicos, así como en mensajes SMS o MMS, en algunos casos el atacante llegaría a pedir dinero a la víctima a cambio de no revelar la información sustraída.

Mensajes Premium: Existe cierto tipo de malware que se encarga de dar las ordenes al smartphone para enviar mensajes a números premium sin el consentimiento de la víctima. Otra variedad de este ataque no implica la infección por parte de código malicioso, sino que hace uso de ingeniería social y consiste en instar a la víctima a realizar una llamada o enviar un mensaje a los números premium, con la promesa de que recibirá un premio o recompensa por el envío del mensaje.

Secuestro del dispositivo: Esto hace referencia a que cierto malware conocido como “ransomware” bloquea el acceso a la información o a ciertas funcionalidades, solicitando un rescate para recuperar el estado funcional del dispositivo.

Botnets: Las botnets son redes formadas por un gran número de dispositivos infectados conocidos como bots o zombis. Estos dispositivos están controlados por un programa malicioso, que permite manejarlos de forma remota por un dispositivo central, encargado de monitorear toda la red y de

dar órdenes a los zombis. Algunas de las funcionalidades son el envío de información sobre el hardware del dispositivo, así como información sensible de la víctima (contactos, datos de red, IMEI, etc.).

Algunas formas de infección empleadas por los atacantes son: las redes sociales, correo electrónico, tiendas de aplicaciones, redes locales (WiFi), sólo por mencionar algunas.

El malware en Android se mantendrá al alza, por ser el sistema operativo que cuenta con gran número usuarios, que en otras palabras representan víctimas potenciales para los atacantes. Con base en datos de kaspersky lab, desde el año 2012 se logró identificar tres grupos principales de malware: Troyanos SMS, adware y exploits para acceder a la raíz del dispositivo.

Para 2013 Android siguió siendo el blanco de los ataques maliciosos con un 98.05%. De estos ataques la mayoría tenía como objetivo robar dinero a las víctimas, durante el transcurso de ese año la cantidad de programas maliciosos para phishing, robo de información de tarjetas de crédito y robo de dinero de las cuentas bancarias de los usuarios se multiplicó. A continuación se muestra una gráfica con distribución de los principales tipos malware durante ése año.

Para el primer trimestre de 2014, las amenazas para Android han superado el 99% del total de amenazas para dispositivos móviles. Los módulos publicitarios (Adware), cuya principal función es mostrar publicidad (mientras extraen información sensible del usuario o del dispositivo), ocupan el primer lugar de la estadística, mientras que los troyanos SMS, que durante largo tiempo dominaron el campo del malware móvil, han bajado al segundo puesto y durante el trimestre su cantidad ha caído del 34% al 22%. Sin embargo esta categoría sigue teniendo una presencia significativa en los programas maliciosos móviles detectados.

El código malicioso se aprovecha de vulnerabilidades tanto de los sistemas operativos como de los usuarios, pero al existir varias herramientas que brindan protección a estos dispositivos ante ciertos ataques, es difícil para los usuarios primero saber que su dispositivo móvil está en riesgo o incluso saber si ha sido víctima de algún ataque, y si observa o nota que hay cambios en su configuración, cargos que no reconoce en su estado de cuenta o cualquier otra afectación, saber qué hacer o qué tipo de herramienta ejecutar o qué y cómo configurar para su protección. Así, se vuelve

indispensable contar con una guía de seguridad que incluya buenas prácticas dirigidas a los usuarios para que mantengan tanto su dispositivo y su información bajo un buen resguardo.

Objetivo general:

- Establecer una guía de seguridad que incluya buenas prácticas dirigidas a los usuarios de smartphones, con el fin de: prevenir la infección de código malicioso y brindar parámetros para mantener la seguridad de su información.

Objetivos particulares:

- Identificar los sistemas operativos más propensos a la infección por malware e identificar los tipos de código malicioso más comunes.
- Conocer y analizar el malware en los smartphones y sus afectaciones a la seguridad de la información de los usuarios.
- Proporcionar parámetros a los usuarios para que identifiquen si su dispositivo está infectado por algún tipo de malware. Así como para detectar los sitios seguros para la descarga de aplicaciones.
- Establecer la guía de seguridad con el fin de prevenir infecciones por malware que puedan hacer mal uso de la información del usuario.

De manera que para alcanzar los objetivos planteados, este trabajo se compone de 5 capítulos, donde:

En el primero de ellos titulado "Impacto de los smartphones en la sociedad", se expone la evolución de los teléfonos móviles que en un inicio eran dispositivos de gran tamaño y peso considerable, dedicados únicamente a llamadas de voz, pero que con el avance de la tecnología y respondiendo a las necesidades del día a día de los usuarios, los teléfonos móviles fueron integrando funcionalidades que permiten agilizar el trabajo del usuario así como tener una opción de entretenimiento e interacción con otras personas. En este capítulo se hace mención que el auge de estos dispositivos los posiciona como objetivos de los ciberdelincuentes ya que cubren un mercado en constante crecimiento y la información que se procesa en ellos es un punto de interés para obtener un beneficio económico.

En el segundo, titulado: “El malware en los principales sistemas operativos de smartphones”, se presenta lo que es el malware, la evolución de éste, debido a que dejó de tener como principal objetivo de ataque a las computadoras convencionales para pasar a lo que actualmente se conoce por smartphones. Además se presentan datos por zona geográfica de las infecciones por malware en smartphones en los principales sistemas operativos.

Así, en el tercer capítulo: “La seguridad en los smartphones”, se muestran los conceptos de seguridad de la información y seguridad informática, así como la seguridad en estos dispositivos que se vuelve un punto muy importante debido a la información que los usuarios manejan por medio de los smartphones. También se hace una revisión de las amenazas, vulnerabilidades, riesgos y ataques ante los cuales los smartphones y los usuarios están expuestos.

Avanzando en el presente trabajo, se tiene el capítulo cuarto: “Análisis de malware”, en el cual se exponen las bases de la elaboración para el laboratorio, dedicado a analizar una muestra de código malicioso, partiendo desde los recursos de hardware y software con los que se cuentan para hacer posible el análisis de una muestra de una aplicación infectada; que expone una visión muy amplia de cómo la información confidencial de los usuarios se ve comprometida y da lugar al capítulo final.

“Guía de seguridad para Smartphones con sistema operativo Android”, es el título del quinto y último capítulo en donde se proporcionan una serie de medidas básicas con la finalidad de que al aplicarlas el usuario final de un Smartphone tenga un grado razonable de seguridad sobre éste y sobre la información que opera en él. Las medidas descritas en este último capítulo se enfocan en las dos amenazas más comunes a las cuales un usuario está expuesto en su día a día, que son: el malware y el robo o pérdida del dispositivo.

Capítulo 1

Impacto de los Smartphones en la sociedad

1.1. Aparición y evolución de los smartphones.

El smartphone o teléfono inteligente es un término comercial que se ha asociado al teléfono móvil que permite realizar actividades similares a las de una computadora personal en relación al procesamiento y almacenamiento de la información, además de poseer mayor conectividad que un teléfono móvil[1] común. Este concepto se ha desarrollado desde la década de los años noventa, pero a partir del año 2007 se popularizó con el lanzamiento del iPhone de Apple.

En su origen el concepto de smartphone se desarrolló pensando en la gente de negocios, integrando al teléfono móvil características propias de un PDA (Personal Digital Assistant), como son: calendario, agenda, procesador de texto, entre otros. Es así que en 1992 IBM diseña y desarrolla un dispositivo que integraba las funciones de un teléfono móvil y un PDA de aquella época, denominado "IBM Simon Personal Communicator", este dispositivo empleaba una interface basada completamente en un pantalla táctil, como se puede apreciar en la figura 1.1.

Figura 1.1 IBM Simon Personal Communicator.

La comercialización de este dispositivo no se hizo bajo el concepto de smartphone y sólo estuvo a la venta en los Estados Unidos de América durante agosto de 1994 y febrero de 1995 por parte de la BellSouth Corporation. El Simon de IBM sólo funcionaba en 190 ciudades a lo largo de 15 estados de ese país, lo que representaba una opción poco favorable para las personas que viajaban constantemente y necesitaban una comunicación eficiente, aun así se vendieron aproximadamente 50 000 unidades, teniendo un costo aproximado entre $1 100 y $900 dólares. Algunas de sus especificaciones se muestran en la tabla 1.1.

Tabla 1.1 Especificaciones técnicas del IBM Simon Personal Communicator.

Desarrollador:	IBM
Comercializador:	BellSouth Corporation
Sistema operativo:	Data light ROM-DOS (Compatible con MS-DOS)
CPU:	Vadem 16 MHz, 16-bit, compatible con una arquitectura x86.
Masa:	510 gramos.
Dimensiones:	Altura de 200 mm, ancho de 64 mm y profundidad de 38 mm.
Pantalla:	LCD monocromática táctil a través de estilete o dedos. Dimensión: 114x36 mm Resolución: 160x293pixeles
Memoria:	RAM: 2 MB ROM: 2 MB
Interfaz:	PCMCIA, que resultaba de gran utilidad para instalar nuevas funcionalidades a partir de programas de terceros.

En Europa en el año de 1996 Nokia lanzó su modelo Nokia 9000 de la serie Communicator, éste al igual que el Simon de IBM combinaba en un dispositivo las funciones de un teléfono móvil con las de un PDA, siendo comercializado con el nombre de “PDA-Phone”.

Figura 1.2 Nokia 9000.

Este dispositivo en comparación con el de IBM poseía un tamaño y peso relativamente menor y fue el primer predecesor de los smartphones de esta compañía finlandesa, algunas de las sus especificaciones se muestran en la tabla 1.2. Un aspecto relevante de los productos de Nokia es que el modelo Nokia 9210 de la serie Communicator fue el primer dispositivo en emplear el sistema operativo SymbianOS, este sistema operativo es importante porque durante algunos años tuvo una presencia en el mercado altamente dominante.

Tabla 1.2. Especificaciones técnicas del Nokia 9000.

Desarrollador:	Nokia
Sistema operativo:	GEOS V3.0
CPU:	Intel 386EX, 24 MHz. Set de instrucciones x86(i386)
Masa:	397 gramos.
Dimensiones:	Altura de 173mm, ancho de 64 mm y profundidad de 38 mm.
Memoria:	RAM: 4 Mb. ROM: 4Mb. De los cuales 2Mb eran accesibles por el usuario para almacenar información.
Pantalla	Principal: Monocromática con 4 escalas de grises. Resolución: 640 x 200 pixeles. Secundaria: Monocromática con 2 escalas de grises. Resolución: 50 x 38 pixeles
Teclado:	Principal: QWERTY de 74 teclas. Secundario: Numérico de 21teclas.
Bandas de frecuencia:	GSM 900 y GSM 1800
Interfaces:	Serial RS-232 con capacidad de transferencia de 115.2 Kbps Puerto infrarrojo con capacidad de transferencia de 115.2 Kbps

Para el año de 1997 Ericsson lanzó el modelo GS88, este dispositivo fue el primer teléfono móvil en comercializarse bajo el concepto de “Smart Phone” como se puede observar en la figura1.3, pero al igual que los dos teléfonos móviles que se han mencionado anteriormente era la fusión de un PDA

con un teléfono celular. Contaba con el sistema operativo GEOS V3.0. (El mismo del Nokia 9000 como se muestra en la tabla 1.2), también empleaba la banda GSM 900 y contaba con la función de poner el dispositivo en modo vuelo, desactivando todas las comunicaciones inalámbricas. Este dispositivo es muy similar tanto en su diseño como en sus funcionalidades al Nokia 9000 por lo que no hubo característica alguna que marcara gran diferencia entre ambos dispositivos.

Figura 1.3. Ericsson GS88 Smart Phone

En este mismo año Nokia lanzó el modelo 9000i, que posee prácticamente todas las características técnicas como en diseño del modelo 9000, con la única excepción de estar diseñado para soportar la banda GSM 1900 que es usada en la mayoría de los países de América.

A partir del año 2000 se produjo un aumento significativo en la comercialización de smartphones de diversos fabricantes que evolucionaban introduciendo nuevas características y funcionalidades, por ejemplo: reducción en peso y tamaño, pantallas a color, incremento en la capacidad de almacenamiento, navegadores de internet, cámaras, reproductores de música, infrarrojos, bluetooth, por mencionar algunos. Dentro de los acontecimientos más importantes de esos años están: el lanzamiento del primer smartphone de BlackBerry en 2003, el surgimiento de Windows Mobile, pero la marca que revolucionó el mercado de los teléfonos inteligentes fue Apple.

En enero de 2007 durante la inauguración de la MacWorld, Steve Jobs presentó por primera vez el iPhone con su sistema operativo iPhone OS, con las siguientes palabras: “An iPod, a Phone and an Internet Communicator”, y sería hasta junio de ese año que saldría oficialmente a la venta, teniendo un precio de $599 dólares. Dentro de los factores de éxito por los cuales el iPhone destacó

en el mercado de los smartphones es por convertirse en un centro de medios móvil, cambiando así la concepción de que los teléfonos inteligentes estaban diseñados exclusivamente para las personas de negocios (ejecutivos), otro aspecto de su éxito fue la interfaz que era muy amigable e intuitiva para el usuario esto gracias a su sistema operativo iPhone OS, por último dentro de su diseño cabe destacar su pantalla que para ese momento era considerada una de las más grandes y con mejor definición, característica que lo hacía más atractivo.

En 2008 se pone a la venta el smartphone HTC Dream, siendo el primer dispositivo móvil de comunicación en implementar el sistema operativo de Google, Android, basado en el kernel de GNU/Linux. Este dispositivo tuvo un costo aproximado de $180 dólares en E.U.A, siendo más accesible que el iPhone. Por otra parte en Junio de este año Apple lanzó el iPhone 3G, entre sus principales innovaciones estuvieron: GPS asistido, soporte para voz y datos mediante 3G1, Tribanda2, con sistema operativo iPhone OS 2.0 y la integración de la App Store, en la cual se pueden obtener aplicaciones de terceros. Google en respuesta del lanzamiento de la App Store, lanzó en Agosto del mismo año su tienda de aplicaciones Android Market.

Durante 2009, en el mes de mayo Nokia también sacó al mercado su tienda de aplicaciones denominada Ovi Store. En Junio salieron a la venta los siguientes smartphones: el iPhone 3GS (con sistema operativo iPhone OS 3.0), el Samsung Galaxy i7500 (siendo el primer smartphone de Samsung con sistema operativo Android y poniendo fin a su sistema operativo Bada) y el Palm Pre con el sistema operativo WebOS que sustituyó al fallido sistema Palm OS, debido a que éste último no era capaz de soportar 3G. Durante el mes de septiembre Nokia puso a la venta su modelo N900 con sistema operativo Linux Maemo 5, basado en debían GNU/Linux.

Para el año de 2010, en el mes de marzo Sony lanzó al mercado el modelo Xperia X10 siendo su primer smartphone con sistema operativo Android, dejando atrás a Windows Mobile de Microsoft. En junio Samsung anunció el lanzamiento de su modelo Galaxy S, este dispositivo fue elegido el

1 3G: Es la abreviación de la tercera generación de transmisión de voz y datos para la telefonía móvil mediante UMTS (Universal Mobile Telecommunicatios System).

2 Tribanda: Termino en telecomunicaciones para referirse a un dispositivo capaz de soportar las bandas GSM 900/1800/1900 MHz (usadas generalmente en Europa, Asia, África y uso limitado en Norteamérica) o las bandas 850/1800/1900 MHz (usadas en América y de uso limitado en el resto del mundo).

mejor smartphone del año por parte de la Asociación Europea de Imagen y Sonido (EISA) por contar uno de los GPU más novedosos de entonces capaz de dibujar 20 millones de triángulos por segundo. En este mismo mes Apple lanzó su iPhone 4 con sistema operativo iPhone OS 4, durante la presentación de este dispositivo Steve Jobs anunció que iPhone OS pasaría a ser llamado oficialmente iOS.

En el año de 2011, durante el mes de febrero Stephen Elop CEO de Nokia y Steve Ballmer CEO Microsoft anunciaron su asociación comercial con el objetivo de que Nokia adoptaría como principal sistema operativo a Windows Phone para sus futuros smartphones de la serie Lumia, reemplazando tanto a Symbian como a MeeGo. En el mes de mayo Samsung lanzó a la venta su nuevo modelo Galaxy SII con sistema operativo Android 4.1.2. Para el mes de agosto Google anunció oficialmente la compra de Motorola, cabe hacer la aclaración que esta compañía se separó en dos empresas: Motorola Solutions y Motorola Mobile, siendo adquirida únicamente la división móvil por parte de Google. Por otra parte en el mes de septiembre Nokia lanzó su modelo N9 con sistema operativo MeeGo, este sistema surge de la unión de los sistemas operativos Maemo de Nokia y Moblin de Intel, teniendo como objetivo competir con Android. En octubre Apple anunció la salida al mercado del iPhone 4S con el sistema operativo iOS 5, mientras que Samsung lanzó su modelo Galaxy Note el cual iniciaría una nueva tendencia conocida como "Phablet" que viene de la fusión de un smartphone con una tableta. En noviembre Nokia lanza su primera generación de smartphones Lumia con el sistema operativo Windows Phone 7, con los modelos Lumia 710 y Lumia 800.

En el año de 2012, durante el mes de mayo Samsung puso a la venta su modelo Galaxy S III contando con notables características, entre las cuales destacan:

- Smart Stay: Hace referencia a que la pantalla del dispositivo permanece encendida mientras el usuario dirige la mirada hacia ella.
- Direct Call: Permite al usuario llamar a una persona cuyos mensajes de texto se encuentran actualmente en la pantalla con sólo dirigir el teléfono al oído.
- Pop Up Play: Permitiendo reproducir un video en pantalla mientras se realizan otras tareas en el dispositivo.
- Y referente al hardware, está: un procesador de cuatro núcleos Exynos 4412 a una frecuencia de 1.4 GHz, procesador gráfico (GPU) ARM Mali-400 de cuatro núcleos al igual que su

predecesor, carga inalámbrica, pantalla Súper HD de 4,8 pulgadas, memoria interna de 16 o 32 GB, RAM de 1GB, capacidad de soportar tarjeta Micro SD de 64 GB y cámara de 8 mega pixeles capaz de grabar en HD (1080 pixeles).

En el mes de septiembre se lanzaron los siguientes teléfonos inteligentes:

- El primero de estos lo lanzó Nokia iniciando así su segunda generación de smartphones Lumia con sistema operativo Windows Phone 8, con el modelo Lumia 920 con las siguientes características: microprocesador de doble núcleo Qualcomm Krait Snapdragon de 1.5 GHz y pantalla 4.5" HD LCD, una cámara trasera de 8.7 mega pixeles, almacenamiento de 32 GB, memoria RAM de 1 GB y posibilidad de carga inalámbrica.
- El segundo dispositivo corresponde al iPhone 5 algunas de sus características son las siguientes: sistema operativo iOS 6, un procesador Apple A6 doble núcleo de 1.2 GHz, cámara trasera de 8 mega pixeles, 1 GB de memoria RAM y capacidad de almacenamiento interno de 16, 32 y 64 GB.
- El tercero es el Samsung Galaxy Note II, destacando por las siguientes características: una pantalla HD de 5,55 pulgadas, es más largo y más fino, con una capacidad de batería mayor, y un procesador de cuatro núcleos que multiplica su poder respecto a la versión anterior. Conserva el uso del "S Pen", un estilete que posibilita utilizar mejor las capacidades del phablet. También posee la opción de poner una "doble pantalla", es decir, la pantalla partida en dos, lo que permite hacer dos cosas a la vez.

En 2013 los smartphones más destacados fueron los siguientes:

- Samsung Galaxy S4, lanzado el 14 de marzo. Con este dispositivo Samsung alcanzó un record de ventas, ya que en los primeros 4 días se vendieron 4 millones de unidades, y para octubre de ese mismo año alcanzó los 40 millones. Dentro de sus innovaciones más importantes destacan, su diseño que lo hacen más delgado, ligero y estilizado, su cámara de 13 mega pixeles, sus sistema operativo Android con la versión 4.2.2, pantalla de 5 pulgadas Super Full HD, por mencionar algunas.
- En el mes de julio Nokia lanzó el modelo Lumia 1020 con una cámara de 41 mega pixeles, contando con un sistema operativo Windows Phone 8. Este smartphone destacó por su extraordinaria cámara así como el software que hace del uso de la cámara una experiencia muy agradable, obteniendo fotos de un estilo profesional.

- El iPhone 5S de Apple se lanzó en septiembre, éste dispone de un procesador doble núcleo con frecuencia de 1.3GHz y arquitectura de 64 bits convirtiéndose así en el primer dispositivo celular producido con esta tecnología. Además, destaca su tecnología touch ID de reconocimiento de huellas dactilares para desbloquear el teléfono, utiliza el último sistema operativo iOS 7 y una pantalla táctil de 4 pulgadas y cámara trasera de 8 mega pixeles.

1.2. Tendencia en el mercado de los smartphones.

Como se mostró previamente la evolución en hardware y software que han tenido los smartphones con el transcurso de los años desde su aparición ha marcado una gran diferencia tanto en la capacidad de procesamiento como en la de almacenamiento de información, lo que ha permitido que sean más útiles en el día a día de los usuarios ya que integran características que hasta hace algunos años eran exclusivas de las computadoras portátiles, además de ser más prácticos y contar con una mayor conectividad.

Por estos motivos, el mercado de los smartphones ha tenido un incremento notable en los últimos años, de acuerdo a un estudio realizado por la Strategy Analytics en 2011, los mercados de Europa y Norteamérica mostraron el principal crecimiento a partir de 2009, como se muestra en la gráfica de la figura 1.4, aproximándose a los 500 millones de dispositivos vendidos.

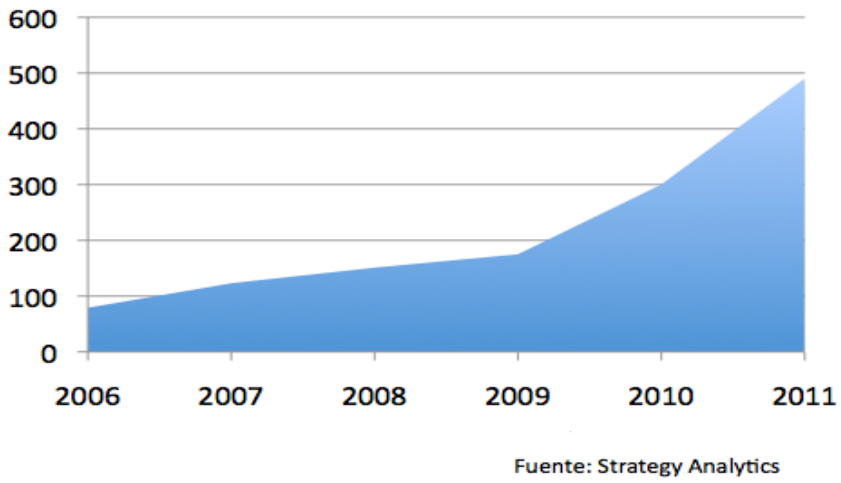


Figura 1.4. Ventas de smartphones (en millones de unidades) durante 2011.

Ese mismo estudio también proporciona el comportamiento de los principales fabricantes durante 2011, siendo Apple y Samsung las principales marcas en ventas, tendencia que se mantiene actualmente. Además indicó como Nokia a partir de 2010 tuvo un decremento en sus ventas después de haber sido líder en el mercado, como lo indica la figura 1.5.

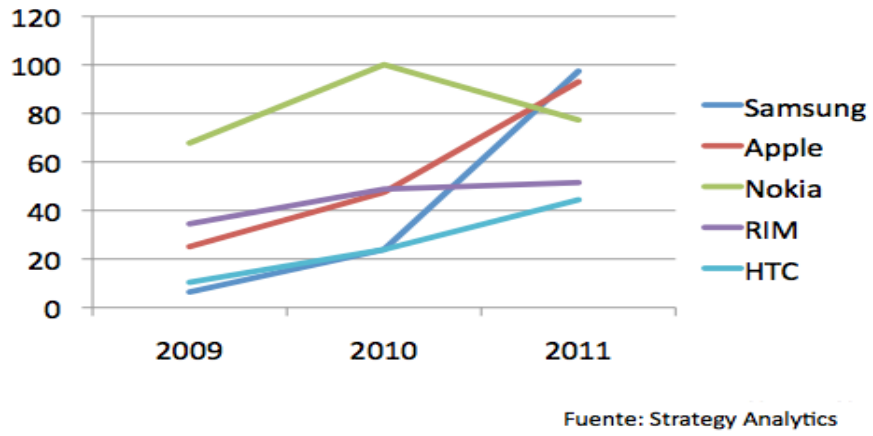


Figura 1.5. Evolución de las ventas (en millones de unidades) de smartphones por fabricante.

Un factor que ha contribuido al auge del mercado de los smartphones es la tendencia con el nombre de bajo costo, que surgió para enfocarse a mercados en desarrollo que representan un mercado con gran potencial para los fabricantes de estos dispositivos, debido a la lentitud con que se renuevan los smartphones en mercados maduros. Esta tendencia surge para hacer más asequibles los smartphones teniendo como fin llegar a cualquier persona rompiendo la creencia de que estos dispositivos son exclusivamente para las personas con altos ingresos (smartphones de gama alta).

Con base en la información de la CEA (Asociación Electrónica de Consumo por sus siglas en inglés), señala que en México los usuarios prefieren adquirir un smartphone de bajo costo en lugar de uno de gama alta, teniendo como estimado gastar $2 000 pesos por un celular nuevo.

Por otra parte un artículo publicado en El financiero en mayo de 2014, indica que los smartphones de bajo costo están teniendo una aceptación muy favorable por parte del mercado mexicano, según datos de la consultora IDC (International Data Corporation) a partir del segundo trimestre de 2013 se comenzaron a vender smartphones con precios que rondan los $1 500 pesos, sin la necesidad de contratar un plan de datos. La creciente demanda de este tipo de dispositivos en el país se atribuye a lo accesible de sus precios teniendo como principal objetivo aumentar las ventas, que de acuerdo

al artículo, en 2012 se cerraron en 12.9 millones de unidades, para 2013 aumentaron a 20.48 millones, estimando que en 2014 se eleven a 37.27 millones de unidades, y se prevé que a futuro rebasen los 50 millones de unidades según el instituto federal de telecomunicaciones (IFT).

Además un estudio publicado por google en 2013 reveló que el 37% de la población mexicana cuenta con un smartphone, también proporciona datos sobre el uso de smartphones por parte de usuarios mexicanos que participaron en dicho estudio, destacando los siguientes aspectos:

- 73% se considera cada vez más dependiente de su dispositivo.
- El uso que se le da a estos dispositivos en diversos lugares es el siguiente: 96% lo utiliza en casa, un 90% en el trabajo, 88% en restaurantes, 84% en movimiento (esté donde esté), 83% en cafeterías, el 82% en un evento social, 80% en el transporte público, en la escuela un 74%, en una consulta médica el 70% y en el aeropuerto un 69%.
- 48% se conectó a internet a través de su teléfono.
- 40% de los participantes prefiere dejar de ver la televisión antes de dejar de usar su smartphone.
- 97% de los usuarios accede a redes sociales a través de su teléfono.
- 33% realizaron una compra mediante su dispositivo.
- 91% buscó algún producto o servicio.
- 93% de los participantes muestra interés por la publicidad presentada en aplicaciones o navegadores.

Por otro lado a principios de 2014 Deloitte publicó un estudio que involucró a dos grupos conformados por los países que se indican en las tablas 1.3 y 1.4, que se muestran a continuación.

Tabla 1.3. Corresponde a países desarrollados que integraron el grupo 1.

Fuente: Deloitte Global Mobile Consumer Survey 2013.

País	Muestra
Bélgica	2000
Finlandia	1000
Francia	2000
Alemania	2000
Japón	2000
Holanda	2000
Portugal	607
Singapur	2000
Corea del Sur	2000
España	2000
Reino Unido	4020
Estados Unidos	2000

Tabla 1.4.Correspondiente a países en desarrollo que integran el grupo 2.

Fuente: Deloitte Global Mobile Consumer Survey 2013.

País	Muestra
Argentina	2000
Brasil	2000
China	2000
India	2000
Indonesia	2000
México	2000
Rusia	2000
Turquía	1000

En este estudio se revelaron datos interesantes como los siguientes:

- Los smartphones lideran el interés de compra de los usuarios, tanto en mercados desarrollados como en desarrollo, como lo indican las figuras 1.6 y 1.7.

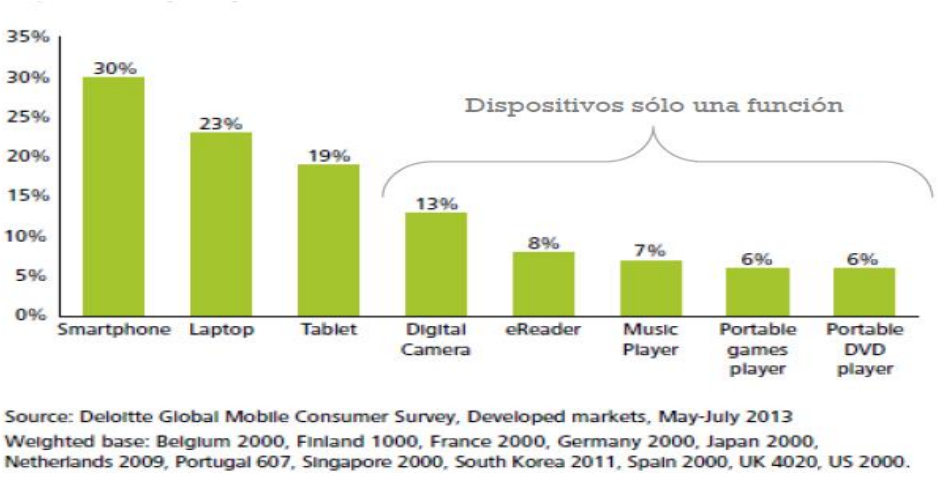
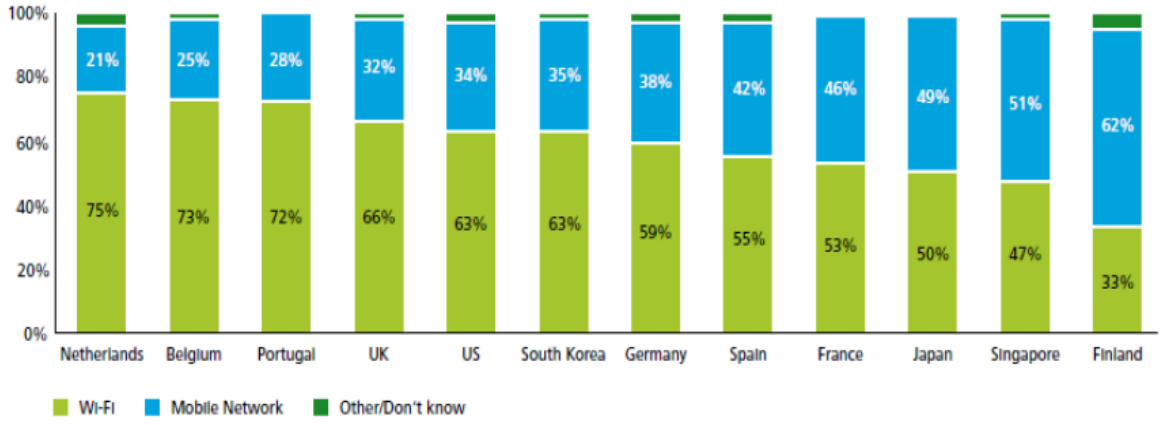


Figura 1.6. Gráfica que representa el interés de compra de los usuarios hacia dispositivos multifuncionales en los mercados desarrollados.

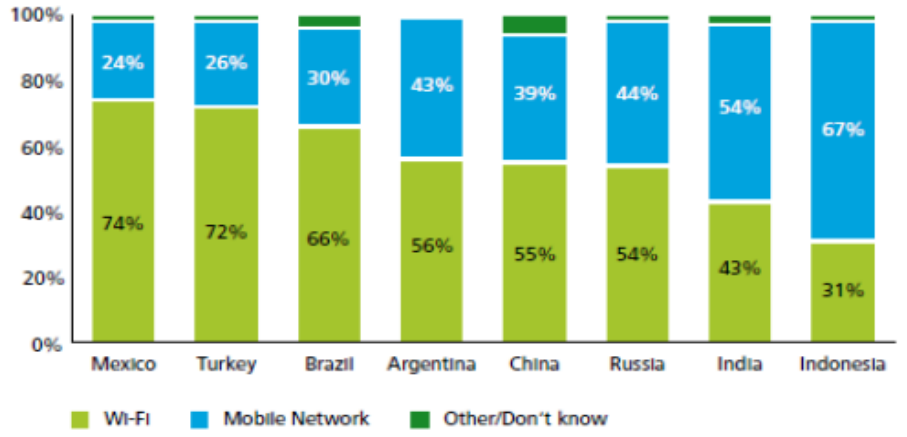
Figura 1.7. Gráfica que representa el interés de compra de los usuarios hacia dispositivos multifuncionales en los mercados en desarrollo.

- La mayoría de los usuarios de smartphones opta por el Wi-Fi como principal forma de conexión, como se indica en las figuras 1.8 y 1.9, correspondiendo a los mercados desarrollados y en desarrollo respectivamente.



Source: Deloitte Global Mobile Consumer Survey, Developed countries, May-July 2013
Weighted base: Respondents who use their smartphone to connect to the Internet: Belgium 576, Finland 325, France 724, Germany 723, Japan 516, Netherlands 975, Singapore 1,292, South Korea 1,297, Spain 1,006, UK 1,847, US 826.

Figura 1.8. Gráfica que indica el tipo de conectividad usada en los smartphones en países desarrollados.



Source: Deloitte Global Mobile Consumer Survey, Developing countries, May-July 2013
Weighted base: Respondents who use their smartphone to connect to the Internet: Argentina 654, Brazil 523, China 1,271, India 1,088, Indonesia 984, Mexico 790, Russia 617, Turkey 483.

Figura 1.9. Gráfica que indica el tipo de conectividad usada en los smartphones en países en desarrollo.

Una de las principales razones por la cual el Wi-Fi es la forma de conexión más utilizada, es porque de esta forma los usuarios evitan tener una cuenta muy alta en sus facturas, debido al modelo de cobro por megabytes o gigabytes que ofrece cada operadora. Estos datos sustentan el estudio reportado por CNN en 2013, en que se establece que la mayoría de los usuarios prefieren conectarse a través de Wi-Fi antes que pagar un plan de datos.

Para finalizar este segmento, el uso de teléfonos inteligentes tanto en México como en el resto del mundo está en constante crecimiento como se ha demostrado, debido a que son cada vez más asequibles y a que los usuarios son cada vez más dependientes a estos dispositivos para: ver videos, consultar el correo electrónico, enviar mensajes, jugar, actualizar su estado en redes sociales, realizar transacciones bancarias y compras, entre otras. Como resultado los smartphones han modificado la forma en que los usuarios actualmente navegan y buscan información en internet, viéndose desplazada para este fin la computadora personal.

