Universidad de Alcalá
Escuela Politécnica Superior

Grado en Sistemas de Información

Trabajo Fin de Grado

Peligros en la sincronización de datos Android

Autor: Raúl Moya Barez

Tutor/es: José María Gutiérrez Martínez

Ana Castillo Martínez

2017

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

GRADO EN SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Peligros en la sincronización de datos Android

Autor: Raúl Moya Barez

Tutor/es: José María Gutiérrez Martínez

Ana Castillo Martínez

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

FECHA:

Índice Resumido

Índice General

Índice de Tablas

Índice de Imágenes

Resumen

Este proyecto tiene como principios la función de sincronización de datos de los Sistemas Operativos de Android además de los beneficios y daños que otorga a los usuarios.

Durante el desarrollo del proyecto se va a demostrar que la sincronización de datos ayuda a tener conectados en distintos lugares, distintos dispositivos en un mismo tiempo, así como la sincronización de aquellas aplicaciones que hacen que los usuarios estén actualizados en todo momento.
Pero por otro lado tiene una parte negativa y delicada en la cual los usuarios no perciben que ocurre con sus datos privados, donde van o si están en buen estado de seguridad.

Palabras claves:
Sincronización, amenazas, Android, usuario, seguridad.

Abstract

This project is based in the function of synchrony of data in the Android System, also the benedicts and risks that give to the users.

During the development of the project, we can demonstrate that data synchrony can help to have connected us in the same time, in different places, and with different dispositive. As well the synchronization of those applications that make the users are actualized always.
But on the other hand, it has a negative and delicate part in which the users do not perceive that it happens with their private data, where they go or if they are safe.

Keywords:
Synchronization, threats, Android, user, security.

Resumen extendido

El presente proyecto se compone de una investigación y revisión de un marco tecnológico cada vez más utilizado por diferentes objetos de este mundo, la sincronización, a través de la cual, los datos que generan las distintas aplicaciones de los dispositivos móviles y los propios dispositivos permiten tener conectados a las personas con datos actualizados en todo momento.

La sincronización de datos es utilizada por toda aquella persona que tiene conexión a Internet, dado que la simple acción de descargar archivos, subir archivos en la nube, mirar en las redes sociales que está haciendo el circulo de contactos de un contacto, mirar cualquier periódico o página de noticias, mirar el correo, todas estas acciones llevan un proceso de actualización a través de la cual se sincronizan estos datos nuevos que el usuario está pidiendo para mantenerse actualizado.
Concretando más en el marco que engloba el proyecto que es el sistema operativo Android, de primera mano surgen ideas como los Smartphone los cuales utilizan este sistema operativo y las Tablet, pero existen multitud de dispositivos que utilizan Android como televisiones, relojes, gafas, libros electrónicos o automóviles.

Relacionado con el funcionamiento de Android, sus evoluciones, características y los métodos de seguridad que tienen para no afectar a sus usuarios de ningún riesgo hay que destacar una importante inversión de tiempo y dinero por parte de esta empresa para mitigar cualquier riesgo de seguridad y evitar la pérdida de datos de los usuarios que puede ser aprovechado por terceras personas.
Hay que remarcar también notables esfuerzos en el mundo que rodea a Android en relación con la seguridad como pueden ser las aplicaciones, las cuales cada vez son más seguras y pasan por filtros de seguridad más robustos o aquellos servidores Web que alojan datos en la nube los cuales han reforzado y actualizan todas las posibles lacras de seguridad que existen.
Aunque a lo largo de la vida de Android se ha mejorado la seguridad de Android, este mismo sistema operativo no puede evitar que ciertas aplicaciones que cumplen los parámetros de seguridad requieran de más recursos de los que realmente necesita y que son otorgados por los usuarios o que en algún momento un servidor Web sufra algún ataque y los datos generados por el dispositivo móvil se hayan puesto en peligro.

Volviendo a la sincronización que es un proceso el cual beneficia a todos los usuarios dado que se realiza de forma automática y los usuarios se encuentran actualizados en todo momento sin tener que realizar manualmente la actualización de datos de cada aplicación que tenga o de función del teléfono que tenga que sincronizar datos nuevos como puede ser actualizaciones de software, actualización de aplicaciones propias del teléfono móvil.
Es promovida por todas las aplicaciones, marcas de teléfonos móviles y software de

móviles por temas de seguridad y de mantener a sus usuarios actualizados y a la última en temas de software actualizados.

Por otro lado, existe una parte negativa y de un carácter delicado que años atrás la gente no era consciente y actualmente hay muy pocas personas que comprenden realmente que problemas puede otorgar la sincronización.
En esta parte negativa cabe destacar todos los datos que genera un usuario en cualquier aplicación, en cualquier dispositivo, estos datos de gustos y aficiones de los usuarios, donde se encuentran estos usuarios, que planes de futuro tienen previstos, son utilizados por las empresas para generar una oportunidad de negocio ya sea a través de la venta de datos conjuntos, nunca personales sino de grupos de personas, como de aprovechamiento de estos datos para generar oportunidades de ventas y obtención de beneficios a través de los conocimientos que se tienen de las personas ya sean para promover ofertas especiales de ciertos productos, como de actividades que realicen los usuarios.

A nivel de empresa el aprovechamiento de los datos que se producen en los dispositivos y son trasmitidos a través de la sincronización tiene un gran impacto para aquella persona que es afectada, pero en un marco más cerrado en el cual se produzca un robo de cuentas, de información o de un dispositivo, por parte de terceras personas que averigüen todo lo relacionado con un usuario puede a llegar a repercutir en conocer donde vive el usuario, cuando está en casa, cuando está fuera de casa, quienes son sus familiares y contactos más cercanos, generando así una oportunidad de delincuencia o de grupos coordinados que mantienen en vilo la seguridad del usuario.

En el presente trabajo se expresan las vías y lacras que pueden tener los datos sincronizados relacionados con la seguridad de los mismos así como ejemplos claros de cómo puede ocurrir todo lo anteriormente mencionado, donde la perspectiva de un futuro y posiblemente en estos momentos sea conocer todo acerca de un usuario sin que sea consciente de lo mismo, generando cantidades de datos que pueden ser explotados y aprovechados por empresas para en ciertos casos ofrecernos ventajas de ciertos productos que necesitemos o en casos totalmente opuestos de que la privacidad de un usuario no exista y se conozca todo del mismo.

1. Introducción

El presente documento tiene como finalidad demostrar de manera teórica y con casos prácticos que la sincronización de datos ofrece una serie de beneficios como son mantener conectados a los usuarios y actualizados en todo momento y que también al mismo tiempo se encuentran amenazas existentes relacionadas con estos datos que reciben y envían los usuarios.

La importancia en auge de la sincronización viene precedida de un mundo cada vez más conectado y con más dispositivos cada año dado que la conexión de dispositivos a Internet crece cada día a través del lanzamiento de nuevas tecnologías y uso de antiguas.
En el año 2016 se estima que hubo aproximadamente 22.000.000.000 (22 mil millones) de dispositivos conectados a la red de Internet [1], al mismo tiempo que red de Internet se expande y llega a nuevos dispositivos, por otro lado, los problemas de seguridad y/o dispositivos afectados por problemas aumenta un 32% de las empresas mundiales, en el último periodo de un año han sufrido algún ataque o amenaza. Tomando datos elaborados por El Mundo; España, se encuentra en el top 3 de países con más ciber-ataques a través de la red a los dispositivos y para entender el avance y los constantes problemas de amenazas la diferencia entre los ataques producidos entre 2015 y 2016 (los datos de 2017 aún no se tienen en cuenta al no haber terminado el año) la diferencia es de un 130% entre los dos años [2]. En relación con los Smartphone y su definición: es un tipo de teléfono móvil construido sobre una plataforma informática móvil, con mayor capacidad de almacenar datos y realizar actividades, semejante a la de un ordenador y con una mayor conectividad que un teléfono móvil convencional. El término inteligente, que se utiliza con fines comerciales, hace referencia a la capacidad de usarse como un ordenador de bolsillo [3].
El crecimiento de estos dispositivos cada año es progresivo, situando en 2016 tantos dispositivos móviles como personas hay en el planeta. Al igual que con los dispositivos tecnológicos, cuantos más dispositivos móviles hay más oportunidades de amenazas llegan a ellos.

Planteado el escenario en el que nos encontramos actualmente, en el cual la delincuencia cibernética se encuentra en un punto de auge y de una fácil penetración para usuarios que desconocen que sus datos y cuentas en un dispositivo son atractivos para los delincuentes para obtener valor por parte de ellos ya sea económicos o intelectuales.
Nos incorporamos al desarrollo del proyecto comenzando por definir el objetivo principal del mismo.

2. Objetivos y plan de trabajo

2.1. Objetivo general.

El objetivo de principal de este proyecto es:

Ayudar a los usuarios que utilizan los dispositivos Android a ser conscientes de que aquellos datos privados y personales que generan en sus dispositivos tienen un valor, los cuales se ven amenazados al ser compartidos.

El proyecto tiene como meta, obtener una serie de resultados que se puedan comprobar y que sean reales de aquellas amenazas que pueden sufrir los usuarios, relacionado con sus datos y su privacidad.

2.2. Objetivos secundarios.

- Conocer el contexto que engloba a Android y sus amenazas.
- Investigar cómo actúa la sincronización y como se trasmite.
- Comprender cuales pueden ser los próximos caminos que puede utilizar la sincronización y que generen nuevas amenazas
- Realizar casos prácticos demostrando que existe amenazas reales por parte de la sincronización.
- Poder realizar recomendaciones de cómo evitar las amenazas.

2.3. Alcance y finalidad del proyecto.

En relación con el alcance del proyecto es aportar una nueva información y un nuevo punto de vista acerca de las amenazas en la sincronización de datos en el sistema operativo Android, a través de información que ha sido investigada y procesada para elaborar este punto de vista.
Por otro lado, aporta a aquella persona que esté interesada en este tema, o en temas que tengan relación con este, como, por ejemplo: amenazas en la sincronización en ordenadores u otros sistemas operativos móviles cuales son las vías más seguras e inseguras que existen, que métodos se pueden dar para que se produzcan amenazas a través de la vía de la sincronización

Como finalidad se pretende obtener conocimiento sobre las amenazas y peligros que existen a través de una vía de comunicación como es la sincronización de datos, así como lograr desarrollar un conocimiento propio por parte del lector y del autor del propio proyecto.
Lograr entender que la sincronización es una gran ventaja para tener conectados a todos los usuarios pero que también existen campos dentro de la misma que no se han explicado detalladamente, ni han llegado a un nivel de usuario común, en

ciertos casos por no preocupar a los usuarios y por otro para aprovechar la ventaja de datos de usuarios que se trasmiten por sincronización.

2.4. Estructura del documento.

En la estructura del proyecto se plasma de forma resumida cada una de las partes por las que está formada el proyecto para aportar una pequeña idea de que van a tratar:

- Capítulo 1: Introducción.

Introducir de manera sencilla el contexto en el que se engloba el proyecto.

- Capítulo 2: Objetivos y plan de trabajo.

Declarar el objetivo que se trata de alcanzar en el proyecto y cómo se organiza el propio proyecto.

- Capítulo 3: Estado del arte.

Engloba todo el marco teórico en el cual se desarrolla el proyecto.

- Capítulo 4: Análisis de los problemas en la sincronización.

Estudiar los distintos posibles casos de las amenazas en la sincronización.

- Capítulo 5: Casos prácticos de amenazas en la sincronización.

Mostrar empíricamente algunos casos analizados sobre las amenazas.

- Capítulo 6: Resumen, conclusiones, líneas futuras y recomendaciones.

Se engloban los puntos finales de finalización del proyecto.

- Capítulo 7: Presupuesto

Conseguir tener una idea de cuánto cuesta la inversión de tiempo en un proyecto.

- Capítulo 8: Bibliografía

Referencias de todas aquellas fuentes que han sido útiles para el proyecto.

- Capítulo 9: Anexos

Ampliación de distintos puntos del proyecto con información extra.

3. Estado del arte

Independientemente de que tipo de proyecto se desarrolle y de qué tipo de metodología se pueda aplicar en un proyecto (investigación, desarrollo de un producto, realización de memoria). Una buena práctica es entender el entorno en el cual se engloba el proyecto.
En este apartado se define el marco teórico que engloba el contexto de: Sincronización de datos en el Sistema Operativo Android con el objetivo de embarcar al lector en el proceso de entender algunas de las reflexiones que se han ido tomando a lo largo del desarrollo del proyecto.
El Sistema Operativo Android, las amenazas más comunes y la historia de las propias amenazas no es un tema nuevo que se de en la amplia gama de proyectos finales de carrera, pero es adecuado describirlos y entrar en ellos de una manera detallada para entender una nueva rama de amenazas que se producen con más frecuencia en el mundo de Internet a través de la sincronización de datos.
Para un mejor entendimiento de la lectura de investigación, el estado del arte está dividido en dos partes (Android y Amenazas).

3.1. Estado del Arte: Android

3.1.1. ¿Qué es Android?

Android se define como un Sistema Operativo (S.O), diseñado para funcionar principalmente en dispositivos móviles con pantalla táctil; así como teléfonos inteligentes (Smartphone), tabletas inteligentes, televisores inteligentes, relojes inteligentes (SmartWatch) e incluso en automóviles [4] (como es el caso de Android Auto, que permite a los dispositivos móviles tener una comunicación integra con el panel del automóvil [5]).
Este sistema operativo se basa en el núcleo de Linux que se considera un Sistema Operativo de software libre y código abierto, que está basado en Unix [6] (sistema operativo portable, multitarea y multiusuario [7]).
Al inicio de su historia fue desarrollado por Android Inc. Empresa respaldada económicamente por Google, que finalmente en 2005 fue adquirida por esta multinacional, 2 años más adelante (2007) fue presentado Android y en 2008, fue lanzado el primer dispositivo móvil, en este caso un Smartphone (HTC Dream).

En la actualidad, los dispositivos con el sistema operativo Android venden más dispositivos que otros S.O como IOS (Apple), Windows Phone (Windows) y Symbian (Nokia) juntos, gracias a la comunidad de desarrolladores que tiene Android, esto se debe sobre todo por el software libre en el que está diseñado este S.O. Permitiendo que los desarrolladores puedan codificar nuevas aplicaciones que extiendan las funcionalidades y características de los dispositivos con Android.

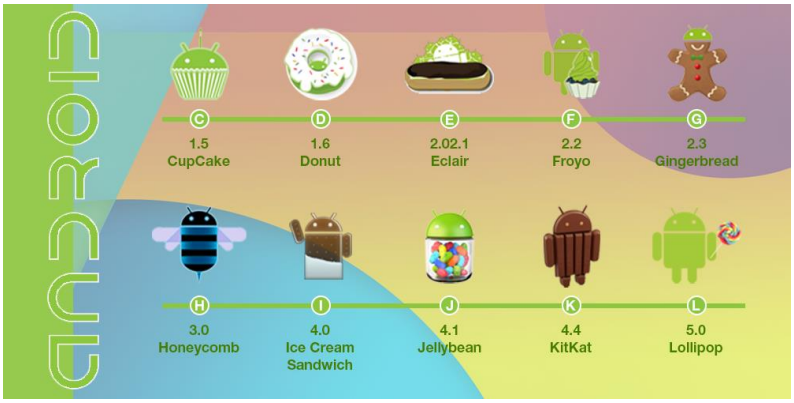


Imagen 1. Iconos de la evolución de Android.

3.1.2. Características principales de Android

Código abierto:
Gracias al código abierto existe la posibilidad de compartir, modificar y estudiar el código interno y promover la colaboración entre usuarios para un desarrollo más rápido del Sistema Operativo aprovechando las herramientas que ofrece.

Diseño de dispositivo:
Basado en OpenGL ES una variante de la API gráfica de OpenGL diseñada para dispositivos móviles, Android es capaz de adaptar su diseño a los distintos tamaños de pantalla del mercado, así como el uso de 2D y 3D y VGA entre otros tipos de pantalla.

Almacenamiento:
Se basa en SQLite un sistema de gestión de datos relacional que permite clasificar un conjunto de órdenes que se ejecutan formando una unidad de trabajo que es indivisible, gracias a esto su almacenamiento se ejecuta de forma liviana para que lleve un peso ligero en el sistema

Conectividad:
Android soporta las siguientes tecnologías de conectividad: GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE, HSDPA, HSPA+, NFC y WiMAX, GPRS, UMTS y HSDPA+.

Mensajería:
Soporta SMS (Short Message Service) y MMS (Multimedia Messaging Service) además incluye Android Cloud to Device Messaging framework (C2DM) que es un servicio de mensajería desarrollado por Google, que permite el envío de mensajes y datos desde los servidores de Android y de Google Chrome.

Navegador Web:
El navegador Web incluido en Android está basado en el motor de renderizado de código abierto Web Kit (es un motor de navegación Web de código libre), emparejado con el motor JavaScript V8 (es un motor de código abierto) de Google Chrome.

Soporte de Android :

→ *Soporte de java :*
En Android no existe una máquina virtual de Java. El bytecode Java no es ejecutado, sino que primero se compila en un ejecutable Dalvik y se ejecuta en la máquina virtual Dalvik.

→ *Soporte multimedia:*
Android soporta una gran cantidad de formatos multimedia entre los que se pueden encontrar formatos Web, de imágenes, de video y de sonido.

→ *Soportes adicionales de hardware:*
Android soporta cámaras de fotos, de vídeo, pantallas táctiles, GPS, acelerómetros, giroscopios, magnetómetros, sensores de proximidad y de

presión, sensores de luz, gamepad, termómetro, aceleración por GPU, se resumen en que todos los componentes hardware que tenga el dispositivo tiene compatibilidad con el sistema operativo del mismo y no ocurran problemas de funcionalidad entre ellos.

Entorno de desarrollo:
Incluye un emulador de dispositivos, herramientas para depuración de memoria y análisis del rendimiento del software, como entorno de desarrollo integrado (IDE) oficial está Android Studio.

Google Play:
Se trata de un catálogo de aplicaciones gratuitas o de pago en el que pueden ser descargadas e instaladas en dispositivos Android.

Multitáctil:
Android tiene soporte para pantallas capacitivas con soporte multitáctil técnica de interacción persona-computador y al hardware que la aplica).

Videollamada:
Android soporta videollamada a través de Hangouts, así como también las distintas aplicaciones de su tienda oficial (Google Play) que permiten este tipo de llamadas con vídeo como, por ejemplo: Skype, Facebook Messenger, Viber, Tango y WeChat entre otras.

Multitarea:
Android dispone de esta característica de los Sistemas Operativos actuales donde, se permite que varios procesos o aplicaciones se ejecuten aparentemente al mismo tiempo, compartiendo uno o más procesadores, dando servicio a más de un proceso a la vez para permitir la ejecución de más programas.

Tethering:
Android soporta tethering, que permite al teléfono ser usado como un punto de acceso alámbrico o inalámbrico a partir de la versión 2.2 de Android, esto permite que el dispositivo actúe como módem o enrutador inalámbrico para todo tipo de dispositivos ya pueden ser móviles como Smartphone o fijos, como ordenadores de sobremesa con antena para obtener wifi entre sus conexiones.

3.1.3.Evolución

Se trata de un enfoque rápido sobre las distintas versiones de Android qué más importancia han tenido en el mercado de los dispositivos móviles y sus características incluidas en cada actualización [8].

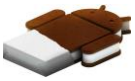
Número y nombre de versión	Características nuevas	Versión
1.6. Donut.	1. Cuadro de búsqueda rápida. 2. Diversidad en los tamaños de pantalla. 3. Android Market. (Pre-Google Play)	
2.1. Eclair.	1. Google Maps Navigation. 2. Pantalla de inicio personalizable. 3. Síntesis de voz para el teclado.	
2.2. Froyo.	1. Acciones de voz. 2. Zona Wifi portátil. (como dispositivo) 3. Mejoras en el rendimiento.	
2.3. Gingerbread	1. Apis de Juegos. 2. NFC. (Near field communication) 3. Gestión de la batería.	
3.0. Honeycomb	1. Diseño optimizado para Tablets. 2. Barra de sistema. 3. Ajustes rápidos.	
4.0. Ice Cream Sandwich	1. Mejoras en la pantalla de inicio. 2. Control de uso de datos. 3. Android Beam.	
4.1. Jelly Bean	1. Google Now. 2. Notificaciones accionables. 3. Multiusuario.	
4.4. KitKat	1. Voz: Ok Google. 2. Diseño envolvente. 3.Mejoras en la definición de SmartPhone	
5.0. Lollipop	1. Material desing. 2. Multipantalla. 3. Notificaciones en la pantalla de bloqueo.	
6.0. Marshmallow	1. Google now más accesible. 2. Permisos más personalizables. 3. Mejoras en la batería inteligente	
7.0. Nougat	1. Cifrado a nivel de archivos. 2. Ahorro de datos. 3. Función descanso para baterías.	

Tabla 1. Versiones de Android

3.1.4. Cuota de mercado mundial.

En relación de la cuota de mercado que ofrecen los dispositivos móviles Android comparados con sus competidores más próximos que son: Apple (iOS), Windows Phone (Windows), Tizen y BlackBerry [9].

	2Q16 UNIDADES	2Q16 CUOTA EN %	2Q15 UNIDADES	2Q15 CUOTA EN %
Android	296,912.8	86.2	271,647.0	82.2
iOS	44,395.0	12.9	48,085.5	14.6
Windows	1,971.0	0.6	8,198.2	2.5
Blackberry	400.4	0.1	1,153.2	0.3
Others	680.6	0.2	1,229.0	0.4
TOTAL	344,359.7	100.0	330,312.9	100.0

Imagen 2. Cuota de mercado mundial en telefonía móvil.

Se puede apreciar a simple vista y atendiendo a los resultados de la cuota de mercado de 2016, dado que a fecha actual y en el año 2017 los informes de la cuota de mercado aún no han sido realizados.

Por lo tanto, más de 8 móviles de cada 10 que existen en el mercado tienen el Sistema Operativo Android, seguido por muy lejos por iOS de Apple. También se puede observar una tendencia creciente si comparamos por años, en que Android está consiguiendo una mayor cuota de mercado que la de años anteriores.

3.1.5.Arquitectura de Android

En este apartado del proyecto se plasma una imagen sobre la arquitectura del Sistema Operativo Android el cual está dividido en 6 capas principales caracterizadas por ser de software libre y accesible para los usuarios [10].

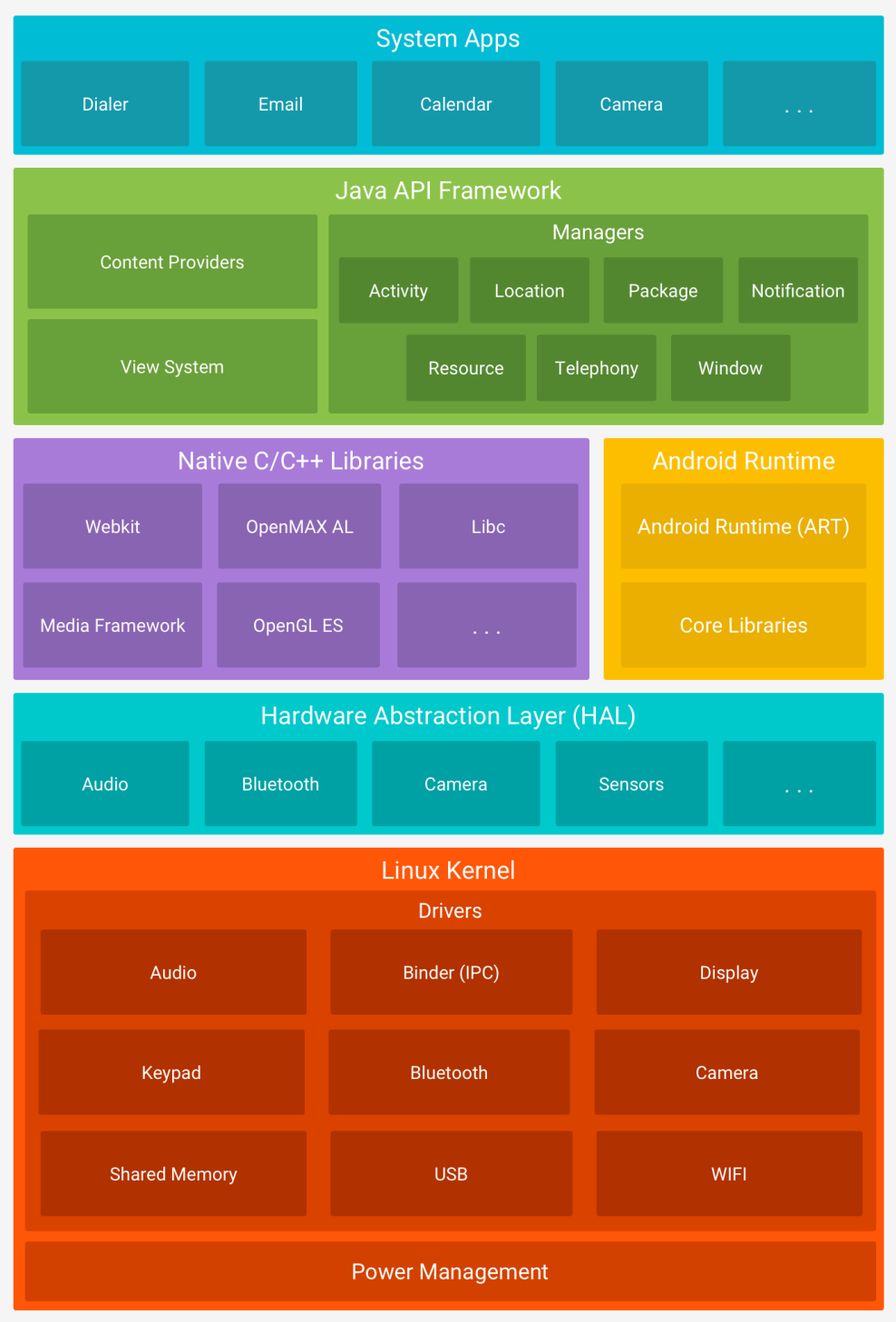


Imagen 3. Arquitectura de Android.

La arquitectura está descrita de manera ascendente, por lo cual empieza por Linux Kernel y la última capa descrita es la de System Apps.

Linux Kernel:
Se puede definir como la base de Android, está formado por el Sistema Operativo, como ya fue nombrado antes, Linux. La característica principal es que contiene los drivers necesarios para las interacciones con el hardware por parte del usuario, por lo que, si un fabricante nuevo quiere añadir un nuevo hardware en su dispositivo, para que funcione correctamente en Android, debe de crear las librerías pertinentes para dicho hardware dentro del Kernel de Android.
Además de esta característica, también proporciona servicios de manejo de memoria, multiprocesos, y pila de protocolos.

Hardware Abstraction Layer (HAL):
Su función es similar a la de una interfaz entre el software y el hardware de Android, consiste en varios módulos de biblioteca y cada uno de estos implementa una interfaz para un tipo específico de componente de hardware, por lo tanto, cuando el Framework de una API realiza una llamada para acceder al software deseado, Android realiza una carga de la biblioteca de dicho hardware.

Bibliotecas nativas de C/C++:
Como bien dice el mismo nombre, incluye aquellas librerías en dichos lenguajes de programación usados en los componentes y servicios de Android, muchas de estas están realizadas en código abierto, aquellas librerías que aparecen en la foto superior son definidas para una mejor compresión.

Biblioteca	Descripción
WebKit	Proporciona un motor para las aplicaciones de tipo navegador y forma el núcleo del actual navegador incluido por defecto en la plataforma Android.
OpenMAX AL	Proporciona bibliotecas de streaming y la portabilidad de las aplicaciones
Libc	Incluye todas las cabeceras y funciones según el estándar del lenguaje C
Media Framework	Proporciona todos los códecs necesarios para el contenido multimedia soportado en Android
OpenGL ES	Representan las librerías gráficas de Android

Tabla 2. Bibliotecas Nativas de Android.

Android Runtime :
Se puede dividir en dos etapas dentro de la historia de Android, antes de la versión 5.0 Lollipop y después de dicha versión.

Versión	Información
Después de la versión 5.0 Lollipop	Cada app ejecuta sus propios procesos con sus propias instancias del tiempo de ejecución de Android (ART), este ART ejecuta varias máquinas virtuales en los dispositivos de memoria baja ejecutando archivos DEX.
Antes de la versión 5.0 Lollipop	Dalvik era el tiempo de ejecución del sistema operativo.

Tabla 3. Android Runtime.

Java API Framework:
Representa el conjunto de funciones del Sistema Operativo de Android que está disponible en la API diseñadas en Java, más concretamente son las bases de las creaciones de aplicaciones.
Se compone principalmente:

Función	Definición
Administrador de recursos	Brinda acceso a recursos sin código, como strings localizadas, gráficos y archivos de diseño
Administrador de notificaciones	Permite que todas las apps muestren alertas personalizadas en la barra de estado.
Administrador de actividad	Administra el ciclo de vida de las apps y proporciona una pila de retroceso de navegación común.
Proveedores de contenido	Permiten que las apps accedan a datos desde otras apps, como la app de Contactos, o compartan sus propios datos

Tabla 4. Componentes del Api de Java en Android.

System Apps:
Están formadas por todo el conjunto de aplicaciones instaladas en el dispositivo Android, tanto las de orígenes desconocidos, como las de tiendas oficiales (correo electrónico, juegos, redes sociales, Internet, contactos).
Todas estas aplicaciones utilizan los servicios, las API y librerías de los niveles anteriores.

3.1.6.Mecanismos de seguridad Android

En este apartado se define qué mecanismos tiene Android para todos los aspectos de seguridad que le concierne, para después, más adelante en el proyecto, en el Estado del Arte: Amenazas, definir los problemas y amenazas de este Sistema Operativo [12].

3.1.6.1. Seguridad en el kernel de Linux

En relación con la seguridad más básica de un dispositivo móvil, que es la propia de su sistema operativo, Android proporciona la seguridad del kernel de Linux, así como una facilidad de comunicación entre procesos (IPC) para permitir una comunicación segura entre las aplicaciones que se ejecutan en diferentes procesos, un modelo de permisos basado en el usuario con un aislamiento entre procesos que otorga una capacidad de poder eliminar las partes innecesarias e inseguras del kernel.

3.1.6.2. Partición del Sistema y el modo seguro

La partición del sistema contiene el kernel de Android, las bibliotecas del sistema, el tiempo de ejecución de aplicaciones, infraestructura de aplicaciones y las propias aplicaciones, esta partición tiene la peculiaridad de establecerse en modo lectura. Por lo tanto, cuando un usuario accede al dispositivo en modo seguro las aplicaciones de “terceros” o descargadas por el usuario no son ejecutadas al estar en otra partición distinta, pero, aun así, el usuario tiene la posibilidad de ejecutar la aplicación si desea manualmente.

3.1.6.3. Cifrado del sistema de archivos

El cifrado es un proceso de codificación de todos los datos de usuario en un dispositivo Android usando claves de cifrado simétrico. Una vez que se encripta un dispositivo, todos los datos creados por el usuario se cifran de forma automática antes de comprometerse en el disco, si se necesita realizar un proceso de lectura de datos, se encarga de descifrar automáticamente los datos y los vuelve a encriptar una vez concluido el proceso. Gracias a la encriptación de datos que se produzca en un dispositivo móvil, asegura un aumento de seguridad dado que si terceras personas, o aplicaciones indebidas intentan acceder a los datos de usuario y consiguen llegar a ellos, no van a poder leerlos dado que lo que van a sacar son símbolos y números sin lógica.

Android dispone de dos métodos de cifrado:

- Cifrado de disco completo: el cual está disponible a partir de Android 5.0 Lollipop, en el cual se protegen todos los datos del usuario a través de la encriptación, pero el usuario puede acceder a sus datos a través de

credenciales (una contraseña) facilitadas por él mismo antes de realizar el cifrado, esto significa que los datos del usuario no son totalmente inmediatos, sino que dependen de su acceso por credencial de usuario.

- Cifrado de archivos: Android 3.0 y posteriores Es parecido al cifrado de disco completo, su diferencia principal es la capacidad de cifrar distintos tipos de datos con distintas contraseñas o credenciales por parte del usuario.

Cómo funciona este cifrado de datos:

El cifrado de Android completo como de archivos se basa en un cifrado dm-crypt, una nueva infraestructura del núcleo Linux 2.6 que provee cifrado de dispositivos de bloque, donde las escrituras a este dispositivo (por ejemplo de datos) serán cifradas y las lectura de estos datos descifradas, se trata de un sistema de archivos similar al sistemas pre-encriptación pero con la característica de no poder acceder a los datos sin clave, esta clave se cifra con 128 bit AES a través de llamadas a la librería OpenSSL.

Como problema encontrado a la hora de implementar la encriptación a través del núcleo de Linux, se encontraba en la acción de obtener la contraseña del usuario en el arranque del sistema, como solución se tomó crear una interfaz que apareciese a la hora de arrancar el sistema pidiendo la contraseña, obtener la contraseña y verificar que es la correcta y a continuación de esta acción ejecutar el marco de arranque inicial, otra parte negativa del cifrado suele ser una bajada en el rendimiento del dispositivo de un 10% en los dispositivos de baja-media gama.