1.3. Los smartphones como una nueva área de oportunidad para el desarrollo de malware.

Como se mencionó previamente los smartphones actualmente son los dispositivos preferidos por los usuarios tanto para entretenimiento como para navegar en internet, esto ha hecho que hoy en día haya más de 1 000 millones de estos dispositivos activos en el mundo, siendo un aspecto por el cual se han convertido en un blanco de los ciberdelincuentes, además de que son dispositivos que cuentan con aplicaciones para que los usuarios consulten su correo electrónico, contenido multimedia y realicen transacciones bancarias, haciendo de éstos un almacén de datos personales, de los cuales pueden sacar provecho obteniendo ganancias ilícitas.

El primer malware para smartphones fue desarrollado para infectar dispositivos con sistema operativo Symbian y fue detectado en 2004, denominado como "Cabir" clasificado como gusano ya que fue diseñado sólo para propagarse mediante conexiones de bluetooth a otros dispositivos, sin representar algún otro peligro sobre todo a la información almacenada, fue desarrollado por "Vallez" un integrante del grupo 29A. Este año y evento es considerado de principal importancia ya que fue el primer caso de malware en smartphones, lo cual marcaría una nueva tendencia del malware, que hoy en día tiene una gran cantidad de variantes por la simple razón de que los smartphones representan una fuente muy buena para obtener rentabilidad a través de la información que en ellos se almacena y procesa en día a día de los usuarios.

Otro aspecto relacionado con los ciberdelicuentes y los smartphones, que quizás sea más popular actualmente es el robo de fotografías de personas del medio del espectáculo, en la mayoría de los casos son sustraídas de los dispositivos para estafar a sus propietarios, con el fin de que paguen cierta cantidad de dinero o por el simple hecho de dañar la privacidad de las víctimas.

1.4. Legislación sobre delitos informáticos.

Antes de empezar a desarrollar este punto, se considera pertinente saber el significado de los siguientes conceptos:

- Legislación: es el conjunto o cuerpo de leyes por las cuales se gobierna un Estado, o una materia determinada.
- Delito: culpa, quebrantamiento de la ley. Acción o cosa reprobable. Acción u omisión voluntaria o imprudente penada por la ley.
- Informática: conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Establecido lo anterior, se aborda el primer tratado internacional que fue creado para enfrentar los delitos informáticos y los delitos en internet, sus objetivos son los siguientes: armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones integrantes del tratado. Este tratado es conocido como el convenio de Budapest y fue elaborado por el consejo de Europa, entró en vigor el 1 de julio de 2004. Posteriormente se integraron más países, como: Estados Unidos de América, Canadá, Japón y Sudáfrica.

Los delitos cibernéticos que se sancionan en el convenio de Budapest, son los siguientes:

- Acceso ilícito a sistemas,
- Interceptación ilegal de información,
- Interferencia de información,
- Interferencia de un sistema,
- Mal uso de los dispositivos,
- El fraude y la falsificación relacionado con la informática,
- Los delitos relacionados con la pornografía infantil,
- CiberTerrorismo,
- CiberAcoso, y
- Los delitos relacionados con los derechos de autor y derechos conexos.

En el caso de México, los delitos cibernéticos están contemplados en el código penal federal, el cual fue reformado y publicado en el Diario Oficial de la Federación el 17 de mayo de 1999, para

incluir el capítulo de: “Acceso ilícito a Sistemas y equipos de informática”, conformado por tres categorías:

- Acceso ilícito a sistemas y equipos de informática de particulares.
- Acceso ilícito a sistemas y equipos de informática de gobierno.
- Acceso ilícito a sistemas y equipos de informática del sector financiero.

Analizando lo que se establece en el código penal federal, se sanciona lo siguiente:

- Al que sin autorización (o estando autorizado) modifique, destruya o provoque pérdidas de información contenida en sistemas o equipos de informática (particulares, estatales o financieros) protegidos por algún mecanismo de seguridad.
- Al que sin autorización (o estando autorizado) conozca o copie información contenida en sistemas o equipos de informática (particulares, estatales o financieros) protegidos por algún mecanismo de seguridad.

Comparando las sanciones que en México se establecen contra las del tratado de Budapest, aún se tiene trabajo legislativo por realizar en cuanto a: malware, ciber-acoso, el secuestro de información, fraude, suplantación de identidad (Phising), ataques DoS/DDoS, por mencionar algunos.

En el mes de julio de 2014, México se integró al Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia, que incluye también a países como: Argentina, Ecuador, Chile, Uruguay, Panamá, Perú, Colombia y España, entre otros. El principal objetivo de este convenio es: establecer una línea de acción común y de cooperación mutua entre los 21 países iberoamericanos en contra de la ciberdelincuencia y constituir la base para la armonización de la regulación de las normativas internas iberoamericanas en la lucha contra los delitos cibernéticos.

La integración de México a este convenio representa un avance importante para disminuir este tipo de conductas delictivas de tipo informático, además de que ayudará a solventar algunos faltantes en el código penal federal como son: el abuso de dispositivos informáticos, suplantación de identidad, estafa informática, por mencionar algunos. Pues de acuerdo a un artículo de la CNN en México podrían aumentar los delitos cibernéticos en un 300% respecto al año 2013, esto según datos de la división científica de la policía federal, atribuyendo esto a la falta de legislación que permita

actuar de forma inmediata y a la falta de conciencia entre la población general sobre seguridad cibernética, entre otras.

Capítulo 2

El malware en los principales sistemas operativos de smartphones

2.1 Malware (definición y variantes).

La palabra malware se conforma de las siguientes palabras en inglés: malicious y software, es un programa (secuencia de instrucciones) con código que tiene la finalidad de infiltrarse y/o dañar una computadora o un sistema de información, esto sin el consentimiento del propietario. Los autores de este tipo de programas tienen diferentes razones para elaborarlos, que van desde la simple demostración de sus capacidades y conocimientos, cuestiones de vandalismo, hasta obtener un beneficio económico, por mencionar algunas.

El malware es un término que generalmente se asocia con las computadoras tanto de escritorio como portátiles (laptops), y que en los últimos años ha evolucionado al grado de infectar dispositivos como smartphones y tabletas electrónicas, por tal motivo el presente trabajo tiene como finalidad describir los conceptos relacionados con el malware orientado a los smartphones de acuerdo a su clasificación por comportamiento de acción maliciosa (también conocida como payload), siendo:

Malware infeccioso, esta clasificación se asigna al código malicioso que tiene como objetivo principal propagarse a otros programas dispositivos o programas, algunas de sus afectaciones son: modificar el funcionamiento del dispositivo infectado, así como el robo y/o modificación de la información. Perteneciendo a esta clasificación los siguientes conceptos:

- **Virus**, es el código malicioso que se inserta en el programa ejecutable de una aplicación y necesita de la intervención del usuario para que se copie a otras aplicaciones libres de éste y así de comienzo con sus acciones nocivas para afectar a la víctima. Se propaga de dispositivos infectados a través de una red (local o internet) a otros que estén “sanos”, también a través de medios extraíbles.

Algunas de sus características son:

- Su incapacidad de funcionar como ejecutable por sí solo, siendo ésta la principal razón por la cual se anexa a otros programas.
- La autorreplicación, se refiere a la capacidad que tiene de crear copias automáticamente de sí mismo, independientemente del lugar en que se encuentre.
- El polimorfismo, hace referencia a la capacidad que tiene este tipo de malware de cambiar su estructura, para evitar ser detectado por algún antivirus.

- Su ciclo de acción se consideraría en dos fases; la primera: es cuando se aloja en un directorio y posteriormente se disemina por éste; en la segunda: se lleva a cabo la acción nociva para la cual fue creado, generalmente esta parte es realizada por la payload, que va desde la modificación o eliminación de archivos del sistema operativo o propios de la víctima, el envío de información de la víctima hacia el autor del virus u otro remitente, proveer acceso a la maquina infectada por medio de una puerta trasera, entre otras.

- **Gusanos,** el objetivo principal de este tipo de malware es el de copiarse a sí mismo, a diferencia de los virus no necesitan alojarse en otro programa, ni la intervención del usuario para empezar su acción maliciosa, por lo general no se enfocan en alterar archivos o eliminarlos. Se replican a través de las redes informáticas y dispositivos USB por lo general explotando alguna falla en el sistema, el daño más común que producen es el de consumir recursos de los dispositivos, así como de las redes por las cuales se distribuyen.

Malware oculto, este tipo de código malicioso tiene como objetivo principal llevar a cabo sus acciones maliciosas de forma oculta, para que así el usuario no pueda terminar los procesos iniciados por el malware permitiendo que éste continúe la ejecución de sus objetivos.

- **Backdoors (puertas traseras)**, el objetivo de este programa malicioso, es crear un acceso oculto a un dispositivo sin la autorización del dueño, mediante la evasión de los procedimientos de autenticación comunes, de esta forma el atacante tiene acceso libre y remoto al dispositivo para realizar diversas actividades.
- **Rootkit**, es un programa que oculta determinados elementos (archivos, procesos, direcciones de memoria, conexiones de red, por mencionar algunos) que permiten el acceso con privilegios a un dispositivo y su objetivo radica en corromper el funcionamiento normal del sistema operativo o de otras aplicaciones, como se aprecia se conforma de dos palabras en inglés, que son: root (raíz, que es el nombre tradicional de la cuenta con mayor número de privilegio en sistemas operativos Unix) y kit (conjunto de herramientas, haciendo referencia a los componentes de software que implementa este código malicioso).
- **Drive by download**, este tipo de malware se oculta en sitios web inseguros y para que se lleve a cabo la infección sólo basta con abrir la página infectada ya que el código malicioso

es insertado mediante un script en el código HTML de la página, de modo que cuando el usuario carga la página en el navegador hace que se contamine el dispositivo.

- **Troyanos**, son programas disfrazados como aplicaciones legítimas o atractivas para los usuarios pero tienen oculto el código malicioso con diversos objetivos, como: modificar o eliminar archivos del sistema operativo, abrir determinados puertos para que a través de éstos se tome el control remoto del dispositivo infectado, otra opción sería combinarse con spyware que recolecta y envía datos confidenciales de la víctima, esta última suele ser muy empleada por los ciberdelicuentes para robar datos bancarios.

Malware para obtener beneficios, este tipo de código malicioso tiene por objetivo recolectar toda la información posible de personas u organizaciones sin su consentimiento, robando todos los datos a su alcance con el fin de que los autores del código se beneficien económicamente o también para fines publicitarios. Dentro de esta clasificación están los siguientes conceptos:

- **Spyware**, o programa espía, este código malicioso quizás es el más inquietante para la privacidad de los usuarios, ya que se entromete por completo en la vida privada de éstos. La información que recopilan es muy diversa, como: nombre y contraseña de correo electrónico, dirección IP y DNS del dispositivo infectado, hábitos de navegación y datos bancarios que los usuarios utilizan al realizar compras a través de internet, de toda la información sensible[3] antes mencionada, la que es robada con más frecuencia es la relacionada con las cuentas bancarias de esto se encargan los troyanos bancarios.
- **Adware**, es una palabra formada por la contracción de dos palabras: advertising y software, se refiere al malware que tienen como fin mostrar publicidad empleando cualquier medio, como: ventanas emergentes, banners[4], cambios en la página de inicio del navegador, en la barra de herramientas, entre otras. En general este tipo de malware no representa una amenaza en cuanto a causar daños a los dispositivos o a la información de los usuarios, simplemente es molesto por la cantidad de publicidad que llega a mostrar.

[3] Información sensible: es el nombre que se asigna a la información personal privada de una persona

[4] Banner: es un formato publicitario de internet, que consiste en incluir un anuncio dentro de una página web.

- **Malvertising,** se forma de las palabras: malicious y advertising, hace referencia a publicidad maliciosa que tiene como fin infectar a los usuarios con malware. Este código malicioso es insertado en la publicidad que se muestra por medio de internet en sitios web legítimos y tiene por objetivo explotar las vulnerabilidades de software o plugins desactualizados.
- **Keylogger**, o registrador de teclas principalmente almacena en una lista todas las teclas que pulsa un usuario en su dispositivo, para posteriormente ser enviadas a terceros y que éstos conozcan la información personal de la víctima principalmente sus contraseñas, por lo general este tipo de malware se distribuye a través de un troyano, virus o gusano.
- **Stealers**, este tipo de código malicioso se especializa sólo en contraseñas de acceso a diferentes servicios que permiten la opción de "recordar contraseña", por ejemplo, en los navegadores para acceder a cuentas de correo, redes sociales y mensajería instantánea, una vez conseguidos los objetivos se recopilan en un archivo que posteriormente es enviado al autor del código.
- **Ransomware**, este concepto se asocia al código malicioso que tiene como objetivo principal restringir el acceso a ciertas aplicaciones o archivos del dispositivo infectado, además de solicitar a la víctima el pago de un rescate a cambio de quitar las restricciones para que el dispositivo continúe con su funcionamiento normal. Este tipo de malware se popularizó en Rusia y se expandió en el resto del mundo a partir de junio del 2013.
- **Rogue**, este código malicioso hace creer a la víctima que su dispositivo está infectado por algún virus u otro tipo de malware, induciendo a la víctima a pagar cierta cantidad de dinero por una aplicación que supuestamente eliminará dicha amenaza, en la mayoría de los casos tal aplicación contiene otro tipo de malware oculto.

Malware para realizar ataques distribuidos de denegación de servicios (DDoS), éste tipo de ataques tiene como principal objetivo provocar que un servicio ofrecido por medio de internet sea inaccesible para los usuarios, la forma en que se lleva a cabo este tipo de ataques es generando demasiadas peticiones desde distintos puntos de conexión, provocando que el servidor se sobrecargue y así impedir que siga prestando sus servicios de forma habitual. La forma más común de realizar este tipo de ataques es mediante:

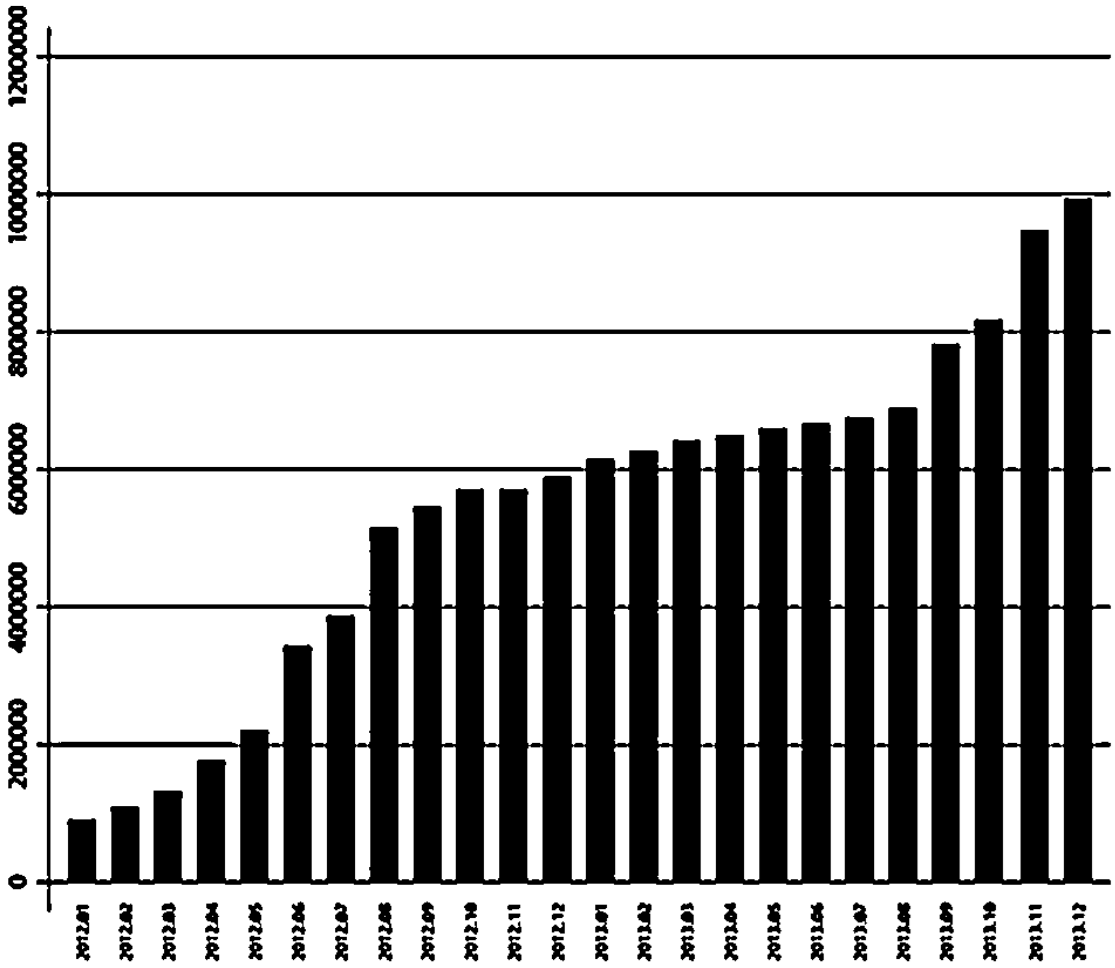
- **Botnets,** son un conjunto de dispositivos infectados por un código malicioso que permite ejecutar en ellos una serie de comandos con distintos propósitos, estos dispositivos deben

estar conectados a una red y son conocidos como bots (diminutivo de Robots) debido a que son controlados de forma remota, autónoma y automática**.** Las funciones que se llevan a cabo por medio de las botnets son diversa y dependen de gran medida de las intenciones de la persona que elabora el código malicioso, pero lo más común es que se empleen para enviar spam o para realizar ataques de denegación de servicios, por mencionar algunos.

El malware no se limita a actuar en una sola variante, ya que se vale de fusión de varias de las clasificaciones que previamente se mencionaron para llegar a infectar a la víctima, por ejemplo, es común que un ransomware llegue a infectar a la víctima por medio de un troyano que se presenta como una aplicación atractiva o legitima para el usuario, sin que éste sospeche que tipo de código malicioso está oculto, por otra parte una botnet se propagaría por medio de un gusano, esto no limita a que sea la única forma de distribuir el malware. Las formas en que se combinan las clasificaciones del malware para infectar a la víctima dependen de las intenciones que tenga el autor del código malicioso así como de su astucia para aumentar el número de objetivos a los cuales hacer daño.

El malware ha evolucionado en gran medida desde sus inicios cuando sólo era una forma de demostrar las habilidades técnicas por parte de sus autores, hasta ser hoy en día una de las bases del cibercrimen con el fin de lucrar con la información de las víctimas. Hace algunos años el malware únicamente tenía por objetivo principal las computadoras de los usuarios u organizaciones, actualmente con la gran expansión que han tenido los dispositivos móviles en el mercado, los cibercriminales han optado por atacar a estos dispositivos y así obtener ganancias ilícitas que les resulta un negocio muy rentable.

Para los smartphones de acuerdo a información de Kaspersky labs., los años más importantes para el desarrollo del malware fueron 2012 y 2013, ya que se registró un crecimiento muy notable respecto a años anteriores, como se aprecia en la figura 2.1. En 2013 se descubrieron cerca de 10 millones de paquetes de instalación nocivos únicos, además de haber registrado 143 211 modificaciones nuevas a los programas maliciosos con el propósito de infectar a éstos dispositivos.



Fuente: www.viruslist.com**, Amenazas para dispositivos móviles en 2013.**

Figura 2.1. Gráfica del aumento en paquetes de instalación nocivos detectados entre 2012 y 2013.

Por otra parte, con base en el artículo publicado en abril de 2014 por Kaspersky labs., en donde se detalló que del 100% de ataques registrados en 2013 a dispositivos móviles, tuvieron los siguientes objetivos:

- Primer objetivo con 33,5% se dedicó al robo de dinero del usuario, por medio de código malicioso los cibercriminales conseguían ganancias económicas a través del envío de SMS y llamadas a números de tarifación especial, la intercepción de contraseñas para uso de servicios de banco en línea o mediante el robo a través de servicios de pagos móviles.
- Segundo objetivo se enfocó en el espionaje con 26,5%, en este aspecto el malware dedicado a espiar tenía como fin conocer la localización de los usuarios, analizar mensajes y registros

de llamadas, además de vigilar a través del micrófono y la cámara del dispositivo a los usuarios.

- Tercer objetivo con un 20.6% corresponde al robo de datos, por medio del malware los cibercriminales llevaron a cabo las siguientes acciones: robaron fotos, documentos, así como lectura remota de mensajes SMS y correos electrónicos, con el fin de venderla en el mercado negro o para solicitar a la víctima un rescate a cambio de su información.
- Por último, el cuarto objetivo con un 19.4% de los ataques se centró en generar dinero por medio de los dispositivos, en este caso los desarrolladores de malware se enfocaban a configurar botnets o estafas a través de anuncios falsos.

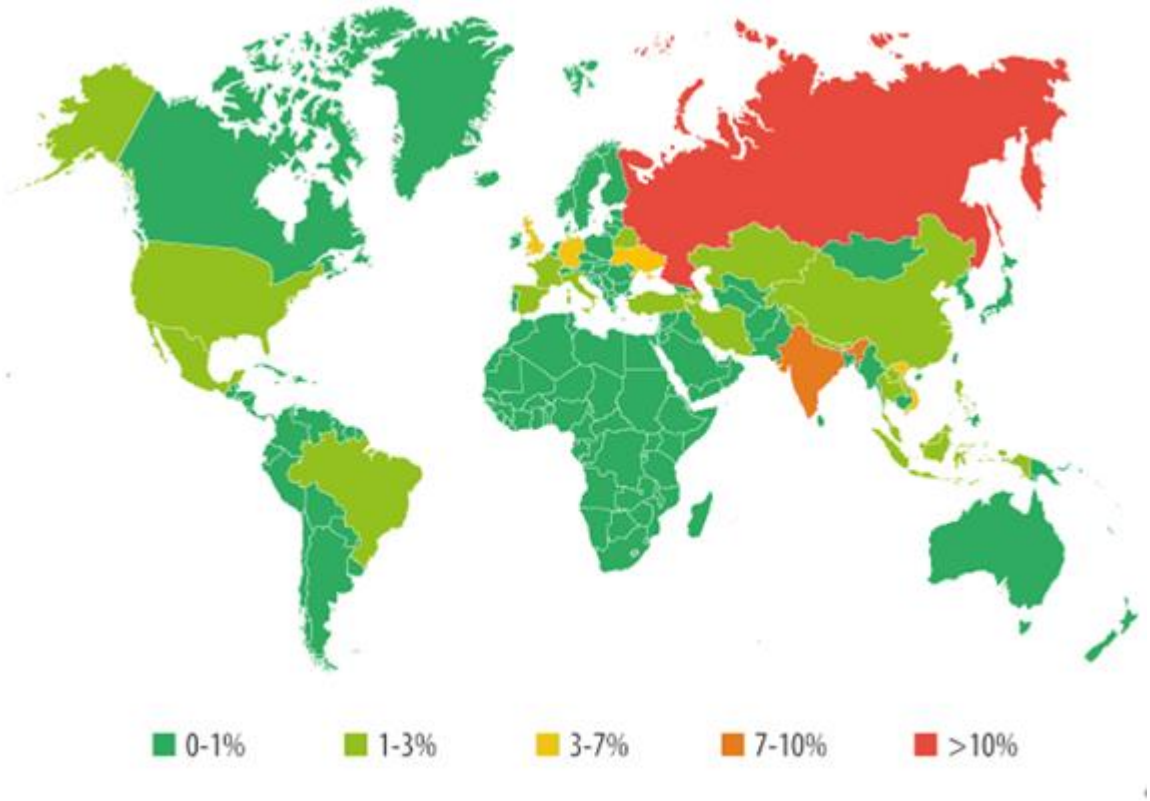
En ese mismo artículo se señalan los diez países principales con mayor índice de usuarios atacados por malware, que se enlistan en la tabla 2.1.

Tabla 2.1. Países con mayor porcentaje de ataques por malware en 2013.

Fuente: **www.viruslist.com**, Amenazas para dispositivos móviles en 2013.

Posición	1	2	3	4	5	6	7	8	9	10
País	Rusia	India	Vietnam	Ucrania	Inglaterra	Alemania	Kazajistán	E.U.A	Malasia	Irán
% del total de usuarios atacados	40,34%	7,90%	3,96%	3,84%	3,42%	3,20%	2,88%	2,13%	2,12%	2,01%

Por último, antes de pasar a los sistemas operativos que son los más atacados por malware, se presenta la geografía de las amenazas de código malicioso durante 2013, que se aprecia en la figura 2.2, y en la cual se observa que dentro de los países del continente americano con mayor porcentaje de intentos de infección están: Estados Unidos de América, Brasil y México, aunque sus porcentajes estén entre el 1 y 3 por ciento son los países más representativos del continente.



Fuente: www.viruslist.com, Amenazas para dispositivos móviles en 2013.

Figura 2.2. Mapa con los porcentajes de intentos de infección de malware en 2013.

2.2 Los sistemas operativos de Smartphones con mayor índice de ataque por malware.

Un sistema operativo es el software que tiene como objetivo principal asignar una gestión ordenada y controlada del hardware del dispositivo (procesador, memoria y dispositivos de entrada y salida), entre los diversos programas de aplicación que compiten por estos recursos a causa de la interacción del usuario, como lo indica la figura 2.3.

Figura 2.3. Interacción del sistema operativo.

Desde la aparición de los Smartphone ha habido una gran variedad de sistemas operativos, evolucionando de sistemas embebidos hasta contar actualmente con sistemas operativos móviles, orientados a la conectividad inalámbrica así como a realizar una mayor capacidad de cómputo. La mayoría de los actuales sistemas operativos para Smartphone están basados en el siguiente modelo de capas, integrados por:

- **Interfaz de usuario**, es el medio por el cual el usuario interactúa y se comunica con las distintas aplicaciones, con el fin de procesar información en el dispositivo.
- **Middleware**, es el software que asiste a una aplicación para comunicarse o interactuar con otras aplicaciones, redes, bases de datos y diferentes sistemas operativos, de esta forma se provee al desarrollador una mayor simplicidad al momento de realizar conexiones con sistemas de información distribuidos.

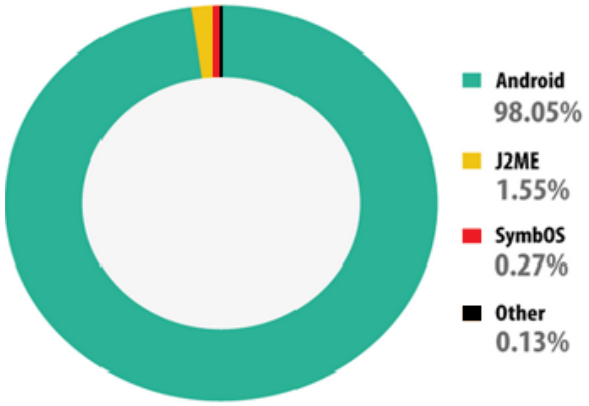
- **Entorno de desarrollo de aplicaciones**, se conforma por un conjunto de herramientas (API[5]) que permite una mejor comunicación entre los componentes de software, con el fin de que los desarrolladores creen aplicaciones de una forma más ágil.
- **Kernel**, o núcleo del sistema operativo es el encargado de realizar funciones básicas para el sistema operativo como: control de periféricos, comunicación entre procesos, gestión de memoria y control de interrupciones.

El primer sistema operativo de smartphones en ser atacado por malware fue Symbian, como previamente se ha mencionado en el subcapítulo 1.4, esto se originó porque en ese tiempo era el sistema más utilizado por una gran cantidad de empresas de telefonía móvil, como son: Sony Mobile Communications, Samsung, Siemens, Benq, LG, Motorola, entre otras. Provocando que gran cantidad de smartphones operaran bajo dicho sistema operativo, alcanzando una participación en el mercado durante el año de 2009 del 46,9% mientras que Android contaba apenas con el 3,9%.

Symbian destacó del resto de los sistemas operativos de su época porque fue desarrollado exclusivamente para smartphones como plataforma de destino, además de ser abierto permitiendo así que terceros desarrollaran aplicaciones, haciendo su debut en 2001. En comparación con otros sistemas de esa época que eran adaptaciones de sistemas genéricos para distintos dispositivos, Symbian era compatible con las distintas tecnologías telefónicas de entonces.

A pesar de que actualmente ya no salen al mercado Smartphone con sistema operativo Symbian, debido a que en 2013 se lanzó el último Smartphone con éste, en el informe de Kaspersky labs., sobre sistemas operativos móviles más atacados en 2013, Symbian aun aparecía entre las plataformas más atacadas por malware aunque con un porcentaje muy pequeño, como se aprecia en la figura 2.4.

[5] API: Application Programming Interface (Interfaz de Programación de Aplicaciones), es un conjunto de funciones que están disponibles a través de bibliotecas que facilitan la comunicación entre diversos componentes de software.



Fuente: www.viruslist.com, Amenazas para dispositivos móviles en 2013.

Figura 2.4. Distribución por plataforma del ataque por malware en dispositivos móviles en 2013.

Otro aspecto relevante de la figura anterior es el porcentaje de ataques hacia Android que ocupó el 98,05% en 2013. Y actualmente se mantiene como uno de los principales sistemas operativos que dominan el mercado, esto con base al informe de IDC correspondiente al segundo trimestre del año 2014, que se muestra en la tabla 2.2.

Tabla 2.2. Principales sistemas operativos de smartphones en el mercado (en millones de unidades), correspondientes al segundo trimestre de 2014.

Fuente: IDC

Sistema Operativo	Volumen de unidades, 2° trimestre de 2014	Acción en el mercado, 2° trimestre de 2014	Volumen unidades, 2° trimestre de 2013	Acción en el mercado, 2° trimestre de 2013	Crecimiento en 2014 respecto a 2013
Android	255.3	84.7%	191.5	79.6%	33.3%
iOS	35.2	11.7%	31.2	13.0%	12.7%
Windows Phone	7.4	2.5%	8.2	3.4%	-9.4%
Blackberry	1.5	0.5%	6.7	2.8%	-78.0%
Otros	1.9	0.6%	2.9	1.2%	-32.2%
Total	**301.3**	**100%**	**240.5**	**100%**	**25.3%**

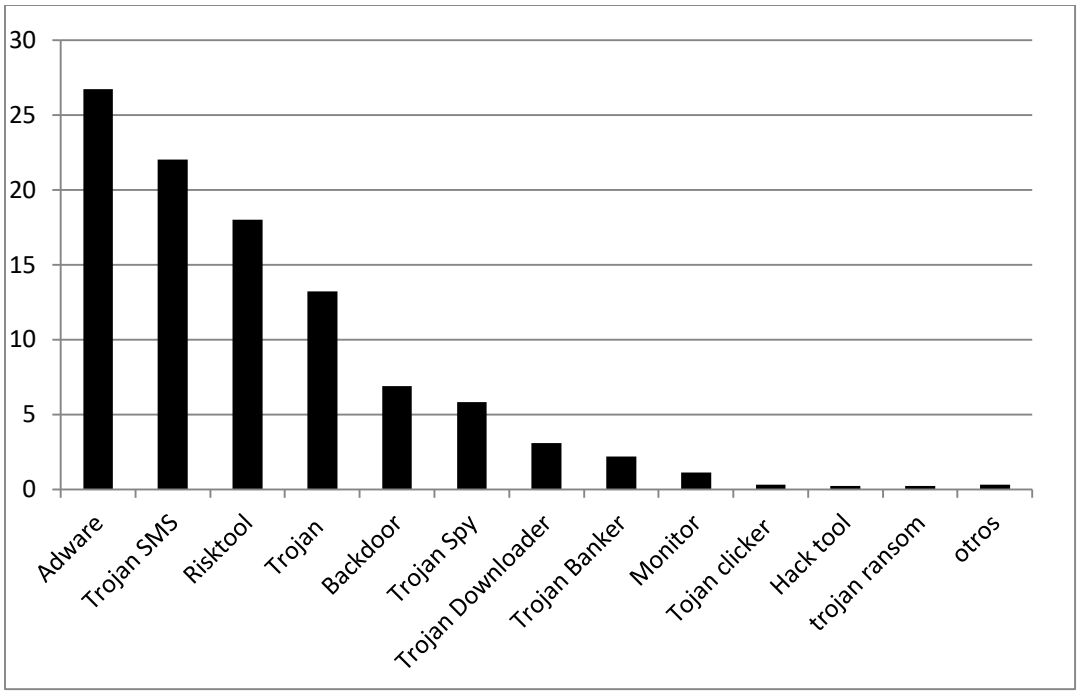
Android, al ser el principal sistema operativo en el mercado se vuelve el objetivo principal del malware como se pudo observar en la figura 2.4, pero datos más recientes correspondientes al segundo trimestre de 2014 indican que el 99% del malware tiene como objetivo a Android, esto no quiere decir que sistemas como iOS y Windows Phone queden fuera del interés de los ciberdelicuentes, sólo que presentan un porcentaje menor en comparación con el sistema operativo de Google.

La distribución que presentó el código malicioso para smartphones correspondiente al segundo trimestre de 2014, se presenta en la tabla 2.3 y figura 2.5.

Tabla 2.3. Distribución del tipo de malware en el segundo trimestre de 2014.

Fuente: www.viruslist.com, escenario de ciberamenazas en el segundo trimestre de 2014.

Malware	Porcentaje
Adware	26,7%
Trojan SMS	22%
Risktool	18%
Trojan	13,2%
Backdoor	6,9%
Trojan Spy	5,8%
Trojan Downloader	3,1%
Trojan Banker	2,2%
Monitor	1,1%
Tojan Clicker	0,3%
Hack Tool	0,2%
Trojan Ransom	0,2%
Otros	0,3%
Total	**100%**



Fuente: www.viruslist.com, escenario de ciberamenazas en el segundo trimestre de 2014.

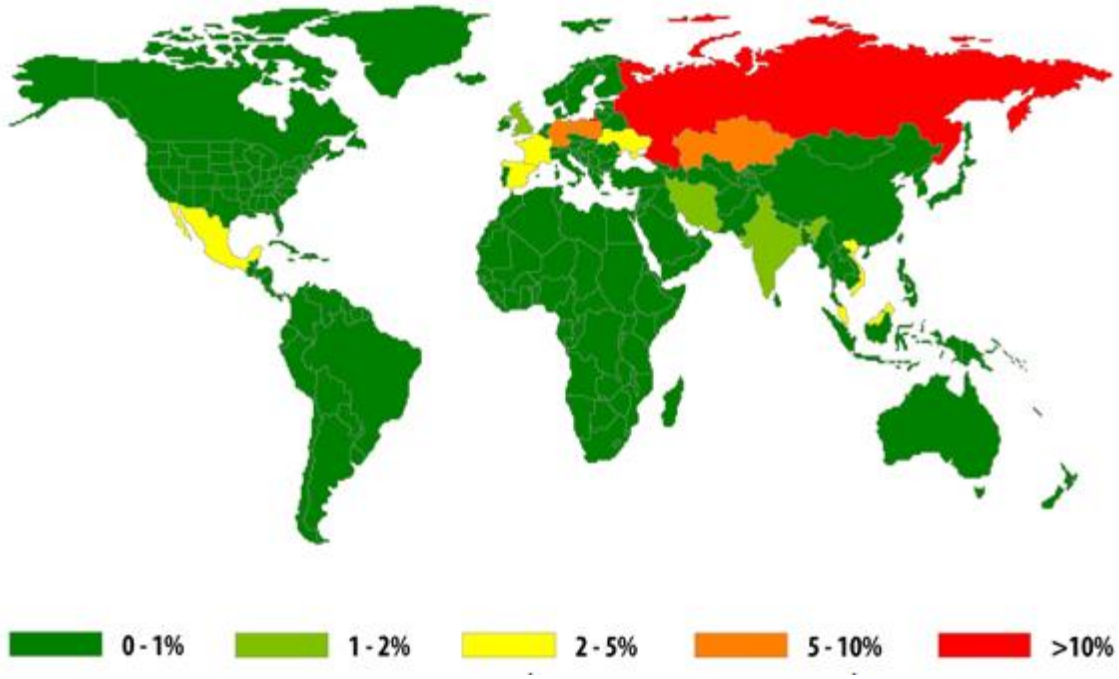
Figura 2.5. Distribución del tipo de malware en el segundo trimestre de 2014.

Un aspecto relevante que corresponde al segundo trimestre de 2014 es un cambio en la distribución de la geografía por intentos de infección de malware móvil, como se indica la figura 2.6, en la cual se observa que México se ubica en un rango del 2 al 5% que comparada con la del año anterior (2013, indicada en la figura 2.2) nuestro país ya se encuentra dentro de los diez países con mayor intento de infección por código malicioso, como lo indica la tabla 2.4.

Tabla 2.4.Países con mayor porcentaje de ataques por malware en el segundo trimestre de 2014.

Fuente: www.viruslist.com, Escenario de ciberamenazas en el segundo trimestre de 2014

Posición	1	2	3	4	5	6	7	8	9	10
País	Rusia	Alemania	Kazajistán	Polonia	Ucrania	Malasia	Vietnam	Francia	España	México
% del total de usuarios atacados	46,96%	6,08%	5,41%	5,02%	3,72%	2,89%	2,74	2,32%	2,28%	2,02%



Fuente: www.viruslist.com, Escenario de ciberamenazas en el segundo trimestre de 2014.

Figura 2.6. Mapa con los porcentajes de intentos de infección de malware a dispositivos móviles correspondiente al segundo trimestre de 2014.

Dentro de los tipos de malware más relevantes para las plataformas antes mencionadas, están:

- **Cabir:** primer malware para smartphones infecta a los teléfonos móviles que funcionan con el sistema operativo Symbian. El gusano intenta propagarse a otras terminales a través de señales inalámbricas Bluetooth.
- **Commwarrior:** conocido como el primer gusano capaz de propagarse entre dispositivos mediante mensajes MMS[6], tanto por 3G como por Bluetooth, sólo afecta a dispositivos que trabajan con el sistema operativo Symbian. Una vez ejecutado el gusano, éste se propaga mediante la cobertura Bluetooth a otros dispositivos cercanos (en un radio aproximado de 16 metros) enviando datos infectados con nombres aleatorios.

[6] MMS: Multimedia Messaging System (Sistema de Mensajería Multimedia) es un estándar de mensajería que permite enviar y recibir a través de los teléfonos móviles contenidos multimedia, como: sonido, video, fotos, entre otros.

- **Skulls**: se trata de un troyano que afecta al sistema operativo Symbian, una vez descargado el virus reemplaza todos los iconos del escritorio del teléfono con imágenes de un cráneo, también inutiliza todas las aplicaciones del teléfono incluyendo la recepción y envió de SMS y MMS.
- **Gingermaster:** troyano desarrollado para plataforma Android que se propaga mediante la instalación de aplicaciones que incorporan de forma oculta el malware para su instalación en segundo plano. Aprovecha la vulnerabilidad de la versión Gingerbread (2.3) del sistema operativo para utilizar los permisos de súper-usuario[7] mediante una escala de privilegios. Luego roba información del dispositivo infectado (como: número telefónico, IMEI[8], IMSI[9], resolución de pantalla, hora local, entre otros) y la envía a un servidor remoto.
- **Geinimi,** este malware se detectó en China afectando a smartphones con Android, una vez que se instala en el dispositivo tiene la capacidad de recibir órdenes de un servidor remoto, que permite al dueño del servidor controlar el teléfono por medio de una serie de comandos. Además de recopilar datos del teléfono cada cierto tiempo y enviarlos a un servidor.
- **Droid Dream: e**ste malware se detectó en varias aplicaciones legítimas para Android que eran modificas para incluir este código malicioso que enviaba la información personal de la víctima a un servidor remoto, además de explotar la vulnerabilidad CVE-2010-EASY que permitía al cibercriminal tener control absoluto del dispositivo infectado.
- **Droid Kung-Fu:** es un troyano contenido en aplicaciones de Android, que al ser ejecutadas, obtiene privilegios de root e instala el archivo: "com.google.ssearch.apk", que contiene una puerta trasera que permite eliminar ficheros, abrir páginas de inicio suministradas, abrir direcciones web y descargar e instalar paquetes de aplicación. Además de recopilar y enviar a un servidor remoto todos los datos disponibles sobre el dispositivo.

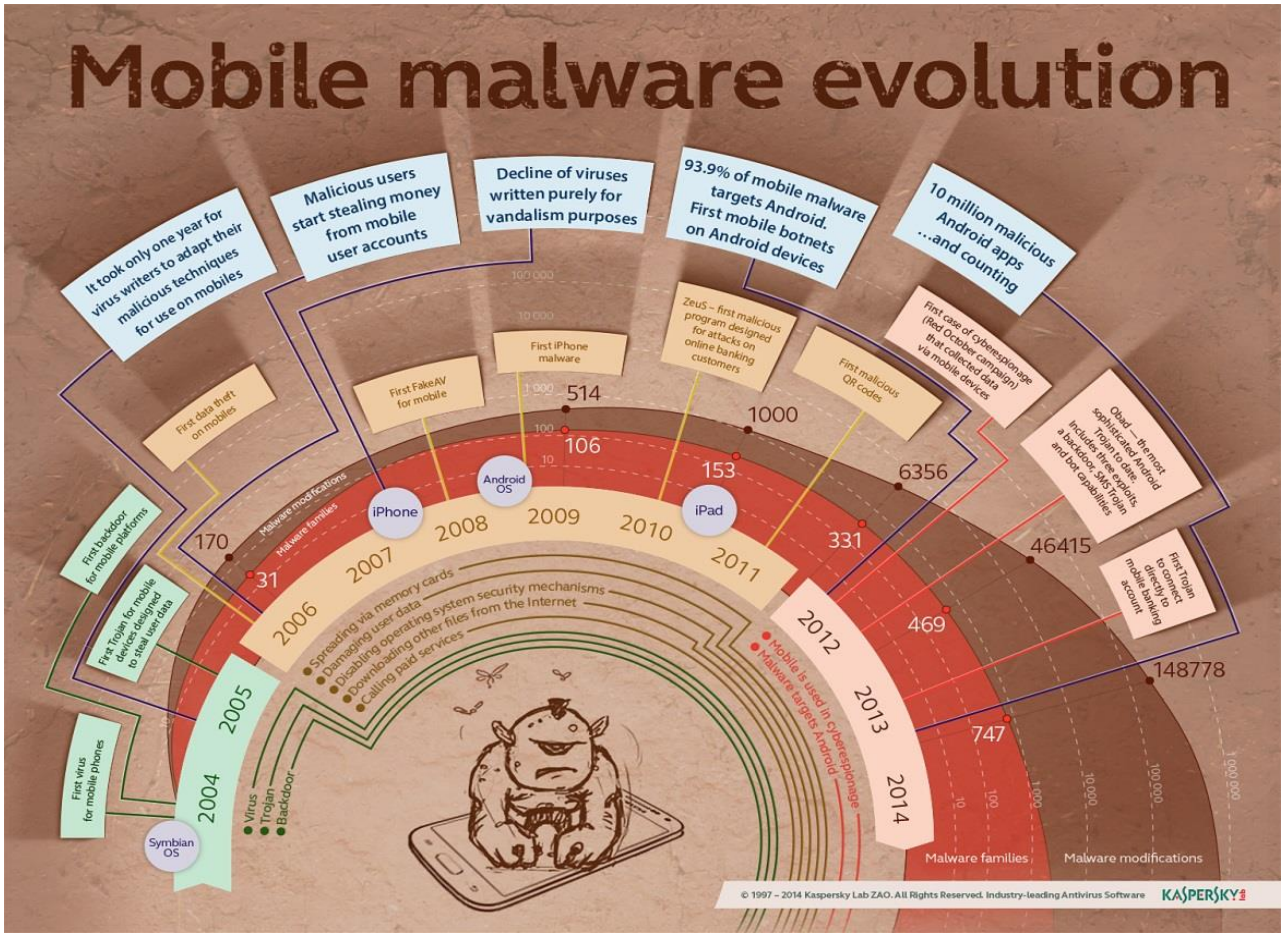
[7] Super-usuario: se refiere a la cuenta con mayor número de privilegios administrativos de un sistema operativo.

[8] IMEI: es el acrónimo de International Mobile Equipment Identity (Identidad Internacional de Equipo Móvil), es un código único en cada teléfono móvil GSM y permite identificar al dispositivo a nivel mundial.

[9] IMSI: corresponde al acrónimo de International Mobile Subscriber Identity (Identidad Internacional del Subscritor de un Móvil), es un código de identificación único para cada celular, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

- **Ikee:** primer gusano conocido para plataformas iOS. Sólo actúa en terminales que se les han hecho previamente un proceso de jailbreak[10], este gusano utiliza la contraseña por defecto del usuario root en el servicio SSH que permite acceder al dispositivo y ejecutar una serie de comandos

Para cerrar este subcapítulo sobre el malware en los principales sistemas operativos de smartphones, se presenta la imagen 2.3, que muestra cuales han sido los hitos más significativos en la aparición y evolución del malware móvil.



Fuente: www.kaspersky.com, Mobile malware evolution in 2013

Figura 2.7. Evolución del malware en dispositivos móviles.

[10] Jailbreak: es un proceso que se aplica a dispositivos con sistema operativo iOS, con el fin de eliminar algunas limitaciones impuestas por Apple.

2.3 Principales vectores de propagación de malware para smartphones.

Los vectores para la propagación del malware en smartphones, se refieren a los agentes que emplea el malware para propagarse en este tipo de dispositivos, el objetivo de esta sección es establecer los medios por los cuales el malware infecta un smartphone, considerando los siguientes medios:

- **Mensajería,** por medio de los distintos servicios de éste tipo que emplean los smartphones (como: MMS, correo electrónico, entre otros) para comunicar a los usuarios, los autores del malware ven en éstos una gran oportunidad para replicarse en los contactos de la víctima y así continuar su ciclo de reproducción, por medio de archivos adjuntos infectados con malware que son enviados a las nuevas víctimas.
- **Bluetooth,** este tipo de tecnología de redes inalámbricas de área personal también es explotada por el malware, en particular mediante vulnerabilidades en los sistemas operativos que permiten la transferencia de datos de forma ajena al usuario por este medio, de tal forma que así logra propagarse el código malicioso a los dispositivos que estén dentro del alcance del emisor.
- **Repositorios de aplicaciones,** es el método más empleado por los ciberdelicuentes para propagar malware oculto en las aplicaciones, en especial en aquellos repositorios no oficiales que carecen de medidas de seguridad facilitando así que los creadores del código malicioso tengan un medio de distribución.
- **Códigos bidimensionales (QR-codes),** son códigos bidimensionales que almacenan información en una matriz de puntos y son interpretados por aplicaciones en smartphones, este tipo de códigos está formado por distintos módulos de color negro sobre un fondo blanco. La infección por este medio se da cuando por medio de este tipo de códigos el usuario es redirigido a una página web con contenido malicioso que permitiría explotar alguna vulnerabilidad en el navegador.
- **Fuentes de energía en lugares públicos,** esta modalidad es nueva y aprovecha la necesidad de los usuarios de recargar la batería de su dispositivo en lugares públicos. Este medio de propagación se da por medio del puerto USB, por donde se hace la instalación del malware capaz de rastrear la ubicación, robar notas, contactos, registros de llamadas, contraseñas, entre otras.

2.4 La seguridad en los principales sistemas operativos de smartphones.

Seguridad es un término que proviene del latín "securitas" se refiere a la cualidad de estar seguro (libre y exento de cualquier peligro, daño o riesgo), por lo tanto este concepto se vuelve fundamental en el desarrollo de los sistemas operativos a través de los cuales se opera y almacena información sensible, la seguridad en los sistemas operativos de smartphones está orientada a administrar el acceso a todos los componentes del teléfono tanto de hardware como de software que son solicitados por las aplicaciones.

Antes de comenzar a desarrollar este aspecto de la seguridad en los sistemas operativos de smartphones, es conveniente hacer la aclaración que sólo se tomarán en cuenta los sistemas operativos que actualmente tienen mayor presencia en el mercado, como son: Android de Google, iOS de Apple y Windows Phone de Microsoft. Por otra parte si bien se hizo mención en que Symbian fue un sistema operativo muy importante debido a su presencia en el mercado en años anteriores y que además fue en esta plataforma en donde se dieron los primeros indicios de malware que marcó una tendencia que hoy en día sigue creciendo, este sistema operativo ya no será considerado debido a que el último dispositivo que salió al mercado fue en el año de 2012 y después de esto se descontinuo.

Android, es un sistema operativo basado en el kernel de GNU/Linux su diseño se orientó a dispositivos móviles con pantalla táctil. Fue desarrollado por Android Inc., con el respaldo económico de Google y fue en el año de 2005 que esta compañía compró a la desarrolladora, Android se encuentra en el mercado desde septiembre de 2008 y a partir de entonces ha tenido un crecimiento muy importante, dando como resultado que en la actualidad sea el sistema operativo para smartphones con el más alto porcentaje de malware.

La seguridad de Android se sustenta en tres pilares:

1. Toda aplicación tendrá un acceso limitado tanto a hardware como a software, a esto se le conoce como ejecución en caja de arena (Sandbox), se refiere al aislamiento de procesos (entiéndase por proceso dentro de éste contexto a un programa en ejecución), este aspecto se heredó de GNU/Linux.
2. Toda aplicación debe ser firmada con un certificado digital, con el fin de:

- Identificar al autor.
- Establecer cierta confianza en las aplicaciones.
- Garantizar que el archivo no haya sido modificado.

3. Modelo de permisos, con este aspecto se tiene la intención de que cada usuario conozca los permisos que le dará a la aplicación antes de instalar, esto afecta de manera directa al primer punto, pues de los permisos que otorgue el usuario a las aplicaciones dependerán los recursos a los que éstas tengan acceso.

Android con este modelo de seguridad da al usuario el control absoluto de instalar las aplicaciones que quiera sin importar el lugar de donde provengan. Un punto importante de la seguridad es que ninguna aplicación tiene permisos por defecto para realizar operaciones que puedan tener un impacto negativo en el sistema operativo, usuarios y otras aplicaciones, esto incluye la lectura o escritura de datos privados del usuario, acceso a la red, entre otras. Las aplicaciones necesitan la aprobación por parte del usuario para poder instalarse en el dispositivo y así realizar las funciones que tiene que llevar a cabo para su ejecución, para lo anterior Android implementa los denominados "manifest permissions" que notifican al usuario los permisos que otorgará a las aplicaciones y depende del usuario si los acepta o no.

Como se mostró previamente Android pone al usuario a cargo de la evaluación de los requisitos que emplearan las aplicaciones antes de sean instaladas, por el contrario Apple controla todo el proceso. Esta forma de hacer la evaluación de las aplicaciones resulta para algunas opiniones la manera más segura de proteger a los usuarios, pero el proceso de evolución no está claramente detallado, dando como resultado que no se sepa qué comprueba exactamente la compañía. Sea cual sea el proceso de evaluación ha permitido que gran cantidad de aplicaciones sean vetadas por Apple, ya que presentaban alguna vulnerabilidad o porque no realizaban de forma estricta lo que en ellas se establecía.

iOS, al igual que Android implementa la técnica de "Sandbox", con la cual no se permite que una aplicación acceda a los datos de otra así como a todos los recursos del dispositivo, también exige que las aplicaciones estén firmadas digitalmente, este hecho dificulta que sean manipuladas con fines maliciosos. En cuanto a la seguridad física del dispositivo ofrece las siguientes posibilidades:

- Passcode, o código de acceso tiene la función de autenticar al usuario para que éste pueda acceder a las diversas funciones que ofrece el dispositivo. Este aspecto establece una serie de políticas de seguridad, por ejemplo: longitud mínima del passcode, caducidad, número máximo de intentos, por mencionar algunas.
- Borrado remoto, con esta opción en caso de robo o pérdida del dispositivo el dueño envía de forma remota un comando, con el cual borrará los datos contenidos en el dispositivo.
- Borrado local, esta característica borra los datos del dispositivo si se introduce de manera errónea el passcode un determinado número de veces.

Windows Phone, al igual que Android e iOS implementa técnicas de aislamiento de procesos (Sandbox), en este sentido vale la pena resaltar que la versión más reciente del navegador Internet Explorer implementada en los smartphones utiliza esta técnica, con la cual se pretende reducir el impacto de los códigos maliciosos basados en web. Este sistema operativo emplea el concepto de "chamber" o cámara y se refiere a que cada aplicación corre en su propio espacio delimitado, la gestión de dicho espacio está regulado mediante políticas del sistema, estas políticas definen las características del sistema a ser usadas por cada una de las 4 cámaras en las que se basa el sistema operativo, y son:

- TBC (Trusted Computing Base), corresponde a la cámara con más privilegios del sistema operativo, prácticamente permite el acceso sin restricciones a la mayoría de funciones del dispositivo incluyendo la modificación de las propias políticas de seguridad. Es en esta cámara donde se ejecuta el kernel del sistema.
- ERC (Elevated Rigths Chamber), esta cámara cuenta con una serie de privilegios del sistema operativo, pero a diferencia de la anterior (TBC) no permite modificar las políticas de seguridad.
- SRC (Estándar Rigths Chamber), es la cámara asignada como la opción por defecto en donde se ejecutan todas las aplicaciones preinstaladas en el dispositivo.
- LPC (Least Privileged Chamber), corresponde a la cámara en donde se ejecutan todas las aplicaciones de terceros (que no son desarrolladas por Microsoft).

En cuanto al cifrado de los recursos del dispositivo, Windows Phone soporta varios algoritmos de cifrado, como: AES, SHA-1, SHA-256, por mencionar algunos. Otra característica destacable de

este sistema operativo es que bloquea la tarjeta de memoria (SD[11]) si es extraída del dispositivo y por lo tanto no será posible leerla desde otro dispositivo o computadora. La versión 8 de este sistema ha recibido una importante certificación de seguridad por parte del gobierno de los E.U.A, se trata del estándar FISP 140-2, este estándar garantiza la protección de la información por medio de módulos criptográficos incluidos en el sistema operativo.

Por otra parte un estudio elaborado por Symantec, en el cual se examinó la seguridad entre Android e iOS, en los siguientes aspectos:

- Ataques basados en la web y en redes.
- Software malicioso.
- Ataques de ingeniería social.
- Abuso de disponibilidad de servicios y recursos.
- Pérdida de datos por acción maliciosa y no intencionada.
- Ataques a la integridad de los datos del dispositivo.

Reveló los siguientes datos:

- Número de vulnerabilidades en iOS: alrededor de 200 en la diferentes versiones de iOS, de éstas la mayoría fue catalogada de bajo impacto lo que quiere decir que sólo permitían al atacante apropiarse del control de un proceso, algunas otras se consideraron de alto impacto ya que permitía escalar privilegios hasta tomar el control del dispositivo como administrador.
- Número de vulnerabilidades en Android: 18 en las diversas versiones de Android, de éstas la gran mayoría se catalogaron como de bajo impacto lo cual implica que sólo permitían tomar el control de un proceso. Y muy pocas fueron clasificadas como de alto impacto, que implica que el atacante pueda obtener el nivel de root para controlar el dispositivo.

Al analizar estos datos la cuestión que viene a la mente es por qué a pesar de estos parámetros, el índice de ataque a Android por malware lo convierte en el principal objetivo. Como se había hecho mención previamente, los ciberdelicuentes prefieren atacar al sistema que tiene mayor presencia en el mercado (lo que significa que el número de víctimas es mayor), y un aspecto

[11] SD: corresponde el acrónimo de Secure Digital, es un estándar de tarjetas de memoria para dispositivos portátiles.

importante al que se llega a partir de la información previa, es que Android deja en manos del usuario la decisión de otorgar o no, los permisos a cada aplicación (como lo indica el tercero de sus pilares de seguridad), en cambio iOS en este aspecto provee al usuario mayor protección contra malware debido a que tiene un proceso más riguroso en comparación con Android tanto para el proceso de certificación de aplicaciones como el de certificación del desarrollador.

Así que el ataque de malware no tiene que ver con que Android sea un sistema demasiado inseguro ya que si de esto se trata iOS lleva la delantera en cuanto al número de vulnerabilidades que el estudio de Symantec reveló, sino que los autores del malware aprovechan en la gran mayoría de los casos el eslabón más débil en la cadena de la seguridad informática o sea el usuario, para que a través de las aplicaciones, que sin duda captan la mayor parte de la atención de éstos por las diversas funcionalidades que ofrecen el autor del malware aprovecha esto para insertar en ellas el código malicioso, explotando así las vulnerabilidades del sistema en una gran variedad de formas.

Otro aspecto relacionado con la seguridad en Android tiene que ver con la vigilancia mundial revelado por documentos filtrados entre 2013 y 2014, debido a que se ha descubierto que agencias de inteligencia estadounidenses y británicas como: la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) y el Cuartel General de Comunicaciones del Gobierno (GCHQ por sus siglas en inglés), respectivamente, tienen acceso a información de los usuarios de Android e iOS, como son: llamadas telefónicas, mensajes de texto (SMS) y multimedia (MMS), geolocalización, correos electrónicos, notas, contenido multimedia, por mencionar algunos. Todo esto con base en documentos filtrados por Edward Snowden considerados de alto secreto, en estos documentos se establece que se han establecido métodos con el fin de vigilar a las personas, introduciendo software espía en aplicaciones muy populares como: Angry Birds y Google Maps, además de interceptar información personal a través de internet y redes sociales. Posterior a la publicación de estos hechos la NSA y la GCHQ, argumentaron que esas actividades cumplen con las leyes nacionales e internacionales, pero esto hace que la preocupación de los usuarios (informados) aumente en países donde no se cuenta con leyes lo suficientemente sólidas en temas de protección de datos personales.

Por otra parte China y Rusia han acusado a Apple de que iOS cuenta con puertas traseras que cuestionan la privacidad de los usuarios. Este aspecto fue puesto a la luz pública por el hacker llamado “Jonathan Zdziarski” quien cuestionó a Apple por tener partes de código sospechosas que

según él podrían ser rastreadores que leen los datos, así como servicios que evaden el cifrado de datos para ser transmitidos, por su parte Apple respondió que los aspectos señalados correspondían a las funciones de diagnóstico y que nunca ha trabajado con ningún gobierno con el fin de crear puertas traseras en sus dispositivos y facilitar datos de los usuarios. Bajo este contexto Rusia solicitó a Apple el código fuente de iOS, a través del ministro de comunicaciones Nikolai Nikiforov, ya sea directamente o a través de una tercera empresa (como lo hizo Microsoft en el pasado).

Con base en la información anterior se concluye que el código malicioso no es exclusivo de los ciberdelicuentes, sino que también es utilizado por agencias de seguridad según éstas con objetivo de vigilar y proteger los intereses de sus respectivos países, siempre con apego y respeto a las leyes correspondientes. Haciendo de este aspecto de la seguridad algo muy delicado que sin duda debe ser tomado muy enserio por los usuarios.

2.5 Las tiendas de aplicaciones para Smartphones.

El modelo de las tiendas de aplicaciones fue impuesto por Apple por medio de la App Store, tiempo después Google lanzó el Android Market que actualmente tiene el nombre de la Google Play y por ultimo está Microsoft con su Windows Phone Store. El objetivo de estas tiendas es concentrar en un punto de distribución oficial las aplicaciones desarrolladas para cada sistema operativo de smartphones, de esta forma se pretende controlar a las aplicaciones para que estén libres de código malicioso.

- **Google Play**, es para Android el repositorio oficial para aplicaciones de este sistema operativo, en un principio sólo bastaba con que: el desarrollador creara una cuenta de programador válida, declarara que permisos necesita la aplicación para funcionar, firmara su aplicación digitalmente para que estuviera disponible en la tienda, así como acatar lo establecido en el "Acuerdo de distribución de programadores de Google Play" y las "Políticas del Programa para Desarrolladores de Google Play" en general esta tienda es más "flexible" para la publicación de aplicaciones ya que no establece más procesos que hacen más tardada la aprobación de una aplicación. Debido a esto los creadores de malware aprovechaban esas facilidades que brindaba esta tienda para introducir aplicaciones con

malware oculto, ante esta situación Google con el transcurso de los años ha ido haciendo un poco más estrictas sus políticas de contenido en las aplicaciones de la tienda, como por ejemplo: los desarrolladores se tendrán que abstener de usar nombres y/o iconos muy similares a los de aplicaciones muy populares con el fin de evitar engañar a los usuarios, en la descripción de la aplicación se debe especificar lo que realmente realiza y no estar llena de palabras clave para manipular la clasificación o la relevancia en los resultados de búsqueda dentro de la tienda, quedan prohibidas todas aquellas aplicaciones que promuevan la pornografía o incluyan contenido sexual explícito, productos peligrosos; este aspecto prohíbe a los desarrolladores redirigir a los usuarios a enlaces en donde se pueda descargar cualquier tipo de malware así como recopilar información del usuario sin su consentimiento, entre muchos otros aspectos que se encuentran con mayor detalle en **"Políticas del Programa para Desarrolladores de Google Play"**

Con los cambios que se han mencionado, Google pretende poner un poco más de orden en las más de 600 000 aplicaciones disponibles en su tienda y acabar con las aplicaciones llenas de spam o con malas prácticas, con el fin de proteger a los usuarios. A pesar de estas medidas no se debe olvidar, que al final el usuario es quien tiene el control total sobre lo que instala en su dispositivo y por lo tanto debe de estar al pendiente de los permisos que otorga a cada aplicación. En el caso de ser necesario Google podrá acceder remotamente al dispositivo de cada usuario con el fin de eliminar una aplicación que esté catalogada como peligrosa.

- **App Store**, esta tienda de aplicaciones perteneciente a Apple establece que los desarrolladores deben crear una cuenta como tales, pagar una tarifa anual, acatar lo establecido en el "acuerdo de licencia del desarrollador para iPhone" y someter su aplicación a un proceso de aprobación realizado por la misma compañía, este proceso a grandes rasgos valida que la aplicación funcione tal cual como lo describe el desarrollador y que no desestabiliza el funcionamiento del iPhone. Con todas estas medidas aunadas a la serie de restricciones que Apple impone a los desarrolladores es como logra mantener el malware alejado de su sistema operativo iOS.
- **Windows Phone Store**, es la tienda de aplicaciones para smartphones perteneciente a Microsoft, en ésta se obtienen aplicaciones desarrolladas por terceros. Los desarrolladores

deben de pagar una cuota anual de suscripción y acatar lo establecido en sus respectivas políticas de contenido que establece la compañía, algunos ejemplos del contenido prohibido por estas políticas incluyen: pornografía, promoción de violencia, la discriminación, alcohol, drogas, entre otros.

Como se ha mencionado las tiendas oficiales implementan una serie de controles con el fin de proporcionar aplicaciones seguras y libres de malware, pero en la internet hay una amplia variedad de tiendas alternativas (no oficiales) de aplicaciones para las distintas plataformas móviles, siendo en ciertos casos más atractivas que las oficiales porque ofrecen características diferentes de las que hay en repositorios oficiales, y es por estas razones que muchos usuarios acuden a ellas para descargar aplicaciones, sin tener presente en ese momento los riesgos que implica, como: no estar reguladas por una serie de políticas que les prohíba mostrar cierto contenido inapropiado y/o no contar con un análisis que permita detectar código malicioso.

De acuerdo con el informe de la firma F-Secure correspondiente al primer trimestre de 2014, sólo el 0,1% del malware para Android está en la tienda oficial Google Play y ésta realiza varias acciones día con día con tal de mejorar su seguridad y eliminar lo más pronto posible alguna aplicación maliciosa que se llegue alojar ahí. Por lo tanto el 98,9% del malware restante se aloja en las tiendas de aplicaciones no oficiales, destacando: Android159 (con 33,3%), Mumayi (7 %), Wandoujia (5 %), Anzhi y Baidu (ambas con 3%, éstas últimas cuatro operan en China), entre muchas otras.

Capítulo 3

La seguridad en los Smartphones

3.1 Los datos y la información.

Los datos son una representación por medio de símbolos (numéricos, alfabéticos, alfanuméricos, entre otros) de un atributo o variable, se obtienen de la observación y análisis a hechos concretos. Por lo tanto los datos, son un conjunto discreto de hechos, que se almacenan en un medio físico o digital, permitiendo clasificarlos como:

- **Cuantitativos**, se refieren a la representación por medio de números de ciertas características.
- **Cualitativos**, se emplean para describir un conjunto de características que describen a las personas, seres vivos o cosas.

Los datos poseen características como:

- **Ser identificables**, esto se debe a que están constituidos por una serie de símbolos que no dan posibilidad a confusión.
- **Ser contrastables**, este aspecto se refiere a determinar si son verdaderos o falsos.

Los datos por sí mismos en forma aislada no representan información relevante debido a que carecen de sentido, contexto e interpretación. Por lo tanto son irrelevantes para la toma de decisiones.

En tanto que, la información se conforma por un conjunto ordenado de datos los cuales son procesados según la necesidad de los usuarios, teniendo como base un contexto y enfoque específico dando como resultado una estructura útil a partir de la cual se puede obtener algún tipo de conocimiento y por lo tanto ayuda a la toma de decisiones. Se considera que los datos se convierten en información cuando cumplen con alguno de los siguientes atributos:

- **Contextualizados**, de tal forma que se sabe para qué propósito fueron recabados.
- **Categorizados**, con el fin de que tengan un orden y sean más fáciles de operar.
- **Calculados**, de esta forma se tiene la certeza que los datos han sido analizados matemáticamente.
- **Corregidos**, de tal forma que se han eliminado datos erróneos.
- **Condensados**, dando como resultado datos más concisos.

Entre algunas de las características más representativas de la información, están:

- **Significado**, está relacionado con la semántica y es extraído del conjunto de datos y responde a la pregunta: ¿Qué quiere decir? Depende de la interpretación de cada individuo así como del contexto en el que se está analizando la información.
- **Importancia**, es asignada por el receptor y está asociada a la pregunta: ¿Aborda alguna cuestión importante? En este sentido la importancia de la información para el receptor, se basa en el grado que se modifica su actitud o conducta ante ciertas circunstancias.
- **Vigencia**, tiene una estrecha relación con el tiempo y depende de éste para evaluar si la información es útil al momento en que se conoce.
- **Validez**, se fundamenta en la fiabilidad del emisor de proporcionar indicios verídicos y comprobables, que den certeza de que la información que proporciona es verídica.
- **Valor**, es un aspecto que depende del destinatario y de la situación de uso, teniendo en cuenta aspectos subjetivos y objetivos que influyen al momento de evaluar los datos para obtener a partir de éstos información bajo un determinado contexto.

3.2 Seguridad de la información y seguridad informática.

La seguridad de la información es un término que está relacionado con el conjunto de medidas preventivas y reactivas que tienen como principal objetivo, mantener las siguientes propiedades de la información que se pueden observar en la figura 3.1 y son considerados los pilares de la seguridad de la información:

Figura 3.1. Los pilares de la seguridad de la información.

- **Confidencialidad**, se refiere a la confianza y seguridad reciproca que existe entre dos o más personas, dentro del contexto de la seguridad de la información se considera como un propiedad de ésta. La confidencialidad ha sido definida por la Organización Internacional de

Estandarización (ISO) en la norma ISO/IEC 27002 como: “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso”, garantizando así la protección de la información intercambiada entre un emisor y uno o varios destinatarios frente a terceros.

- **Disponibilidad**, es la propiedad que garantiza el acceso a la información por quienes estén autorizados para acceder a ella, siempre y cuando se cumplan los controles de seguridad previamente establecidos.
- **Integridad**, se establece como una propiedad que tiene como objetivo mantener los datos libres de modificaciones no autorizadas, asegurando que la información es exacta y completa. La exactitud de la información se debe mantener en todo momento en el ciclo de vida de la información (como se muestra en la figura 3.2), porque de esta forma se conoce al autor y el momento de las modificaciones, dando así certeza y fiabilidad de la información.

Figura 3.2. Ciclo de vida de la información.

Por lo tanto la seguridad de la información abarca todos los medios y formas donde se almacena y/o procesa la información (no sólo el medio informático y la parte técnica).

La seguridad informática, de acuerdo a la RAE se define como: el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Siendo la seguridad informática una disciplina que se enfoca en la protección de la infraestructura computacional, y todo lo relacionado con ésta, en especial, la información almacenada, procesada y circulante. Se ocupa de diseñar normas, procedimientos, métodos y herramientas técnicas con el propósito de conseguir un sistema de información con un nivel de seguridad razonable y confiable. Tiene como objetivos principales: la confidencialidad, la disponibilidad y la integridad de la información, siendo así un subconjunto de la seguridad de la información como se ilustra en la figura 3.3.

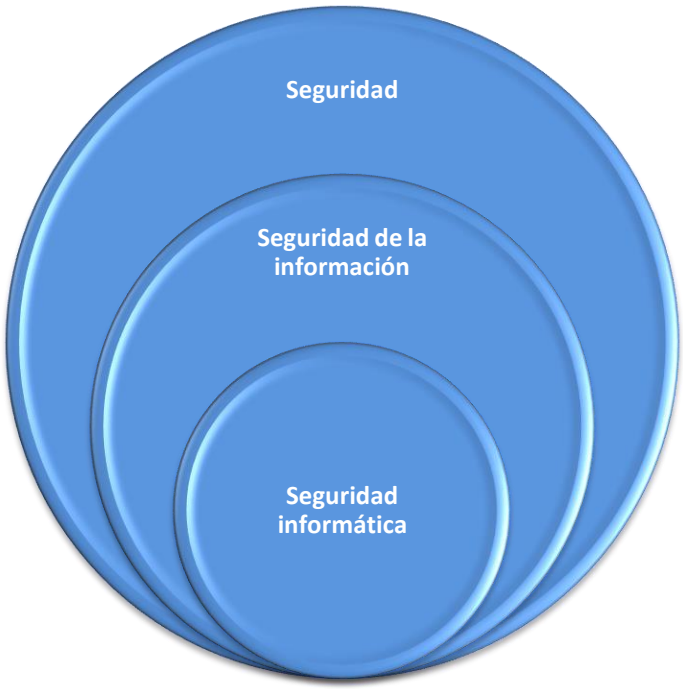


Figura 3.3. Relación entre seguridad de la información y seguridad informática.

Se considera apropiado establecer el ámbito dentro de la seguridad en donde quedarán establecidos los smartphones para el presente trabajo, pues bien, como se hizo mención en capítulos previos, los smartphones son el producto de años de investigación y avances tecnológicos en el ámbito de la electrónica y la computación, al grado de tener hoy en día computadoras de bolsillo capaces de procesar información tanto para fines recreativos, como de trabajo y sociales. Es por esta

razón que la seguridad informática representa la base de estos dispositivos, pues gracias a éstos la información se procesa y almacena de forma automática, y debido a que también considera a todo lo relacionado a ellos, por lo tanto; el usuario, al ser el principal operador del dispositivo y ser considerado como el aspecto más débil en cuestiones de la seguridad informática, proporciona los fundamentos necesarios para que se desarrolle en torno a él una serie de buenas prácticas que le permitan mantener su dispositivo e información libre del malware, que como también se mencionó en capítulos previos es el vector más utilizado en estos dispositivos para sustraer o modificar información sensible.