3.1.6.4. Protección de contraseñas

Android puede ser configurado para verificar una contraseña proporcionada por el usuario antes de proporcionar acceso a un dispositivo, esto se traduce en el típico bloqueo de pantalla que configura el usuario al obtener su dispositivo, en la mayoría de dispositivos, se encuentra en Opciones > Seguridad > Bloqueo de pantalla. Existen distintos tipos de bloqueos de pantalla que se han ido implementando a través de las versiones de Android, con la versión más actual de Android 7.0 Nougat, se encuentran estos tipos de bloqueos de pantalla:

- Ninguno: Si no quieres configurar una pantalla bloqueada, selecciona "Ninguno". Esta opción no brinda protección, pero te permite acceder a tu pantalla principal rápidamente.
- Deslizar: La opción "Deslizar" te permite deslizar el dedo por la pantalla para desbloquear tu dispositivo. Esta opción no brinda protección, pero te permite acceder a la pantalla principal rápidamente.
- Patrón: La opción "Patrón" te permite trazar un patrón simple con el dedo para desbloquear tu dispositivo.
- PIN: La opción "PIN" requiere al menos cuatro números. Los PIN más largos suelen ser más seguros.

- Contraseña: La "Contraseña" requiere al menos cuatro letras o números. Esta es la opción más segura, siempre que crees una contraseña fuerte.

Imagen 4. Distintos bloqueos de Pantalla en Android.

3.1.6.5. Administración de dispositivos

Un punto importante en el proyecto dado que afecta directamente a la seguridad que se trata más adelante, desde la versión 2.2 de Android, se crea una nueva API de administración de dispositivos en la cual se proporciona funciones de administración de dispositivos en un nivel de sistemas, permitiendo crear aplicaciones de seguridad que son útiles, sobre todo para empresas que manejan distintos dispositivos de este sistema operativo y tienen la intención de capar ciertos parámetros que no cumplen con los credenciales de la empresa, es un punto importante como nombre anteriormente dado que sincronizar archivos a servidores compartidos de la empresa a través de la sincronización trae consigo lacras de seguridad como ransomware dados en mayo de 2017.

3.1.7.Seguridad en las aplicaciones

En este apartado dentro de los mecanismos de seguridad, se basa en el entorno relacionado con las aplicaciones, a grandes rasgos, entre los permisos que obtienen, para entender el contexto de las aplicaciones voy a describir a grandes rasgos cómo están desarrolladas [11].

Las aplicaciones son desarrolladas de forma habitual en un entorno de lenguaje de programación Java (donde se tiene que tener mayor conocimiento para un desarrollo efectivo de las aplicaciones) mezclado con Android Software Development Kit (Android SDK), pero además Android incluye para gente inexperta en el mundo de desarrollo de aplicaciones Google App Inventor con un entorno visual más sencillo. Una vez creada la aplicación, esta está “guardada” en un fichero con una extensión. APK para que el dispositivo lo reconozca como una aplicación a instalar, es similar con los ordenadores con sistema operativo de Windows y los programas con extensión .EXE.
Para subir las aplicaciones a esta tienda, hay que tener una cuenta de Google y aceptar una serie de condiciones que son ajenas a este proyecto

3.1.7.1. El modo SandBox

El sistema Android asigna un ID de usuario único (UID) a cada aplicación de Android y lo ejecuta como un proceso independiente, esto configura un modo SandBox, un modo seguro en a nivel de aplicaciones de kernel, en el cual, el kernel refuerza la seguridad entre las aplicaciones de tal forma que las aplicaciones no puedan interactuar entre ellas y tengan un acceso limitado al sistema, por lo cual si una aplicación de Gestión de Carpetas quiere acceder a leer los datos de una aplicación de Redes sociales, el sistema operativo de Android protege esta acción dado que la aplicación de Gestión no tiene los privilegios adecuados.

3.1.7.2. Permisos en las aplicaciones

Para la seguridad del Sistema Operativo Android y la seguridad de los usuarios; Android requiere que las aplicaciones soliciten permiso antes de que las aplicaciones puedan utilizar ciertos datos y funciones del sistema. Dependiendo de cómo sea la sensibilidad de esa área en términos de seguridad, el sistema puede dar a las aplicaciones permisos automáticamente o requerir que el usuario apruebe ciertos permisos para la aplicación.

- **Permisos normales**

Aquellos permisos que cubren áreas en las que su aplicación necesita acceder a datos o recursos fuera del entorno limitado de la aplicación (de su sandbox), pero donde hay poco riesgo para la privacidad del usuario o el funcionamiento de otras aplicaciones. Distintos ejemplos de este tipo de permisos son: Ajustar/editar el

volumen del terminal, alarma, vibración.

- **Permisos con riesgo**

Cubren áreas en las que la aplicación solicita datos o recursos que implican la información privada del usuario, o podrían afectar a los datos almacenados por el usuario o el funcionamiento de otras aplicaciones. Un ejemplo de estos permisos peligrosos puede ser la capacidad de leer los contactos que tenga el usuario en el dispositivo móvil.

3.1.7.3. Firma y verificación de aplicaciones.

Otro mecanismo de seguridad que tienen las aplicaciones Android se basa en conocer qué usuario fue el encargado de subir una aplicación a través de su firma (ID único que tiene), a través de este ID se puede conocer su firma y sus datos por lo cual aquellas aplicaciones que no tengan la firma de su desarrollador, son rechazadas por Google Play o el instalador de Android, en caso de estar permitido en el dispositivo móvil el poder instalar aplicaciones de fuentes desconocidas, sabiendo de quién es la aplicaciones, Android dispone de distintos esquemas para poder “procesar la aplicación” a través de sus firmas.

Android soporta dos tipos de esquemas de firma de aplicaciones:

- Versión V1 (pre versión Android 7.0) esta versión de firma de aplicaciones no llega a cubrir algunas partes de las APK (aplicaciones) como el metadata, esta firma necesita procesar muchas estructuras de datos no confiables, además de descomprimir todas las entradas comprimidas (rectángulo en azul claro), consumiendo así más tiempo y memoria.
- Para solucionar el consumo de tiempo y de memoria en Android lanza la Versión V2, un esquema de firma que aumenta la velocidad de verificación y fortalece garantías de integridad mediante la detección de cualquier cambio en las partes protegidas de la APK. La diferencia entre las dos versiones, como se aprecia a simple vista es: APK Singing Block; donde las firmas v2 y la información de identidad del firmante se almacenan en dicho bloque.

Imagen 5. Firma de aplicaciones Android.

La verificación de aplicaciones se da en Android a partir de la versión 4.2, se define como una opción que tiene el dispositivo móvil llamada: “Verificar aplicaciones”, en la cual todas las aplicaciones son evaluadas por un sistema verificador de las mismas, esta opción avisa al usuario si una aplicación es perjudicial para él, o en casos extremos, si el verificador conoce que la aplicación es maligna puede bloquear la instalación.

3.1.7.4. Seguridad sobre el acceso a la tarjeta SIM del usuario.

Android dispone de mecanismos seguridad para que ninguna aplicación de terceros acceda a la tarjeta SIM y además a los datos personales del usuario, el sistema operativo, es el único encargado de acceder a la tarjeta SIM.

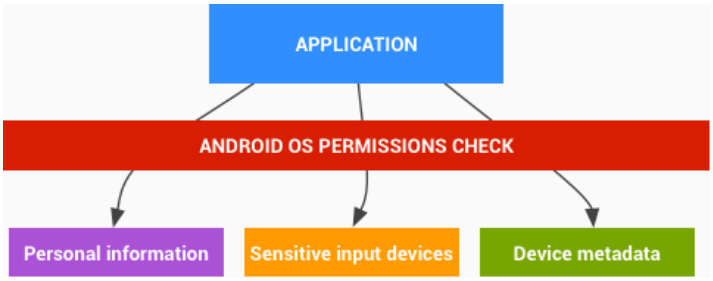


Imagen 6. El acceso a datos sólo está disponible a través de API protegidas.

Además, con la evolución de los pagos a través de Internet y de pagos a través de dispositivos móviles en devaluación del pago en efectivo; Android ha desarrollado una API que es sensible a aquellas aplicaciones que puedan generar un coste al usuario o a su red, en esta API, se incluyen los siguientes parámetros protegidos por el Sistema Operativo: Telefonía, SMS/MMS, Red/Datos, NFC.

Además de desarrollar esta API, recientemente (versión 4.2 Android) incluyeron un permiso dentro de ella en la cual, en caso de generarse un coste adicional para usuario, la API mande un SMS al teléfono del usuario con el cargo hecho y de qué aplicación proviene.

3.1.8.Actualizaciones de Seguridad.

Gracias al desarrollo de conexiones inalámbricas en los últimos años, las actualizaciones de seguridad que reciben los dispositivos móviles suelen ser actualizaciones OTA; Over The Air (Por El Aire), se trata de una actualización de software la cual el dispositivo informa de que hay una actualización disponible a través de una notificaciones en el mismo, este tipo de actualizaciones suelen ser lanzadas por los fabricantes del dispositivo (Samsung) o por el Sistema Operativo (Android) y necesitan cumplir una serie de requisitos tales como:

- El dispositivo debe de estar conectado a una red wifi dado que estas actualizaciones suelen ser de una gran capacidad lo que asegura a los usuarios no tener un coste adicional al utilizar otros métodos de conexión de red como puede ser el uso de datos del operador.
- Tener un nivel de carga de batería mínima del 70% (varía según el dispositivo del 50% al 90%) y mantener al dispositivo conectado a una corriente de carga, estas medidas de seguridad proceden dado que, si el dispositivo se queda en estado de “congelación” en el momento en el que se produce una actualización de software, existen altas posibilidades de que quede inservible.

Imagen 7. Ejemplo de una actualización OTA.

3.1.9. Modo Recovery

El modo Recovery es una partición del Sistema Operativo independiente del sistema, pero con propiedades de arranque por lo que si el sistema de Android no arranca y no responde se puede acceder a este modo de recuperación para intentar recuperar el dispositivo, para acceder a este modo hay que tener el dispositivo apagado y dependiendo del fabricante del dispositivo hay que realizar una serie de combinaciones (botones de sonido, home…), en caso de no poder entrar a través de las combinaciones de teclas, también hay la posibilidad de entrar a este modo con un ordenador.

Las funciones principales del modo Recovery engloban:

- Actualizaciones del dispositivo software a través de OTA, lo cual devuelve al dispositivo a la versión de Android que venía por defecto en el dispositivo.
- Reajustar y reiniciar el dispositivo a modo de fábrica en el cual se borran todos los datos del usuario
- Wipe cache partition lo cual permite eliminar la caché del dispositivo y liberar espacio de memoria que se ha ido ocupando con los archivos basura con el uso del dispositivo
- Ejecutar herramientas externas

Por otro lado, existen dos tipos de modo Recovery:

- Stock: Proviene de del fabricante del dispositivo móvil, en el cual el fabricante ofrece un mínimo de posibilidades para poder recuperar el sistema Android por lo que suele tener una serie de opciones más limitadas que los custom.
- Custom: Desarrollados por la comunidad de Android para tener una serie de opciones más avanzadas en la instalación de Roms o Root, al ser desarrolladas por la comunidad, no a todos los dispositivos les llega este tipo de modo Recovery.

3.1.10. Rooteo

Una vez mencionado los aspectos de seguridad de Android y posteriormente, las amenazas que hay en este Sistema Operativo diseñado por Linux, hay que mencionar un aspecto particular de los dispositivos móviles de Android; root

Una definición simple de root podría abarcar la acción por la cual se obtiene un control absoluto por parte del dispositivo (permisos), obtener privilegios de superusuario o de administrador en el dispositivo, como Android está basado en Linux, las aplicaciones del dispositivo móvil suelen estar limitadas a una serie de permisos que da a cada aplicación los recursos que necesitas y son necesarios para su funcionamiento [13].

Por lo tanto, la diferencia entre un dispositivo que ha sido rooteado a uno que no, es simplemente lo que he nombrado en la parte superior; conseguir un control total sobre el dispositivo a través de los privilegios de superusuario, por lo tanto, se abre un nuevo camino hacia la posibilidad de cambiar/editar todo lo que el usuario desee del terminal, entre las acciones más típicas de los usuarios root se encuentra:

- Eliminar aplicaciones del sistema que vienen impuestas por el fabricante o por la propia compañía de teléfono.
- Modificar la configuración de elementos de hardware, como la CPU, el chip del GPS, la GPU...
- Instalar un firewall que por ejemplo nos permita la conexión a Internet de alguna aplicación en concreto
- Hibernar cualquier aplicación para que no trabaje en segundo plano consumiendo recursos
- Actualizar o cambiar nuestro sistema operativo. Con los permisos root podremos cambiar nuestro sistema operativo instalando cualquier ROM que sea compatible con nuestro dispositivo
- Quita restricciones impuestas por la compañía telefónica o del fabricante.

Sobre las ventajas y desventajas que tiene un dispositivo root o no root, realmente depende de la función que haga cada usuario con su dispositivo al tener la capacidad de instalar aplicaciones especiales o “root”, realizar un root para no instalar aplicaciones root y dejar el dispositivo igual, es una pérdida de seguridad en vano, en relación con que pueden hacer las aplicaciones root comparándolas con las aplicaciones de las “tiendas oficiales de Android”:

- Reducir el consumo de batería: como he nombrado en la parte superior, eliminar procesos en segundo plano, o eliminar ciertas características del sistema operativo que el usuario no utiliza y consume recursos de la batería
- Tener la posibilidad de un menú de reinicio avanzado, dado que una cantidad importante de terminales móviles, no cuentan con un menú de reinicio y la

posibilidad de realizarlo, se centran meramente en hacer que el usuario encienda y apague su terminal para simular el “reinicio”.

- Explorador de archivos internos del sistema, para poder ver todos los archivos que se guarda en las “entrañas “de nuestro Sistema Operativo de Android
- Cambiar la famosa “bootanimation” cambiar la imagen que da el fabricante del dispositivo móvil a la hora de encenderlo, como ejemplo: el logo de Samsung en sus dispositivos.
- Limpieza de memorias externas de manera completa, al poder ver todos los archivos que contiene, incluidos los ocultos en los que en ocasiones son maliciosos al ocupar un espacio de memoria que no se puede borrar sin ser usuario root.
- Restringir el acceso de permisos de ciertas aplicaciones, por ejemplo, en aplicaciones de redes sociales que acceden a los contactos de nuestro teléfono, podemos eliminar esta restricción a nuestro gusto.

3.1.10.1. Amenazas de realizar un root a un dispositivo móvil

Toda ventaja, descritas arriba, sobre lo que puede realizar un root, también tiene su parte inconvenientes, en este caso realizar un root afecta a la seguridad del dispositivo de tal forma que implica una serie de riesgos, entre ellos está la garantía con el fabricante del dispositivo dado que se pierde.

Otro problema común es el “brick” es el estado en el que el teléfono se queda inutilizado y deja de funcionar al tener problemas al instalar una room al dispositivo realizando el rooteo. Como he descrito antes, el estado de root permite editar, quitar y añadir privilegios a las aplicaciones, en este caso y sin el conocimiento oportuno de las aplicaciones dotarlas de más privilegios de los que necesitas llevan consigo una falta en la seguridad y robo de información/datos del usuario del dispositivo móvil, un ejemplo claro, es una aplicación que tenga un virus y le demos permisos extras, está en si ya es peligrosa, pero con más permisos puede acceder a las capas más internas del dispositivo de una forma más rápida y eficiente

3.1.10.2. El root en la actualidad (2017)

El uso del root se popularizó desde 2011 hasta 2016 dado que muchos de los terminales móviles se quedaban obsoletos de memoria a los pocos meses de ser comprados, llegando a realizar un root que diese al dispositivo más memoria, dado que se produce el borrado de aplicaciones preinstaladas, más velocidad al limitar las aplicaciones de segundo plano y más duración de batería.

Desde 2016 hasta la actualidad el root ha ido en decadencia por la propia evolución del sistema operativo Android, dado que ciertas aplicaciones de Android siguen desarrollándose llegando a obtener los mismos resultados que las aplicaciones de root anteriormente descritas. De forma más actual y con el lanzamiento de Samsung

Pay, (posibilidad de pagar con el teléfono móvil, similar a una tarjeta bancaria con acceso Pay Wifi) Samsung ha limitado el uso de esta función a los usuarios que no hayan realizado un proceso de root en su dispositivo por seguridad para el usuario dado que se trata de información y uso de dinero por parte del terminal.

Aplicaciones de gran peso e interés por la comunidad de Internet como es el caso de Netflix, (empresa comercial estadounidense de entretenimiento) la cual ha bloqueado su aplicación a los usuarios con Android root o no certificados por Google, llegando a “obligar” al usuario que tiene que realizar un pago mensual por los servicios de la aplicación a tener un dispositivo seguro para poder visualizar el contenido.

El futuro del root, cada vez está más en declive, una noticia por parte de Google a fecha de 17/mayo/2017, indica que Google no va a permitir la descarga de aplicaciones de su tienda Google Play a aquellos usuarios con acceso a root, por lo tanto, se quedarían sin la mayoría de las aplicaciones del mercado si su terminal cumple alguno de estos tres requisitos:

- Personas que tengan rooteados el móvil.
- Personas con ROM personalizada.
- Personas que tengan el móvil con versiones no certificadas por Google.