Actualmente los smartphones son los dispositivos móviles que más presencia tienen en el mercado como ya se ha señalado, y están en constante expansión en el mercado, presentando así para gran parte de los usuarios un artículo indispensable en su día a día, en especial por la información que en ellos se consulta y almacena, de manera que la información representa un activo muy importante en estos dispositivos.

Por otra parte el acceso a internet que proporcionan los smartphones a los usuarios se vuelve fundamental para la consulta de cualquier tipo de información que demande el usuario, así como para la obtención de cualquier aplicación que les brinde cierta funcionalidad tanto para sus actividades de trabajo o de entretenimiento. Siendo la internet parte indispensable, se muestra a continuación en la figura 3.4 el registro de usuarios de internet en México, de acuerdo al: "Estudio sobre los hábitos de los usuarios de internet en México 2014.", en dicha imagen se puede apreciar cómo ha incrementado de manera notable el acceso a la red por parte de la sociedad mexicana.

Figura 3.4. Usuarios de internet en México de 2006 a 2013, las cifras en millones calculadas por el IFETEL al mes de diciembre de 2013 con base a información del INEGI y la AMIPCI.

Fuente: AMIPCI, "Estudio sobre los hábitos de los usuarios de internet en México 2014"

Ese mismo estudio también indica que el hogar de los usuarios es el principal lugar de conexión, seguido por el trabajo; accediendo a través de redes inalámbricas (de acceso público y privado), siendo el viernes el día con mayor índice de conexión y dedicando en promedio un tiempo de conexión al día de 5 horas con 36 minutos, en la figura 3.5 se detallan mejor los datos previamente mencionados.

Por otra parte en la figura 3.6, se aprecian los tipos de dispositivos más utilizados por los usuarios de México para conectarse a la red, los tres más destacados son: en primer lugar la Laptop, seguida por la PC de escritorio y por último los smartphones haciendo mención a que 5 de cada 10 internautas acceden por medio de éste, teniendo abierta la posibilidad que incrementará de forma considerable en los próximos años debido a que estos dispositivos se vuelven más asequibles.

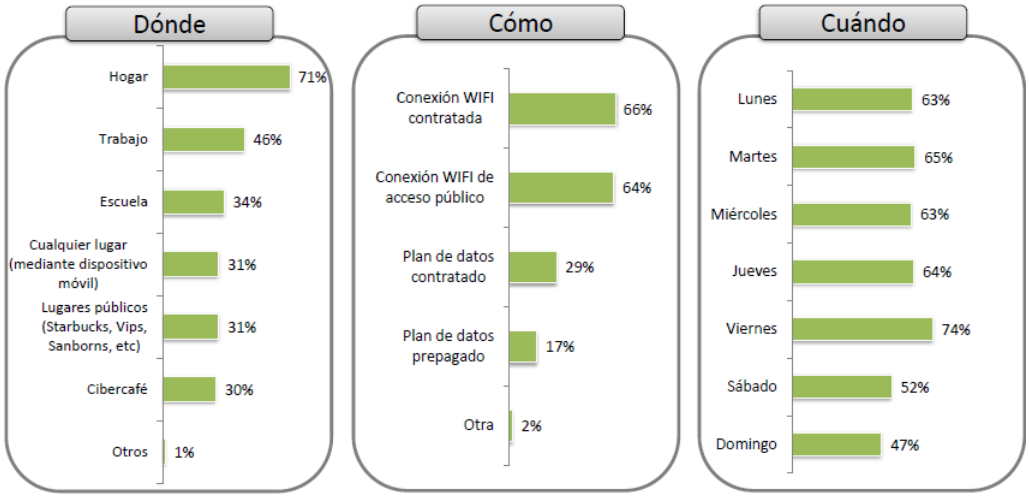


Figura 3.5. Indica el lugar, medio y día de conexión a internet de los usuarios en México.

Fuente: AMIPCI, "Estudio sobre los hábitos de los usuarios de internet en México 2014"

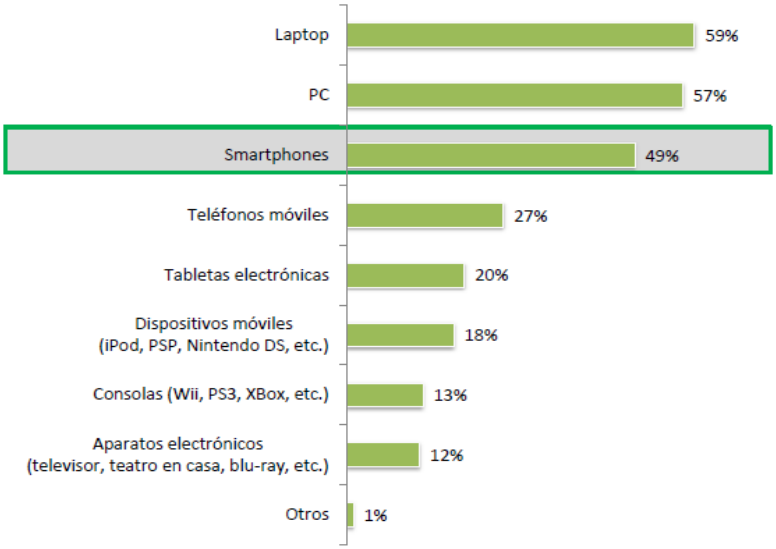


Figura 3.6. Índice de los dispositivos para conectarse a internet de los usuarios en México en 2014.

Fuente: AMIPCI, "Estudio sobre los hábitos de los usuarios de internet en México 2014"

Retomando el aspecto de la información las actividades más comunes a través de la red, se muestran en la figura 3.7. Siendo el año de 2014 donde las redes sociales superaron la búsqueda de información, respecto años previos, dando como resultado que 9 de cada 10 internautas acceden a una red social.

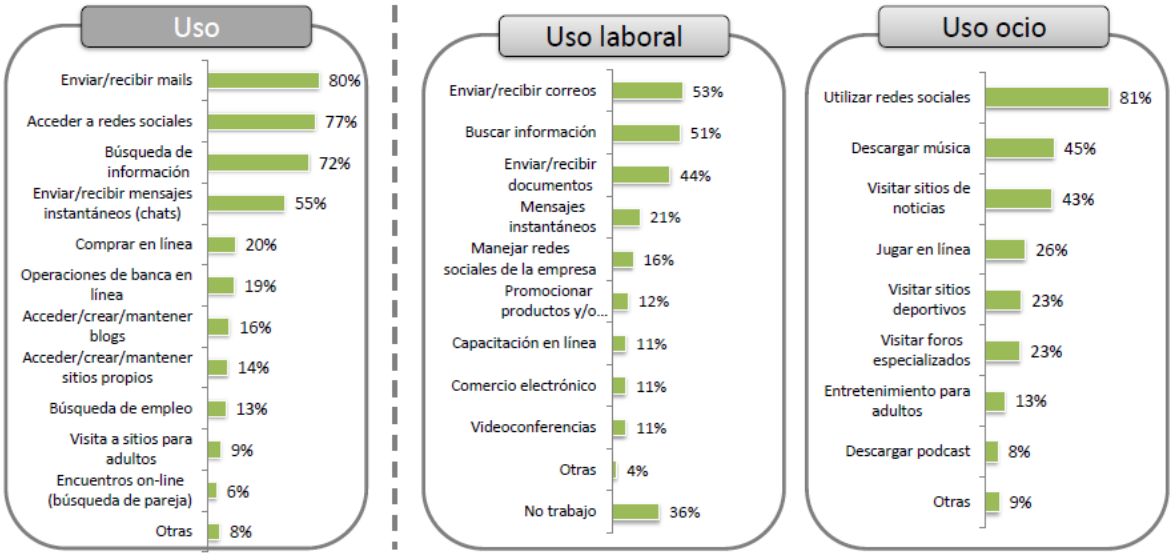


Figura 3.7. Información consultada en internet por los usuarios en México en 2014.

Fuente: AMIPCI, "Estudio sobre los hábitos de los usuarios de internet en México 2014"

Otro aspecto que está a la alza relacionado con los smartphones, es la banca móvil y en especial los pagos móviles[12], este último relacionado con el comercio electrónico. Con base en el artículo publicado en "El Financiero" el 12 de diciembre de 2014, PayPal estimó que a finales de 2014 el gasto online crecería un 26 por ciento, a 97 mil 183 millones de pesos, de los cuales las plataformas móviles abarcan 15 mil 227 millones de pesos y tendría un avance casi del doble, a un 46 por ciento respecto a años anteriores. Mientras que para 2015 se estima que el gasto por medio de dispositivos móviles aumente otro 39 por ciento, colocándose en 21 mil 91 millones de pesos, mientras que el comercio electrónico crecerá un 19 por ciento, a 116 mil 50 millones de pesos. Estas tendencias son impulsadas por instituciones bancarias como: Visa, Banorte y tiendas online como: Linio, Privalia y Dafitti, las cuales para 2015 esperan obtener buenos resultados de las plataformas móviles. Para cerrar lo mencionado en este artículo, se muestran en la figura 3.8 los dispositivos empleados para llevar a cabo compras en línea y en la figura 3.9 se muestra una proyección económica de los próximos dos años de cómo evolucionará el gasto tanto en móvil como en línea.

Figura 3.8. Dispositivos empleados para las compras en línea.

Fuente: El Financiero, articulo:" Pagos móviles suben 46%, el doble que comercio electrónico"

[12] Pagos móviles: se refieren al conjunto de servicios que permite realizar transacciones financieras por medio de smartphones o tabletas electrónicas.

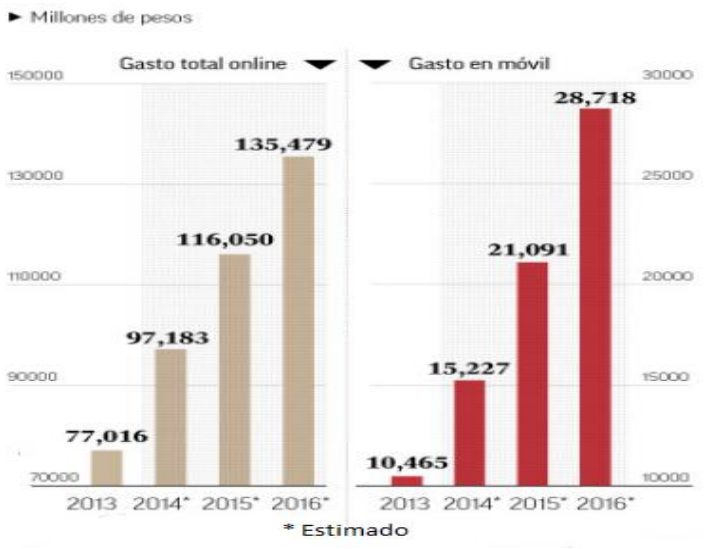


Figura 3.9. Estimación (en millones de pesos) para los próximos dos años, que el comercio en línea registre un crecimiento del 76 por ciento, mientras que las compras mediante un dispositivo móvil aumenten hasta 174 por ciento.

Fuente: El Financiero, articulo:" Pagos móviles suben 46%, el doble que comercio electrónico"

El objetivo de mencionar estos aspectos está en establecer la importancia que van adquiriendo los dispositivos móviles, en especial los smartphones para realizar transacciones financieras y el impacto económico que generan, si bien se debe de poner atención en los protocolos, estándares y regulaciones que deberán de cumplirse para brindar a los usuarios la certeza de que su información al momento de realizar estas operaciones se manejen bajo los pilares de confidencialidad, disponibilidad e integridad y así proporcionar la confianza al usuario para emplear estos servicios en su beneficio, esto será responsabilidad de quienes ofrezcan tales servicios, pero no se debe de olvidar el aspecto que es considerado el más débil, el usuario, que podría ser susceptible a fraudes por medio de la ingeniería social o mediante el desarrollo de un tipo específico de malware que logre comprometer la información sensible que se opera en estas transacciones, por tales motivos los usuarios deben prestar atención a las medidas que deberán de emplear en caso de hacer uso de estos servicios financieros mediante sus dispositivos móviles, pues como se mostró en la figura 3.9 las cantidades monetarias que se manejan no son nada insignificantes y aunque sea

mínimo el porcentaje del cual se beneficien los ciberdelicuentes, representarían ganancias bastante lucrativas.

3.3 Amenazas, vulnerabilidades, riesgos y ataques.

La constante evolución y desarrollo de nuevas tecnologías de información suele generar un gran interés para quienes las utilizan en su trabajo o como parte de su entretenimiento y hasta como medio para socializar, siendo un ejemplo de esto, lo relacionado con los teléfonos inteligentes que integran en cada dispositivo de última generación aplicaciones cada vez más sofisticadas con el propósito de brindar al usuario una simplificación de sus tareas cotidianas y así volverse parte indispensable en su vida, dando lugar a que la mayoría de las veces los usuarios sólo se centren en las soluciones a cuestiones específicas de su día a día, descuidando la necesidad de comprender las consecuencias que tendría si estos dispositivos o sus aplicaciones llegasen a fallar, de tal forma que su información quede expuesta a diversos eventos que probablemente le afecten. Teniendo presente lo anterior es indispensable establecer conceptos básicos relacionados con la seguridad informática, como son:

A) Amenazas

Dentro del contexto de la seguridad informática están las amenazas, las cuales son consideradas como probables eventos subyacentes no deseados, que de materializarse pueden llegar a causar alteraciones a la información y/o ponerla a disposición de terceros sin autorización del propietario. Con lo cual se comprometen las tres propiedades que se mencionaron anteriormente (Confidencialidad, Disponibilidad e Integridad), las amenazas se consideran ajenas al usuario y por lo tanto no es posible que las controle y mucho menos que las elimine, así que la forma de protegerse de las amenazas es estableciendo una serie de medidas para protegerse de éstas. Las amenazas tienen diversos orígenes, siendo: amenazas de tipo: humano, de hardware y de software.

Las amenazas de tipo humano, están relacionadas directamente a las personas y pueden propiciar eventos que afectan alguna de las propiedades de la información, entre este tipo de amenazas, tenemos:

- **Ingeniería Social**: Es una práctica por la cual se obtiene información confidencial a través de la manipulación de usuarios legítimos, empleando para esto un conjunto de técnicas

psicológicas y habilidades sociales utilizadas de forma consciente y premeditada por parte del atacante.

- **Fraude**: Esta actividad consiste en alterar, borrar o robar datos, como por ejemplo: los contactos, imágenes, documentos, entre otros, que lleguen a comprometer a la víctima ante alguna situación específica con el fin de obtener algún beneficio por parte del o los autores del fraude.

- **Robo de dispositivo:** Se refiere a la extracción física del dispositivo por parte de un tercero. Este aspecto abrió en México una oportunidad de negocio para las firmas de seguridad, las operadoras telefónicas y los desarrolladores de aplicaciones, alcanzando en el año de 2013 un valor de mercado de 3 mil millones de dólares de acuerdo a información de Symantec. Tan sólo en la ciudad de México durante 2013 se registraron 156 mil 681 reportes de robo, según datos del Consejo Ciudadano de Seguridad Pública y Procuración de Justicia, aunque la incidencia es mucho mayor.
- **Curiosidad:** Se trata de personas que acceden a un dispositivo que no les pertenece, con la finalidad de conocer la información confidencial del usuario, motivados por la curiosidad o alguna otra razón que puede causar daños al usuario legítimo.

Las amenazas de hardware, son las relacionadas con fallas en los componentes físicos de los dispositivos, como:

- **Defectos de fabricación:** Están relacionados con los desperfectos en el desarrollo del hardware del dispositivo, y generalmente el fabricante repara los desperfectos apegándose a una serie de normas, para hacer válida la garantía del dispositivo durante un tiempo definido.

- **Mal diseño de hardware:** Se refiere a que los componentes de hardware del dispositivo no son los apropiados para cumplir con los requerimientos necesarios de uso bajo ciertas circunstancias dando como resultado un fallo en el dispositivo.

- **Mal uso por parte del usuario:** En la mayor cantidad de los casos este aspecto tiene que ver con la falta de cultura del usuario, pues no lee ni sigue las indicaciones que el fabricante proporciona para obtener un funcionamiento óptimo del dispositivo, provocando que sufra

daños, en este caso el fabricante no se hará responsable de la compostura, ya que el usuario no tomó las medidas necesarias para operar el dispositivo

En las amenazas de software, se consideran las fallas tanto del sistema operativo o de aplicaciones, teniendo las siguientes:

- **Software de desarrollo:** Es un software personalizado, creado con el fin de atacar un sistema específico por completo o aprovechar alguna de sus vulnerabilidades para violar su seguridad y así extraer información del usuario.

- **Software de aplicación:** Este tipo de software no es creado con la finalidad de atacar el sistema con el cual funciona el dispositivo, sino que es un software legítimo pero con la característica de que han explotado en él alguna vulnerabilidad para extraer información.
- **Código malicioso:** Como se mencionó previamente, el código malicioso es desarrollado con objetivos específicos que van desde obtener información sensible de la víctima hasta dejar inhabilitados los dispositivos, valiéndose de ingeniería social para captar la atención de las víctimas y que sean éstas mismas quienes llevan a cabo la infección, este tipo de amenaza resulta ser el más empleado por los atacantes y el que más auge ha tenido debido a las ganancias que genera, además de que el usuario aún no tiene la cultura de investigar o informarse sobre los permisos que da a las aplicaciones que instala en su teléfono inteligente.

- **Mal uso por parte del usuario:** Este aspecto está relacionado con el uso indebido por parte del usuario, como por ejemplo la descarga de aplicaciones de repositorios no oficiales, en donde se aloja gran cantidad de malware. Otro aspecto es que el usuario no cambie los valores de seguridad que vienen de fábrica y que resultan ser bien conocidos por los atacantes.

B) Vulnerabilidades

Una vulnerabilidad es considerada como un error o debilidad en las características del dispositivo o su entorno que lo hacen susceptible a amenazas, se le asocia un grado de daño ya sea tanto en forma cuantitativa o cualitativa de un evento. En general las vulnerabilidades son explotadas por las amenazas y tienen diversos factores, siendo de carácter:

- **Humano,** se asocia a las vulnerabilidades en el comportamiento del usuario, como: las medidas de seguridad débiles y los controles insuficientes que derivan en incidentes que comprometen su privacidad y confidencialidad de sus datos sensibles e incluso de su identidad, como ejemplo está: el desconocimiento por parte de los usuarios, y esto es aprovechado por los desarrolladores de código malicioso para infectar los dispositivos valiéndose también de ingeniería social, dando como resultado que actualmente el malware para smartphones sea una tendencia que está creciendo muy rápido. Un caso reciente que ejemplifica lo anterior, está relacionado con la nueva funcionalidad de WhatsApp para realizar llamadas de voz disponible a partir de marzo de 2015, en un boletín lanzado por Kaspersky, se detectó una campaña cuyo principal objetivo eran usuarios de Brasil y otros países de Latinoamérica, en lo que consiste es que se distribuyen enlaces de instalación de aplicaciones móviles ilegítimas que instalan Adware para las plataformas iOS y Android. El ataque comienza con la llegada de un mensaje por parte de un contacto conocido, en el mensaje se invita al usuario a entrar a un sitio en donde es posible activar la nueva funcionalidad de llamadas, bajo la condición de compartir dicho sitio con 10 contactos. Aunque por el momento solo se instala Adware, que es código que muestra publicidad, no se descarta la posibilidad de que se distribuya malware más peligroso como troyanos bancarios, bots o troyanos SMS, los cuales roban dinero directamente de las víctimas.

- **De hardware**, representan los posibles defectos de fabricación o configuración de los componentes físicos del dispositivo que probablemente permitieran la materialización de un ataque.

- **De software**, son los errores relacionados con la programación tanto de aplicaciones como de los sistemas operativos, entre las más comunes están las vulnerabilidades de “día cero”, que son defectos que están presentes en las aplicaciones desde que salen al mercado y son desconocidas por el fabricante y el usuario, hasta el momento en que son explotados por atacantes o personas que se dedican a investigar estos errores y hacerlos públicos al fabricante para que corrija el error.

C) Riesgo.

Es considerado como el producto, de que una amenaza encuentre y explote una vulnerabilidad produciendo así un ataque o evento de seguridad, teniendo como consecuencia un impacto negativo para el usuario. Por lo tanto, cuanto mayor es la vulnerabilidad mayor es el riesgo, una forma de expresar este concepto es mediante la siguiente expresión matemática:

$$Riesgo = Amenaza * Vulnerabilidad$$

Donde:

$$Amenza = Probabilidad\ de\ que\ suceda\ un\ evento$$

$$Vulnerabilidad = Grado\ del\ daño$$

Al hablar del riesgo es necesario abordar el proceso denominado como gestión del riesgo que se puede aplicar a diversos contextos, siendo su función principal mitigar los riesgos, es decir, que tengan un nivel aceptable para el usuario. En el contexto de los teléfonos inteligentes implicaría una serie de métodos que tienen como propósito mantener y garantizar la privacidad de los datos de los usuarios. A continuación las cuatro fases las que conforman dicho análisis:

- **Fase 1**

  Análisis del riesgo, tiene como objetivo conocer y determinar qué componentes de un sistema requieren protección, identificando las vulnerabilidades y amenazas que lo ponen en una situación de riesgo, hasta llegar a un nivel aceptable y tolerable. Durante este proceso se llevan a cabo los siguientes cuatro pasos:

  1. Identificar y clasificar los datos e información en los siguientes rubros: confidencial, privado, sensitivo y público.
  2. Identificar y valorar los riesgos y las amenazas así como determinar su probabilidad de ocurrencia (baja media y alta). Dentro de los diversos métodos de como valorar un riesgo, en el ámbito de la seguridad informática se emplea la matriz para el análisis de riesgos, que a su vez se apoya de la expresión matemática, que anteriormente se mencionó:

$$Riesgo = Amenaza * Vulnerabilidad$$

A partir de esta expresión, la representación del riesgo se grafica en dos dimensiones siendo el producto de multiplicar la amenaza por la vulnerabilidad, siendo el eje "x" (horizontal) el que representa la probabilidad de amenaza y eje "y" (vertical) el que se asocia al grado del daño provocado por el riesgo, como se puede observar en la figura 3.9.

Figura 3.10. Matriz de riesgo.

La probabilidad de amenaza y grado del daño tiene los siguientes valores: 1=insignificante, 2=bajo, 3=mediano y 4=alto. Esta escala no es fija ya que se ajusta a las necesidades de cada contexto, además depende de la literatura consultada pues algunas veces toma hasta seis diferentes valores.

En este método el riesgo se agrupa en tres rangos que corresponden a los colores: verde (1-6)=riesgo bajo, amarillo (8-9)=riesgo medio y rojo (12-16)=riesgo alto.

La probabilidad de amenaza, para estimar este aspecto debe tomar en cuenta las siguientes consideraciones:

- ✓ ¿Cuál es el interés o la atracción por parte de otros individuos para atacar? Algunas razones pueden ser que los usuarios manejan información que contiene

algo significativo, como información comprometedora, que sea del interés de competidores de trabajo o sólo por dañar la imagen pública.

- ✓ Conocer el nivel de vulnerabilidad, a partir de la identificación de las vulnerabilidades y valorándolas en: baja, mediana y alta. Para la primera es donde existen condiciones que hacen muy lejana la posibilidad del ataque, en la segunda existen condiciones para que el ataque se presente en un corto o largo plazo y por último en la que el ataque es inminente y no existen las condiciones que impidan el desarrollo del mismo.

- ✓ La frecuencia con la que ocurren los incidentes, en este aspecto los ataques que ya se han materializado sirven para identificar una amenaza y si la ocurrencia es frecuente, mayor será la probabilidad de que ocurra otra vez. En el caso de que ya existan medidas implementadas de protección es importante llevar un registro, que muestre los casos en que la medida se aplicó exitosamente y en los que no, porque de esa manera se sabrá en primer lugar si todavía existe la amenaza y segundo, cuál es su riesgo actual.

3. Determinar el impacto de las amenazas, teniendo presente los siguientes escenarios: pérdida de la información, acceso a la información por personas ajenas, manipulación de la información por gente no autorizada. Lo anterior repercute directamente en los objetivos principales de la seguridad informática (disponibilidad, confidencialidad e integridad).

4. Establecer controles para contrarrestar las amenazas.

- **Fase 2**

Clasificación del riesgo, se determina hasta qué punto es factible combatir los riesgos identificados, la factibilidad depende de tres aspectos: la voluntad del usuario, su posibilidad económica y su entorno. Una vez hecho el análisis de riesgos, siempre estarán presentes riesgos imposibles de evitar y se les denomina riesgos residuales y no queda más que

aceptarlos. Esta fase se contempla en los pasos 2 y 3 del análisis de riesgos, justamente donde se establece la matriz de riesgo.

- **Fase 3**

  Mitigación del riesgo, se definen e implementan medidas de protección, basadas en establecer controles que reduzcan la incidencia (probabilidad) o severidad (impacto) de eventos no deseados, incluidos los riesgos residuales. Siendo esta fase parte del paso 4 del análisis de riesgos.

- **Fase 4**

  Control del riesgo, en esta última fase se analiza el funcionamiento, la efectividad y el cumplimiento de las medidas (controles) con el fin de mejorarlas y/o adaptarlas a nuevas necesidades.

D) Ataque.

Dentro del contexto de la seguridad informática es la materialización de las amenazas que han aprovechado las vulnerabilidades, y generan un impacto para la víctima. Según el tipo del impacto se tienen los siguientes casos para el usuario:

- ✓ Pérdida de información.
- ✓ Terceros tienen acceso a información.
- ✓ La información es manipulada o está incompleta.
- ✓ La información no está disponible.

Como se observa de los puntos anteriores, el hablar de un impacto repercute directamente en afectar los pilares de la seguridad de la información.

3.4 Estándares.

En la medida en que la tecnología ha permitido procesar y almacenar información por medio de las computadoras y todo lo que este contexto engloba, se han desarrollado medidas de seguridad para proteger la información en dicho entorno dando como resultado la creación de guías y documentos que ilustran cómo abordar la seguridad de una forma responsable, teniendo así los estándares, los cuales son documentos con contenido técnico y administrativo que establece un modelo o referencia a lineamientos a seguir para cumplir una actividad o procedimiento. Actualmente los estándares están centrados en los procesos y actividades de las organizaciones y algunas entidades como: ISO (International Standar Organization), IEEE (Institute of Electrical and Electronic Engenieers), por mencionar algunas, las cuales proponen documentos que son creados a partir de la experiencia y conocimiento de diferentes grupos de expertos.

Las buenas prácticas son un conjunto de acciones coherentes que han rendido un buen resultado en un determinado contexto, por lo tanto se prevén resultados similares en contextos similares. Éstas han probado ser eficientes y eficaces tanto para cumplir una tarea o resolver un problema, como para alcanzar una meta u objetivo.

A continuación, se presentan algunos estándares internacionales dentro del contexto de la seguridad de la información, empleados para el aseguramiento de la información, el activo más valioso, teniendo como pilar la protección a nivel de integridad, disponibilidad y confiabilidad:

Dentro de los estandares se encuantran cuatro varias clasificaciones que abordan diferentes aspectos de la seguridad como: controles (por ejemplo COSO), procesos (por ejemplo CMMI, ISO 9001, entre otros), que están más orientados a las grandes organizaciones que cuentan con una amplia infraestructura de TI y por lo tanto un mayor número de usuarios en diversas áreas. Y para los fines de este trabajo se mencionan los relacionados con los riesgos y buenas prácticas, como se presenta a continuación:

- **Riesgos.**
  - ✓ **BS 7799-3:** Se publicó en 2006 por British Standards Institution (BSI), corresponde a la tercera parte de BS 7799, está enfocado a la gestion de riesgos de seguridad de la informacion en una organizacion. Brinda directrices sobre como: evaluar, tratar, re-

evaluar y monitorear riesgos, así como el proceso de toma de desicisiones por parte de la direccion de la organización en donde se implementa.

- ✓ **ISO 27005:** Este estandar se publicó en 2008 proporciona directrices relacionadas con la gestion de riesgos de la seguiridad de la informacion de cualquier organización, se sustenta en los requerimientos establecidos por la norma ISO 27001. Al ser aplicable a cualquier tipo de organización, no establece una metodología estricta ni específica.

- ✓ **ISO 31000:** Brinda una serie de principios y directices genéricas para la gestión de riesgos, es apta para cualquier organización . Su enfoque se sustenta en tres elementos claves, que son:
    - Principios de gestión del riesgo.
    - Marco de trabajo para la gestion de riesgos.
    - El proceso de gestion de riesgos.

- ➢ **Buenas practicas.**
    - ✓ **ISO/IEC 27002:** Proporciona una serie de recomendaciones basadas en las mejores prácticas de gestion de seguridad de la información, su version más actual es la ISO/IEC 27002:2013, en la cual se establecen trece dominios principales,que son:
        1. Organización de la Seguridad de la Información.
        2. Seguridad de los Recursos Humanos.
        3. Gestión de los Activos.
        4. Control de Accesos.
        5. Criptografía.
        6. Seguridad Física y Ambiental.
        7. Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

8. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.
9. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
10. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.
11. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.
12. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.
13. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

- ✓ **COBIT:** Es el acrónimo de Control Objetives for Information and related Technology (Objetivos de Control para Información y Tecnologías Relacionadas), una guía de mejores prácticas enfocada al control y supervisión de tecnología de información (TI), contienen una serie de recursos para establecer: resumen ejecutivo, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente una guía de técnicas para la gestión. La primer edición fue publicada en 1996 y la versión más actual es la 5, la cual se enfoca en el gobierno de TI y a la información como protagonistas en la creación de valor para las empresas. COBIT 5 integra otros marcos de referencia y normas como: VAL IT, Risk IT, ITIL y normas ISO relacionadas.

- ✓ **BS 25999:** Se publicó en 2006 por British Standards Institution (BSI) y define una serie de buenas prácticas dedicadas a la gestión de la continuidad del negocio basadas

en Bussines Continuity Management, está orientado a cualquier tipo de organización sin importar el sector al que pertenezca.

- ✓ **ITIL:** Es el acrónimo en inglés para Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información), es un conjunto de conceptos y buenas prácticas para: la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con TI. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

Los estándares que se mencionaron fueron elaborados para ser adaptados a grandes organizaciones y por lo tanto a las diversas áreas en las que éstas se puedan dividir y así brindar cierto grado de seguridad razonable a la información que manejan para las necesidades de su negocio. Considerando estos estándares, se tiene como meta elaborar una guía de buenas prácticas enfocada al usuario de los smartphones que le sea de ayuda para evitar ser víctimas de los ciberdelicuentes que explotan las fallas de seguridad en los dispositivos, en especial las relacionadas con el malware.

Capítulo 4

Análisis de malware

Como se mencionó en el segundo capítulo, el malware (código malicioso) dejó de tener como principal objetivo a los equipos de escritorio y se extendió a los dispositivos móviles los cuales han tenido un gran impacto en el mercado y su crecimiento sigue hasta el día de hoy. En el caso de los dispositivos móviles con sistema operativo Android requiere especial atención ya que la cantidad de usuarios de esta plataforma es la que más predomina, por esta razón el llevar a cabo un análisis de malware para esta plataforma se vuelve indispensable y se hace necesario hacerlo sobre alguna muestra de malware para saber: cómo es que afecta al usuario, cuál es el tipo de vector de infección que emplea y sobre todo cómo evitarlo.

4.1 Tipos de análisis de malware.

Dentro de las técnicas para analizar malware, son dos los enfoques más utilizados: el análisis estático y el análisis dinámico. A continuación, su explicación.

- **Análisis estático**: consiste en examinar el archivo malicioso sin tener que ejecutarlo, por decirlo así es como realizar una autopsia para conocer qué es lo que hace o cuales son las consecuencias que generará si llegara a infectar un objetivo. Este tipo de análisis permite conocer: si el malware está empaquetado, el lenguaje en el cual fue desarrollado, las librerías que importa, las funciones que utiliza, entre otras características más. Esta técnica proporciona una vista "superficial" del código malicioso, la cual es muy útil para darse una idea de cómo es que funciona, sin embargo no sería posible conocer y monitorear información que se envíe o reciba a través de la red.
- **Análisis dinámico:** consiste en examinar el código malicioso, ejecutándolo en un entorno controlado observando el comportamiento en la interfaz de usuario, obteniendo así más información sobre su comportamiento con ayuda de herramientas que hacen posible ver el comportamiento del código.

Para llevar a cabo el análisis de malware es necesario establecer los siguientes aspectos:

- **Laboratorio para el análisis de malware**, un laboratorio es un entorno seguro que posee los medios necesarios para realizar investigaciones, experimentos, prácticas y trabajos de carácter científico, tecnológico o técnico bajo condiciones controladas de modo que:

- ✓ Se puede asegurar que no hay condiciones extrañas que alteren el resultado del trabajo.
- ✓ Se garantiza que el experimento o prueba es repetible, bajo los mismos lineamientos.

- **Procesos** (código en ejecución), se vuelven muy importantes tanto para ver el rendimiento del entorno de análisis como el de la máquina anfitriona.

- **Virtualización y emulación**, estos aspectos son importantes dentro del análisis del malware porque gracias a éstos se puede ejecutar el código malicioso dentro de un entorno seguro sin tener la preocupación de que una aplicación maliciosa afecte o modifique el sistema anfitrión (host) de la computadora sobre la cual se lleva a cabo el proceso de análisis, a continuación se explicara en que consiste cada uno de estos términos.

  La virtualización se explica como la creación por medio de software de una versión virtual de algún recurso, pudiendo ser: una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento e incluso recursos de red. Para gestionar la virtualización se necesita de un recurso instalado en la computadora anfitrión, llamado Virtual Machine Monitor (VMM), esta plataforma gestiona y arbitra los cuatro recursos más importantes de la computadora anfitrión (unidad de procesamiento central, memoria, dispositivos periféricos y conexiones de red) con el fin de repartirlos entre las máquinas virtuales dando como resultado tener varias computadoras virtuales ejecutándose en una sola maquina física, como lo muestra el ejemplo en la figura 4.1.

Figura 4.1. Virtualización de tres sistemas operativos diferentes compartiendo hardware del sistema anfitrión.

Un emulador consiste en un software que simula la funcionalidad de otro o de un componente de hardware, permitiendo ejecutar programas en una plataforma diferente de la cual fueron escritos originalmente. En el caso del análisis del malware que se llevará a cabo, la emulación permitirá ejecutar aplicaciones que fueron hechas específicamente para Smartphone con sistema operativo Android dentro del sistema operativo de la computadora (ya sea el sistema anfitrión de la máquina física o en un sistema huésped tratándose de una máquina virtual).

4.2 Recursos disponibles para el llevar a cabo el análisis de malware.

Como ya se establecieron aspectos que se abordarán en el análisis del malware, ahora es momento de establecer los recursos con los cuales se cuenta para llevar a cabo tal análisis. En primer lugar se mencionan las características de hardware con las que cuenta la computadora sobre la cual se va a implementar el laboratorio para el análisis de código malicioso para Smartphone con sistema operativo Android, siendo: una notebook Toshiba satellite con procesador AMD A6-4400M, frecuencia de 2.7 GHz (Giga Hertz) y con posibilidad de aumentar a 3.2 GHz gracias a la funcionalidad "Turbo core"[13], 4 GB (Giga Bytes) de memoria RAM, y 750 GB de almacenamiento en disco duro. Ahora es turno de hacer mención sobre el software (sistema operativo) con el cual se cuenta: de los 750 GB de disco duro, 550 están destinados para Windows 8 (que es el sistema que traía la computadora de fábrica) y los 200 GB restantes los emplea Ubuntu versión 14.04 LTS.

Una vez establecidas las características del equipo de cómputo con el cual se va a trabajar y sabiendo que cuenta con dos sistemas operativos diferentes, lo más acertado será comparar su rendimiento bajo un uso normal (monitoreando el uso del CPU y la memoria RAM) antes de empezar a instalar software para virtualizar las máquinas sobre las cuales se va a analizar la muestra de malware y así poder decidir sobre qué sistema operativo es conveniente trabajar, a continuación en la figura 4.2 se muestra una captura de pantalla de la aplicación Administrador de tareas del sistema operativo Windows 8.

[13] Turbo core: Es una funcionalidad de algunos procesadores AMD, la cual permite incrementar la frecuencia del funcionamiento del procesador bajo ciertas condiciones optimizando así el consumo de energía.

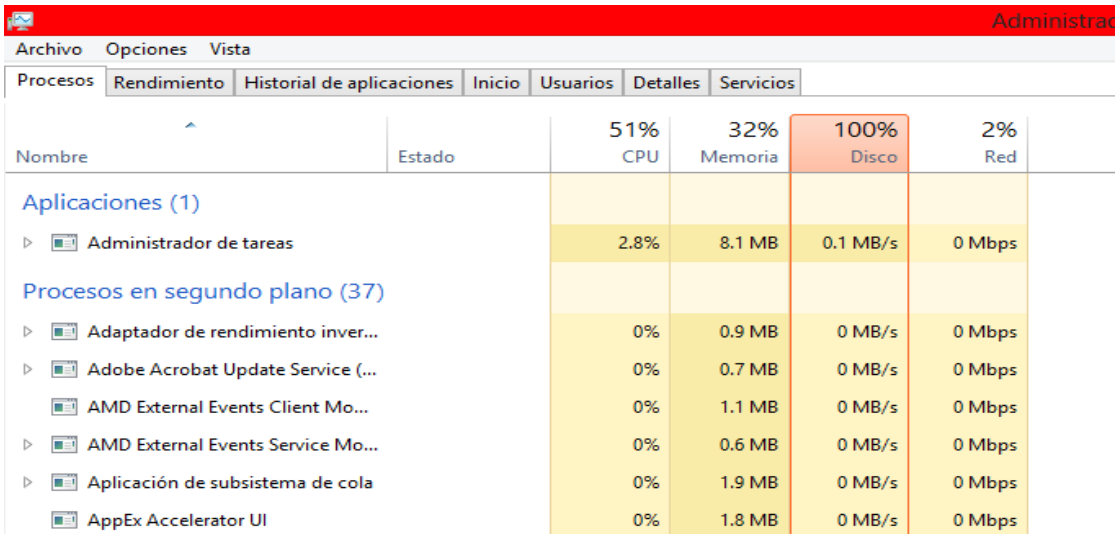


Figura 4.2. Captura de pantalla de la aplicación "Administrador de tareas", en el sistema operativo Windows 8.

De la imagen 4.2 se puede observar que sólo está en ejecución la aplicación Administrador de tareas y en segundo plano 37 procesos asociados con el funcionamiento del propio sistema operativo o de aplicaciones como el antivirus, entre otras. Por lo tanto el sistema no tiene más aplicaciones que demanden más recursos, y se puede observar que aun así el porcentaje de la CPU está a un 51% de su capacidad, la memoria a un 32% (siendo la memoria que reconoce el sistema de 3.5 GB, el 32% equivale a que está en uso 1.12 GB) y el disco duro (acciones de lectura y escritura de archivos) a un 100%. Por lo tanto, si tan sólo con una aplicación ejecutándose en primer plano que no demanda demasiados recursos como lo haría el software necesario para virtualizar, el cual necesitaría una cantidad de memoria mínima de acuerdo al sistema que se virtualice para poder garantizar un desempeño razonable, Windows 8 parece hasta el momento no ofrecer las capacidades suficientes para llevar a cabo el laboratorio de malware sobre este sistema operativo.

Ahora es turno de verificar el rendimiento del hardware con el sistema operativo Ubuntu versión 14.04 LTS, ejecutando la aplicación Monitor del sistema que indica los porcentajes utilizados tanto de la CPU como de memoria RAM, que se observan en la figura 4.3.

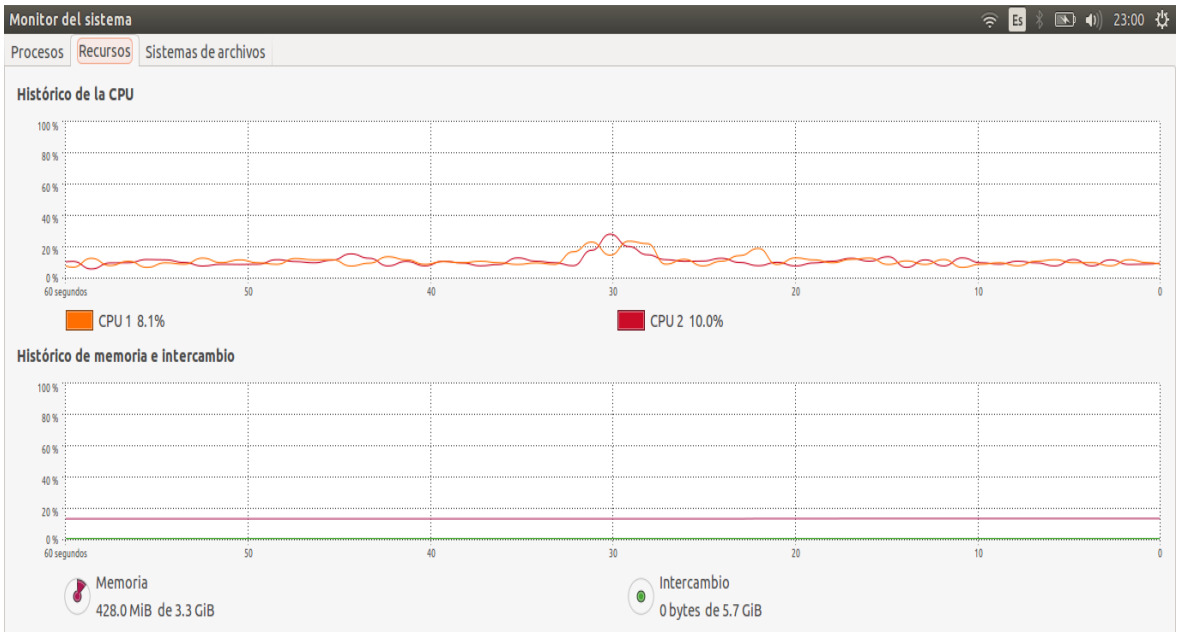


Figura 4.3. Captura de pantalla de la aplicación Monitor del sistema, en el sistema operativo Ubuntu versión 14.04 LTS

De la imagen anterior se observa que el uso registrado por la CPU va del 8.1% al 10% al momento de la captura y el porcentaje utilizado por la memoria RAM es de 428 MB (Mega Bytes, **siendo la memoria que reconoce el sistema operativo de 3.3 GB, por lo tanto la memoria utilizada por el sistema operativo corresponde aproximadamente al 12.67 %).**

Ahora comparando los valores utilizados por Windows 8 y Ubuntu de los recursos de la computadora, se tiene lo siguiente:

- **Para la CPU en Windows 8 ocupa un 51% del procesador, ejecutando en primer plano una aplicación similar que en Ubuntu en donde el procesador como máximo alcanzó el 10%, dando una diferencia de 41% que bien puede ser aprovechado para ejecutar más aplicaciones.**
- **Ahora, comparando los valores de la memoria RAM: en Windows 8 se llegó a ocupar un 32% de la memoria que equivale a 1.12 GB mientras que en Ubuntu sólo se utilizó 428 MB, a pesar de que ambos sistemas presentaban una variación en la cantidad de memoria que reconocen (siendo Windows 8 con 3.5GB y en Ubuntu con 3.3 GB, la diferencia es de sólo 0.2 GB que equivaldría a 204.8 MB) no es una cantidad tan considerable (204.8 MB) si se compara con los (718.88 MB) que Windows 8 utiliza de más al ejecutar la aplicación similar**

que en Ubuntu.

Con base en las razones anteriores del rendimiento de cada sistema operativo, se considera conveniente llevar a cabo la virtualización y por lo tanto el análisis de malware para Smartphone con sistema operativo Android sobre el sistema operativo Ubuntu que debido a la evidencia del rendimiento de hardware es el que presenta mejor desempeño tanto de la CPU como de la memoria RAM.

4.3 Elección del software para la virtualización.

Ya establecido el sistema operativo sobre el cual se va a trabajar, es turno de elegir el software que se va a utilizar para la virtualización de las máquinas, en este punto hay una gran cantidad de opciones, sin embargo no todas son acordes a las necesidades de este trabajo, así que es pertinente discriminar entre la diferentes opciones y elegir aquellas que sean compatibles con el sistema operativo sobre el cual se va a trabajar que como se dijo va a ser Ubuntu, otro parámetro muy importante para elegir el software es el tipo de licencia de la cual hace uso. Bajo estas consideraciones se tiene a VMware Workstation Player y VirtualBox OSE, ambas soportan tanto en sistema anfitrión como en huésped a sistemas GNU/Linux y Windows, entre otros. VMware Workstation Player es una versión con licencia gratuita mientras sea de uso personal y no comercial, aunque comparado con la versión Workstation Pro, posee menos funciones, sin embargo, para las necesidades del presente trabajo son suficientes. Por otra parte Virtual Box a partir de 2007 lanzó su versión Open Source Edition (OSE) y está disponible en el repositorio de software de Ubuntu. Ahora considerando que estas dos opciones se alinean con las necesidades de este trabajo y a los recursos con los cuales se cuenta (ya que son capaces de ejecutarse sobre un sistema anfitrión GNU/Linux, que es el caso de Ubuntu y además de que poseen una licencia gratuita), lo más indicado es ver su desempeño en el consumo de recursos de la máquina anfitrión y así elegir la que mejores resultados tenga, con el fin de aprovechar de una mejor forma los recursos con los cuales se va a llevar a cabo el laboratorio de análisis de malware.

Primero se va a analizar Virtual Box, pero antes de pasar a la instalación es recomendable actualizar en primer lugar el índice de paquetes local del sistema (este índice de paquetes es en esencia una

base de datos de los repositorios de paquetes disponibles, definidos: en el archivo /etc/apt/sources.list y en el directorio /etc/apt/sources.list.d) dando como resultado la actualización de los repositorios. Para actualizar el índice de paquetes local con los últimos cambios hechos en los repositorios, se teclea el siguiente el comando desde la terminal:

sudo apt-get update

Al concluir la actualización de los repositorios, es recomendable actualizar tanto el sistema operativo como los paquetes de aplicaciones instalados en él, pues con el transcurso del tiempo se añaden actualizaciones y para llevar a cabo esto basta con ejecutar el siguiente comando desde la terminal:

sudo apt-get upgrade

Hecho lo anterior se procede a instalar Virtual Box, con el siguiente comando:

sudo apt-get install virtualbox

Una vez que se ha instalado VirtualBox aparecerá el icono en la barra de aplicaciones, para ejecutar la aplicación se da clic sobre éste o también desde la terminal con sólo escribir el nombre de la aplicación en este caso: VirtualBox y presionar la tecla de enter. Hecho lo anterior se desplegará una ventana en la cual se da una bienvenida y una breve explicación de la distribución de la misma, así como los pasos a seguir para crear una máquina virtual.

Para la prueba del rendimiento se va a virtualizar una máquina con sistema operativo Microsoft Windows 7 de 64 bits edición Home Premium, en cuanto a la licencia de uso se empleará la versión de prueba de 30 días. Empezando con la creación de esta máquina el nombre que se le asignara es el de: Prueba 1, con 1024 MB de memoria RAM para un funcionamiento óptimo ya que el recomendado son 512 MB y en cuanto al tamaño del disco duro virtual se le asignaran 25 GB ya que como sólo es una prueba no se necesita una gran cantidad espacio para instalar aplicaciones adicionales que demanden más espacio de almacenamiento, de esta forma se tiene configurado el sistema para la máquina virtual como lo muestra la figura 4.4.

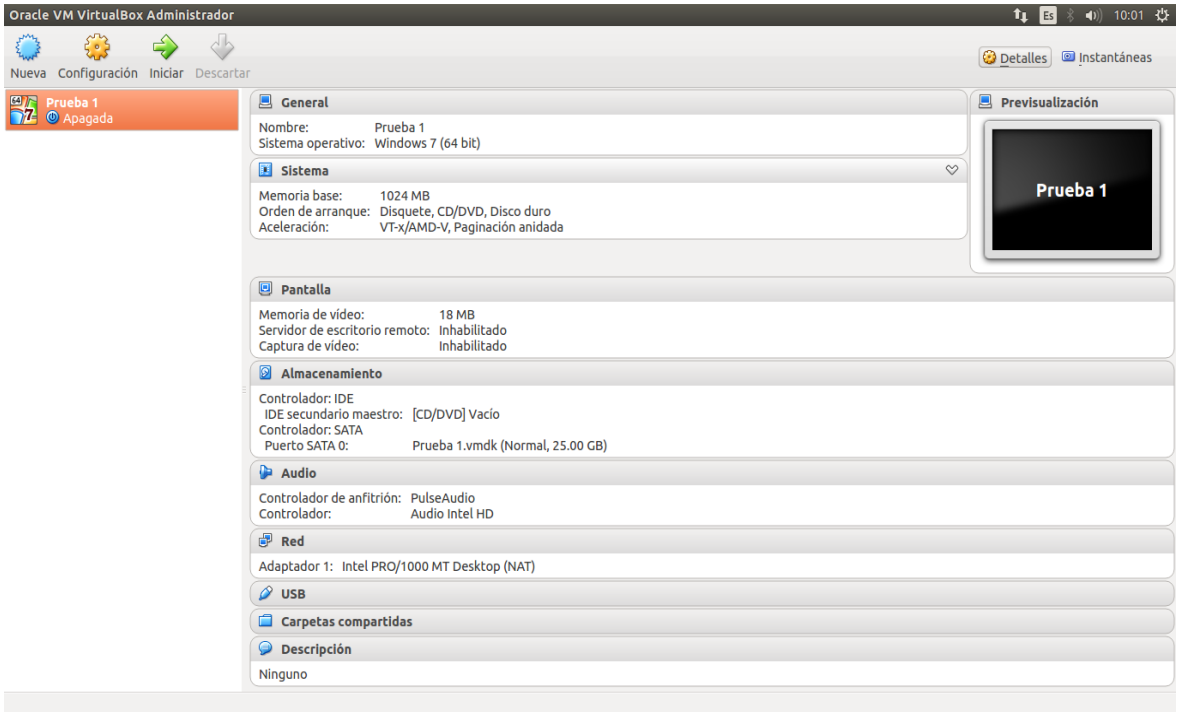


Figura 4.4. Configuración del sistema anfitrión para la prueba de rendimiento de Virtual Box.

Una vez que se ha configurado el sistema sobre el cual se va a instalar la máquina virtual, es necesario cargar el sistema operativo que previamente se ha mencionado sobre la unidad de disco duro virtual, para esto se hace ejecuta el botón iniciar que aparece en el ventana principal de Virtual Box, posteriormente se selecciona la ruta en donde se localiza el sistema operativo y se procede a su instalación, dando como resultado el proceso de instalación de Windows 7 Home Premium como si se llevara a cabo en un equipo físico.

Una vez terminada la instalación del sistema operativo se tiene lista la máquina virtual a la que se le asignó el nombre de Prueba 1, con sus respectivas configuraciones de hardware como lo indica la figura 4.5. Además en esta figura se aprecia con ayuda de la aplicación Monitor del sistema el consumo de recursos del sistema anfitrión Ubuntu, ejecutando la máquina virtual con sistema huésped Microsoft Windows 7.

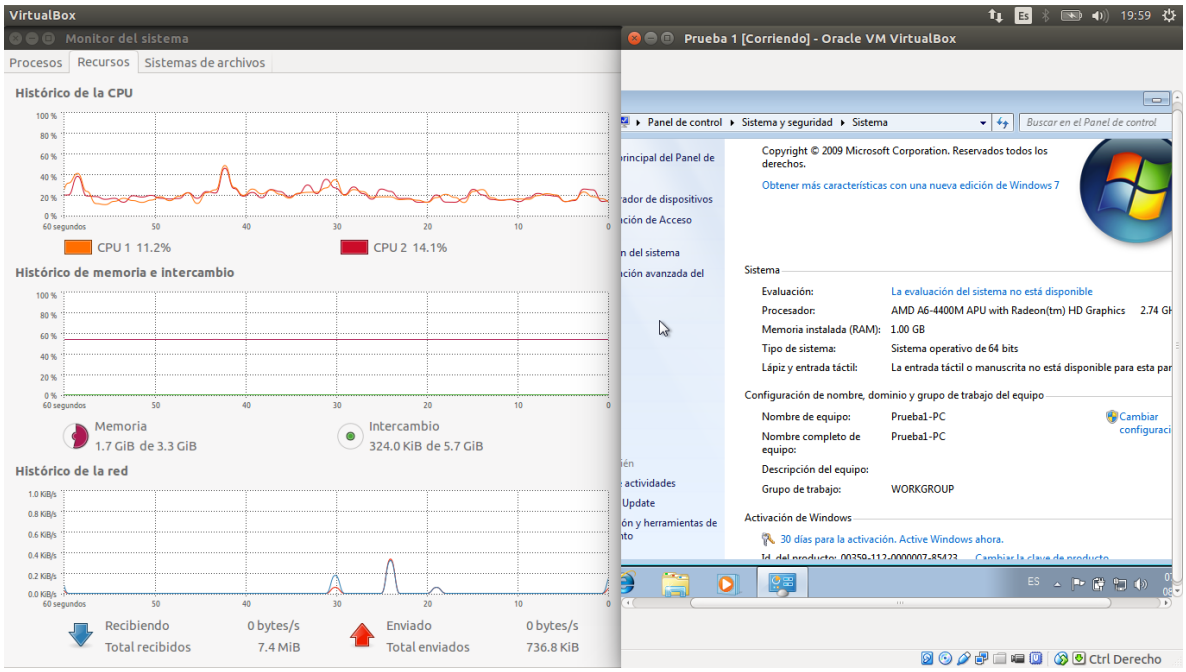


Figura 4.5. Consumo de recursos de la máquina virtual "Prueba 1" empleando Virtual Box.

De la figura 4.5 se observa que el uso de la CPU esta entre el 11.2% y 14.1% de su capacidad, por otra parte el uso de la memoria RAM es de 1.7 GB de los 3.3 GB disponibles del sistema. Cabe hacer la aclaración que el sistema huésped al momento de la captura de pantalla del rendimiento no tiene en ejecución aplicaciones que le demanden recursos de procesador o de memoria RAM adicionales (como podrían ser el navegador web, aplicaciones de ofimática por mencionar algunos) a los del sistema operativo en ejecución.

Ahora es turno de probar el rendimiento de la misma máquina virtual pero utilizando el software de virtualización VMware Player 12. Para instalar esta aplicación, primero hay que descargarla de la siguiente dirección web: "https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0", el archivo correspondiente al sistema anfitrión que en este caso es Ubuntu por lo tanto se descarga el archivo para Linux (Vmware-Player-12.0.0-2985596.x86_64.bundle). Una vez que terminó la descarga del archivo, desde la terminal se tendrá que acceder al directorio en donde está el archivo de VMware Player 12 con extensión bundle.

Para instalar este tipo de archivos con dicha extensión sólo basta con ejecutar el comando: "*sh*", con

permisos de administrador seguido del nombre del archivo con su respectiva extensión, resultando:

sudo sh Vmware-Player-12.0.0-2985596.x86_64.bundle

Hecho lo anterior se despliega una ventana que va a indicar los pasos de forma gráfica para la instalación de VMware Player 12, este proceso es sencillo pues sólo basta con leer, aceptar y/o configurar los directorios que empleará la aplicación. Una vez finalizada la instalación se tendrá el icono de dicha aplicación, para ejecutarla basta con dar clic sobre éste o desde la terminal escribiendo el nombre y presionado la tecla enter.

Al ejecutar la aplicación se despliega una ventana de bienvenida y las opciones que brinda como: crear una nueva máquina virtual, abrir una máquina virtual existente, actualizar a la versión Workstation Pro y por último la parte de ayuda. De las opciones ya mencionadas, se selecciona crear una nueva máquina virtual, posteriormente se desplegarán una serie de pantallas en las cuales se debe de indicar: la ruta del sistema operativo huésped, la ruta del directorio en donde se almacenará la máquina virtual, así como las configuraciones de hardware correspondientes. Para esta última parte se repetirán los valores configurados en Virtual Box, siendo: 1024 MB de memoria RAM y 25 GB de disco duro virtual, una vez terminada la configuración del hardware, se instala el sistema operativo huésped en el disco duro virtual y terminado este proceso la máquina virtual estará lista como lo indica la figura 4.6 en la cual se puede observar parte de su configuración así como el consumo de recursos del sistema anfitrión con ayuda de la aplicación Monitor del sistema.

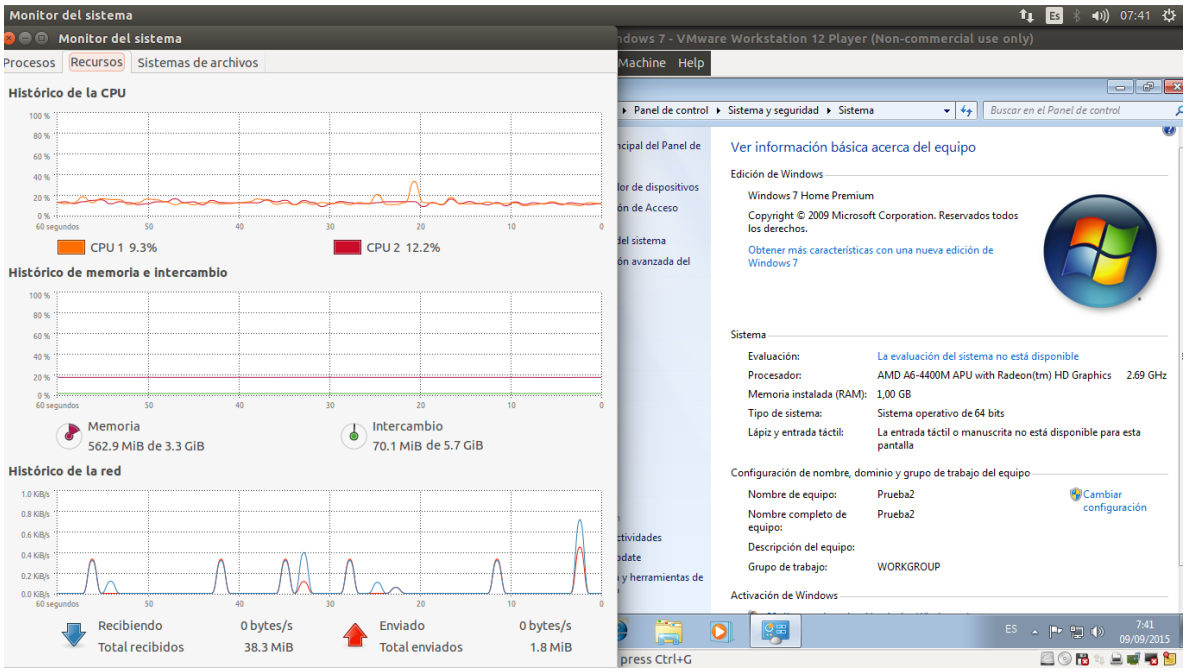


Figura 4.6. Consumo de recursos de la máquina virtual "Prueba 1" empleando VMware Player 12.

De esta imagen se aprecia que el rendimiento de la CPU está entre 9.3% y 12.2 % de su capacidad, por otra parte la cantidad de memoria RAM que demanda del sistema anfitrión es de 562.9 MB.

Ahora, comparando los recursos que el sistema anfitrión consumió durante la ejecución de cada una de las aplicaciones de virtualización, se tiene lo siguiente:

- Al llevar a cabo la virtualización del sistema operativo Windows 7 Home Premium con Virtual Box el uso del procesador estuvo entre el 11.2% y el 14.1% de su capacidad, mientras que el consumo de memoria RAM fue de 1.7 GB de los 3.3 GB disponibles del sistema anfitrión.
- Por otra parte al virtualizar con VMware Player 12, el rendimiento del procesador en el sistema anfitrión tuvo un rendimiento entre el 9.3% y 12.2% de su capacidad, en cuanto al uso de memoria RAM el sistema anfitrión utilizó 562.9 MB de los 3.3 GB del sistema anfitrión.

Por lo tanto la aplicación de VMware Player para llevar a cabo la virtualización brinda un mejor aprovechamiento de los recursos del sistema anfitrión, pues los valores de uso entre Virtual Box y VMware Player 12, relacionados con el procesador y la memoria RAM tuvieron una diferencia del:

1.9% y 1177.9 MB, respectivamente. Siendo la memoria RAM el recurso que tuvo una diferencia más notable en cuanto a su uso por parte del sistema anfitrión, ya que sólo demandó 562.9 MB, esto corresponde aproximadamente a un 32.34% de los 1.7 GB que utilizó Virtual Box y significa un ahorro aproximado del 67,66% de lo que demandó Virtual Box, cabe hacer la aclaración que las máquinas virtuales al ser ejecutadas tanto en VMware Player 12 como en Virtual Box ejecutaron la misma aplicación y procesos durante la toma de los valores de rendimiento. Con base en el análisis de los valores de rendimiento del sistema anfitrión, VMware Player 12 es la aplicación de virtualización elegida para llevar a cabo la creación del laboratorio para analizar el código malicioso dirigido a Smartphone con sistema operativo Android.

4.3 Selección de la muestra de malware.

En el segundo capítulo se hizo mención de la gran variedad de tipos de código malicioso que existen para la plataforma Android, que van desde aquellas con la finalidad de estafar al usuario hasta los que facilitan el espiar gran parte de su actividad permitiendo tener acceso a los diversos archivos que la víctima puede tener en su dispositivo, siendo este último tipo el que tienen más relación con el presente trabajo ya que representa un buen ejemplo con el cual se puede apreciar la forma en que la privacidad de la información es vulnerada.

El tipo malware del cual se trata es denominado como "AndroRat+AndroRatBinder" se trata de una RAT (Remote Administration Tool) de código abierto para dispositivos Android, la cual es una aplicación cliente-servidor desarrollada en el lenguaje de programación Java, entre algunas de sus funciones están:

- Obtener contactos de la víctima,
- Obtener el registro de llamadas y mensajes,
- Localización del dispositivo,
- Obtener acceso a los archivos almacenados tanto en la memoria externa como en la interna del dispositivo, por mencionar algunas.

Y la aplicación "AndroRatBinder", la cual permite ocultar "AndroRat" en una aplicación legitima.

4.4 Análisis de la muestra de malware.

Como se mencionó, la muestra de malware a analizar es denominada como "AndroRat+AndroRatBinder" para llevar a cabo este análisis es necesario crear una máquina virtual con sistema operativo Windows 7 de 64 bits con la versión y licencia que previamente fue mencionada en las pruebas para la elección de software de virtualización, sólo con la diferencia en la configuración de hardware que esta vez tendrá una memoria RAM asignada de 2 GB y un disco duro virtual de almacenamiento de 60 GB.

Una vez que se tiene la máquina virtual lista es necesario descargar e instalar el kit de desarrollo de java (JDK), para descargar del JDK es necesario ingresar a la página Oracle en la parte de descargas y seleccionar la opción de java para desarrolladores edición estándar (SE) (http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html), posteriormente hay que seleccionar la versión del sistema operativo sobre la cual se va a instalar, en este caso se selecciona la correspondiente a Windows de 64 bits.

Después de descargar e instalar el JDK, es necesario instalar la aplicación Android Studio, la cual es un entorno de desarrollo integrado para la plataforma Android que cuenta con una licencia de software libre (por medio de la Licencia Apache 2.0) y está disponible para Microsoft Windows, Mac OS X y GNU/Linux. Algunos de los requisitos que demanda esta aplicación para ser instalada en el sistema operativo Windows, son los siguientes:

- Microsoft Windows 8/7/Vista/2003 (32 or 64-bits).
- 2 GB de memoria RAM (mínimo), 4 GB de memoria RAM (recomendado).
- Espacio de 1 GB en el disco duro.
- Java Development Kit (JDK) 7.

En el caso de la máquina virtual que se creó, cumple con dichos requerimientos, por lo tanto se procede a la instalación. Tanto el JDK como Android Studio son aplicaciones de gran ayuda para llevar a cabo el análisis de la muestra de malware, pues con éstas es posible ejecutar el código y emular dispositivos Android para saber qué tipo de funciones es capaz de realizar la muestra de código malicioso.

La muestra de malware se descargó de la siguiente dirección: “https://mega.nz/#!UkpFVBCR”, al descargar el archivo: “AndroidRat+AndroidRatBinder.rar”, debido a que se trata de un archivo comprimido es necesario extraer su contenido para analizar el funcionamiento de malware. Al extraer los archivos se tiene lo que se observa en la Figura 4.7.

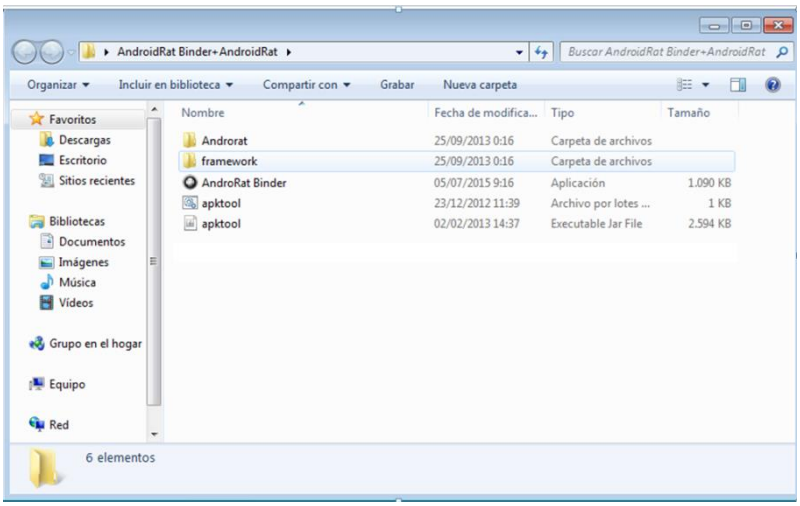


Figura 4.7. Contenido de archivo “AndroidRat+AndroidRatBinder.rar”

De la imagen anterior se observa que el contenido del archivo descargado se conforma de:

- Dos carpetas:“Androrat” y “framework”,
- Un archivos de aplicación “AndroRat Binder”,
- Un archivo de procesamiento por lotes (.BAT) con el nombre de “apktool” y
- Un archivo java ejecutable (.jar) “apktool”.

Revisando el contenido de los archivos que previamente se describieron se tiene que, las carpetas de “Androrat” y “framework” fueron generadas al crear un proyecto para Android dentro del entorno de desarrollo integrado (IDE) eclipse.

Dentro de la carpeta “Androrat” se localizan:

- Cuatro carpetas con los siguientes nombres: “.settings”, “bin”, “download” y “src”. De estas carpetas la que contiene el código fuente de la aplicación es la que tiene por nombre “src”, ya que dentro de ésta existen los archivos con extensión java que conforman todo el código con el cual funciona la aplicación. En la carpeta “bin” se tienen los archivos con extensión class que corresponden a los

archivos compilados del código fuente en java. Por último están las carpetas: “download” y“.settings”, en esta última se tiene un archivo con la extensión “prefs”, que contiene información sobre la versión del IDE eclipse.

- Un archivo sin nombre pero con extensión “.classpath”, que contiene la ubicación de los directorios “src” y “bin” en la computadora donde se realizó dicho proyecto para Android bajo el IDE eclipse.
- Un archivo sin nombre con extensión “.project”, que almacena información sobre la descripción del proyecto desarrollado con eclipse.
- Y finalmente se tiene un archivo Java ejecutable (.jar) con el nombre de “AndroRat”, el cual corresponde a la aplicación del servidor.

En la carpeta “framework”, se localizan:

- Dos carpetas: “res” y “smali”, éstas contienen los archivos necesarios para que la aplicación sea capaz de ejecutarse sobre el sistema operativo Android, dentro de la carpeta “res”, se localizan las capetas: “drawable-hdpi”, “drawable-ldpi”, “drawable-mdpi” y “drawable-xhdpi, las cuales contienen un archivo de imagen (.png) con el nombre “ic_launcher”, también se tienen las carpetas “layout”, “values” y “xml”, éstas con código en XML, que entre algunas de sus funciones tienen la distribución de los elementos que tendrá la aplicación al ejecutarse sobre Android. Por otra parte en la carpeta “smali” hay archivos con los mismos nombres de la carpeta “Androrat” con la diferencia que tienen la extensión de un archivo “.SMALI”, este tipo de archivos son necesarios para que la aplicación se ejecutan sobre la plataforma Android.
- Un archivo con el nombre de “AndroidManifest”, en el cual se establecen los permisos que el usuario otorgara a la aplicación (apk), una vez que este instalada en su dispositivo Android.

Para comenzar con el funcionamiento de esta aplicación el primer paso consiste en ejecutar la aplicación “AndroRat Binder”, la cual aparece en la figura 4.8. Al ejecutar dicha aplicación se despliega una ventana que consta de tres pestañas, cada una con un objetivo en particular. La primer pestaña corresponde a “Build +Bind”, en esta vista de la aplicación aparecen tres campos: el primero está designado a la dirección “IP” hacia la cual se va a comunicar la aplicación una vez que se haya infectado a la víctima, el segundo campo corresponde al puerto “PORT” éste será la interfaz por la cual se va a comunicar la aplicación estando instalada en el Smartphone con la computadora en donde se esté ejecutando el servidor, y por último el campo “TARGET APK” que sirve para especificar la ruta de una aplicación (APK) legítima y posteriormente inyectarle el código malicioso. En este caso como se va a ejecutar en un emulador de un Smartphone Android en la misma máquina

virtual, basta con conocer la dirección IP local y asignarle un puerto que esté disponible, para conocer la dirección IP local de la máquina virtual es necesario ejecutar la venta del símbolo del sistema y escribir el comando: "ipconfig", siendo la dirección IPv4 la que se coloca en el campo correspondiente a la IP, en el puerto se coloca el 5689 y en la parte de "TARGET APK" se especifica la ruta de una aplicación que corresponde a un juego llamado "flappy-bird" para finalizar la inyección del código malicioso se presiona el botón "Go" y la aplicación mostrará el avance del proceso hasta que éste haya terminado, como también se puede apreciar en la figura 4.8.

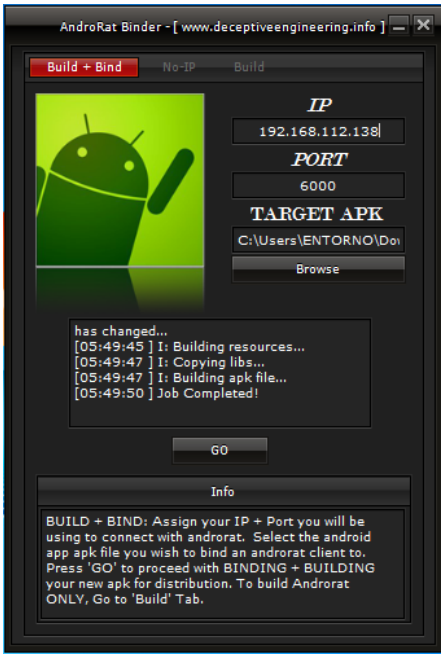


Figura 4.8. Ejecución de la aplicación "AndroRat Binder", vista de la pestaña "Build+Bind".