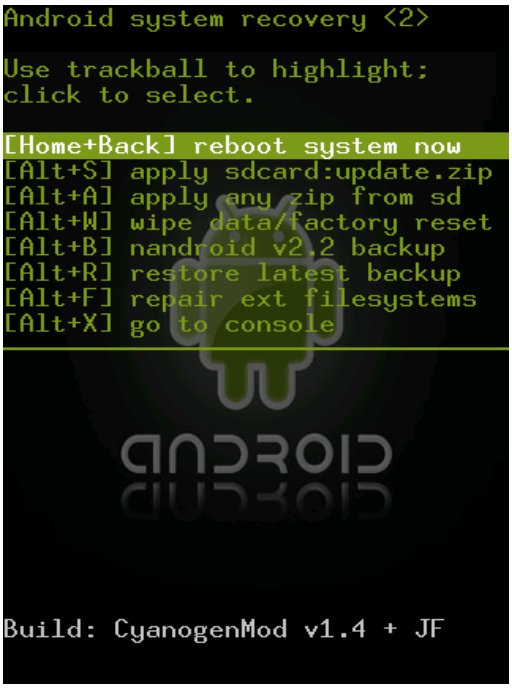


Imagen 8. Imagen del menú root de Android.

3.2. Estado del Arte: Amenazas

3.2.1. ¿Qué es un malware?

Malware o software malicioso, (soporte lógico de un sistema informático) que se define como un término o contexto que engloba a todo código informático o programa (software [15]) malicioso, cuya finalidad a la hora de su creación fue dañar total o parcialmente un sistema informático, con objetivos principal monetarios y de sustracción de privacidad con la peculiaridad de acceder al sistema informático de una forma inadvertida, sin conocimiento del usuario ([14] y [16]).
Existe una gran cantidad de malware en el contexto temporal en el que nos encontramos, los cuales son nombrados y definidos de una manera adecuada en apartados posteriores.

Definiendo el contexto histórico en el cual se desarrolló el malware, anteriormente a 1990, fue conocido como virus informático (en gran parte acogido a que no existían dispositivos tales como móviles, tabletas y similares antes de ese año y se producían y se extendían para ordenadores), el primer virus en el entorno informático fue dado en 1972, llamado enredadera (creeper), se trataba de un virus que mandaba un mensaje a la pantalla “atrápame si puedes”, el cual para eliminarlo se creó otro virus (segadora) que se basaba en encontrarlo por los archivos, a partir de este punto, el desarrollo de virus se disparó cada año más como se muestra en puntos posteriores.
En relación con los dispositivos móviles el primer virus que se dio fue en el Sistema Operativo: Symbian con el virus llamado cabir/caribe en el año 2004, en referencia al proyecto y al Sistema que engloba, el primer virus de Android fue Trojan-SMS.AndriodOS.FakePlayer.a y se dio en: 2010, el cual se encargaba de enviar mensajes a servicios de pago como su principal función. [17 y 19].

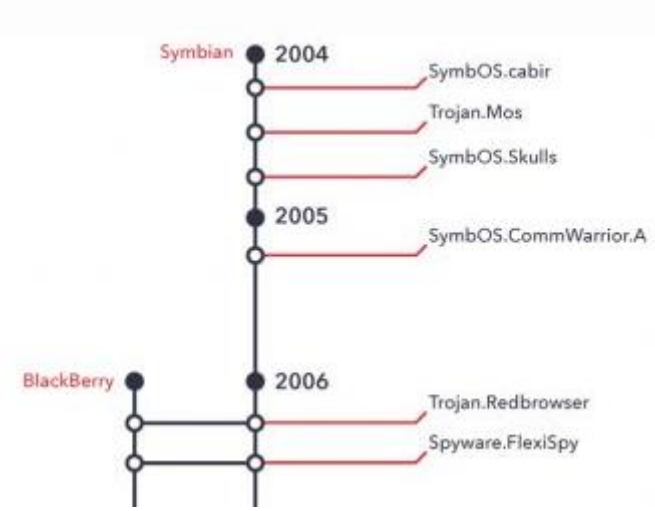


Imagen 9. Primeros malwares dados en Symbian y BlackBerry.

3.2.2.Características básicas del malware

Al existir muchos tipos de malware con sus características especiales, es difícil agruparlas en un solo punto, pero entre todos los tipos que existen, comparten una semejanza en ciertos puntos, los cuales se van a nombrar a continuación:

Característica	Definición
Tamaño	Los tamaños del código de los virus son muy pequeños
Versatilidad	Capacidad para atacar genéricamente a distintos sistemas
Propagación	Una vez afectado un programa, se puede propagar a los demás
Eficacia	Desde reiniciar un dispositivo a pérdida total de archivos y sistema
Funcionalidad	Distintas funciones que tiene según el virus (ver más adelante)
Persistencia	Dificultad de eliminar un virus en una red comparado con local

Tabla 5. Características del Malware.

3.2.3.Tipos de malware

En este apartado se describe todo tipo de malware existentes en los dispositivos móviles en el Sistema Operativo Android y sus funcionalidades [14].

→Backdoor.
Lo pongo en primer lugar por que engloba a todos los tipos del malware, debido a que es “una puerta trasera” que accede al dispositivo que es potencialmente perjudicial para el mismo el cual permite ejecutar operaciones de cualquier tipo de malware.

→Spyware.
Se define, como cualquier aplicación que transmita información confidencial del dispositivo sin el consentimiento del usuario y no muestra una notificación o información de que esto está sucediendo en el dispositivo.

→Recolección de datos.
Cualquier aplicación que recopile al menos una de las siguientes sin el consentimiento del usuario:

- Información sobre aplicaciones instaladas.
- Información sobre cuentas de terceros.
- Nombres de archivos en el dispositivo.

→Negación de servicios.
Ejecución de un ataque de denegación de servicio o que es parte de un ataque de denegación de servicio distribuido contra otros sistemas y recursos.

→Downloader malware.
Se trata de una aplicación que no es dañina, actúa como un gestor de descarga de aplicaciones que ofrece aplicaciones exclusivas las cuales si son dañinas.

→Fraude basado en la facturación telefónica
Aplicación que se encarga de aplicar un coste adicional monetario al usuario de una manera engañosa.

→Fraude por SMS
Aplicación que obliga a los usuarios a enviar SMS Premium sin consentimiento, o intenta ocultar las actividades de las notificaciones de SMS donde el operador móvil informa al usuario de los cargos o cuando se ha confirmado la suscripción.

→Llamada fraudulenta.
Al igual que los SMS, pero con las llamadas, donde se llama a teléfonos Premium sin consentimiento del usuario

→Suplantación de identidad o Phishing.
El phishing consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.

→Suplantación de privilegios.
Una aplicación que compromete la integridad del sistema al saltarse el SandBox de una aplicación o al cambiar o deshabilitar el acceso a las funciones principales relacionadas con la seguridad.

→Ramsonware.
Es un código malicioso que cifra la información del dispositivo e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

→Spam.
Se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero con el objetivo de obtener información, Phishing por correo electrónico.

→Adware.
El adware es un software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario.

→Gusano.
El gusano intenta obtener las direcciones de otros ordenadores mediante tus listas

de contactos para enviarles sus copias y tratar de infectarlos también.

→Keylogger.
Es aquel malware encargado de registrar todo lo que el usuario teclea en la pantalla del dispositivo y también en el teclado que se incluye en la misma, obtenido información de sitios Webs, como usuarios y/o contraseñas en el que al concluir la infección manda un correo electrónico al distribuidor de este malware con los datos.

→Troyano.
Un troyano trata de pasar desadvertido para acceder al dispositivo con la intención de ejecutar acciones ocultas con las de abrir una puerta trasera para que otros programas maliciosos puedan acceder a él.

3.2.4.Malwares con más impacto en la historia de los móviles

Malware/s	Descripción	Año
Cabir	Malware para Symbian, de tipo gusano, trasmitido por bluetooth.	2004
Drever	Primer antivirus falso, eliminaba otros antivirus para no ser detectado.	2005
CommWarrior	Afectaba al envió de MMS a través de bluetooth.	2005
Xrove	Virus que se trasmitía desde Windows Pc a Windows Mobile.	2006
RedBroswer	Primer troyano multiplataforma para móviles con Java Micro Edition 2.	2006
FlexiSpy	De los primeros Software espía consolidados.	2007
Meiti	Malware que roba datos a través de una interfaz de videojuegos.	2008
InfoJack	Troyano que infectó a Windows Mobile cuando se conectaba a Internet.	2008
Ikee	Primer malware diseñado para IPhone, cambiaba la apariencia del dispositivo.	2009
Zitmo	Malware de robo de datos bancarios de tipo troyano.	2010
Wallpapers	Una vez instalados como tal, robaba datos del teléfono y SIM.	2010
DroidDream	Troyano introducido en Google Play con aspecto de juego inofensivo.	2011
Broxer	Primer troyano de Android que infectaba a través de SMS.	2012
KongFu	A través del famoso juego Angry Birds, se creó una copia que obtenía datos.	2012
FakeDefender	Primer ejemplo de ramsonware que encripta los datos de un terminal.	2013
MasterKey	Aplicaciones maliciosas que pasaban como aplicaciones de fabricantes.	2013
Koler	El famoso ramsonware que encripta los datos a través de una cara policial.	2014
Simplocker	Ramsonware que encriptaba la tarjeta SD del teléfono móvil.	2014
Gazon	Pishing a través de SMS que regala tarjetas de Amazon en un link.	2015
SMS Thief	Robo de almacenamiento de mensajes que permite reenviar mensajes y llamar	2016

[20]

Tabla 6. Historia de ataques malware.

3.2.5.Anexo de familias de malware

Familia del malware, puede definirse como el cambio, mutación, diferenciación del código original que se ejecuta de un malware que está creado y funciona, de esta manera una familia de malware se compone de las diversas variables que se produzcan del malware original.
Una vez definido los malware que existen y cuales han tenido más impacto en la sociedad telefónica desde su inicio, me parece interesante mostrar a modo de tabla informativa en un anexo todas las familias de malware y variantes que existen con unos datos de 2016, este anexo cuenta con 10 páginas, con una información importante para el lector que desee introducirse de una manera más amplia en el mundo de las familias del malware, pero que extendería demasiado y perdería motivación por parte de los lectores que no desee tanta información, por este motivo; se incluye esta tabla en el Anexo 1: Familias del Malware y tipología.

3.2.6.Actualidad

A través de la obtención de un conocimiento cognitivo sobre el malware previamente descrito en el apartado 1: Definición del malware, pasando por su historia, tipos de malware conocidos y todas sus variantes englobadas en sus familias.
Hay que enmarcar más exhaustivamente con datos reales la cantidad de datos que hay sobre los malware y que nos afectan, por este motivo se muestra información detallada del malware a finales del año 2016 donde se obtienen todos los datos del año y parte de los datos de 2017 que ya se han podido obtener.
Con el objetivo de poder enmarcar en que afectan los datos de los malware a la sincronización de Android.

3.2.7.Estadísticas actuales

En relación con ataques detectados en el año 2016, desde principios a finales, se habla de una cifra cercana a los 65.000.000 de ataques por parte de malware a los dispositivos móviles, de los cuales, 19.200.000 (en 2015 se dieron 10,7millones) se trataban de aplicaciones maliciosas para los dispositivos que ya estaban creadas y se instalaban por tiendas oficiales y no oficiales de los dispositivos móviles [21].
Como datos que llaman la atención, recalcar los malware de tipo: Ramsonware (encriptación de datos) que crecieron en torno a un 8,5 veces más que el año anterior con 260.000 detenciones de este tipo de malware los cuales piden un rescate por liberar los datos [22].

Un dato que me ha llamado bastante la atención es el porcentaje de aplicaciones malwares que se instalan en los dispositivos Android el cual en pocos casos superan el 1,5%, en el grafico que muestro a continuación, se divide en dos, aquellos dispositivos que solo instalan aplicaciones por Google Play (azul) y los dispositivos que instalan aplicaciones por Google Play y demás tiendas no oficiales y oficiales de otros desarrolladores [23].

- Por un lado, se encuentra la diferencia básica en la cual Google Play tiene una seguridad mayor en comparación dado que en ningún caso supera el 0,20% mucho más inferior que el 1,58 de máxima por la otra parte

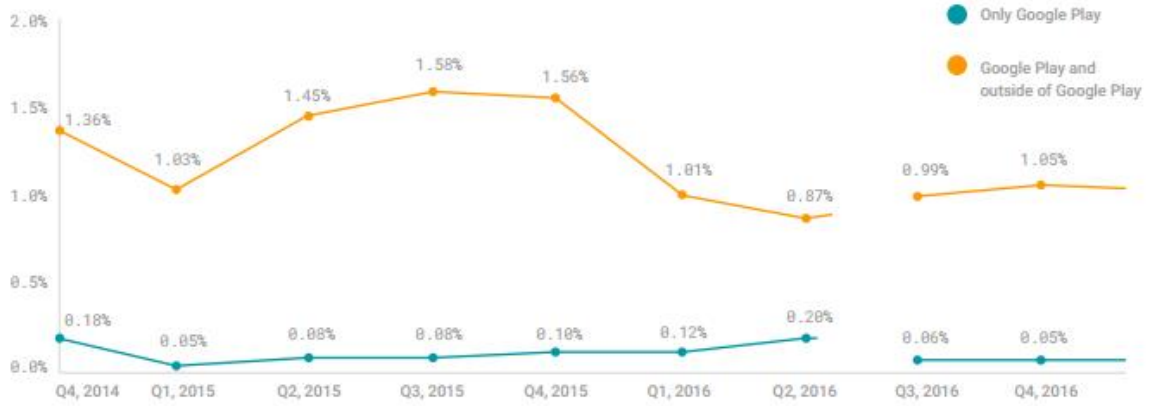


Imagen 10. Aplicaciones maliciosas.

(https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf)

- El punto que más me ha llamado la atención es que los fabricantes de dispositivos y Android informan de los avances producidos en su seguridad contra el malware, en muchos casos avanzando por la imagen de arriba en un orden temporal, podemos ver diferencias de aumento de aplicaciones maliciosas instaladas, por ejemplo, comparando desde Q3 de 2015 hasta el Q2 de 2016, donde subieron.
  Es interesante debido a que hay un tira y afloja entre actualizaciones de seguridad y nuevas familias de malware, donde se ve una tendencia a favor por parte de los malwares que siempre intentan romper las nuevas barreras creadas y las actualizaciones van por detrás intentando eliminar los malwares nuevos y no prevenir que aparezcan

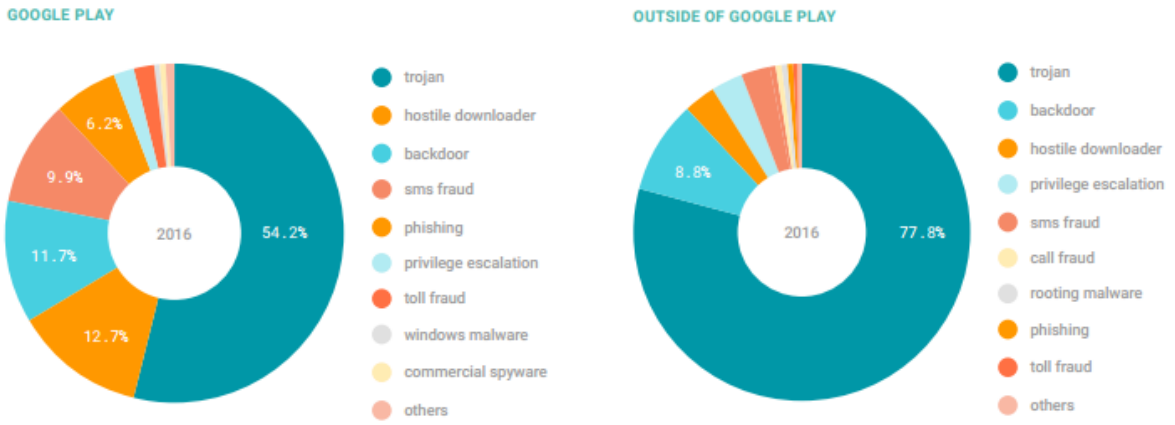


Imagen 11. Malwares más comunes en la tienda Android.

Como apunte y peculiaridad informar de que las posibilidades de 0,2 por parte de las aplicaciones de Google Play tengan algún malware tiene un 54% de ser troyano, 12% de descargador de aplicaciones y un 11% una puerta trasera.
Comparándolo con tiendas fuera de Google Play aumentan los troyanos hasta un 77% y los demás mitigan su proporción.

3.2.8.¿Qué malwares son más comunes?

En este apartado se informa de una manera rápida cuales son los malwares que más probabilidad tienen de afianzarse en los dispositivos móviles, atendiendo a la siguiente tabla, en la cual si se otorgase la posibilidad de que un malware se instalase en nuestro dispositivo podrá ser de mayor a menor probabilidad del tipo:

	Name	% of attacked users *
1	DangerousObject.Multi.Generic	70.09
2	Trojan.AndroidOS.Hiddad.an	9.35
3	Trojan.AndroidOS.Boogr.gsh	4.51
4	Backdoor.AndroidOS.Ztorg.c	4.18
5	Trojan.AndroidOS.Sivu.c	4.00
6	Backdoor.AndroidOS.Ztorg.a	3.98
7	Trojan.AndroidOS.Hiddad.v	3.89
8	Trojan-Dropper.AndroidOS.Hqwar.i	3.83
9	Trojan.AndroidOS.Hiddad.pac	2.98
10	Trojan.AndroidOS.Triada.pac	2.90
11	Trojan.AndroidOS.Iop.c	2.60
12	Trojan-Banker.AndroidOS.Svpeng.q	2.49
13	Trojan.AndroidOS.Ztorg.ag	2.34
14	Trojan.AndroidOS.Ztorg.aa	2.03
15	Trojan.AndroidOS.Agent.eb	1.81
16	Trojan.AndroidOS.Agent.bw	1.79
17	Trojan.AndroidOS.Loki.d	1,76
18	Trojan.AndroidOS.Ztorg.ak	1.67
19	Trojan-Downloader.AndroidOS.Agent.bf	1.59
20	Trojan-Dropper.AndroidOS.Agent.cv	1.54

Imagen 12. Malwares en la actualidad.

Para explicar más detalladamente estos datos, el primer tipo de malware con un 70.09% DangerousObject.Multi.Generic son aquellos programas maliciosos que provienen de la nube, de Internet.
Como precedente y con un porcentaje cercano al 10% Trojan.AndroidOS.Hiddad.an es un malware encargado de copiar juegos de gran renombre e imitarlos con el fin de introducir una agresión de anuncios que generen dinero al clickear por parte del usuario. En orden más general, se puede apreciar sobre todo troyanos en su gran cantidad y como excepciones “backdoor” o puertas traseras.

3.2.9.¿Dónde se dan los malwares en el mundo?

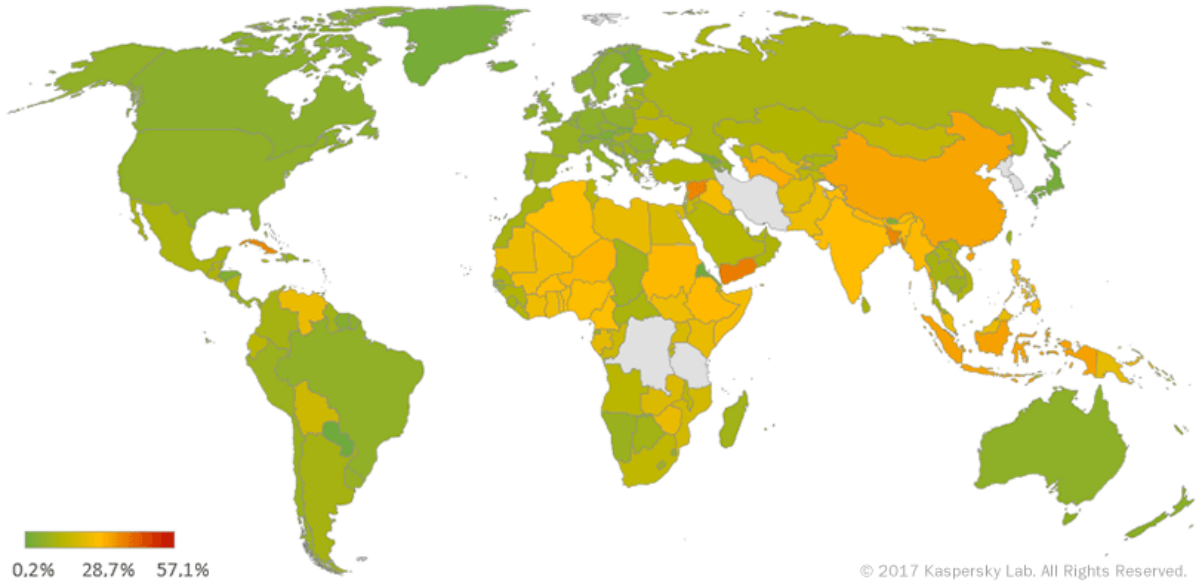


Imagen 13. Malware en el mundo.

En la Figura 13 se muestra el porcentaje de los países en los cuales se ha dado el caso de un usuario afectado por malware, entre aquellos países más afectados y conocidos se encuentran:

Irán fue el país con el mayor porcentaje de usuarios atacados por malware móvil con un 47.35%. Bangladesh se quedó en segundo lugar: 36.25% seguido por Indonesia y China con una proporción de ambos países fue ligeramente superior al 32%.
En relación con países conocidos: Rusia (11,6%) se encuentra en el puesto número 40º de la clasificación, Francia (8,1%) 57 º, los EE.UU. (6,9%) en el puesto 69, Italia (7,1%) en el puesto 66, Alemania (6,2%) con el puesto 72 y Reino Unido (5,8%) en la 75º posición.
Los países más seguros fueron Finlandia (2,7%), Georgia (2,5%) y Japón (1,5%).

3.2.10. Internet of things, ¿siguiente objeto de malware?

Que se entiende por Internet de las cosas, se entiende como cualquier objeto o gadget que tiene una interconexión a Internet, en este cuadro, podemos enfocar, dispositivos móviles, tabletas, smartwatch, pulseras inteligentes, televisores inteligentes, drones, automóviles, una gran cantidad de objetos que cada vez añaden más a su familia [24].

Es interesante poder aportar una pequeña introducción de IOT (Internet of things), debido a que se abre un nuevo marco para los malwares a la hora de sincronizar estos objetos con los dispositivos que llevamos siempre con nosotros; los dispositivos móviles.

4. Análisis de los problemas en la sincronización

Una vez investigado y definido el entorno en el cual se va a basar el proyecto, logramos desarrollar una reflexión la cual podemos adaptar al marco teórico previamente descrito a una serie de situaciones prácticas, este capítulo se va a dividir en cuatro subapartados, los cuales van a ser introducidos para conseguir una idea general de ellos y más adelante, desarrollados de una forma más completa.

- ¿Qué se entiende por sincronización?
  Una definición clara de que es la sincronización y de lo que entiendo por ella, aclarando de una forma visual como actúa con los dispositivos.

- Historia
  Repaso rápido sobre cómo se han producido problemas en la sincronización en los equipos informáticos.

- Transmisión de la sincronización
  Qué canales o vías existen para la trasmisión de malware en la sincronización.

- Público objetivo para los malwares
  Según las características del usuario puede ser un objetivo más específico para una amenaza de malware concreta.

4.1. ¿Qué se entiende por sincronización?

La sincronización nos permite tener de una forma automática, elementos como los contactos, el calendario o ciertas aplicaciones, permitiendo que la información que provenga de estas quede integrada en nuestro teléfono Android [25].

Esta definición es originaria de Internet, dado que es interesante saber el concepto que entiende la mayoría de las personas por sincronización y más aún, remarcar que tipos de ventajas sin ser analizadas se nombran, como, por ejemplo: *La información quede integrada en nuestro teléfono Android.*

Para clarificar que es la sincronización de datos podemos definir la sincronización como un proceso que permite depositar los datos de un usuario en distintos puntos o dispositivos en un mismo tiempo, por un lado, es beneficioso basándonos en la teoría, pero también, tiene su parte negativa, como bien definía aquella definición basada en Internet estos datos, quedan integrados en el dispositivo, pero, nos podemos preguntar ciertos aspectos como:

- ✓ ¿Qué ocurre si estos datos contienen algún tipo de malware?
- ✓ ¿Afectan a todos los dispositivos que conectados?
- ✓ ¿Sabemos si es seguro tener datos personales de importancia sincronizados en la nube?

Una breve respuesta puede resumirse en: todo aquello que otorga un beneficio, en muchos casos gratuitos tiene su desventaja, como que las empresas de estos servicios de sincronización conozcan todo lo relacionado con el usuario.

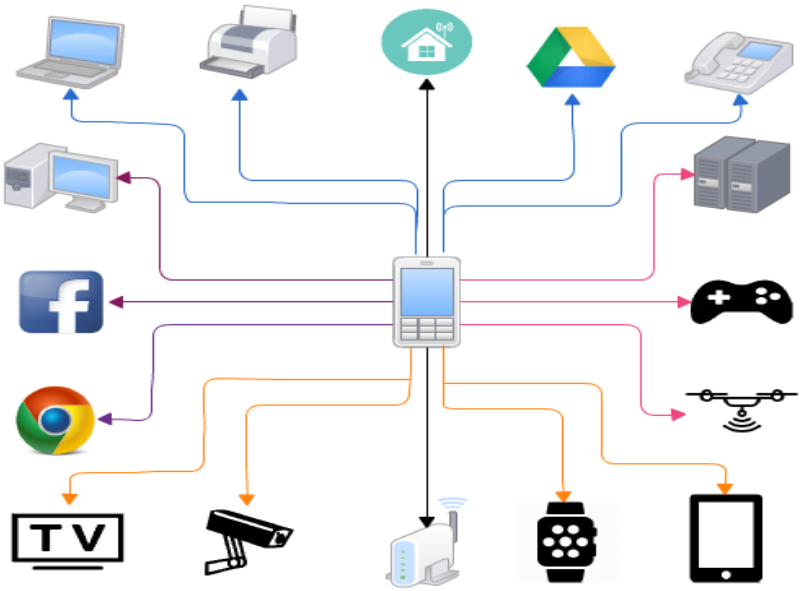


Imagen 14. Dispositivo móvil con Internet Of Things.

4.2. Historia

En este apartado, se introduce de una manera abreviada, la historia de las amenazas más comunes que se han dado en la sincronización de datos, pasando por los equipos informáticos que fueron partícipes en el inicio de estas amenazas, llegando a la telefonía móvil que es el tema que se trata en este proyecto y concretamente en el Sistema Operativo Android.

4.2.1.Ordenadores de sobremesa:

Antiguamente sin el uso de teléfonos móviles y las pocas personas con acceso limitado a disponer de los ordenadores personales en casa, los malware se aplicaban únicamente a ordenadores de sobremesa, el tipo de malware que se daba no tenía tanto riesgo, ni existía tanta variedad de malware como el que hay actualmente, dado que se basaban en muchas ocasiones en malware que limitaba el uso del ordenador al afectar los archivos internos, también eran famosos aquellos virus en forma de juego donde el virus aparecía en la pantalla avisando al afectado de que debía de atrapar a este virus. El riesgo que se encontraba con estos malwares se puede definir con un riesgo menor, donde el único afectado por infección era el ordenador, el cual a través un proceso de formateo o backup, lo devolvía a su estado normal.

Relacionado con las amenazas en la sincronización de datos en esta primera etapa se pueden dar en dos situaciones:

- Casa
  El usuario afectado tenía disponible 2 o más ordenadores donde al pasar los datos de uno a otro se sincronizaba el archivo infectado.

Imagen 15. Historia ordenador sobremesa (A)

- Trabajo
  Aquel trabajo el cual disponía de un servidor de datos físico (no era común) en el cual se volcaban los archivos más importantes, se producía la infección más común que se conoce, se añade al servidor un archivo infectado y al sincronizarlo (bajarlo) otro usuario también acaba siendo afectado.

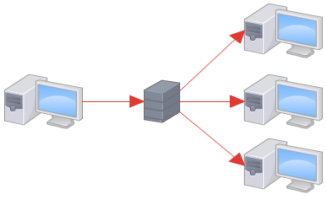


Imagen 16. Historia ordenador sobremesa (B)

4.2.2.Ordenadores portátiles:

Con los avances en el desarrollo de ordenadores menos robustos y la reducción del tamaño de sus componentes, unido con el fomento de uso de los ordenadores portátiles (permiten moverte y seguir trabajando en distintos puntos) los cuales tenían un mayor uso para personas que trabajaban, basado en la comodidad de tener una única unidad de trabajo en el trabajo y en casa, empezaron a darse los primeros problemas móviles de la sincronización. Aquellas personas que disponían de ordenadores portátiles afectados por malware se podían definir como portadores de amenazas igual que en el apartado anterior el uso de ordenadores estaba muy marcado a un domicilio personal y al trabajo, pero con estos ordenadores portátiles se multiplicaron las amenazas por el siguiente motivo:

- Siendo infectado en casa
  Siguiendo las mismas pautas que en la etapa anterior se añadía la posibilidad de llevarse la amenaza al trabajo desde casa causando así una infección en la zona de trabajo al conectar el ordenador en ella.

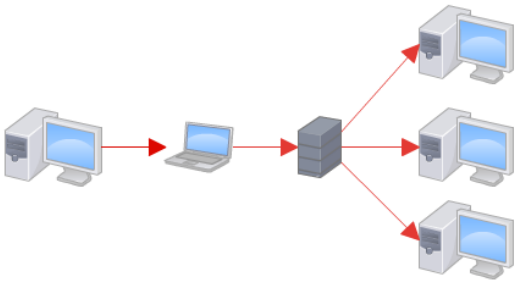


Imagen 17. Historia ordenadores portátiles (A)

- Infectado en la zona de trabajo.
  Similar al caso anterior, el cual se puede resumir:

  El usuario descarga un archivo infectado en la zona de trabajo y a través del portátil sincroniza este archivo en otro lugar, traspasando así el archivo a otro ordenador que no estaba infectado.

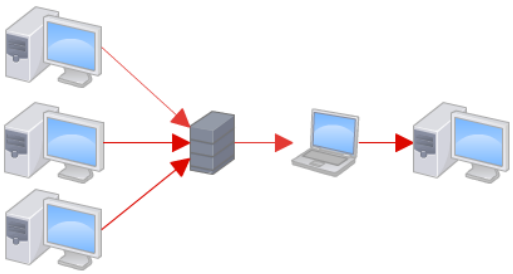


Imagen 18. Historia ordenadores portátiles (B)

4.2.3.Teléfonos móviles

La idea de un lanzamiento de teléfonos móviles no era la misma que percibimos ahora, se limitaba a poder llamar fuera de un lugar fijo, la existencia de amenazas de sincronización no era muy grande debido a la falta de conexión con redes de Internet, las amenazas estaban relacionadas con redes inalámbricas propias del móvil como los bluetooth e infrarrojos, que principalmente sincronizaban datos de la agenda del afectado por malware, los cuales producía borrados o edición de estos mismos datos.

Imagen 19. Historia teléfonos móviles.

4.2.4.Internet en los teléfonos móviles.

Gracias a los beneficios que otorgaban la conexión de Internet a los ordenadores, como poder comunicarte con personas de otra parte del mundo, poder encontrar información y noticias más actualizadas que los periódicos o noticias que se daban en el transcurso del día, está llegaba a los teléfonos móviles en forma de navegador de Internet y correo electrónico, donde se realizaban estas funciones básicas.
Se realizó un avance importante en la sociedad dado que las personas podían comunicarse entre ellas por correo sin estar en casa o en el trabajo dependiendo de un ordenador o podían consultar noticias de la misma forma.
Como ocurre siempre en el mundo de las tecnológicas, siempre que se abre un nuevo marco como oportunidad de negocio, también se abre un marco negativo, relacionado con la sincronización de datos en los teléfonos móviles, aparecen nuevos malwares que permiten conocer los datos de los dispositivos móviles. Estos datos, no ofrecían tanta cantidad de los mismos como los que se pueden procesar actualmente, pero los más importantes como la agenda de contactos, llamadas, mensajes, correos y el historial del navegador resultaba más accesible y por lo tanto interesante para aquellas personas con conocimientos de malware que les aportaba un nuevo canal por donde transmitirlos.
Al tener a las personas conectadas por distintos canales y obtener información de las mismas, también se podía conocer a aquellos individuos que interactúan entre ellos, aumentando así la red de afectados y posibles individuos como objetivos.

Imagen 20. Historia Internet en los teléfonos móviles.

4.2.5.Explosión en el mercado por parte de los Smartphone.

Con el incremento del uso de móviles inteligentes, con capacidad para conectarse a conexiones Wifi, y de banda (3G, 4G) surgen nuevas rutas para sincronizar datos, ya pueden ser aplicaciones en las cuales compartes tus datos con tu red de personas o almacenamiento en la nube.

A través de aplicaciones la sincronización de datos es bastante entendible, existen lacras en este tipo de sincronizaciones las cuales hacen plantearse algunas preguntas como, por ejemplo:

- ✓ ¿Dónde están los datos ubicados?
- ✓ ¿Cuándo subes los datos se quedan en las aplicaciones?
- ✓ ¿Aunque los borres?
- ✓ ¿Por qué son importantes tus datos para las empresas?
- ✓ ¿Tienen algún valor monetario?
- ✓ ¿Es cierta toda la seguridad que nos ofrecen de políticas de privacidad?

Como respuesta socialmente conocida en la mayoría de aplicaciones al dispensarte una plataforma donde alojar tus datos, todos esos datos en gran parte se vuelven propios de la empresa, respetando unas políticas de privacidad, estos datos que conocen al usuario repercuten en oportunidades de negocio para la empresa.