Una vez que se ha generado la aplicación (apk) con el código malicioso, el segundo paso consiste en emular el dispositivo Android para instalar dicha aplicación, para lo cual es necesario ejecutar la aplicación "Android Studio", en la ventana principal de la aplicación está la pestaña "Configure" al dar clic en ésta, aparecen 7 pestañas nuevas, se dará clic sobre "SDK Manager", posteriormente se despliega una ventana en la cual se listan una serie de herramientas para la emulación de los dispositivos así como las versiones de Android con su respectiva API, que van desde la versión 2.2 (API 8) hasta la versión 6.0 (API 23). El código malicioso para su ejecución necesita como versión mínima de Android la 2.2, por esta razón será la que se seleccionará e instalará para emular los

dispositivos, como lo indica la figura 4.9. Después de haber seleccionado la versión de Android e instalado los paquetes necesarios es posible emular el dispositivo, por lo tanto es necesario dar clic en la pestaña “Tools” que aparece en la parte superior de la ventana, como se observa en la figura 4.9, hecho lo anterior se despliegan 4 pestañas, se selecciona la correspondiente a “Manage AVD” y se abrirá una nueva ventana “Android Virtual Device (ADV) Manager”, correspondiente a la figura 4.10.

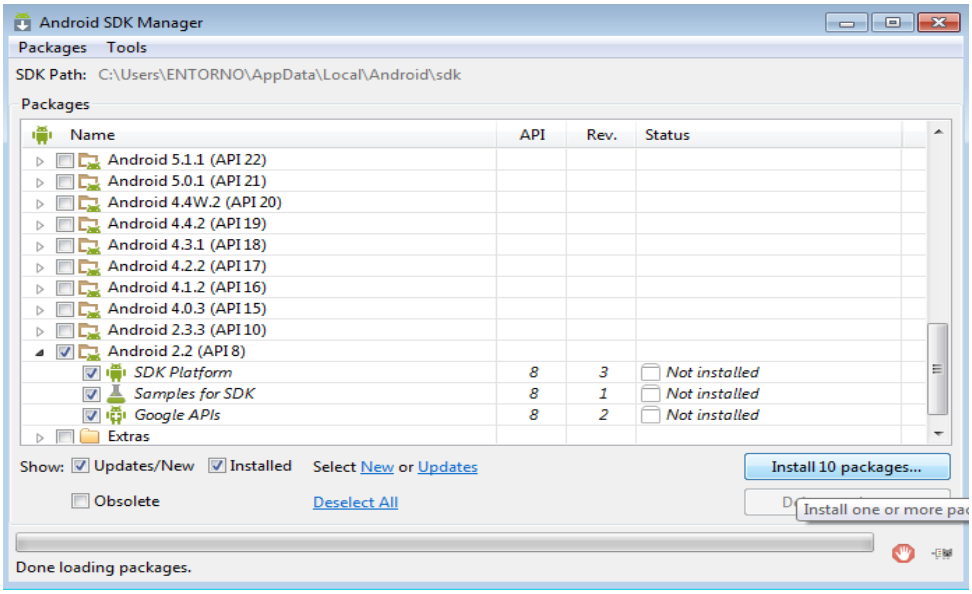


Figura 4.9. Ventana “Android SDK Manager”.

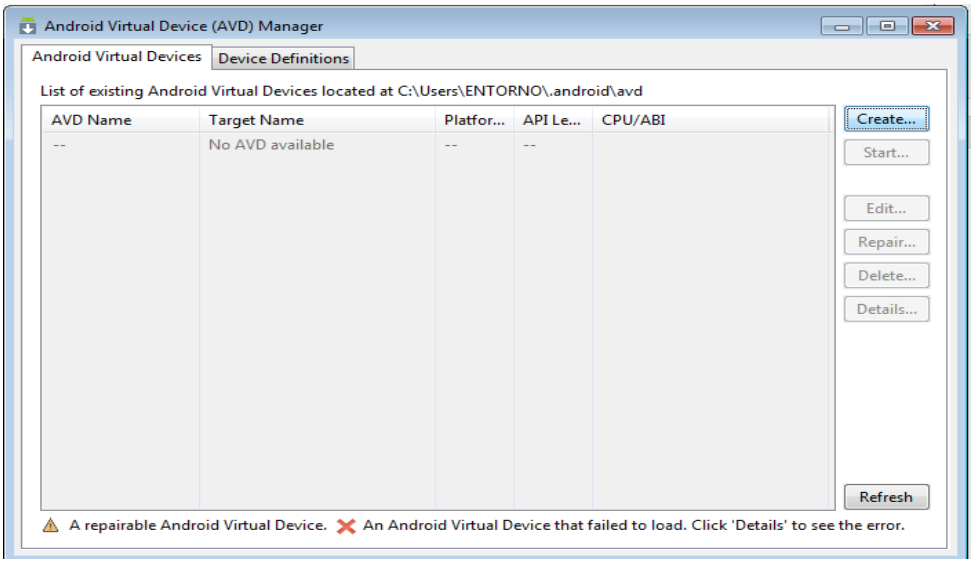


Figura 4.10. Ventana "Android Virtual Device (ADV) Manager", en la cual se creara el dispositivo para emular el smartphone con SO Android.

En la figura 4.10, se aprecia el boton "Create", al ejecutar dicho botón se despliega una ventana para configurar el dispositivo a emular, asignandole: un nombre, el tipo de dispositivo que se requiere, la versión del sistema operativo, la cantidad de espacio de almacenamiento interno del dispositivo, así como el almacenamiento externo (tarjeta SD). Las configuraciones correspondientes al dispositivo se muestran en la figura 4.11.

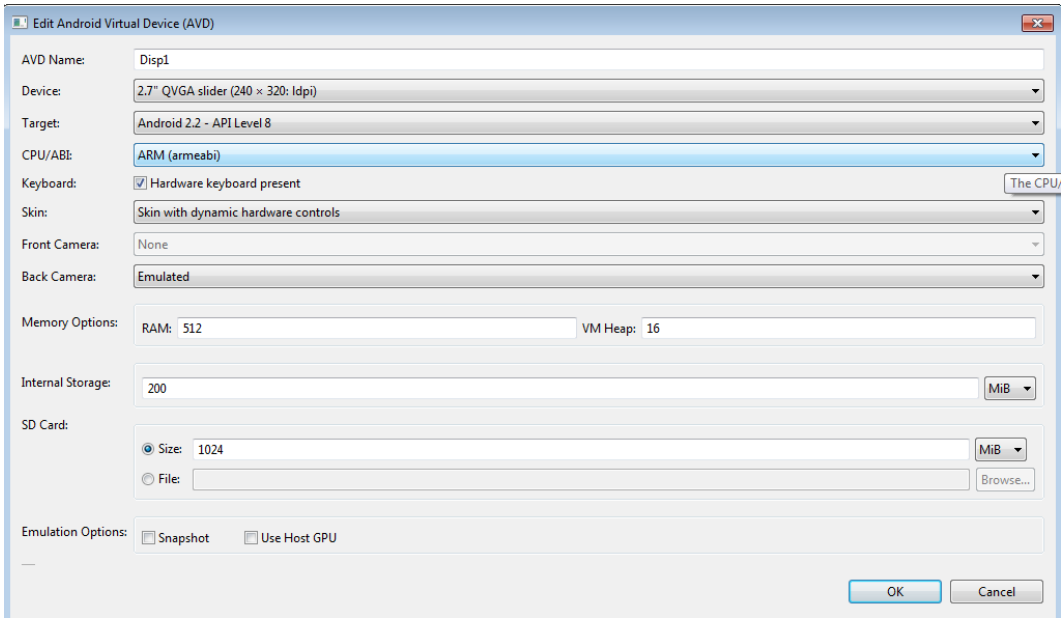


Figura 4.11. Configuración del hardware del dispositivo Android que se emulará.

Estando de acuerdo con la configuración del dispositivo, se presiona el botón "OK" y se regresa a la ventana de la figura 4.10, con la diferencia que ahora está activo el botón "Start" y además aparece el dispositivo que se configuró en la figura 4.11. Para iniciar la emulación se selecciona el dispositivo y se presiona el botón "Start" y así se tiene en ejecución el dispositivo Android, que se muestra en la figura 4.12.

Figura 4.12. Dispositivo Android emulado "Disp1".

Estando en ejecución el dispositivo Android, es necesario instalar la aplicación (apk) que se generó con el código malicioso, para esto es necesario abrir una terminal de línea de comandos y ubicarse en la ruta que corresponde al SDK Path, ésta se puede apreciar en la parte superior izquierda de la figura 4.9 y corresponde a la siguiente: "C:\Users\ENTRORNO\AppData\Local\Android\sdk", después es necesario acceder al directorio con el nombre de "plataform-tools" una vez que se está en dicho directorio es necesario colocar en éste la aplicación (apk) que se va a instalar en el dispositivo emulado. Para este caso se trata de la aplicación del juego con el nombre de "Flappy-birds" a la cual se le inyectó el código malicioso de AndroRat, al tener la aplicación en el directorio que se ha mencionado, desde la terminal se ejecuta la aplicación "adb" (esta aplicación es la encargada de administrar los dispositivos emulados) seguida del parámetro "install" y del nombre completo de la aplicación, como se indica en la figura 4.13

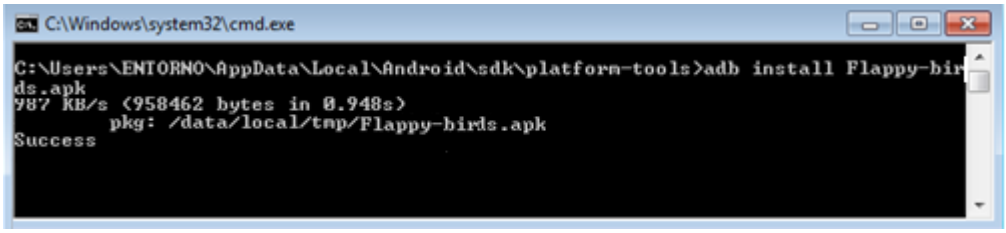


Figura 4.13. Instalación de la aplicación infectada con AndroRat.

Posterior a la instalación de la aplicación en el dispositivo emulado, es necesario ejecutar el archivo de nombre "AndroRat.jar" (Servidor) que está en la carpeta "androrat", ubicada en la carpeta donde se extrajo el malware. Una vez que el servidor establece la conexión con el cliente, se puede apreciar una ventana con titulo "Androrat Project"como la que se muestra en la figura 4.14, en esta figura también se observa información de la víctima como: el IMEI, país en donde se localiza, el número telefónico, el proveedor del servicio de telefonía, por mencionar algunos.

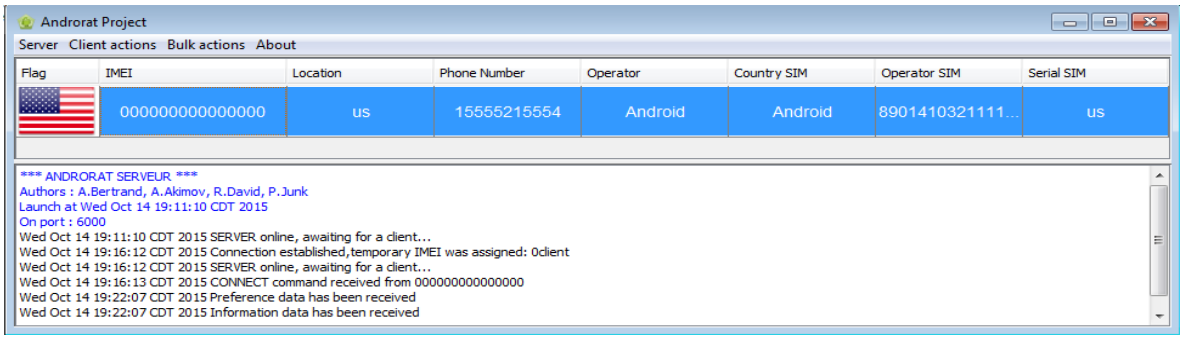


Figura 4.14. Conexión establecida por parte del servidor Androrat con un cliente (dispositivo emulado).

De la figura 4.14 se ve que la ventana del servidor cuenta con cuatro etiquetas: “Server”, “Client actions”, “Bulk actions” y “About”. Por debajo de las etiquetas se tiene el área donde se listan los clientes (dispositivos donde se instaló la apk con el malware), en esta parte se logra ver información de la víctima pero en este caso en particular como se trata de un dispositivo emulado hay algunos valores que no son asignados, como lo son: el IMEI y el proveedor del servicio de telefonía. Finalmente en la parte inferior de la ventana se observan los nombres de los autores del código, así como la fecha en que se está ejecutando el servidor, el puerto por el cual se establece la conexión e información de la conexión establecida con el cliente.

Para conocer el funcionamiento de la parte del servidor, es pertinente explorar las cuatro etiquetas y describir el funcionamiento de las mismas:

- **“Server”**, tiene tres opciones. La primera de ellas es “Exit aplication”, con la cual se cierra la ventana del servidor así como la conexión que se establece con el cliente. La segunda es “Select port”, esta opción permite establecer el puerto por el cual el servidor se comunicará con el cliente, en caso de que no haya sido establecido desde la aplicación “AndroRat Binder” (Figura 4.8). Por último está “Show logs”, ésta permite activar o desactivar los registros de las conexiones con los clientes, así como la información del puerto que está en uso y la fecha correspondiente a la ejecución del servidor (parte inferior de la figura 4.14).
- **“Client actions”**, se conforma de dos opciones. La primera: “Open user interface”, al ejecutar esta opción se despliega una nueva ventana, que corresponde a la figura 4.15. En esta nueva ventana de

nombre “User GUI of Imei”, se aprecian cuatro nuevas etiquetas: “Options”, “Get Android data”, “Send command” y “Monitoring”. Debajo de dichas etiquetas, en la parte izquierda se tiene una pestaña de nombre “Home” que muestra información de diferentes categorías:

- Información general, presenta: el número telefónico del dispositivo, el IMEI, el país, el nombre del proveedor del servicio telefónico así como su código e información correspondiente con la tarjeta SIM del dispositivo.
- Información de la conexión inalámbrica de internet (WIFI), debido a que el dispositivo emulado no cuenta con la interfaz física no tiene asignada información relevante en este campo.
- Información de la red de datos móvil, siendo para este dispositivo la correspondiente a “3G”, así como los parámetros de habilitada y conectada en verdadero.
- Información sobre Android, en esta categoría se especifica la versión 2.2 con la cual cuenta el dispositivo emulado y la versión 8 del SDK.
- Dispositivos, en esta sección se listan los sensores con los cuales cuenta el dispositivo: de orientación, de temperatura y acelerómetro.
- Información de la batería, como: si está presente y la calidad en rendimiento, nivel de carga, tipo de alimentación, la tecnología, temperatura y voltaje.

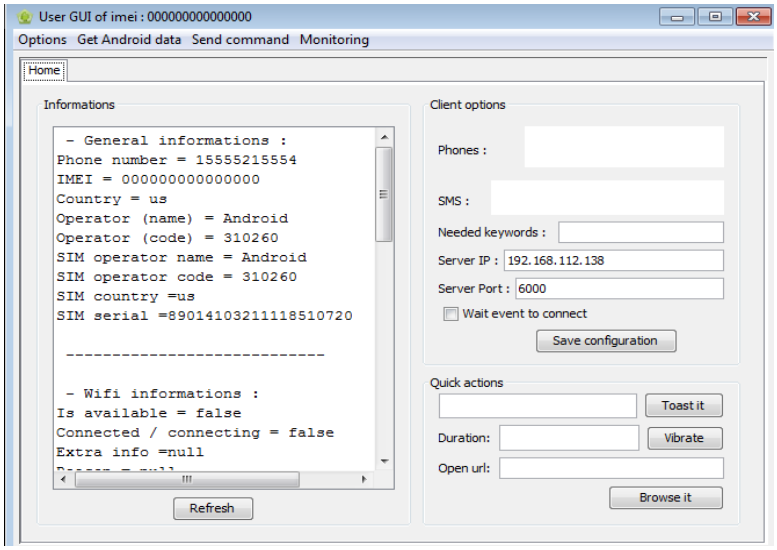


Figura 4.15. Ventana “User GUI of IMEI”.

En la parte derecha de la figura anterior se aprecia una serie de campos, agrupados en dos categorías: La primera corresponde a “Client options”, en esa parte se observan algunos datos del cliente como son la dirección IP del servidor por medio de la cual estable la conexión así como el puerto, entre

otros. Por último en la segunda parte está “Quick actions”, que se conforma de tres campos. En el primero se tiene un campo para escribir texto y en seguida el botón “Toast it”, éste permite enviar cualquier mensaje que se escriba allí y se mostrará en el dispositivo emulado, como muestra la figura 4.16. El segundo campo corresponde a una opción que permite hacer vibrar el dispositivo y se conforma de un campo para ingresar la duración seguido del botón “Vibrate”, como se trata de un dispositivo emulado no tiene la capacidad de mostrar el funcionamiento de esta opción. El último campo permite abrir cualquier página web vía remota en el dispositivo, ingresando la URL del sitio que desee en este caso se hizo la prueba con la correspondiente a la facultad de ingeniería de la UNAM, como se aprecia en la figura 4.17.

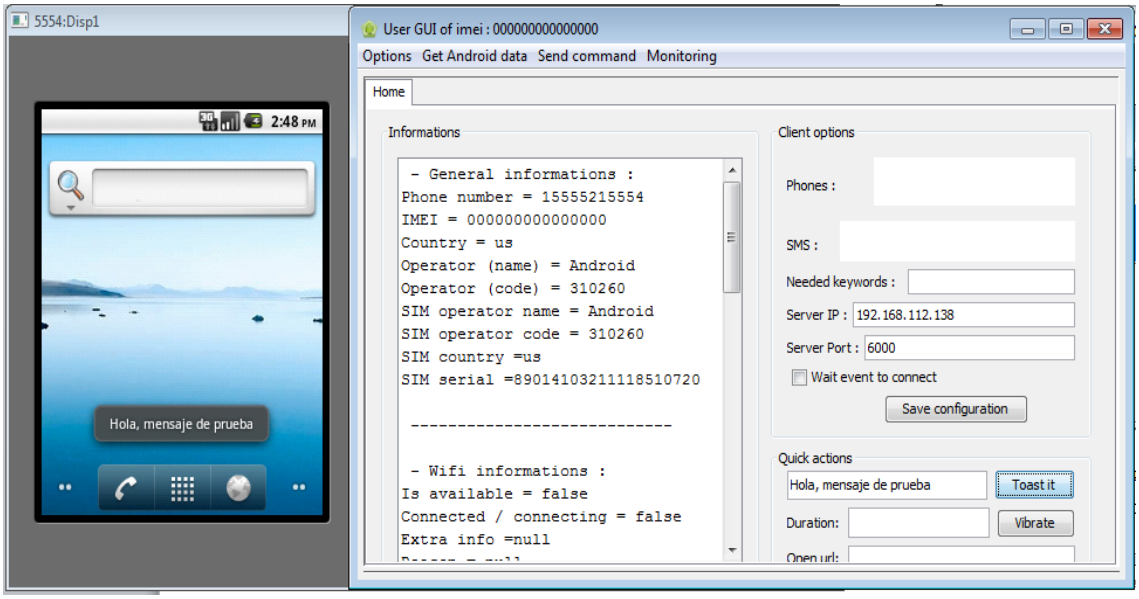


Figura 4.16. Mensaje enviado al dispositivo Android emulado, desde la aplicación AndroRat.

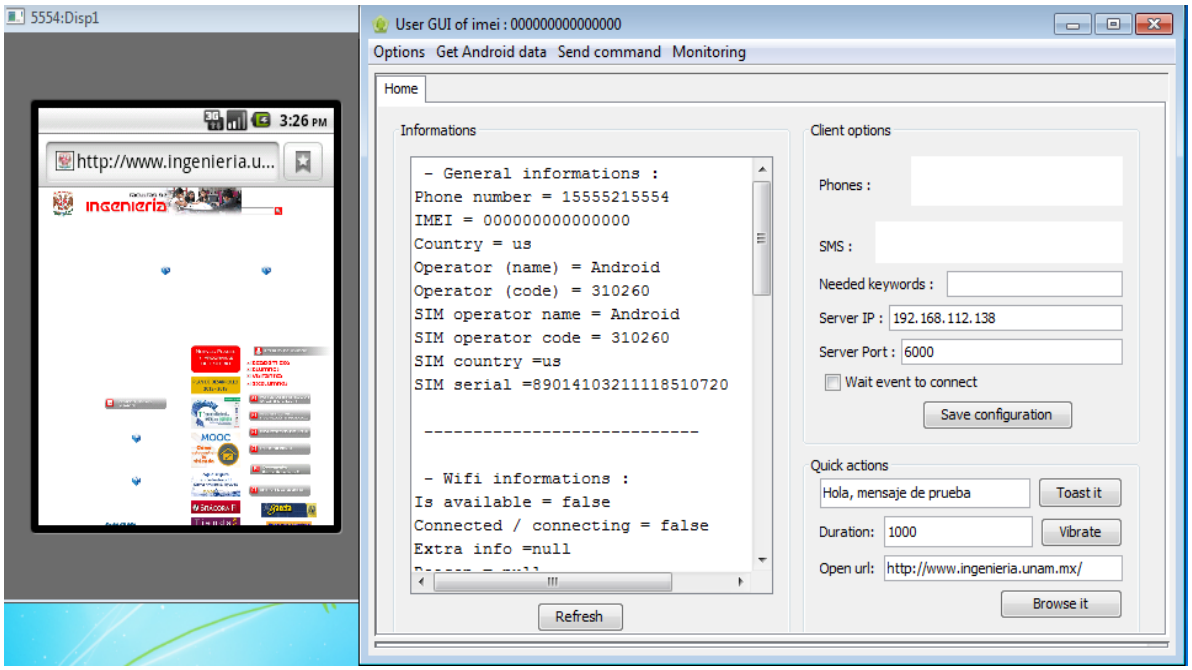


Figura 4.17. Apertura de una dirección URL de manera remota por medio de AndroRat.

Ahora es turno de conocer las funciones que brindan las pestañas:

- ✓ **"Options",** esta pestaña despliega dos opciones. La primera denominada "Close Tab", permite cerrar pestañas abiertas dentro de la ventana "User GUI of imei" y cuenta con su atajo rápido pulsando la tecla "Ctrl" + "R". La segunda opción corresponde a "Close Window", ésta cierra la ventana "User GUI of imei".

- ✓ **"Get Android data"**, despliega seis opciones. La primera corresponde a "Take picture", ésta brinda la opción de tomar una fotografía ya sea con la cámara trasera o frontal del dispositivo, en el caso de este dispositivo emulado no es posible apreciarlo ya que no cuenta con una cámara real. En segundo lugar está la opción "File tree", la cual despliega los archivos almacenados en la tarjeta externa del teléfono mostrando información de los archivos como: nombre, tamaño, fecha de acceso y de modificación así como la opción de descargar los archivos almacenados en la carpeta "download" que se localiza dentro de la carpeta "Androrat" (la cual se aprecia en la figura 4.7), e igual que con la primera opción, el dispositivo emulado no cuenta con dicha tarjeta por lo que no es posible apreciar los archivos. La tercera opción corresponde a "Contacts", esta permite obtener los contactos almacenados en el dispositivo así como la información adicional que esté

asociada a ellos, además de brindar la opción de hacer llamadas o mandar mensajes de texto al contacto seleccionado de la lista, como lo indica la figura 4.18, cuando se realiza una llamada por medio de esta opción, sí aparece registrada en el celular de la víctima, en cambio con la opción de enviar un mensaje de texto, éste no se registra en el dispositivo.

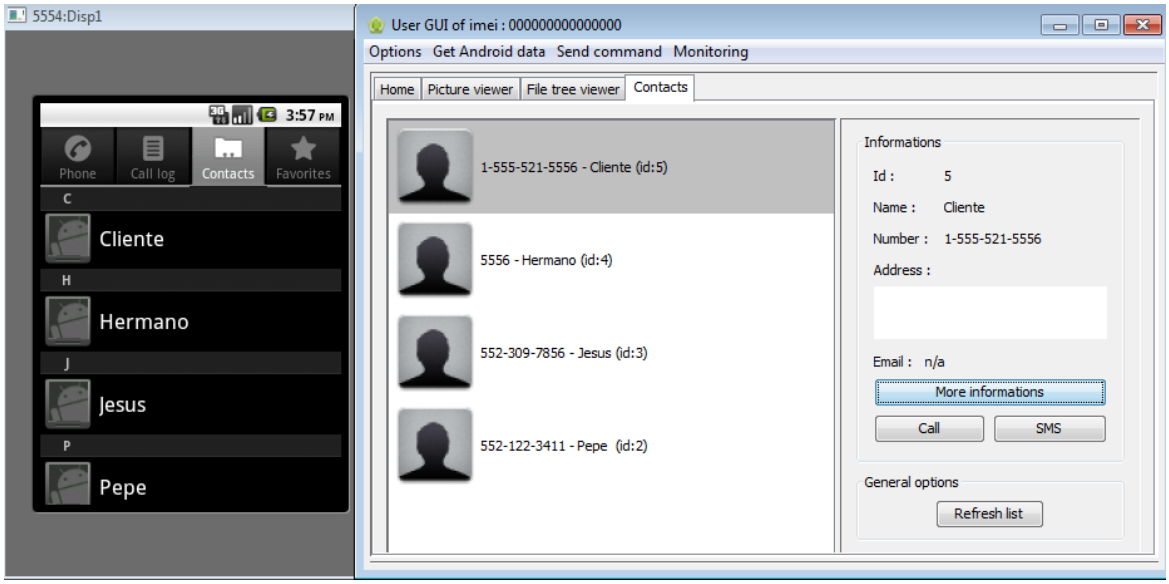


Figura 4.18. Obtención de los contactos almacenados en el dispositivo emulado, por medio de AndroRat.

En cuarto lugar se tiene la opción “Call logs”, la cual permite tener acceso al registro de llamadas del dispositivo. La quinta opción corresponde a “SMS”, ésta permite el acceso a leer los mensajes de texto que el usuario ha enviado o recibido, también brinda la posibilidad de filtrarlos, como se indica en la figura 4.19, para mostrar este ejemplo de los mensajes monitoreados por AndroRat se ha simulado otro dispositivo con sistema operativo Android con las mismas características en hardware que el “Disp1” que se aprecia en la figura 4.11, con las diferencias que éste tendrá el nombre de “Disp2” y el número telefónico “15555215556” y en la lista de contactos del Smartphone emulado aparece con el nombre de “Cliente”.

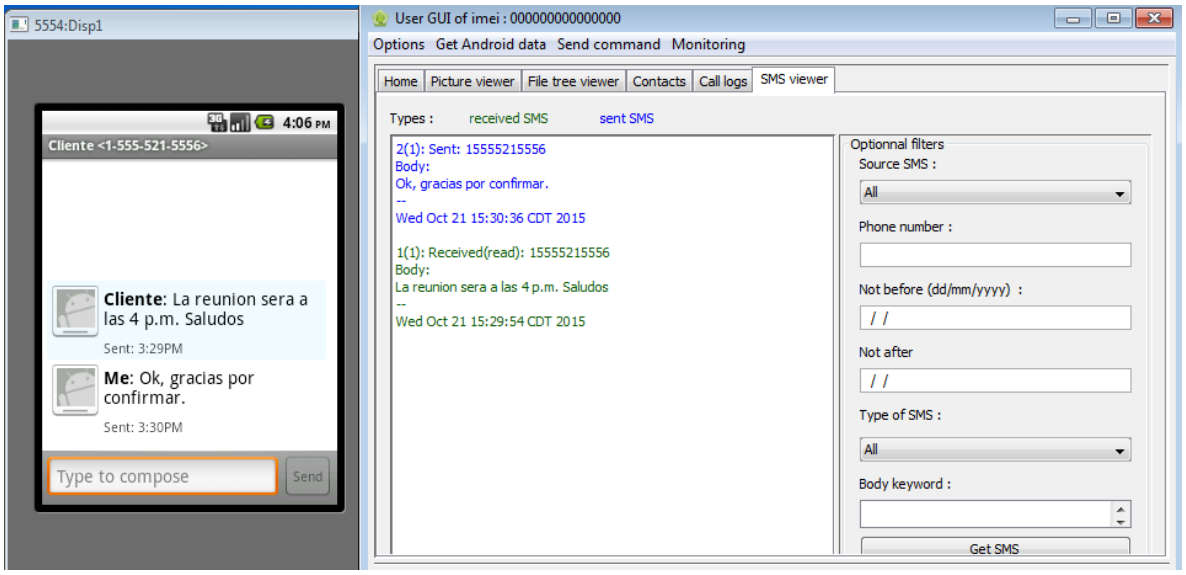


Figura 4.19.Vista de los mensajes de texto obtenidos con AndroRat.

Por último la sexta opción es "Streaming", la cual ofrece la opción de ubicar la posición del dispositivo mediante la señal del GPS, también otra opción que ofrece AndroRat corresponden a escuchar el audio que capta el micrófono del dispositivo, estas opciones con un dispositivo emulado no son posibles de apreciar debido a que se requiere del hardware necesario para poder tener una demostración, pero más adelante en el desarrollo de este trabajo se va a trabajar con un Smartphone real para apreciar las funciones que hasta el momento se han visto limitadas en el dispositivo emulado.

- ✓ **"Send command"**, se conforma de tres opciones. En la primera se tiene "Toast message", esta opción despliega una ventana en la cual pide ingresar un mensaje, el cual se mostrará en la pantalla principal del dispositivo emulado, esta acción es idéntica a la que previamente se analizó en la parte de "Quick accions" de la pestaña "Home" que de igual forma envía un mensaje al dispositivo infectado, como lo indicó la figura 4.16. En segundo lugar está "Send SMS", ésta despliega una ventana para enviar un mensaje de texto al número telefónico que se indique en la parte de "Target cell number", esta segunda opción es similar a la que se presenta en "Contacs" de "SMS", con la diferencia que "Send SMS" no se limita a enviar mensajes únicamente a los contactos del dispositivo infectado. Como última opción está "Give call", la cual permite realizar una llamada por medio del dispositivo infectado a cualquier número que se especifique en

"Enter the target cell number", que pertenece al campo de la ventana que despliega "Give call".

- ✓ **"Monitoring**, cuenta con dos opciones. En primer lugar está "Call monitor", que permite iniciar un monitoreo de las llamadas de la víctima como lo indica la figura 4.20, categorizándolas en: "Incomming call" (llamada entrante), "Missed call" (llamada perdida), "Accepted call" (llamada aceptada), "Sent call" (llamada hecha por el dispositivo de la víctima), "Hanged up call" (llamada finalizada), también es posible especificar un número telefónico como filtro para que sólo aparezcan las llamadas a dicho número.

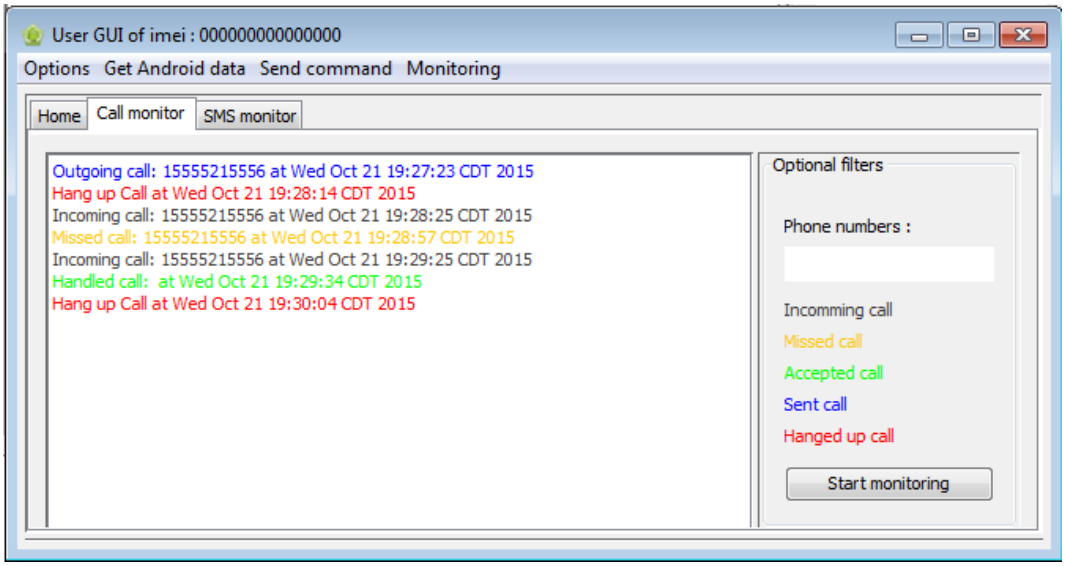


Figura 4.20. Monitoreo de llamadas por medio de Andro Rat.

La segunda opción corresponde a "SMS monitor", que permite iniciar un monitoreo exclusivamente de los mensajes que recibe el teléfono con AndroRat, como se indica en la figura 4.21. Con esto quedan cubiertas las opciones que se incluyen en la ventana "User GUI of IMEI".

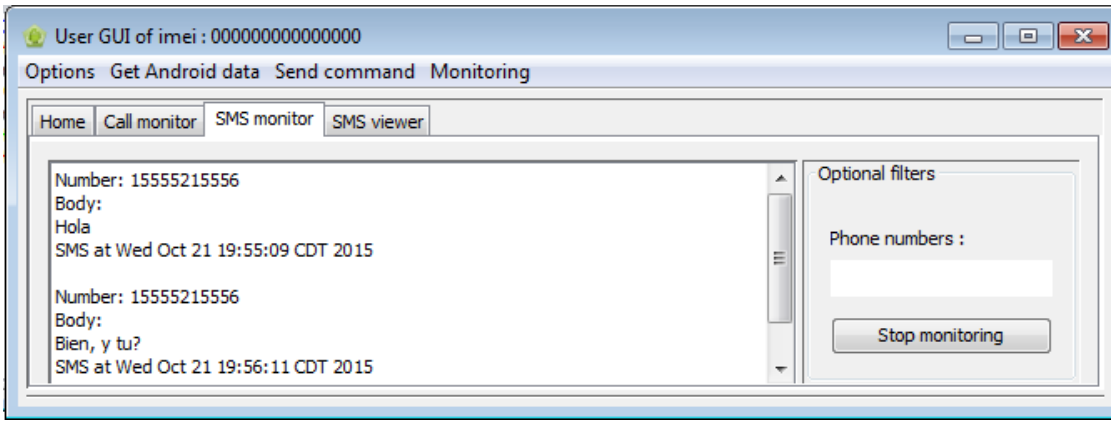


Figura 4.21. Monitoreo de mensajes de texto recibidos en el dispositivo con AndroRat.

- **"Bulk actions"**, despliega tres opciones: "Toast it", "Send SMS" y "Give call", analizando su comportamiento, se llega a la conclusión que tienen el mismo funcionamiento de las opciones que aparecen en "Send command" dentro de la ventana "User GUI of IMEI", por lo tanto el volver a explicar las acciones que permiten llevar a cabo resultaría redundante.