Por otro lado, el almacenamiento en la nube, en sus inicios no generaba confianza en el entorno social, dado que se veía como un acto de fe en el cual depositas tus datos en un servidor, el cual el usuario no tiene conciencia del mismo y de donde está, que es invisible, que no puede ir a buscar sus datos a una ubicación.

Este acto de fe cada vez se ha ido adecuando más con el paso del tiempo y gracias a grandes marcas conocidas como Dropbox, Google Drive, iCloud, OneDrive o Dataprius, generan más confianza en las personas.

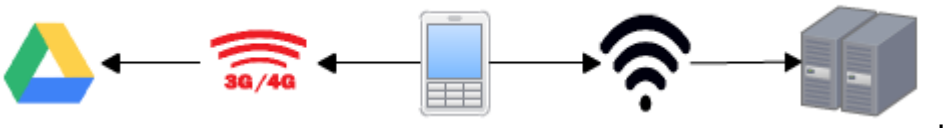


Imagen 21. Historia de los Smartphone.

4.3. Transmisión de la sincronización

Una vez definido qué es la sincronización, que se entiende por ella y que casos se han tratado de una forma simple aquellas amenazas en la sincronización desde distintos puntos tecnológicos, es importante conocer o qué canales se pueden dar para transmitir malware a través de la sincronización, como memoria para entenderlo mejor:

- Marca en rojo: Aquellos archivos, canales o dispositivos que son la cabeza o inicio de los ataques de malware
- Marca en verde: Aquellos canales o dispositivos que son los infectados por malware

4.3.1.Canal A

Dispositivo → nube→ ordenador.

- Etapa 1: El dispositivo contiene archivos con malware que sincroniza con el servidor de la nube

- Etapa 2: El servidor, al tratarse de un archivo del usuario, personal, tal como alguna foto/video/documento que no suele contener virus, la seguridad no lo detecta.

- Etapa 3: El usuario al descargar el archivo en otra ubicación e incluirlo en sus dispositivos, este infecta a los mismos, agravando que si se trata de una red local los demás dispositivos conectados pueden infectarse.

- Escenario visual:

Imagen 22. Canal A

4.3.2.Canal B

Ordenador→ nube→ dispositivo.

- Etapa 1: El ordenador del usuario contiene archivos con malware que sincroniza con el servidor de la nube.

- Etapa 2: El servidor, al tratarse de un archivo del usuario, personal, tal como alguna foto/video/documento que no suele contener virus, la seguridad no lo detecta.

- Etapa 3: El usuario al descargar el archivo en su dispositivo móvil y acaba infectándolo.

- Escenario visual:

Imagen 23. Canal B

4.3.3.Canal C

Canal que comunica los dispositivos y el servidor de la nube tiene lacras de seguridad.

- Etapa 1: El dispositivo u ordenador desde que se van a sincronizar los datos no contiene ningún malware.

- Etapa 2: En el canal de sincronización mientras se está sincronizando con el servidor, se introduce un malware en el canal de unión, el archivo llega al servidor de la nube infectado.

- Etapa 3: Al sincronizar (bajar) el archivo en el dispositivo u ordenador y contener malware infecta a estos mismos.

- Escenario visual:

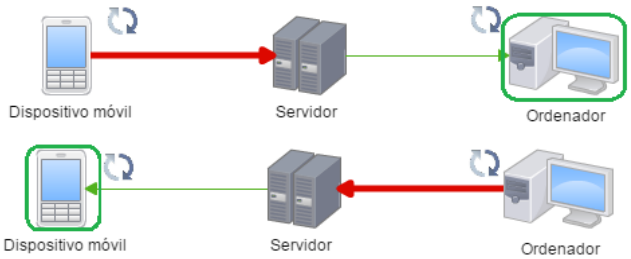


Imagen 24. Canal C

4.3.4.Canal D

Canal que comunica el servidor de la nube y los dispositivos tienen lacras de seguridad.

- Etapa 1: El dispositivo u ordenador desde que se van a sincronizar los datos no contiene ningún malware.

- Etapa 2: El archivo llega en perfecto estado al servidor de la nube y el usuario al realizar la acción de descargar el archivo en el dispositivo u ordenador de destino.

- Etapa 3: En el transcurso del servidor de la nube al dispositivo de destino en el canal de unión se introduce el malware y acaba infectando al archivo y como consiguiente al dispositivo de destino.

- Escenario visual:

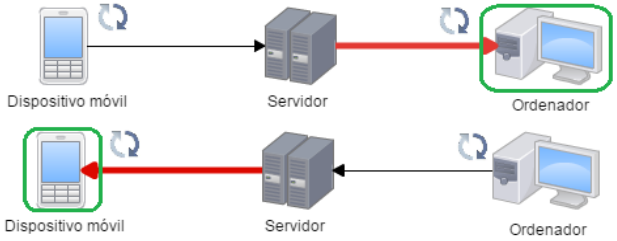


Imagen 25. Canal D

4.3.5.Canal E

Servidor de la nube es atacado e infecta a los dispositivos.

- Etapa 1: El dispositivo de origen el cual sincroniza los datos y el canal de comunicación entre el mismo y el servidor están en perfecto estado.

- Etapa 2: El archivo llega en buenas condiciones al repositorio de la nube, el servidor es afectado por un ataque y provoca que el archivo del usuario acabe infectándose por malware
- Etapa 3: Al descargar un archivo con malware en el dispositivo de destino este acaba siendo infectado.

- Escenario visual:

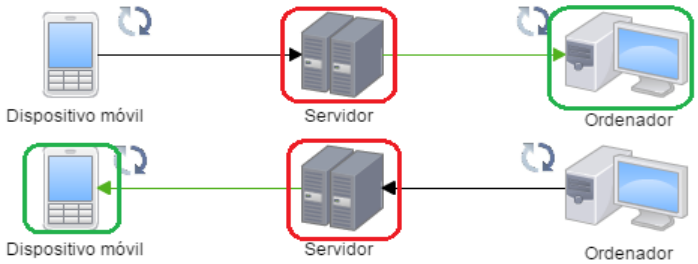


Imagen 26. Canal E

4.3.6.Canal F

Gadget con el dispositivo móvil Android. Utilizaré para el ejemplo una impresora con Wifi.

- Etapa 1: La impresora con conexión inalámbrica Wifi, crea un falso punto de conexión.

- Etapa 2: El dispositivo de origen se conecta e infecta los archivos del mismo, haciendo que el dispositivo crea que está conectado a una red Wifi normal.

- Etapa 3: El dispositivo de destino descarga un archivo con malware y es infectado.

- Escenario visual:

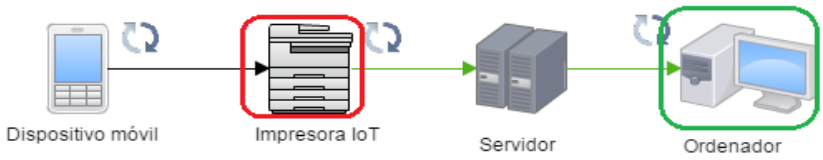


Imagen 27. Canal F

4.3.7.Canal G

Gadget con el dispositivo móvil Android. Utilizaré para el ejemplo una impresora con Wifi.

- Etapa 1: La impresora con conexión inalámbrica Wifi, crea un falso punto de conexión.

- Etapa 2: La impresora crea una doble identidad o pantalla falsa, donde el dispositivo móvil quiere sincronizar sus archivos en la nube estando conectado al gadget (sin saberlo), donde simula que es el servidor de destino donde el dispositivo quiere depositar sus datos, obteniendo así los datos mediante sincronización de archivos.

- Escenario visual:

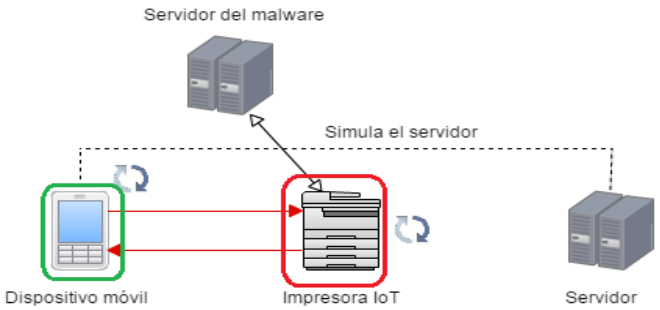


Imagen 28. Canal G

4.4. Público objetivo para los malwares

En este apartado se va a nombrar una idea de la posibilidad de un malware personalizado que puede llegar a los usuarios a través de los datos que se obtiene de ellos por aplicaciones, estos datos pueden ser comprados entre empresas (una acción normal y conocida) o malwares propios que entran al dispositivo y procesa los datos que tiene el usuario.

A través de una división sencilla de la sociedad que es usada para entender mejor la idea de que objetivos de malware existen según la división:

- Género
  Es simple de entender si dividimos entre hombres y mujeres, por ejemplo, para incluir un malware de alguna oferta de prenda de vestir más personalizada según el género, que se mande por correo ofertando esta prenda y el usuario entre a verla a través del link y quede infectado.

- Nivel de vida (ingresos)
  Esta idea va relacionada con el aumento de los malware de tipo Ramsonware (aquel malware que cifra el dispositivo y pide una compensación económica para devolverlo a su estado normal). Según el nivel de vida que lleve el usuario se puede pedir una cantidad de dinero mayor o menor la cual se adapte más al usuario para que pague por la recuperación del dispositivo.

- Edad
  Como pasa en la sociedad, una persona adolescente es más manejable y maleable que una persona adulta y con tablas, por los que un malware de robo de datos de fotos, videos, en resumen, de Media.

  Puede llegar a coaccionar de una manera más sencilla para recuperarlos a adolescentes que a personas adultas.

- Nivel de estudios
  Otra manera fácil de introducir un malware personalizado a través de los datos que genera una persona y los sincroniza con servidores de la nube puede basarse en el nivel de estudios que tenga una persona relacionada con la seguridad relacionada con el ámbito informático, dado que si una persona no tiene conocimientos de malware es un objetivo más claro y sencillo que una persona que sepa de qué trata el tema.

- Resumen
  La sincronización de datos abre una nueva vía para poder personalizar los malware al usuario, a través de ella y todos los datos que genera un procesamiento adecuado de los mismos, puede llegar a utilizarse malware inteligente personalizado para cada persona.

5. Casos prácticos de amenazas en la sincronización

En este apartado se definen los conocimientos aprendidos de cómo actúa la sincronización en una serie de casos prácticos y qué amenazas existen en ellos, en aquellas acciones que todo usuario realiza en su vida cotidiana y ve una actividad normal.

5.1. Android y Google

La relación que tienen Android y Google es conocida desde la creación de Android hasta la noticia de la compra por parte de Google del 100% de Android, conociendo esta relación, existe una sincronización de datos para los usuarios, con el navegador de Google (Google Chrome) y la cuenta Gmail del usuario, que es obligatoria para poder utilizar los dispositivos Android.
Esta sincronización se define como la acción de un usuario el cual inicia sesión en un ordenador diferente, o compra un nuevo dispositivo en el cual introduce su cuenta de Gmail.
Gmail ofrece un servicio para sincronizar todos los datos del usuario como son el historial, marcadores, credenciales, aplicaciones en beneficio del usuario, pero existe una amenaza real en este servicio que ofrece, dado que Google permite recordar las contraseñas de usuario de aquellos sitios que permite.

Atendiendo a la lógica se entiende que también las contraseñas recordadas van a sincronizarse con el nuevo login o dispositivo el cual va a acceder a la cuenta Gmail. Este beneficio que da Google a sus usuarios no solo hace que recuerde contraseñas de los demás productos de Google, como puede ser Gmail o YouTube, sino que también guarda los datos de páginas externas a través de la función autocompletar como pueden ser: Amazon, Facebook, Aliexpress, LinkedIn las cuales desvelan una gran cantidad de datos del usuario.

- ✓ ¿Qué pasa entonces cuando hay un login nuevo en Google con una cuenta de usuario?

La respuesta a esta pregunta es sencilla dado que al usuario se le manda un correo: Nuevo inicio de sesión desde (dispositivo), el cual es un simple aviso, no una confirmación de que se ha iniciado la sesión en un nuevo dispositivo, en el caso de que hubiera sido el usuario o una tercera persona quien ha accedido a su cuenta con todos sus datos anteriormente nombrados hasta que el usuario no desactive el dispositivo nuevo, este dispositivo puede ver toda la información del usuario, en el siguiente apartado se incluirá una foto detallada del mensaje que manda Google de la acción de un inicio de sesión desconocido.

A través de este supuesto caso, pueden surgir muchas preguntas relacionadas con la seguridad de los datos de Google, un servicio muy explotado por muchos usuarios del mundo, como, por ejemplo:

- ✓ ¿Qué ocurre con aquella persona que solo utilice el teléfono móvil y se lo sustraen?
- ✓ ¿Cómo puede recuperar una cuenta si no tienes más dispositivos que el móvil?
- ✓ ¿Cómo puede estar seguro el usuario de que no han autorizado a más dispositivos a utilizar sus datos?
- ✓ ¿Se trata de un beneficio de tener todo más accesible y conectado al usuario o es un agujero de seguridad para aquella persona que tiene un conocimiento mayor de cómo actúa la sincronización de Google con Android?

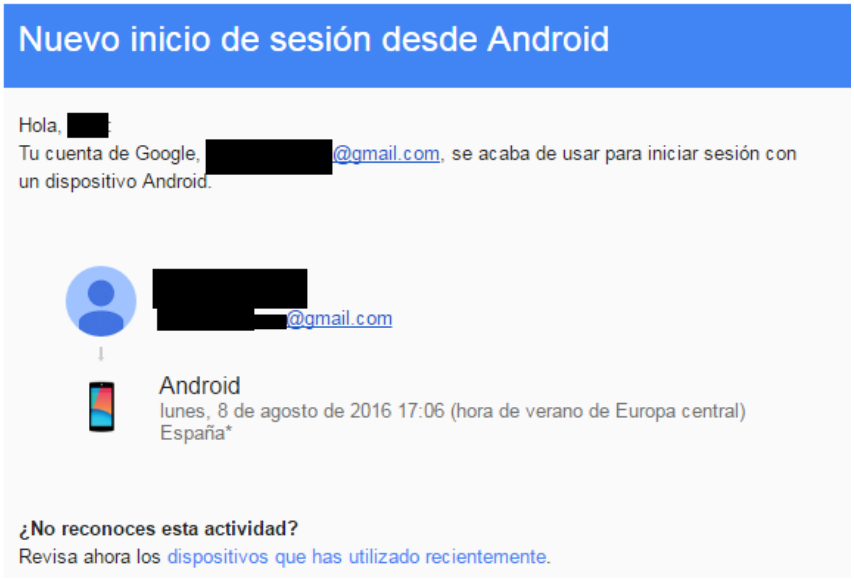


Imagen 29. Caso práctico Google.

5.2. Aplicaciones

En este apartado se remarca otro aspecto de la sincronización que es más conocido por los usuarios, son las aplicaciones, muchos usuarios saben que sincronizan sus datos para mantenerse actualizados sobre todo de redes sociales y correos electrónicos, anteriormente fueron mencionados los problemas de muchas aplicaciones al obtener más permisos de los que realmente necesitan, llegando a tomar control del dispositivo y de los datos que maneja.

A través de ellos se definen una serie de funciones generales que comparten estas aplicaciones para comprenderlas de una manera global:

- Obtienen permisos concedidos por el usuario que les dan funciones de comunicación, así como ubicación, Información sobre la conexión Wifi, Id de dispositivo y datos de llamada, contactos, los cuales permite a la aplicación utilizar los datos del usuario para sincronizarlos con servidores de la nube previo permiso concedido.

- La aplicación ofrece a los usuarios, en forma de beneficio dar más información acerca de sus publicaciones como por ejemplo mostrar donde están a qué hora y con quien, un ejemplo claro es mostrar en Facebook que has estado en Paris X día a Y hora.

- La aplicación esconde funciones, que se pueden desactivar entrando en complejos ajustes, estas funciones pueden ser: posicionamiento y conexión, esta complicidad hace que los usuarios no indaguen en la aplicación y los desactiven.

- Acceso de usuarios externos a una aplicación, que pueden consultar los datos que ha sincronizado el usuario en su cuenta sin consentimiento / conocimiento de que han sido vistos por personas ajenas.

- Generar una amenaza real a través de los datos compartidos que sincroniza el usuario y que no tiene conocimiento de la misma.

5.2.1. Runtastic

En este apartado se va a tratar esta aplicación para poder entender e interactuar con las amenazas de la sincronización, esta aplicación es interesante debido a que es poco conocida fuera del ámbito de aplicaciones más descargadas o aplicaciones de redes sociales, se trata de una aplicación que en se encuentra bien catalogada debido a que fomenta el deporte, sociabilizarse y la relación de malwares y permisos adicionales está fuera de peligro según Google Play y Android.

✓ ¿Qué ofrece esta aplicación?

Según la misma página: *Runtastic registra tus actividades fitness y deportivas como correr, trotar, ciclismo y caminatas, utilizando tecnología GPS para ayudarte a adoptar hábitos saludables y alcanzar tus objetivos*.

✓ ¿Dónde se encuentra la amenaza de la sincronización?

La amenaza se encuentra sobre todo en los permisos que tiene la aplicación para comunicarse a través del móvil, así como el GPS, datos o Wifi automáticamente, ciñéndose a esta idea simple hay que desarrollar como un usuario puede compartir información con esta aplicación de manera gráfica y explicativa:

Ingresando en un navegador de Internet la siguiente dirección:
site:runtastic.com/es/usuarios rutas

Se puede acceder a los perfiles de las personas que utilizan planes de entrenamientos similares a los que se va a mostrar en la siguiente imagen: (se ocultaran nombres y datos de la cuenta)

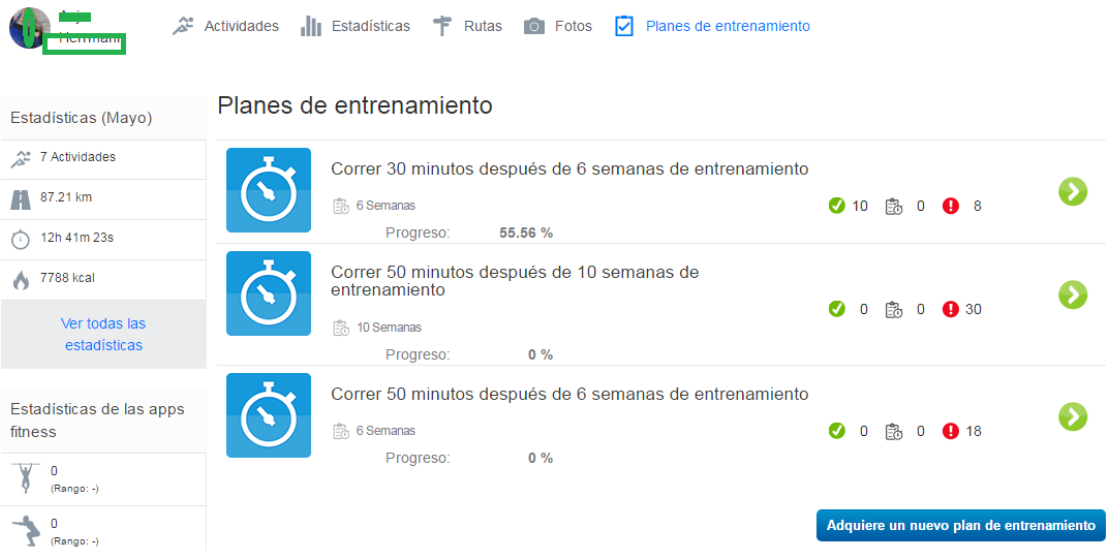


Imagen 30. Perfil de un usuario en Runtastic.

Esta información puede parecer poco adecuada cohesionándola con las amenazas en la sincronización, dado que hace saber la rutina que tiene un usuario de esta aplicación, con pocos datos del usuario, únicamente saber si la está cumpliendo y con qué frecuencia realiza ejercicio físico, pero en la siguiente pestaña nos da unos datos más interesantes para este proyecto:

Imagen 31. Menú de opciones de usuario en Runtastic.

En la pestaña rutas ya podemos obtener algo más de información que puede ser de un carácter importante para terceras personas:

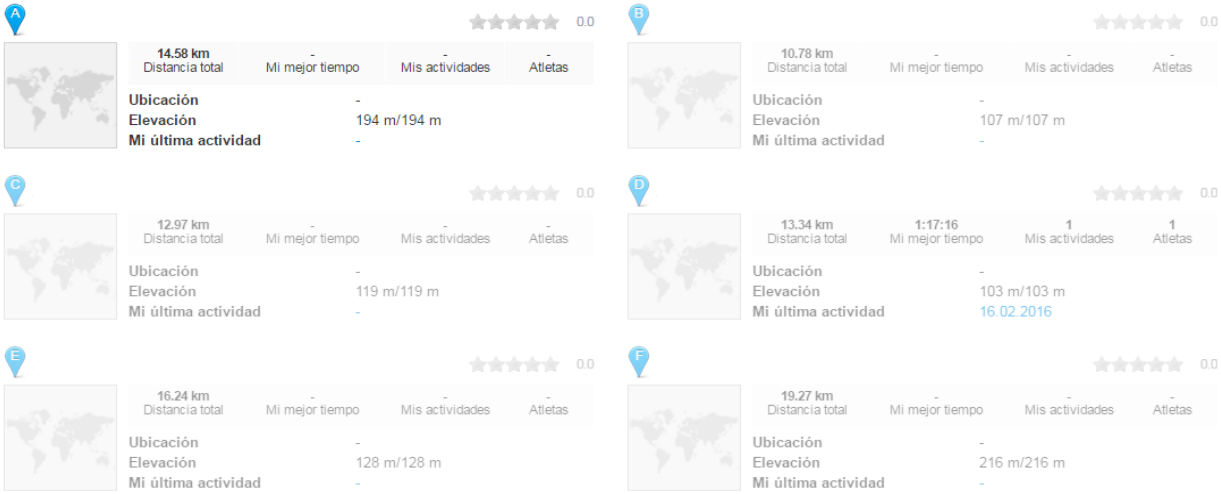


Imagen 32. Rutas de un usuario en Runtastic.

Imagen 33. Ruta realizada por un usuario.

Como se ha mostrado anteriormente y paso a paso, accediendo a través de la pestaña rutas, se nos muestra las rutas de la persona que hemos visitado el perfil, nos encontramos con todas las rutas que ha hecho y tiene nuevas marcadas y para más hincapié puedes ver el inicio y el fin de cada ruta que se ha hecho, ¿qué supone esto?

Una tercera persona con estos mismos conocimientos y con gusto por actividades poco lícitas o incluso ilegales puede conocer:

- Cuáles son los horarios en los que el sujeto está fuera de casa y dónde.
- Cuáles son los horarios en los que el sujeto está dentro de casa.
- Con qué frecuencia si/no está en su casa.
- Cuando tiene programado volver a salir.
- Con qué gente está realizando la ruta.

Nos podemos cuestionar algunas preguntas sobre el uso de esta aplicación como:

- ✓ ¿A que puede conllevar todo esto?
- ✓ ¿Robos?
- ✓ ¿Secuestros?
- ✓ ¿Conocimiento posicional de la persona que deseas encontrar?

5.2.2. Facebook.

Como otro ejemplo práctico que se va a nombrar, es el caso de Facebook, una aplicación conocida a nivel mundial y la red social con más usuarios actualmente también a nivel mundial, el motivo de elegir Facebook una aplicación más general es contrastar y afirmar que la mayoría de las aplicaciones que tenemos instaladas en los dispositivos Android, utilizan datos para comunicarse con el exterior, que son una amenaza real. Este es el motivo por el cual se utilizó una aplicación menos conocida y para un grupo de personas más reducido (Runtastic) y una aplicación con mayor capacidad de usuarios y conocida mundialmente (Facebook).

- ✓ ¿Qué ofrece esta aplicación?

Facebook es la red social con más usuarios a nivel mundial en la cual se ha extendido a la posibilidad de ser un usuario personal o un usuario empresarial en la cual publicitarte a través de esta red social.

- ✓ ¿Dónde se encuentra la amenaza de la sincronización?

Tratando distintos aspectos que utiliza Facebook, remarcando en todo momento que se trata de una de las redes sociales / aplicaciones / páginas Web más seguras del mundo por toda la cantidad de datos que genera y exporta a empresas externas. Ofrece una amenaza de sincronización a nivel de empresa más que incursión de usuarios externos

- <u>Número de teléfono</u>

  Como primer aspecto a tratar seria nombrar o averiguar cómo Facebook obtiene el número de teléfono de un usuario sin este usuario tener la aplicación o haberse creado el perfil de Facebook. Desde hace un año aproximadamente Facebook compró WhatsApp y le concede una vía para conocer los números de teléfonos de usuarios que aún no están en su plataforma.

Por otro lado, al instalar un usuario la aplicación accede a permisos de; *importar la agenda* de contactos esto accede a tener los números de teléfono de la agenda del usuario.

Esto se traduce en el conocimiento u obtención de datos por parte de la empresa Facebook de usuarios que no están en su plataforma aun, aparte de esto, Facebook ofrece una sincronización de amigos que se basa en encontrar los teléfonos de la agenda del usuario con los usuarios de Facebook y así realizar una recomendación de amistad.

- Acceso rápido a la aplicación de Android

Otro aspecto importante que remarcar antes del último aspecto que puede llegar a ser aprovechado por terceras personas. Es el acceso rápido de la aplicación de Facebook y las notificaciones push que tiene la aplicación por defecto.

Con esto nos referimos a que una persona, para consultar esta red social en su dispositivo móvil no tiene que ingresar su contraseña cada vez que quiera entrar, únicamente pulsando el icono de la aplicación, el login a Facebook esta realizado, esto en dispositivos sin pantalla de desbloqueo (que representan un alto número de usuarios) les presenta una amenaza real dado que pueden ver sus datos en caso de que el dispositivo sea sustraído.

El caso anteriormente nombrado puede darse por casualidad y tiene una baja probabilidad que ocurra, por ello se nombraron las notificaciones push al inicio del apartado, las cuales, a través de la evolución del sistema operativo de Android, han aparecido en las pantallas de bloqueo dando información sin tener que desbloquear el dispositivo y clicando al icono de la aplicación como se muestra a continuación.

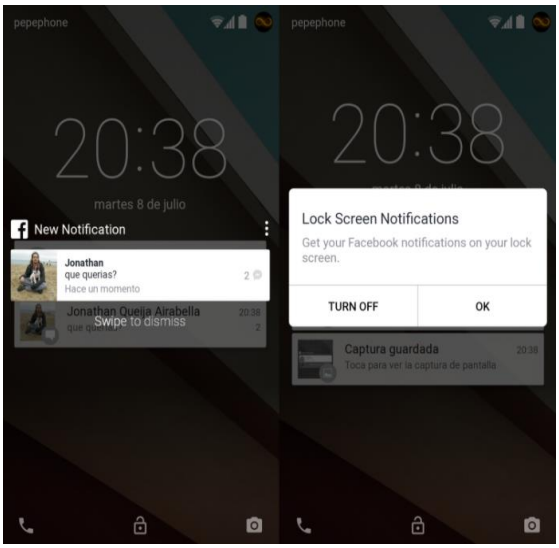


Imagen 34. Acceso rápido a Facebook.

- Función amigos cerca

El último aspecto que se va a nombrar es el último beneficio que ha dado Facebook a la aplicación para dispositivos móviles, se trata de un pequeño radar de distancia que está activo con la función GPS del dispositivo e informa de cuanta distancia hay de un usuario dentro de tu red de contacto de ti en relación con la posición GPS del dispositivo, avisando al usuario cuando está en una distancia cercana que puede configurar el usuario. Es interesante dado que se trata de una función similar a la aplicación anteriormente nombrada Runtastic donde puedes conocer la posición de tus contactos y esto puede aprovecharse en forma de una amenaza más física que en forma de malware utilizando la aplicación de Facebook, juntando esto a la información anterior que se ha aportado en referencia a la notificación de que un usuario está cerca de otro, sin tener que poner el desbloqueo de pantalla del dispositivo, puede crear una oportunidad para terceras personas como amenaza por parte de la sincronización.

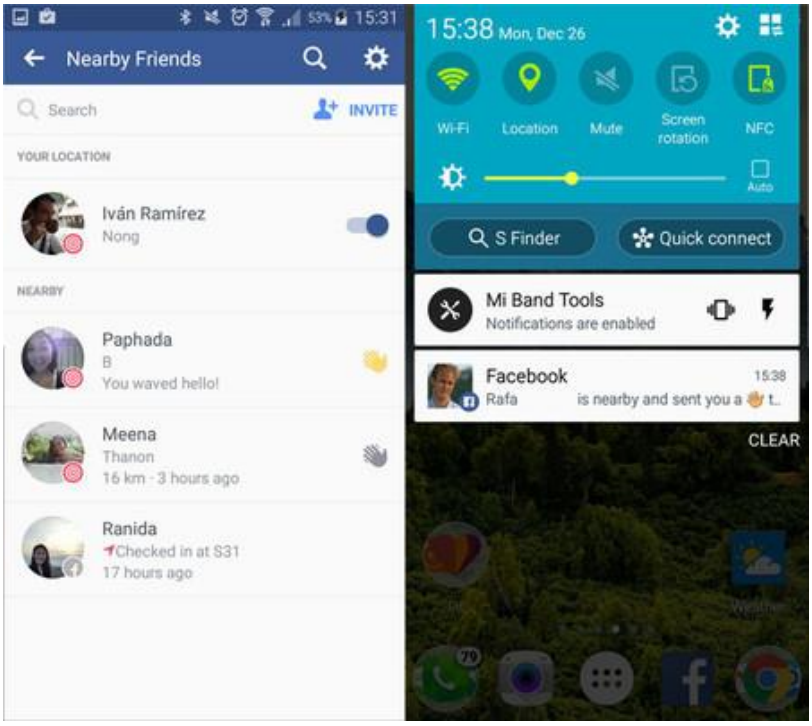


Imagen 35. Amigos cerca Facebook.

En esta imagen se muestra el uso de Facebook para mostrar la ubicación del usuario1 por parte de una cuenta del usuario 2 que se encuentra dentro de la red de contactos del usuario1, además de añadir la notificación push informando de nuestra posición cercana al usuario2.

5.3. Internet de las cosas (IoT)

Una nueva vía de comunicación entre objetos cotidianos y los Smartphone con Sistema Operativo Android, está siendo cada vez más real y útil para los usuarios gracias a la comodidad y beneficio que trae consigo, esto es el Internet de las cosas (definición en el apartado 5.2.4).

Esto es tan simple como utilizar pulseras inteligentes de deportes que aporten información de la salud de un usuario mientras lo realiza, utilizar un reloj inteligente (smartwatch) como nueva herramienta compatible con el dispositivo móvil, la posibilidad de manejar un dron aéreo con el Smartphone, poder reproducir lo que un usuario está viendo en el teléfono móvil en la televisión e interactuar con ella a través del móvil, a través de una casa inteligente y con la domótica con teléfono manejar ciertas funciones de la casa.

Casos más puntuales, como tener un frigorífico inteligente que haga un pedido de comida que falte y confirmes el pago con el Smartphone, o simplemente utilizar el dispositivo móvil como un medio de seguridad para poder ver las cámaras instaladas que tiene un usuario en un domicilio/local.

Todo lo mencionado en la parte superior de este apartado se puede resumir en la conectividad y sincronización entre un objeto cotidiano y un dispositivo móvil, cuya tendencia está en auge de crear o actualizar más objetos para que sean inteligentes y tengan compatibilidad con los teléfonos.

- ✓ ¿Qué relación tiene esta sincronización de objetos con los malware?

Estos objetos se caracterizan por ser objetos simples con posibilidad de conexión a redes, al ser objetos más simples y de nueva tendencia la seguridad en ello también se caracteriza por ser más baja y simple de lo que es un ordenador/Tablet, al tener menos seguridad y ser una nueva vía ocasiona oportunidad a usuarios en este nuevo mundo a aprovecharse de esto mismo. Para el entendimiento de esta idea, daré un par de ejemplo de cómo esto está influyendo y cómo influirá en el mundo de Internet creando oportunidades maliciosas.

- Ataques DDoS a través de IoT.

En este apartado queda remarcar un ataque simple pero más afectivo que se ha realizado y se sigue realizando para denegar el servicio de los dispositivos, este nuevo ataque mejorado por parte del Internet of Things se base en un ataque masivo de envío de paquetes pequeños pero desde muchos puntos para denegar servicio (DDos), llegando a realizar un ataque de una dimensión enorme y desde distintos puntos, consiguiendo que sea difícil de localizar y de solventar, pero, ¿qué tiene que ver con la sincronización? La función de este apartado es dar la idea de

todos los objetos que existen para realizar ataques desde muchos puntos y además como consiguen organizarse (consiguen sincronizarse) para realizarlo.

Un ejemplo que afirma este apartado es el malware Hajime que se dio a conocer a finales de 2016 y principios de 2017, su función es atacar y utilizar los dispositivos de Internet of Things para realizar ataques masivos de DDoS o correos de spam limitando la capacidad de encontrar el punto de inicio de donde se ejecutaba.

- Conexión al dispositivo móvil Android.

Para que un objeto cotidiano pueda catalogarse como objeto inteligente y entrar en la familia de Internet of Thing debe tener la capacidad de conectarse a la red de una forma física o inalámbrica, me gustaría expresar con esta idea las amenazas que existen en los objetos que se conectan a través de una red inalámbrica. Como ejemplo voy a utilizar a un usuario en un centro comercial y como objeto de IoT una cámara de grabación de seguridad que tiene conexión Wifi para transmitir datos.