- **"About"**, es la última opción de la ventana "Androrat Project" y sólo despliega una ventana en la que se aprecian los nombres de los autores de la aplicación así como el lenguaje de programación en el cual fue desarrollado y su tipo de licencia, Figura 4.22.

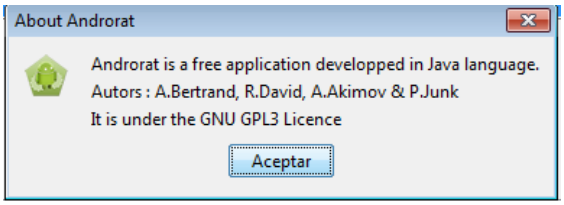


Figura 4.22. Corresponde a información de la aplicación AndroRat.

Con el análisis de AndroRat en el dispositivo emulado se logró apreciar que esta aplicación brinda las opciones necesarias que permiten obtener información del hardware del dispositivo, del proveedor de la red de telefonía, así como acceso a información sensible del usuario como: contactos almacenados en dicho dispositivo, registro de los mensajes de texto, archivos almacenados en la memoria externa del dispositivo, entre otras. Sin embargo, en algunos casos se tuvieron algunas limitaciones debido a que se requería de la funcionalidad del dispositivo físico para apreciar mejor

las opciones con las cuales cuenta AndroRat, es por esta razón que a continuación se van a llevar a cabo las pruebas de esta muestra de malware en un dispositivo físico.

Como se mencionó con anterioridad la aplicación de AndroRat requiere de un puerto y dirección IP para establecer la conexión con el servidor, en el caso de las pruebas con el dispositivo emulado bastó con la IP local. Pero ahora se va a hacer uso de la IP pública de la computadora con la cual se está trabajando, una desventaja de trabajar con la IP pública radica en que el proveedor del servicio de internet asigna direcciones IP dinámicas y si el módem es reseteado tanto por acción del usuario o por falta del suministro de energía eléctrica, la dirección IP cambia y resultaría poco práctico estar configurando de nuevo la aplicación cada vez que esto suceda, es aquí cuando la pestaña con el nombre de "No-IP" que se aprecia en la figura 4.8 resulta útil. Debido a que "No-IP", es un portal que entre algunos de sus servicios brinda la opción de asignar un dominio a la IP utilizada, así que la conexión se hará a este domino sin importar que la dirección IP cambie, para realizar esto es necesario ingresar a la página de "No-IP" (http://www.noip.com/) y crear una cuenta, posteriormente agregar el dominio al cual se comunicará el cliente, como lo indica la Figura 4.23, y como último paso dentro de la página web de "No-IP" hay que descargar el cliente ("Download Cliente", que se aprecia en la parte izquierda de la Figura 4.23). Cabe hacer la aclaración que a partir de ahora algunos campos en las imágenes que sirvan para ejemplificar las pruebas realizadas serán borrados por motivo de mantener la seguridad y privacidad del equipo con el cual se lleva a cabo este análisis de malware ya que estos datos sí son reales y pueden ser usados con fines distintos a los del presente trabajo.

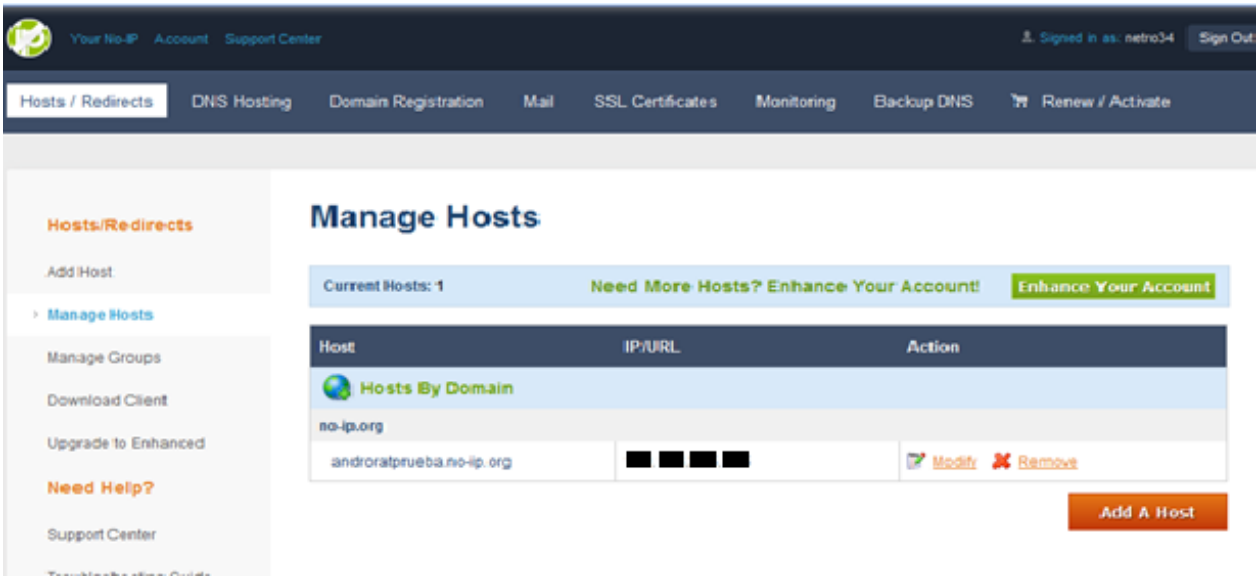


Figura 4.23. Configuración del host en No-IP.

Cuando la descarga del archivo haya concluido, es pertinente ejecutarlo, entonces se desplegará una ventana con el nombre "No-IP DUC" (No-IP Dinamic Update Client), para configurarla es necesario colocar la cuenta de correo electrónico y la contraseña con la cual se hizo el registro para crear la cuenta, si los datos son correctos en seguida desplegará la ventana "Edit Group/Hosts", en ésta se pedirá que se seleccione el host que va a ser asociado con el cliente, por lo tanto hay que marcar la casilla que aparece con el nombre del host "androratprueba.no-ip.org" y guardar los cambios. Finalmente desplegará una ventana en la cual aparece el estado de la conexión entre el cliente y el host de "No-IP", como se observa en la figura 4.24

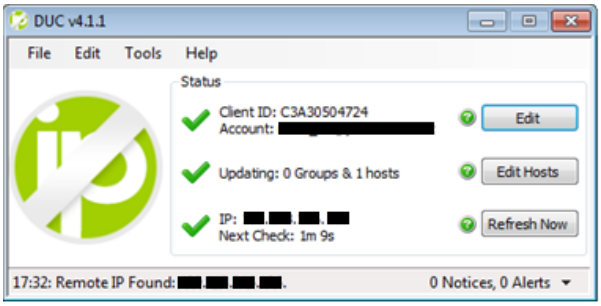


Figura 4.24. Estado de la conexión entre el cliente y el host de "No-IP".

Como siguiente paso es necesario habilitar el puerto en el modem para que la aplicación se logre comunicar con el dispositivo infectado, en esta ocasión el puerto para la prueba es el 5689. Hecho lo anterior es turno de retomar la configuración de la pestaña de "No-IP" dentro de la de la aplicación "AndroRatBinder", como se aprecia en la Figura 4.25, en la sección de "User name" y "Password" se deben ingresar los datos correspondientes a la cuenta que se creó en la página web de "No-IP" y en el último campo "Host name" se colocará el nombre de host que aparece en la Figura 4.23 (androratprueba.no-ip.org), para concluir se ejecuta el botón "Update" para que se establezcan los parámetros asignados y si son correctos en la sección de "Status" se apreciará el mensaje de que la actualización fue exitosa ("Update succesful"), así es como termina esta parte de configurar la cuenta de "No-IP".

Para crear la aplicación infectada se realizan los pasos que se explicaron en la página 86, correspondientes a la pestaña de "Build +Bind" de la aplicación "AndroRatBinder", con la única diferencia que en el campo que corresponde a "IP" se coloca el nombre del host "androratprueba.no-ip.org".

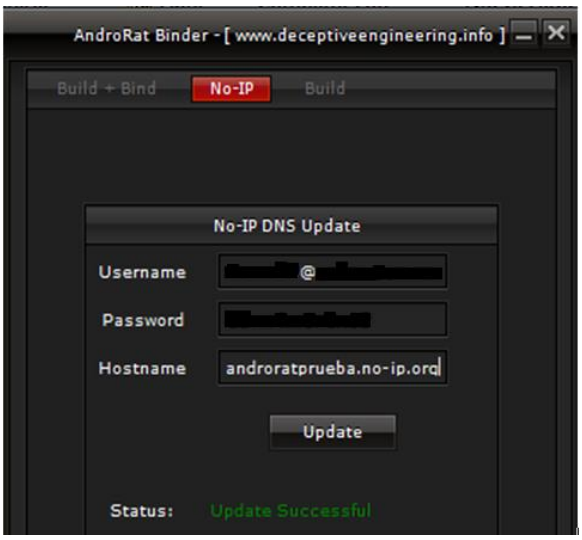


Figura 4.25. Configuración de la cuenta de "No-IP" en la aplicación "AndroRatBinder"

Teniendo la aplicación infectada con la configuración necesaria para que se comunique con el servidor, es posible instalarla en el dispositivo en este caso se trata de Smartphone Samsung Galaxy S5360L (Edición Hello Kitty), indicado en la Figura 4.26. Al momento de instalar la aplicación se informa al usuario el tipo de permisos que éste otorgará a la aplicación por medio de su dispositivo al momento de instalarla, como se puede apreciar en la Figura 4.27.

Figura 4.26. Información del Smartphone (físico) sobre el cual se instala la aplicación infectada con AndroRat.

Figura 4.27. Permisos que la aplicación infectada solicita al usuario

Ya instalada la aplicación en el Smartphone, se puede ejecutar el archivo "AndroRat.jar" como se explicó en la página 90, dando como resultado la ventana con el nombre "Androrat Project", pero esta vez ya con datos reales del dispositivo infectado, puediéndose apreciar en la Figura 4.28.

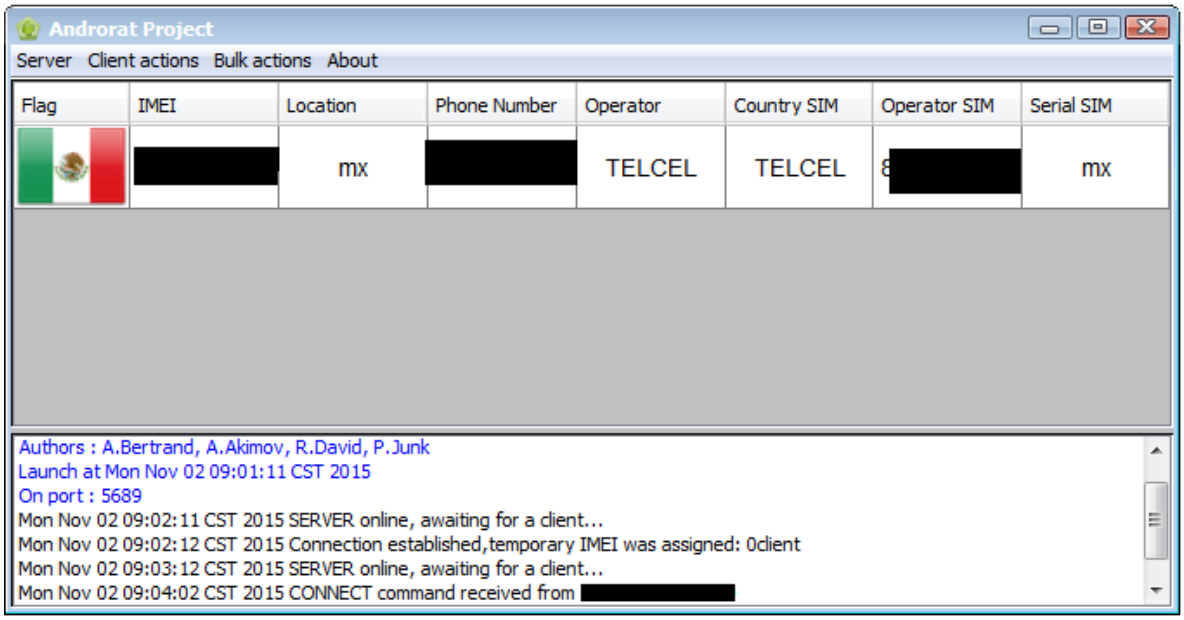


Figura 4.28. Vista de la ventana del Servidor con un cliente conectado.

Debido a que previamente en la parte donde se emuló el dispositivo con sistema operativo Android, se hizo una explicación de cada una de las opciones de las cuales se conforman las ventanas: "Androrat Project" y "User GUI of IMEI". En esta parte del analisis con el dispositivo sólo se llevará a cabo en la ventana "User GUI of imei", ya que en ésta se encuentran los opciones más destacadas de la aplicación AndroRat que permiten conocer y extraer datos relevantes del dispositivo infectado.

La pestaña "Home" como se mencionó con anterioridad se conforma de tres apartados:

1. *"Informations"*, en este campo se brinda información del dispositivo bajo los siguientes parámetros: "general del dispositivo", "conexión inalámbrica de internet", "red de datos móvil", "versión de Android", "Dispositivos" y "Batería". Los cuales se aprecian con detalle en las Figura 4.29.

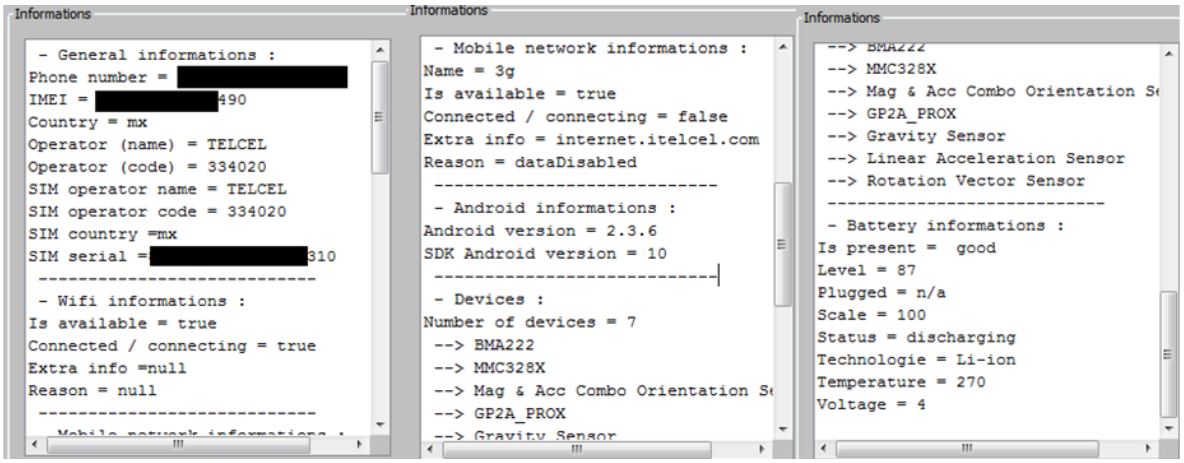


Figura 4.29. Apartado "Informations" de la pestaña "Home".

2. *"Client options",* se conforma de 6 campos: "Phones" y "SMS",en estos dos aparece el número telefónico del dispositivo infectado; "Server IP", aquí debería de aparecer la dirección IP púbilca de la máquina en la cual se está ejecutando el servidor pero como se configuró el host de No-IP, éste es el que aparece (androratprueba.no-ip.org); en "Port", se asigna el puerto por el cual se estable la conexión con el servidor siendo el 5689; "Wait event to conect", si se activa este campo la conexión con el servidor se establecerá al momento de que se ejecuta la aplicación infectada, por otra parte si no se selecciona, la conexión con el dispostivo se establece desde que éste es encendido y por último el campo de "Needed Keywords", permite configurar una palabra para que al momento de ser enviada al dispositivo se lleve a cabo la desconexión con el servidor. Todos los campos previamente explicados se observan en la Figura 4.30

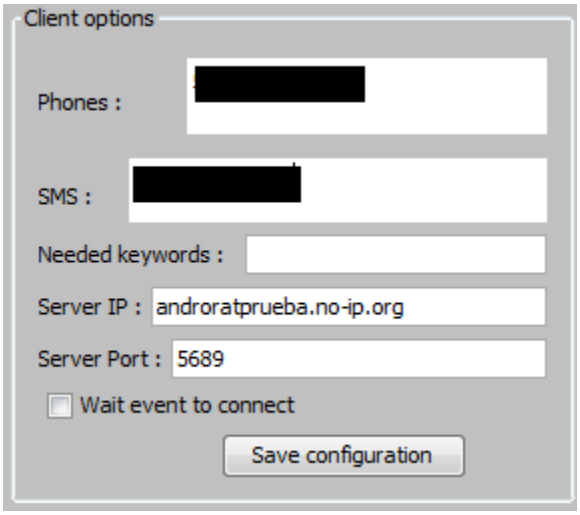


Figura 4.30. Vista de "Client options".

3. *"Quick actions"*, este apartado se conforma de tres opciones de las cuales se ha descrito su funcionamiento en la página 93, ahí se mencionó que el campo correspondiente a "Vibrate" necesitaba del dispositivo físico para comprobar que éste era capaz de vibrar según la duración especificada, haciendo pruebas con el dispositivo se logró apreciar que el valor que se solicita en el campo de "Duration" debe ser establecido en milisegundos por lo tanto para que el dispositivo vibre un segundo se asigna el valor de 1000. La figura 4.31 corresponde a los comandos ejecutados desde la parte del servidor ("Quick actions") y la figura 4.32 corresponde a las capturas de pantalla del Smartphone al momento de ejecutar los comandos "Toast it" y "Open url".

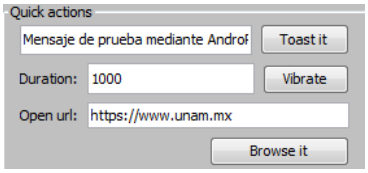


Figura 4.31. Vista de los comandos enviados desde el servidor AndroRat.

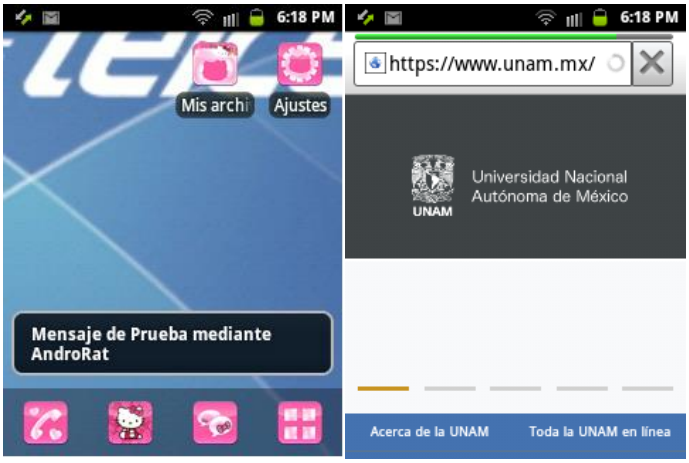


Figura 4.32. Capturas de pantalla del Smartphone, la parte izquierda corresponde a la ejecución del comando "Toast it" y la parte de la derecha al comando "Open Url".

Retomando lo que se vio en la página 94 sobre la pestaña "Get Android data", ahora se va a hacer el análisis de las opciones de esta pestaña con el dispositivo Samsung. Sólo en aquellas opciones que durante su análisis en el dispositivo móvil emulado el resultado presentó limitaciones por la

falta del hardware real, por lo tanto de las 6 opciones de esta pestaña únicamente se analizarán las siguientes:

- "Take picture", esta funcionalidad permite en sus opciones elegir la cámara por la cual se desea tomar la imagen, en este caso se selecciona la cámara trasera, ya que es la única con la que cuenta el dispositivo, por ésta se logra observar lo que capta la cámara en la parte superior derecha de la imagen 4.33 y para capturar la imagen se ejecuta el botón "Take picture". Hecho lo anterior la imagen se puede visualizar en la parte izquierda de la ventana, como lo indica la figura 4.33.

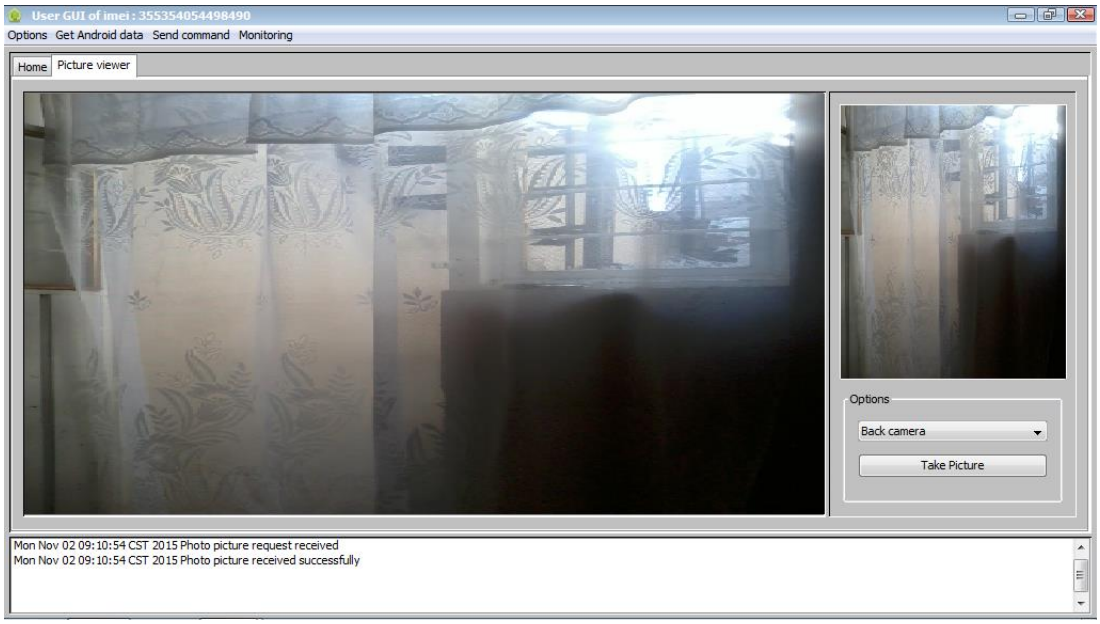


Figura 4.33. Vista de la ventana "User GUI of IMEI", correspondiente a la pestaña "Picture viewer".

- "File tree", con esta opción es posible visualizar los archivos almacenados en la memoria extraíble del dispositivo, apreciándose en la figura 4.34, en donde se desglosa todo el contenido de las carpetas que se almacenan ahí, que van desde: fotografías, videos, archivos de Whatsapp, archivos de ofimática, sólo por mencionar algunos. Como se mencionó en la página 94 con respecto a esta opción de AndroRat es posible conocer destalles de cada archivo almacenado en la memoria así como descargarlo al servidor, como se logra observar en la parte derecha de la figura 4.34.

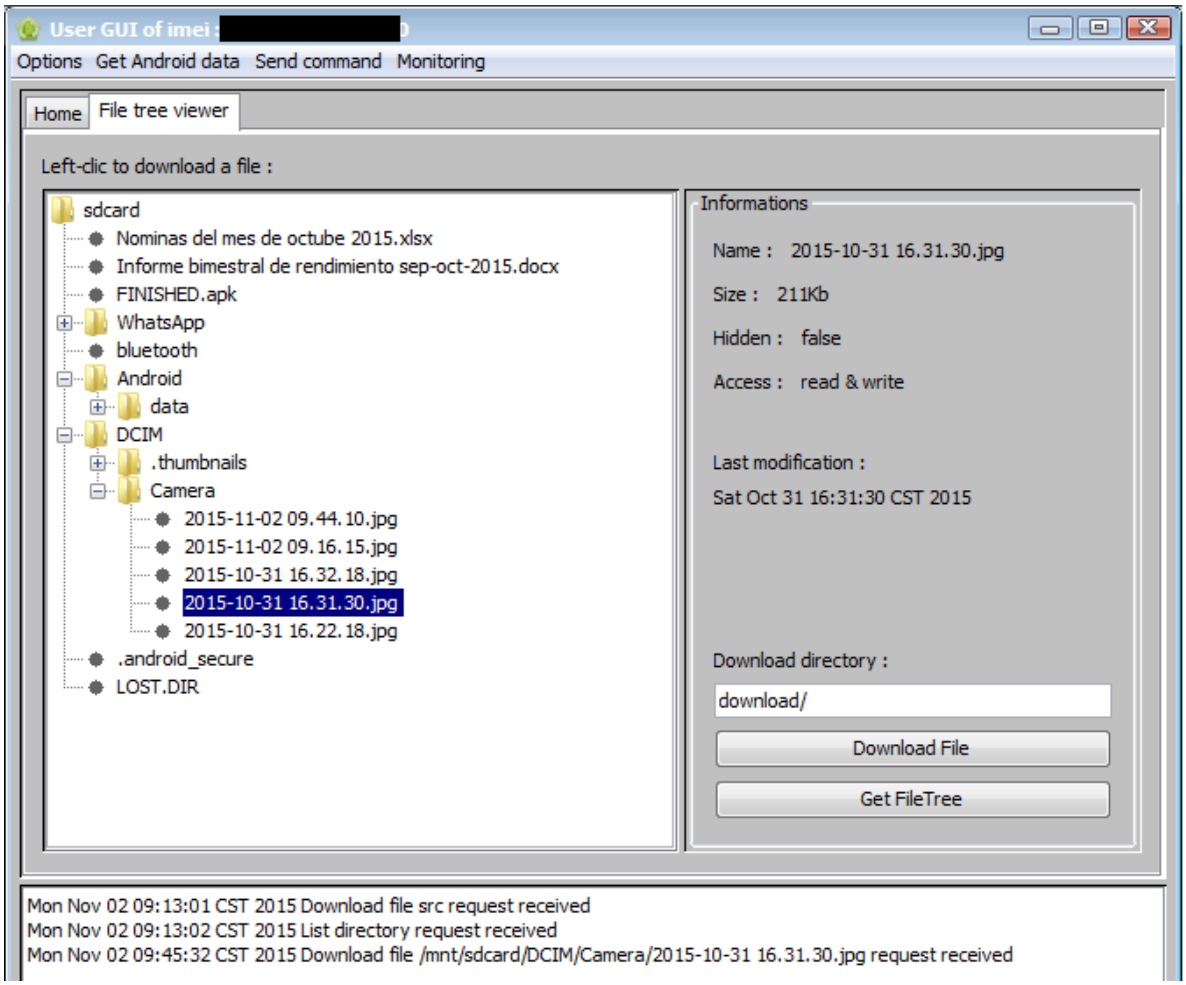


Figura 4.34. Vista de la ventana "User GUI of imei", correspondiente a la pestaña "File tree viewer".

- "Streaming", esta opción brinda dos funcionalidades que son:
  - ✓ "Localisation", con ésta es posible conocer la ubicación del dispositivo mediante el uso del GPS, mientras esté activado en el Smartphone, como se logra apreciar en la figura 4.35.

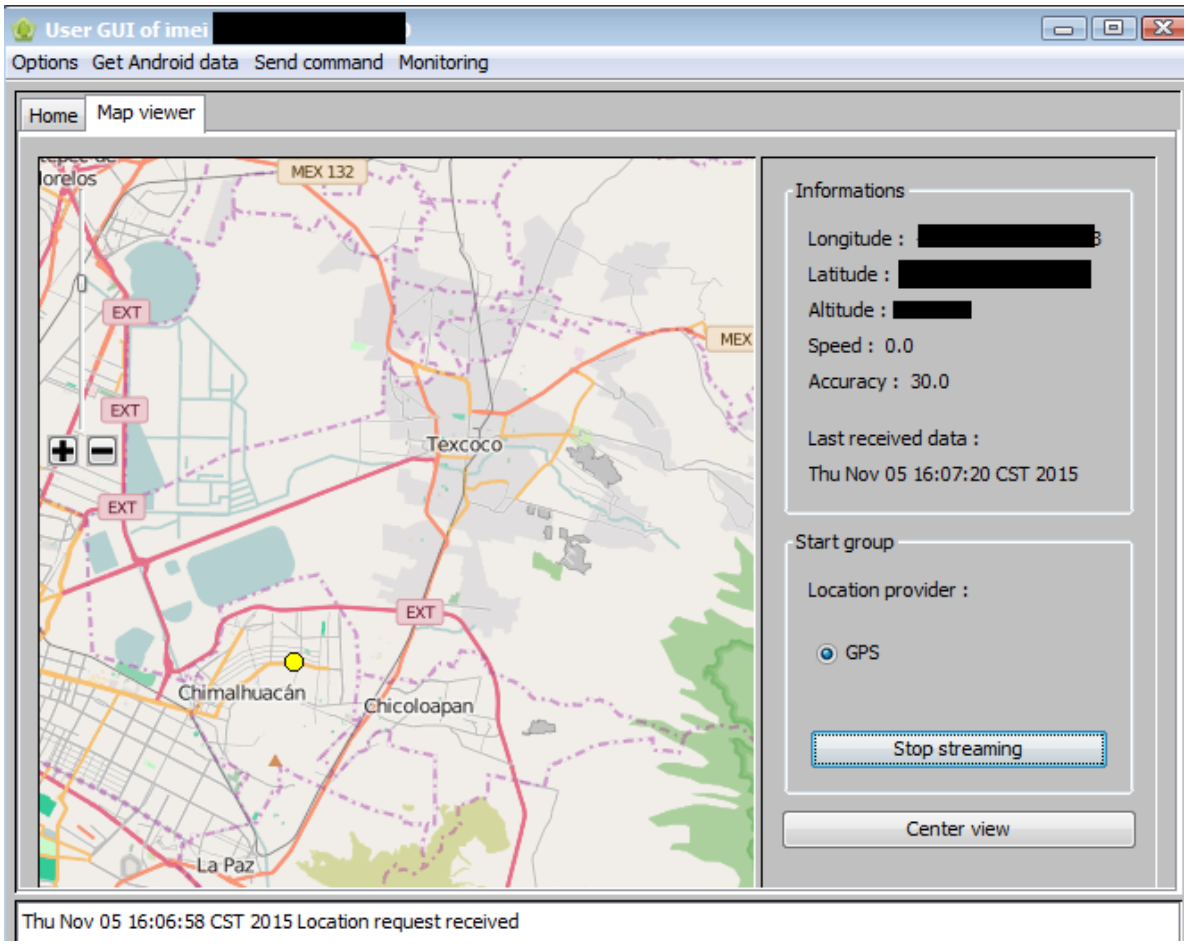


Figura 4.35. Vista de la localización del dispositivo infectado (punto amarillo) con AndroRat por medio del GPS.

- ✓ "Audio", con esta funcionalidad de AndroRat es posible escuchar en la computadora donde se ejecuta el servidor de la aplicación como lo indica la figura 4.36, el audio que el micrófono del dispositivo capta así como grabarlo. Sin embargo la calidad del audio es muy baja ya que se percibe ruido y la voz que se capta es muy aguda.

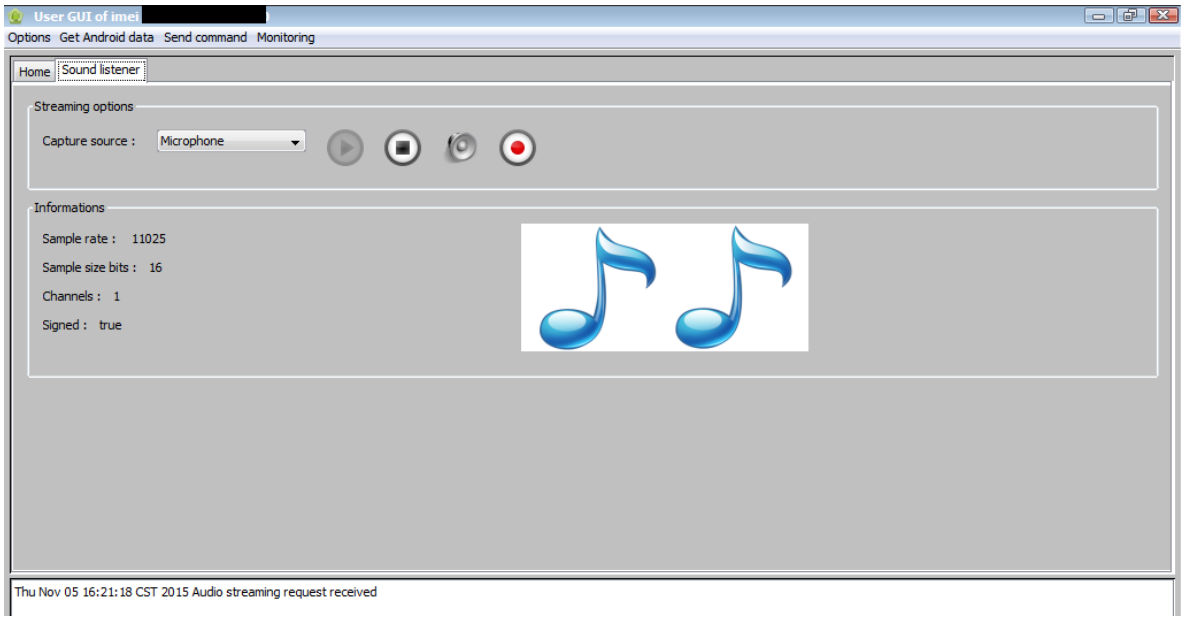


Figura 4.36. Vista de la opción "Streaming audio"

Para concluir este capítulo de la muestra de malware analizada, se logró apreciar que es posible infectar una aplicación legítima y una vez instalada en el dispositivo de la víctima, las funcionalidades con las que cuenta dejan en una situación vulnerable a la información del usuario, pues el hecho de tener la capacidad de extraer cualquier archivo que se almacene en la memoria externa, el enviar mensajes de texto sin que éstos queden registrados, por mencionar algunas. Son aspectos que resultan de gran interés para los atacantes que tienen diversos fines para explotar las acciones que ponen a su disposición este tipo de aplicaciones.

AndroRat es de código abierto y fue desarrollado como un proyecto universitario a finales de 2012 que actualmente ya no tiene soporte ni seguimiento por parte de sus creadores, sin embargo actualmente existen varias fuentes de donde se puede obtener la muestra de malware, pero una desventaja que esto implica es que la aplicación en ciertas compilaciones no brinda la funcionalidad de todas sus herramientas, esto se debe a que quienes la copilan y suben a la red modifican el código y/o los archivos sin seguir un control de los cambios o documentación de los mismos, en algunos casos donde la aplicación lleva a cabo todas las funcionalidades únicamente se proporcionan las

aplicaciones sin el código. Esta RAT que fue descubierta en 2013 por Symantec, abrió el camino para que se desarrollaran aplicaciones similares, como:

- Dendroid, que comenzó a popularizarse entre enero de 2013 y agosto de 2014, este malware a diferencia de AndroRat fue desarrollado con fines lucrativos por: "Morgan Culbertson", debido a que ofrecía su aplicación por un precio de 300 dólares y el código fuente en 65 000, el creador de este malware además ofrecía a sus clientes soporte para la aplicación, dándoles así la seguridad de que cualquier dispositivo era capaz de ser comprometido.
- Droidjack, que actualmente se ofrece en internet, a un precio de 210 dólares con funciones similares a AndroRat y Dendroid. Su autor se hace llamar "L.R Sanjeevi" e igual que "Morgan Culbertson" su aplicación cuenta con soporte para aquellos que la compren.

Con estos ejemplos en donde vulnerar la privacidad del usuario mediante el uso de malware es una realidad que merece la atención necesaria por parte del usuario para evitar que se vuelva una víctima más, se da paso al siguiente capítulo que consistirá en elaborar una guía con buenas prácticas dirigidas a los usuarios de Smartphone con el fin de reducir el riesgo de una infección por malware así como para mantener la seguridad de la información en su dispositivo, pues el hecho de que el dispositivo siempre se encuentre con el usuario no es garantía de que esté seguro.

Capítulo 5

Guía de seguridad para Smartphones con sistema operativo Android (orientado a prevenir la infección por malware)

5.1 Introducción

En este capítulo se presenta la elaboración de la guía basada en buenas prácticas dirigidas a los usuarios de Smartphones con Android con el fin de mantener sus datos bajo un buen resguardo y evitar el malware. Como se observó en el capítulo anterior con la muestra de malware analizada, la información sensible del usuario que se almacena en el dispositivo puede ser comprometida y expuesta a terceros, provocando así en la víctima: pérdida de información, experimentar un mal funcionamiento en el dispositivo, y suplantación de identidad por mencionar algunos ejemplos.

Con base en un estudio de "Ecosistema Competitivo del Mercado de Smartphones 4T14", publicado a finales de 2015, el mercado mexicano de telecomunicaciones alcanzó un estimado de 103.9 millones de líneas móviles al cierre de 2014, de las cuales 52.6 millones corresponde a usuarios que poseen un Smartphone, un equivalente al 50.7%, como lo indica la figura 5.1.

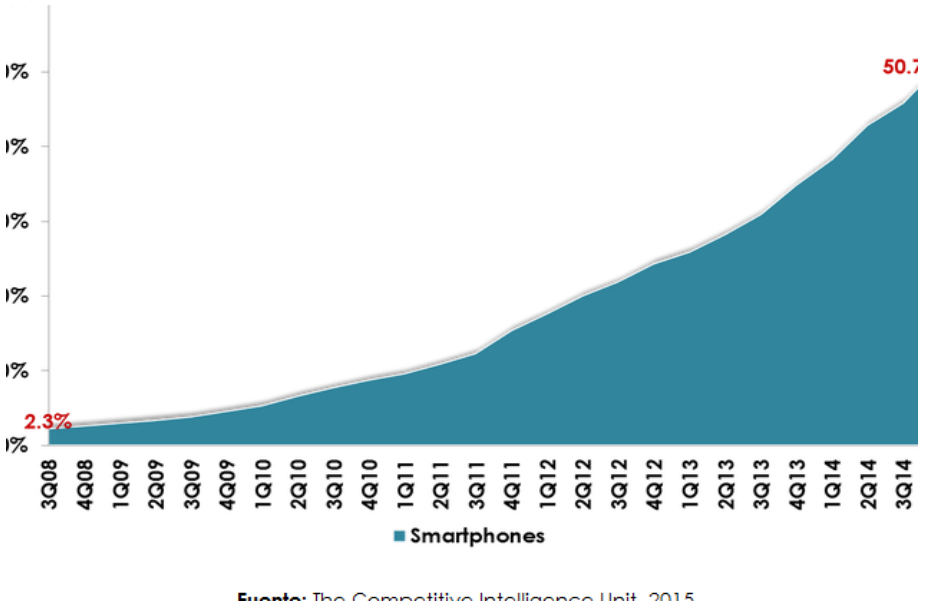


Figura 5.1. Evolución de la penetración de Smartphones en México.

Por otra parte con información de un estudio realizado por comScore denominado “Futuro Digital México 2015”, deja claro que Android es el sistema que domina el mercado de los Smartphones en México; teniendo una participación en el mercado del 82.5% como lo indica la figura 5.2.

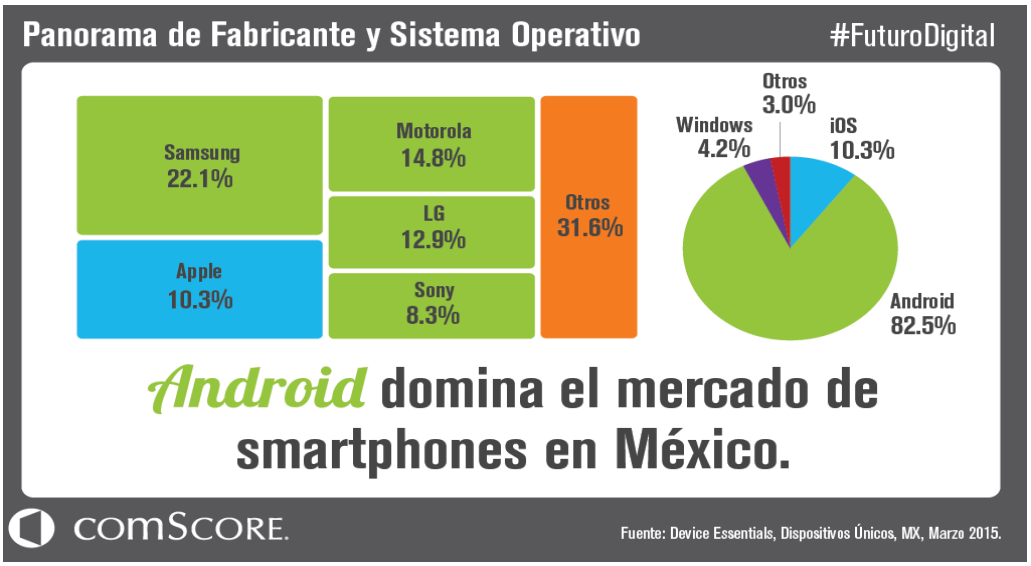


Figura 5.2. Panorama de fabricante y sistema operativo.

Con la información previa se aprecia la importancia que cobra Android en el mercado mexicano de los Smartphones, dando lugar para establecer la guía de seguridad para este tipo de dispositivos que cada día se vuelven más indispensables para muchas personas.

5.2 Contenido

La forma de trabajar esta guía es en función de tomar medidas contra las amenazas más comunes a las que están expuestos los usuarios de este tipo de dispositivos, siendo: el malware y el robo o pérdida del dispositivo, como lo indica la tabla 5.1 el de mayor incidencia.

Tabla 5.1. Amenazas y medidas para mitigar su impacto en los Smartphones

Amenaza / **Medidas a implementar**	Malware	Robo o pérdida del dispositivo
• Control de acceso mediante el bloqueo de pantalla		✓
• Cifrado de la información	✓	✓
• Bloqueo remoto del dispositivo		✓
• Copias de seguridad	✓	✓
• Actualizaciones del software (Vulnerabilidades en el software) (Fragmentación de los fabricantes)	✓	
• Repositorios no oficiales de aplicaciones (Principal fuente de Malware)	✓	
• Redes inalámbricas	✓	
• Rooting del dispositivo	✓	
• Aplicaciones orientadas a mantener la seguridad y confidencialidad del usuario.	✓	✓

- **Medida 1. Control de acceso mediante bloqueo de pantalla**, consiste en verificar a una persona que solicita acceso al sistema del dispositivo, si tiene la autorización para hacerlo se

permite el acceso (mediante la validación de un patrón, PIN o contraseña). En el caso de los dispositivos con Android se tienen las siguientes opciones para el bloqueo de la pantalla (en la parte de Ajustes>Seguridad>Bloqueo de pantalla):

- Ninguna, esta opción no brinda algún tipo de seguridad ya que el dispositivo se desbloquea presionando sólo el botón Encendido/Apagado. Dando como resultado que cualquier persona tenga acceso al contenido del dispositivo.

- Deslizar, al igual que la opción anterior el tipo de seguridad es nula debido a que el dispositivo se desbloquea sólo deslizando un icono en la pantalla del dispositivo. Esta opción es la que gran mayoría de los dispositivos trae configurada desde fábrica y tiene como principal objetivo evitar que el dispositivo se marque estando en el bolsillo del usuario, por lo tanto es necesario cambiarla por un método más eficiente.

- Por patrón, esta opción consiste en un trazo personalizable establecido por el propietario del dispositivo sobre una matriz de 9 puntos (el máximo permitido y el mínimo de 4). El nivel de seguridad que brinda este método va de medio hasta alto, depende el grado de complejidad del trazo, existen estudios en donde se analizan las características que debe cumplir un patrón seguro, siendo:

    1) Emplear combinaciones haciendo uso de 7, 8 y 9 puntos.

    2) Cruzar las líneas

    3) Evitar letras del nombre

- Por PIN (Personal Identification Number), consiste en establecer una combinación de números (como mínimo 4 y máximo 17) se considera como un nivel de seguridad que va de medio a alto en función de la cantidad de números empleados.

- Por contraseña, es una secuencia que se establece a través de la combinación de letras, números, signos de puntuación y caracteres especiales. Las contraseñas se clasifican en dos tipos: débil y fuerte, el primer tipo se caracteriza por ser una palabra de longitud corta (menos de 8 caracteres), emplear letras, números o una combinación de ambos y suelen estar asociadas al usuario (como: nombre y apellido,

fechas, nombres de hijos, placas del automóvil, entre otras). Por otra parte una contraseña fuerte contiene una combinación caracteres alfanuméricos, signos de puntuación y caracteres especiales, además de una longitud mínima de 8 caracteres y está asociada a alguna frase que es fácil de recordar para el usuario, un ejemplo sería el siguiente: "En el mes del natalicio de Benito Juárez yo cumplo años", con esta frase si se eligen las primeras letras se puede formar una contraseña (EemdndBJyca), para hacerla más fuerte se pueden agregar números, símbolos especiales o signos de puntuación (sustituyendo ciertas letras por ejemplo el 3 para sustituir la "e" y el @ para la "a") quedando; E3mdnBJyc@:18++.

- Reconocimiento facial, esta opción sólo es válida para aquellos dispositivos que cuentan con cámara frontal, con esta opción el dispositivo almacena un patrón del rostro del usuario y para desbloquear el dispositivo basta con colocar la cara del usuario frente al dispositivo. Por lo tanto el nivel de seguridad que ofrece es bajo, debido a que con poner una fotografía del dueño del dispositivo éste quedaría desbloqueado o una persona con rasgos similares puede tener acceso, además el mismo sistema hace la indicación que este método es menos seguro que un patrón, PIN o contraseña.

- Reconocimiento de voz, para esta opción se necesita establecer una palabra de 2 a 6 sílabas, la cual se debe de repetir en varias ocasiones para que el dispositivo la reconozca, adicionalmente como método secundario se debe establecer un patrón de desbloqueo ya que en el entorno pudiera existir ruido que interfiera al momento de reconocer el comando de voz, así el dispositivo podrá ser desbloqueado con el patrón. En cuanto al nivel de seguridad que ofrece esta opción es considerada en un nivel bajo, debido a que con una grabación del usuario se puede tener acceso al dispositivo.

- **Medida 2. Cifrado de la información,** el cifrado es un proceso por el cual la información almacenada en el dispositivo se codifica mediante un algoritmo de cifrado y una clave, de tal forma que si alguna persona ajena que desconoce la clave quiere acceder al contenido del

dispositivo no tendrá éxito. El cifrado en Android está disponible a partir de la versión 3.0 (en Ajustes>Seguridad>Encriptación) y se puede aplicar tanto en el almacenamiento interno del dispositivo así como en el externo, para llevar a cabo este método se necesita tener la batería completamente cargada así como tener conectado el dispositivo a una fuente de energía, por otra parte será necesario establecer un PIN o contraseña para acceder al dispositivo ya que ésta será la clave con la cual se descifrará la información, por lo tanto entre más fuerte sea la contraseña establecida, mayor será el grado de seguridad del dispositivo.

- **Medida 3. Bloqueo remoto del dispositivo**, esta opción tiene como objetivo impedir que una persona que no es propietaria del dispositivo tenga acceso a las funciones de éste, entre las formas de bloqueo remoto están:
    - Anti robo móvil, esta opción se configura directamente en el dispositivo (Ajustes>Seguridad>Anti robo) estableciendo un PIN (de 6 a 12 dígitos) así como un número telefónico desde el cual serán enviados ciertos comandos para realizar las siguientes acciones:
        1) Bloqueo remoto del teléfono, se activa enviando el mensaje: #suoding#
        2) Borrado de datos remotamente (restableciendo el dispositivo a sus valores de fábrica), mediante el mensaje: #xiaohui#
    - Bloqueo de dispositivos Android, para dar uso de esta opción es necesario que el dispositivo tenga configurada una cuenta de Google, ya que con ésta se va a acceder a: https://www.google.com/android/devicemanager desde cualquier navegador web, donde se tienen las opciones de bloquear el dispositivo o borrar datos.
    - Bloqueo mediante IMEI, con esta opción el usuario es capaz de solicitar a su compañía proveedora del servicio de telefonía la desactivación del dispositivo, en caso de extravío o robo. Con esta medida se evita que el dispositivo sea reactivado, desbloqueado, flexeado o usado para fines delictivos. Para obtener el IMEI (siendo el acrónimo para de International Mobile Equipment Identity, Identidad Internacional de Equipo Móvil en español) basta con teclear el siguiente código: *#06#, o revisar debajo de la batería, este número (de 15 a 17 dígitos) debe ser guardado por el usuario en caso de que tenga la necesidad de usarlo. El Instituto Federal de

Telecomunicaciones (IFT) en su página web (http://www.ift.org.mx/emai) pone al alcance de las personas la opción de consultar el estado de un dispositivo (si cuenta con reporte de robo o extravío) para evitar ser víctimas de algún fraude al momento de adquirir este tipo de dispositivos, por otra parte el emplear el IMEI también resulta una excelente medida para combatir la venta de teléfonos robados, situación que cada día se vuelve más común.

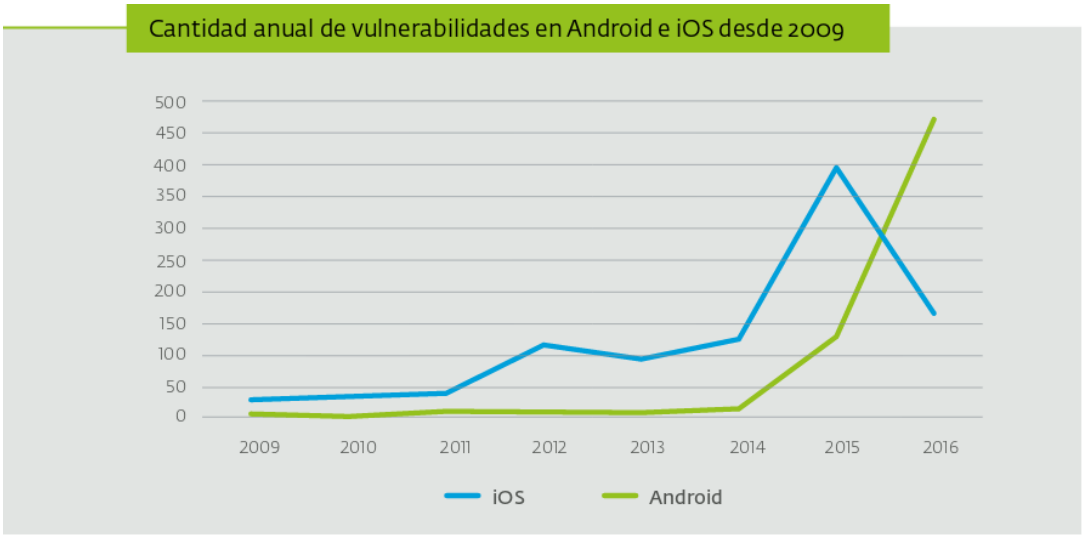
- **Medida 4. Copias de seguridad,** actualmente en el día a día es muy común que en nuestros smartphones almacenemos información importante tanto para el trabajo como para nuestra vida personal, estando conscientes de que por causa de algún tipo de: malware, avería, pérdida o robo del dispositivo, la información almacenada en el dispositivo se encentraría comprometida hasta llegar al punto de perderla.

  Por lo tanto el realizar una copia periódicamente sobre la información que sea considera importante para el usuario minimizará el impacto de las amenazas ya mencionadas, esto no se debe de ver como una pérdida de tiempo sino como una inversión del mismo, ante una eventualidad como las que se mencionaron.
  De hecho el 31 de marzo es considerado como el día internacional del backup, esta fecha no fue promovida por alguna empresa u organización en particular sino que nació mediante un post en la web, dando lugar a: http://www.worldbackupday.com/es/ en donde se publican algunos datos que se ilustran en la imagen 5.3:

Figura 5.3. Datos relacionados a la importancia de realizar respaldo

En el caso de los dispositivos con Android para el respaldo de la información presentan una solución "básica", porque sólo se permite en las opciones del sistema llevar a cabo una respaldo de las configuraciones del dispositivo así como los parámetros asociados a la cuenta de google con la cual está vinculada el teléfono. Esto impacta en que los archivos almacenados como: documentos de texto, hojas de cálculo, fotografías, videos, imágenes, etc. deberán de ser respaldas de forma manual. Pero para solventar esta debilidad en la "play store" están disponibles aplicaciones que automatizan este proceso y brindan al usuario una experiencia más amigable para llevar a cabo el proceso de copias de seguridad.

- **Medida 5. Actualizaciones del software,** las aplicaciones así como el sistema con el cual opera el dispositivo están en constante cambio esto implica una serie de actualizaciones que surgen para corregir vulnerabilidades o para mejorar la eficiencia en rendimiento del software. Lo anterior es una tarea continua que tiene como objetivo brindar al usuario una buena experiencia en el uso del dispositivo en cualquiera de las tareas que realice con éste, como se aprecia en la figura 5.4 se tiene una gráfica que presenta la cantidad de vulnerabilidades encontradas tanto en Android como en IOS desde 2009.



Observación: Las vulnerabilidades de 2016 contabilizan hasta el 14 de noviembre de 2016.

Fuente: http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

Figura 5.4: Vulnerabilidades en Android e IOS desde 2009.

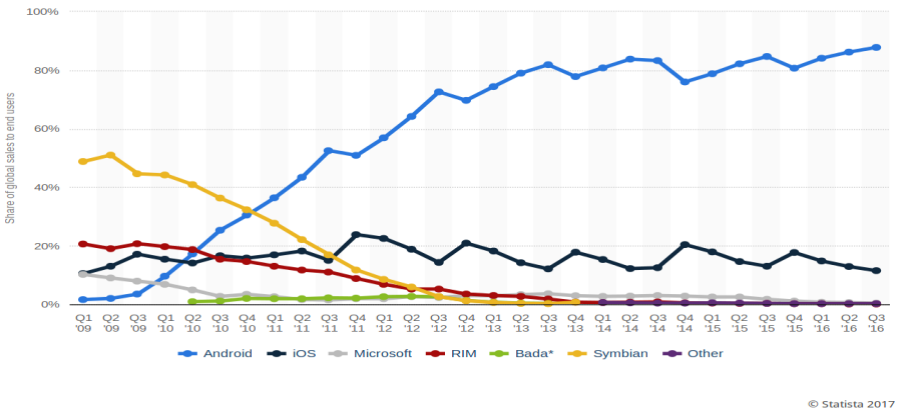
El llevar a cabo la actualización tanto del sistema operativo así como de las aplicaciones tiene como propósito minimizar el impacto que pudieran tener las amenazas de malware si en algún momento se llegan a presentar, debido a que en la mayoría de los casos el código malicioso aprovecha vulnerabilidades conocidas en ciertas versiones de las aplicaciones para ganar privilegio de acceso en el dispositivo de la víctima y así robar datos confidenciales de los cuales se pudiera obtener un fin lucrativo. Las actualizaciones de las aplicaciones instaladas en el dispositivo del usuario son notificadas de forma muy oportuna por el sistema Android, ya que en la parte superior del dispositivo de presentan iconos que muestran la disponibilidad de estás y además pueden ser configuradas para que se actualicen de forma automática.

Como se mencionó, las actualizaciones en las aplicaciones son importantes para solventar fallos en la seguridad además de proporcionar mejoras en el aspecto y rendimiento de éstas, pero ahora toca abordar las actualizaciones del sistema operativo; las cuales no dependen directamente de que Google libere éstas para Android con la finalidad de que el usuario final cuente con la versión más reciente en su dispositivo, si bien Google libera las versiones más recientes del sistema operativo, un aspecto que interviene son los diversos fabricantes de los dispositivos como (Samsung, HTC, Sony, por mencionar algunos), ellos junto con los operadores de telefonía son los encargados de liberar y poner a disponibilidad del usuario las nuevas versiones del sistema Android, pero no en todos los dispositivos por igual ya que la tendencia que se ha seguido es que sólo los dispositivos de gama alta tengan disponible la versión más actual del SO, y en los últimos años algunos dispositivos de gama media.

Lo anterior tiene un impacto notable en el mercado considerando que en México los dispositivos que predominan van de gama baja a gama media, y los de gama alta sí están

presentes pero en un porcentaje pequeño Por lo tanto al no estar al 100% cubiertas las actualizaciones del sistema operativos en todos los tipos de dispositivos hay una brecha que está abierta a dejarlos vulnerables ante códigos maliciosos que aprovechen huecos en la seguridad con el fin de obtener acceso a información personal de los usuarios con el fin de lucrar con ésta. Por lo anterior es que la medida 10 de la tabla 5.1 se vuelve importante ya que al no tener un software que este al día en cuanto a seguridad por parte de fabricante o proveedor del servicio, existen aplicaciones que ayudan a solventar estas vulnerabilidad con el fin de mantener nuestro dispositivo con grado de seguridad aceptable, pero este software al que se refiere también puede ser suplantado si no se tiene en consideración un lugar apropiado de donde obtenerlo es por eso que la medida 6 de la tabla 5.1, que a continuación se describe es importante y esta relacionada con las tiendas de aplicaciones oficiales que brindan un grado de confianza al obtener software para nuestro Smartphone.

- **Medida 6. Repositorios no oficiales de aplicaciones.** Como se muestra en la figura 5.5, el sistema operativo que domina el mercado de los Smartphone a nivel mundial es Android con más del 80% de dispositivos al cierre del año 2016.



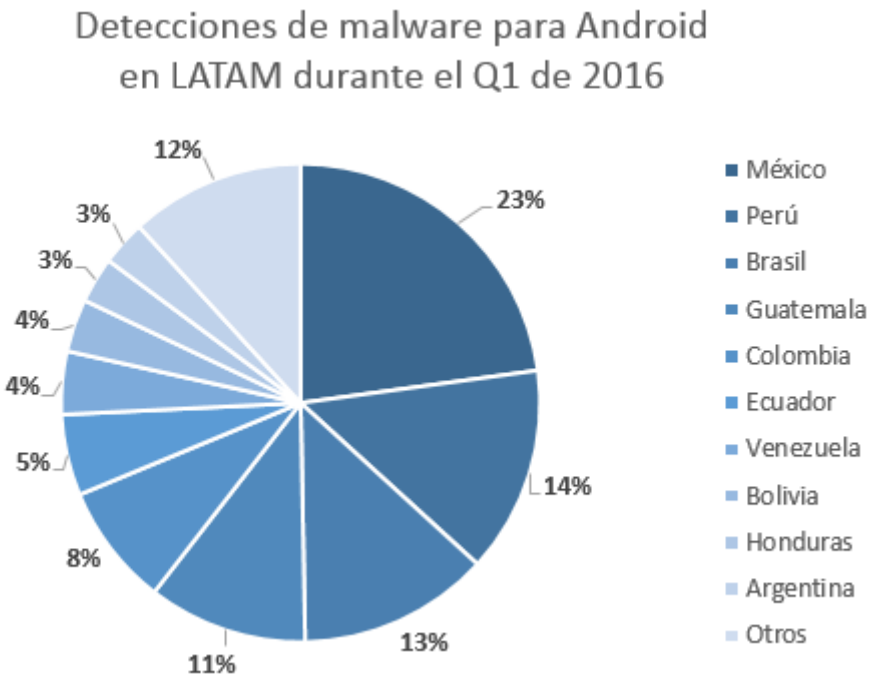
Fuente: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

Figura 5.5: Distribución del mercado global por sistema operativo de Smartphone al 3Q de 2016.

Por lo tanto al ser el sistema con mayor número de usuarios se vuelve el principal objetivo de amenazas, entre las que destaca el malware; que tiene como uno de sus principales vectores de propagación los repositorios no oficiales en donde se alojan cientos de aplicaciones que ofrecen "características" muy llamativas para los usuarios, las cuales en un repositorio oficial no están disponibles; como por ejemplo: obtener de forma gratuita una aplicación que en repositorio oficial tiene un costo o tener la posibilidad de descargar algún juego que aún no está disponible en la tienda oficial.

Este tipo de "características" resultan para un usuario muy tentadoras pues él tendría la impresión que al obtener la aplicación de forma gratuita en vez de pagar su precio, estaría obteniendo un beneficio, pero podría resultar contradictorio si no analiza con debido detenimiento la fuente de donde está obteniendo la aplicación de su interés así como los permisos que está permitiendo.

Con base en el estudio realizado por ESET de las detecciones de malware en América Latina al 1Q de 2016, México encabeza la lista con un 23%, seguido por Perú con un 14 % y Brasil con un 13%. Como se observa en la figura 5.6.



Fuente: http://www.welivesecurity.com/la-es/2016/05/20/malware-movil-en-latinoamerica-ios-android/

Figura 5.6: Detecciones de Malware para Android 1Q 2016 América Latina.

- **Medida 7. Redes inalámbricas,** Es la principal característica de conectividad que ofrecen los Smartphones que dan al usuario una conexión cómoda tanto para navegar por internet así como para compartir recursos como: archivos, impresoras, entre otros. Las tecnologías más comunes son la WI-FI y Bluetooth, debido a su facilidad de uso y en su implementación en varios lugares como: escuelas, oficinas, áreas públicas, por mencionar algunas.

  Debido a que actualmente estas tecnologías se vuelven muy comunes en nuestro entorno es necesario identificar cuando representan un riesgo para la integridad de la información de se opera mediante el Smartphone; relacionadas a una conexión de internet inalámbrica, se tiene como insegura a aquella que no esté protegida por una contraseña así como por un tipo de cifrado ya que es más susceptible a ataques como sniffing o robo de paquetes; en ambos escenarios el punto común es que el tráfico de la red es interceptado para robar credenciales de acceso siempre y cuando la conexión no este cifrada, una forma de prevenir esto es asegurarse que los sitios que se visitan en internet implementen un protocolo seguro, por ejemplo: HTTPS, o emplear la conexión por medio de una VPN.

  Con respecto a la tecnología Bluetooth, esta facilita compartir archivos entre usuarios que se encuentran físicamente cercanos. Pese a que algunos teléfonos vienen con esta función desactivada, mantener activado el Bluetooth no solo consume más batería, sino también expone al usuario a riesgos de seguridad como la posibilidad de que un código malicioso utilice una conexión de este tipo para propagarse de un equipo hacia otro.

- **Medida 8. Rooting del dispositivo**. La palabra "root" viene del inglés que significa raíz, este término dentro del contexto de los sistemas operativos tipo Unix está relacionado con una cuenta de usuario que tiene un control absoluto sobre los archivos del sistema. Entonces el rootear el teléfono implica acceder a éste mediante la cuenta de usuario con el mayor número de privilegios del sistema operativo por lo tanto este proceso lleva consigo una serie de ventajas y desventajas.

  Entre las desventajas que se tienen: que de aplicar mal el proceso de rooting, el dispositivo puede quedar inservible, se pierde la garantía con el fabricante y si algún tipo de malware es instalado en el dispositivo este tendrá acceso sin restricción alguna a los directorios del sistema.

Algunas ventajas son: tener un control más completo sobre la personalización del dispositivo, eliminar aplicaciones preinstaladas por el fabricante, mejorar el rendimiento del hardware y acceso a la más reciente actualización de Android sin importar que el fabricante del dispositivo la haya liberado.

El rooteo del teléfono es un procesos que si bien brinda al usuario una serie de beneficios en la administración del dispositivo, por otra parte implica una serie riesgos ya que de no administrar de forma correcta y consiente el dispositivo éste puede quedar vulnerable si algún tipo de malware se instala en el dispositivo, dándole la libertad de tener interacción con directorios críticos para el funcionamiento del dispositivo.

- **Medida 9. Aplicaciones orientadas a mantener la seguridad y confidencialidad del usuario.** Con la aparición de amenazas a la seguridad de la información de los usuarios en los smartphones, empresas y desarrolladores han enfocado sus esfuerzos en la creación de aplicaciones que ayuden al usuario final a mitigar el riesgo al que está expuesta su información almacenada en su dispositivo. Con base en lo anterior y lo que se ha presentado en los puntos 2,3,4, 5 y 6 de la tabla 5.1, actualmente están disponibles aplicaciones que permiten reforzar los puntos débiles que presente el dispositivo.
  A continuación, se presenta algunas opciones de las aplicaciones que presentan una gama más amplia de servicios, además de servir como protección anti-malware, como son: gestión de lista blanca y negra de llamadas, filtros de SMS, borrado remoto de información en caso de pérdida o robo, administrador seguro de contraseñas. Dentro de esta categoría se encuentran las aplicaciones: Kaspesrky, Avast, Avira por mencionar algunas. Pero en la mayoría para tener acceso a todas las funcionalidades que ofrecen estas aplicaciones es necesario comparar una licencia.

Conclusiones

Para la culminación del presente trabajo se dan a conocer las conclusiones a las que se ha llegado después del desarrollo del laboratorio y las pruebas realizadas.

Establecer una guía de seguridad que incluya buenas prácticas dirigidas a los usuarios de smartphones, con el fin de: prevenir la infección de código malicioso y brindar parámetros para mantener la seguridad de su información, se vuelve algo esencial en el presente ya que los usuarios almacenan y operan gran parte de sus datos sensibles por medio de los smartphones. Dispositivos que hoy día están prácticamente al alcance de toda persona y que por su practicidad e integración con otras tecnologías se vuelven una herramienta esencial en las actividades diarias de cada persona.

El desarrollo de la guía de seguridad para smartphones es un trabajo de grandes retos, debido a que se busca a través de ella brindar a los usuarios de este tipo de tecnología una serie de medidas a implementar en sus dispositivos que como se planteó al inicio del presente trabajo el fin último es prevenir a los dispositivos de infección de código malicioso y brindar parámetros para mantener la seguridad de su información, así, gracias a la investigación realizada y al laboratorio implementado es que se han integrado a la guía medidas para mitigar el impacto de las amenazas más comunes a las cuales los usuarios están expuestos tales como: el malware y el robo o pérdida del dispositivo, ya que ante este último escenario la información sensible de una persona puede ser explotada por un tercero que cuyo principal móvil es obtener un beneficio económico derivado de explotar la información del usuario final; víctima.

La guía, la cual se encuentra en el capítulo cinco está orientada a los dispositivos con sistema operativo Android, debido a que durante la investigación hecha en el desarrollo del presente trabajo se estableció y demostró que es el sistema operativo que abarca el mayor número de dispositivos en el mercado de los smartphones, por este aspecto se vuelve el sistema operativo al que más énfasis ponen los ciberdelicuentes tanto para; vulnerar como para desarrollar software malicioso, dado que Android domina el mercado y por ende se vuelven los dispositivos que cuentan con mayor número de usuarios. No obstante, las medidas de la guía tienen alcance dentro de cualquier sistema operativo de smartphones, con su respectiva adecuación.

Para el análisis de malware se optó por una muestra de malware denominada RAT “Remote Adminstration Tool”, esta muestra fue elegida por la cantidad de opciones que permite explotar en el dispositivo de la víctima, tales como: acceso a mensajes de texto SMS, acceso a los archivos almacenados en la memoria externa del smartphone, acceso al hardware de entrada del dispositivo, acceso a contactos de la víctima así como al registro de llamadas, entre otros. Elegir esta muestra de malware fue acertado ya que crea un impacto dirigido al usuario final, que le permita cobrar conciencia de la importancia y el alcance que tiene el malware respecto a los activos que puede vulnerar y comprometer, y en determinado momento explotar para fines que el atacante requiera. Por lo anterior esta muestra de malware analizada, da un ejemplo muy claro de la información que es posible comprometer en una víctima, y con base al análisis hecho se da inicio al desarrollo de la guía de buenas prácticas en el capítulo cinco.

Un factor crítico que se detectó durante el desarrollo del presente trabajo es que la gran mayoría de los usuarios opta por descargar sus aplicaciones de repositorios no oficiales, con esta acción se eleva de forma considerable la probabilidad para que sean víctimas de un tipo de malware, ya que los repositorios no oficiales no cuentan con medidas que regulen y controlen las aplicaciones que en ellos se ofrece.

El desarrollo de la guía se enfocó a cubrir buenas prácticas orientadas a evitar la infección por malware en el Smartphone con sistema operativo Android, así como las correspondientes para la parte de robo de dispositivo o extravío de éste, con el fin de tener un grado razonable de seguridad a Smartphone del usuario final. Así, para lograr un mayor impacto tanto en usuarios finales como en Ingenieros que en un futuro serán los responsables de los servicios de seguridad de diferentes entornos es que el presente trabajo se pone a disposición del público a través de la sección web del laboratorio de redes y seguridad de la FI de la UNAM

Índice de figuras

Capítulo 1: Impacto de los smartphones en la sociedad

Capítulo 2: El malware en los principales sistemas operativos de Smartphones

Capítulo 3: La seguridad de la información en los Smartphones

Capítulo 4: Análisis de muestras de malware para Android

Índice de tablas

Fuentes de información

Ableson, F., Sen R., King C., *Android in Action*, Manning Publications, 2011.

Gargenta, M., *Learning Android*, O'Reilly Media, 2011.

Areitio J., *SEGURIDAD DE LA INFORMACIÓN. Redes, Informática y Sistemas de Información. España. Editorial: Paraninfo.2008*

Notimex, marzo de 2016. *Smartphones presentan 60% de los malwares*, idconline. https://idconline.mx/juridico/2016/03/24/smartphones-presentan-60-de-los-malwares

Notimex, noviembre 2017. *Dispositivos Android, más vulnerables a ciberataques en 2018, El economista.* https://www.eleconomista.com.mx/tecnologia/Dispositivos-Android-mas-vulnerables-a-ciberataques-en-2018-20171113-0050.html

The CIU, Rolando Alamilla, mayo 2018. *El Ecosistema Competitivo del Mercado de Smartphones al Cierre de 2017*. https://www.theciu.com/publicaciones-2/2018/5/7/ecosistema-competitivo-del-mercado-de-smartphones-al-cierre-de-2017

AyacNet, septiembre 2014. Ecosistema Competitivo del Mercado de Smartphones en México. http://www.ayacnet.com.mx/2014/09/ecosistema-competitivo-del-mercado-de-smartphones-en-mexico/

AyacNet, febrero 2011. *Evolución del Mercado de Smartphones en México en 2015* . http://www.ayacnet.com.mx/2016/02/evolucion-del-mercado-de-smartphones-en-mexico-en-2015/

Eset, septiembre 2014. *Preguntas frecuentes sobre ESET Mobile Security para Symbian.* https://soporte.eset-la.com/kb964/?locale=es_ES&viewlocale=es_ES

Gartner, marzo 2018. *Reviews for Mobile Data Protection Solutions.* https://www.gartner.com/reviews/market/mobile-data-protection-solutions

Kaspersky, junio 2018. *Una buena razón para evitar los smartphones Android baratos.* https://latam.kaspersky.com/blog/preinstalled-android-malware/13055/