Como ya se describieron, estos objetos son más simples y tienen menos seguridad por lo cual son más manejables. ¿Qué ocurriría con esta cámara si hubiese sido modificada por una tercera persona? Como idea simple surge que esta tercera persona pueda utilizar la cámara de vigilancia y poder ver lo que está pasando, pero no tiene correlación con la sincronización de datos.

Relacionado con la sincronización de datos, esta cámara que utiliza conexión Wifi y tiene los mismos protocolos de conexión inalámbrica que cualquier dispositivo móvil, puede ser utilizada como un falso punto de conexión al cual los usuarios se conecten y se recojan los datos mientras navegas, así como crear pantallas falsas de Webs en las cuales los usuarios dan su id y contraseña y esta es sustraída.

Este supuesto caso se ha plasmado en un lugar físico que se suele encontrar a cierta distancia de los domicilios de los usuarios y con un objeto característico de los centros comerciales cuya funcionalidad es evitar robo de objetos, pero, atendiendo a la familia IoT podemos cuestionar ciertas preguntas relacionadas con este supuesto.

- ✓ ¿Qué ocurre con la cámara de vigilancia de un edificio?
- ✓ ¿Qué ocurre con la televisión que solemos usar y tenemos en nuestro salón o incluso en nuestra habitación?
- ✓ ¿Qué ocurre con estos nuevos gadgets de pulseras de deporte, drones y distintos wearables inteligentes que están surgiendo?
- ✓ ¿Sabemos si no han sido modificados?
- ✓ ¿Sabemos si han podido acceder a ellos y al estar conectados a nuestra red, pueden ver todo lo que hacemos y los datos que generamos?

Todas estas preguntas realmente suponen una amenaza real que vienen directamente de una nueva vía que según su base nos beneficia a todos para estar más conectados y facilitarnos la vida: ***La sincronización.***

6. Resumen, conclusión, línea futura y recomendación

6.1. Resumen tras la finalización.

Con el desarrollo de este proyecto podemos resumir que, a través de los diferentes estados del arte, las amenazas que tiene Android y de la seguridad que dispone. Por otra parte a través del análisis de los problemas de la sincronización hemos confirmado la existencia de las amenazas a través de las vías de sincronización de datos y de una manera más prácticas a través de los casos prácticos para demostrar que realmente se cumplen.

Entrando más detalladamente en los puntos tratados en el proyecto:

- ✓ Conocer las principales características de Android.

  A lo largo de este proyecto se ha podido describir sobre todo en el apartado 4: Android. Las características de Android, su seguridad, su estructura interna y su funcionamiento, toda esta documentación que recoge los puntos más importantes de Android está disponible en la propia plataforma del sistema operativo para que los desarrolladores del propio sistema operativo de software libre obtengan un conocimiento del mismo, al ser una documentación gratuita y de libre acceso es fácil de asimilar y de entender lo que permite a los usuarios poder entender mejor el sistema operativo antes de trabajar con él.

- ✓ Profundizar en la seguridad de Android.

  Para conocer las características de seguridad de Android descrito también en el apartado 4 de este proyecto donde podemos encontrar la seguridad en su infraestructura interna (división en capas), conocimientos sobre el Kernel de Android (su núcleo), bibliotecas que usa, cifrados de archivos, particiones de disco, aplicaciones base que traen los terminales para una asegurar la seguridad del mismo, los distintos requisitos para asegurar las nuevas aplicaciones que se introduzcan en el terminal son seguras, por otro lado la división de los recursos del sistema operativo en permisos que se le otorga a cada aplicación.
  Distintos métodos de actualizaciones de seguridad además de las posibilidades de otorgar devolver al dispositivo a su estado inicial por distintos métodos como puede ser root o restablecer valores.

- ✓ Conocer las amenazas de Android.

  En este apartado que se desarrolla en el punto 5 del proyecto se definen las principales amenazas que ha tenido Android a lo largo de su vida y como han ido evolucionando y tomando forma para saltarse los nuevos parámetros de

seguridad que corregía el sistema operativo.
Llegando a realizar un seguimiento de las amenazas más importantes producidas en este sistema operativo hasta llegar a la actualidad donde se ofrecen datos de que tipos de amenazas son las más probables que infecten un terminal.

- ✓ Aportaciones propias al proyecto

  Tratándolo de una manera personal, este proyecto ha aportado al autor la oportunidad de poder descubrir e investigar un nuevo mundo que está emergiendo y es cada vez más visible para el mundo de cómo compartir los datos de un usuario de una manera invisible sin el conocimiento de que ocurre con ellos.
  De cómo realmente los datos se ven amenazados con el simple hecho de tener una aplicación en un dispositivo y de cómo buscar casos prácticos que realmente demuestren las que las amenazas virtuales, llegan a ser una amenaza real.

  Por otro lado, la posibilidad de realizar un proyecto de investigación y desarrollo de una forma real desde un punto de inicio de una ligera idea hasta el desarrollo y la consolidación de esta idea que se ha dado forma, pasando por la redacción de la documentación acorde al proyecto. Y así conocer cómo realizar un proyecto utilizando buenas prácticas introducidas por los tutores para llegar a desarrollarlo de manera apropiada.

6.2. Conclusión.

Como conclusión para este proyecto de fin de carrera se puede resumir de una manera clara y sencilla en que se ha demostrado tanto teóricamente como en casos prácticos que los datos que generamos al utilizar nuestros dispositivos Android tienen un valor que puede ser aprovechado por terceras personas o programas externos.

Estos datos que se mencionan son intangibles, inmateriales por los cual muchas veces el usuario tiene la posibilidad de perderlos a través de distintas amenazas no siente que está perdiendo nada, cuando realmente está dando a conocer o en este caso perdiendo, gran parte de su privacidad al tratarse de datos personales.

A través de esto un usuario está dando a conocer cuáles son sus gustos, hobbies, información donde suele ir, donde se encuentran y con quién a una gran parte de Internet, dado que, si tus datos son publicados y extendidos por Internet, una persona no sabe cuántas empresas/personas tienen sus datos, ni si lo están utilizando con fines beneficioso/perjudicial.

Tratándolo de una forma clara, aquella persona que desee sustraer los datos de un usuario no lo hace con fines beneficioso para el usuario, si no con fines perjudiciales para el mismo como puede ser: pedir a cambio de un valor monetario la devolución de sus datos (puede incluirse una amenaza de Ramsonware) o vender los datos del usuario a empresas para que exploten los gustos del mismo usuario.

Por lo cual, aunque sea un valor intangible que un usuario no nota que está perdiendo, tiene un valor tanto personal como monetario mayor que el propio dispositivo Android del cual se emiten los datos y de la mayoría de los objetos que se pueden comprar.

Para finalizar, tener la seguridad de que tus datos son seguros y tu privacidad no vaga por Internet hay que prestar atención y comprender todas las vías en las cuales los usuarios compartimos los datos, dado que un simple: me gusta, una ubicación, un permiso de más en una aplicación está otorgando a otras personas el conocimiento del usuario.

6.3. Línea futura.

Como trabaos futuros se propone:

- ✓ Ampliación de la documentación de Android que vaya surgiendo con las nuevas versiones entre las que se puedan incluir tanto como mejoras de seguridad y funcionalidad como agujeros de seguridad que puedan ser aprovechados por una mala configuración y se vuelva vulnerable.

- ✓ Ampliación de la documentación de las amenazas de Android de tal forma que aquellas amenazas nuevas que vayan surgiendo o tengan un efecto trascendental en una versión de Android posterior o programa en los cuales los datos que puedan sincronizarse estén amenazados.

- ✓ Ampliación de nuevos objetos o gadget que dispongan del sistema operativo de Android los cuales se pueden documentar para investigar cómo pueden ser amenazados por la sincronización de datos.

- ✓ Realizar pruebas más exhaustivas de cómo la sincronización de datos puede ser una amenaza para los dispositivos de Android, así como demostrar con nuevos casos prácticos que es así.

- ✓ Realizar un estudio y análisis similar a este proyecto, basado en otros sistemas operativos como iOS, Windows o Symbian los cuales comparten un mismo sector de mercado que Android.

- ✓ A través del punto anterior se puede realizar una comparativa entre los distintos Sistemas Operativos que nos aporten más datos relevantes de las amenazas de la sincronización de datos.

6.4. Recomendaciones

Una vez realizadas las conclusiones del proyecto, las recomendaciones para tratar las amenazas en la sincronización de datos en la plataforma de Android son plasmadas desde el punto personal del autor.

- ✓ Como primer punto remarcar el origen de los datos vamos a sincronizar, si se tratan de unos datos un origen dudoso, las amenazas ya pueden estar en ellos desde un inicio.

- ✓ Comprobar y estar seguros del repositorio donde se van a depositar nuestros archivos, un ejemplo sencillo es depositar un archivo en un servidor como Google Drive, Mega o Dropbox en los cuales, sabemos que tienen unos estándares de seguridad garantizados para los usuarios. O depositar el archivo en un repositorio ajeno que nos hayan facilitado o que tenga una seguridad dudosa.

- ✓ Prestar atención a los ataques de seguridad que sufren las infraestructuras y servicios que utilizamos para nuestros datos como emails, redes sociales o servidores, estar informados de estos ataques nos previenen de saber si hemos sido afectados y como solucionarlo.

- ✓ Ser precavidos con las actividades que compartimos, especialmente en redes sociales donde se suele compartir con quien estas, donde y en qué momento, esta información es muy susceptible e interesante para que tengan información sobre nosotros.

- ✓ Relacionado con las aplicaciones que suelen utilizar todas aquellas personas que tienen dispositivos Android, conocer que aplicación nos estamos descargando y en caso de no saber que aplicación estamos descargando y la necesitamos por utilidad, conocer y saber los permisos que nos pide esa aplicación para instalarse en el dispositivo, dado que, si pide más recursos de lo que realmente necesita, esta aplicación esté compartiendo datos del usuario.

- ✓ Otro punto importante para tener en cuenta es la seguridad del propio dispositivo Android, así como utilizar limpiadores de archivos y de datos para comprobar si el rendimiento del dispositivo es correcto, de esta forma podremos saber si algún archivo que tenemos cuenta con amenazas. A este punto se le puede añadir el uso de Antivirus en dispositivos Android que hay disponibles para controlar la seguridad del dispositivo y a la hora de sincronizar nuestros archivos tengan un buen estado.

- ✓ Otra recomendación es realizar formateos de forma periódica a los dispositivos para asegurar al usuario que en caso de que este afectado el dispositivo y sus archivos, pueda retomar la seguridad inicial del dispositivo.

7. Presupuestos

El presupuesto de un trabajo fin de grado, trata de dar un valor monetario al esfuerzo estimado que ha llevado realizarlo desglosándolo en distintos aspectos como mano de obra y materiales utilizados

Costes Humanos:

Función/Concepto	Horas	Coste/horas	Coste total
Investigación	75	10	750,00€
Desarrollo Propio	60	10	600,00€
Conclusiones	30	10	300,00€
Formato final	15	10	150,00€
Total	180	10	1800,00€

Costes Materiales:

Costes de licencias

Descripción	Licencias	Coste	Total
Windows 10	1	121,00€	121,00€
Total	1		121,00€

Costes de hardware

Descripción	Cantidad	Coste	Total
Pc sobremesa	1	850,00€	850,00€
Android gama media	1	200,00€	200,00€
Total	2		1050,00€

Costes Totales:

Descripción	Total
Costes humanos	900,00€
Costes de licencias	121,00€
Costes de hardware	1050,00€
Total	2071,00€

Beneficio Industrial:

Una vez obtenidos los beneficios totales finales, hay que añadir un 20% a todos los costes de los apartados anteriores.

Descripción	Total
Costes humanos	1080,00€
Costes de licencias	145,20€
Costes de hardware	1260,00€
Total	2.485,20€

Por lo tanto, el coste total del trabajo fin de grado es: **dos mil, cuatrocientos ochenta y cinco euros con veinte céntimos.**

8. Bibliografía

[1] Oliguín, M. (2016). *Hay 22 mil millones de dispositivos digitales conectados a Internet*. http://www.gaceta.unam.mx/20160815/hay-22-mil-millones-de-dispositivos-digitales-conectados-a-Internet/ Último acceso: abril 2017.

[2] Benítez, J. (2017). *España, tercer país del mundo con más ciberataques*. http://www.elmundo.es/espana/2017/05/15/5918ae9222601d51718b46d7.html Último acceso: abril 2017.

[3] Wikipedia. (2017). *Teléfono inteligente*. https://es.wikipedia.org/wiki/Tel%C3%A9fono_inteligente Último acceso: mayo 2017.

[4] Wikipedia. (2017). *Android*. http://es.wikipedia.org/wiki/Android Último acceso: mayo 2017.

[5] Wikipedia. (2017). *Android Auto.* https://es.wikipedia.org/wiki/Android_Auto Último acceso: mayo 2017.

[6] Wikipedia. (2017). *Núcleo Linux*. https://es.wikipedia.org/wiki/N%C3%BAcleo_Linux Último acceso: mayo 2017.

[7] Wikipedia. (2017). *Unix*. https://es.wikipedia.org/wiki/Unix Último acceso: mayo 2017.

[8] Android.com. (2017). *Historia de Android.* https://www.android.com/intl/es_es/history Último acceso: mayo 2017.

[9] Egham. (2016). *Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016*. http://www.gartner.com/newsroom/id/3415117 Último acceso: mayo 2017.

[10] Developer.Android. (2017). *Estructura de Android*. https://developer.android.com/guide/platform/index.html?hl=es-419 Último acceso: mayo 2017

[11] Developer.Android. (2017). *Permisos del sistema.* https://developer.android.com/guide/topics/permissions/index.html Último acceso: mayo 2017.

[12] Source.Android. (2017). *Seguridad de Android*. https://source.android.com/security/ Último acceso: mayo 2017.

[13] Iván. (2016) *Para qué sirve el root y cómo aprovecharlo al máximo*. https://elandroidelibre.elespanol.com/2016/02/para-que-sirve-el-root.html Último acceso: mayo 2017.

[14] Rivero, M. (2016). *¿Qué son los Malwares?* https://www.infospyware.com/articulos/que-son-los-malwares Último acceso: mayo 2017.

[15] Wikipedia. (2017). *Software*. https://es.wikipedia.org/wiki/Software Último acceso: mayo 2017.

[16] Avast.com. (2017). *¿Qué es el malware y cómo eliminarlo*? https://www.avast.com/es-es/c-malware Último acceso: mayo 2017.

[17] Pandasecurity.com. (2017). *Información, historia, evolución-Información sobre Seguridad-Panda Security*. http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/ Último acceso: mayo 2017.

[18] Wikipedia. (2017). *Virus de la telefonía móvil*. https://es.wikipedia.org/wiki/Virus_de_telefon%C3%ADa_m%C3%B3vil Último acceso: mayo 2017.

[19] Clooke, R. (2012). A brief history of mobile malware | Retail Dive. http://www.retaildive.com/ex/mobilecommercedaily/a-brief-history-of-mobile-malware Último acceso: mayo 2017.

[20] MuyCanal. (2014). *10 años con malware para móviles* http://www.muycanal.com/2014/06/10/malware-dispositivos-moviles Último acceso: mayo 2017.

[21] Group, I. (2017). *Análisis del panorama de amenazas móviles de 2016* http://www.ituser.es/seguridad/2017/01/analisis-del-panorama-de-amenazas-moviles-de-2016 Último acceso: junio 2017.

[22] Anon, (2017). *La principal amenaza móvil en 2016: troyanos con permiso de superusuario*. http://www.revistaneodigital.com/articles/2017/03/09/la-principal-amenaza-m%C3%B3vil-en-2016-troyanos-con-permiso-de-superusuario Último acceso: junio 2017.

[23] Unuchek, R., Sinitsyn, F., Parinov, D. and Stolyarov, V. (2017). *IT threat evolution Q1 2017.* https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/ Último acceso: junio 2017.

[24] Wikipedia. (2017). *Internet de las cosas.* https://es.wikipedia.org/wiki/Internet_de_las_cosas Último acceso: junio 2017.

[25] Foret, P. (2011). *La sincronización en tu Android, todo lo que debes saber - El Androide Libre*. https://elandroidelibre.elespanol.com/2011/07/la-sincronizacion-en-tu-android-todo-lo-que-debes-saber.html Último acceso: junio 2017.

[26] Alquimista, (2017). *Google Chrome y Android: Una pareja peligrosa e insegura*. https://www.somosbinarios.es/google-chrome-y-android-pareja-insegura/ Último acceso: junio 2017.

9. Anexo

Familias de malware para Android

Leyenda:


Funcionalidad de una Botnet


Gana acceso root o intenta convencer al usuario para que encienda su teléfono


Descargado a través del mercado oficial de Google Play


Envía mensajes SMS pagados o maliciosos


Roba información de ubicación


Información robada a un servidor remoto


Instala otras aplicaciones o binarios


Aplicación potencialmente no deseada ("Hacker" -Tools)


Banking Trojan que es capaz de interceptar y modificar códigos de autenticación bancaria (mensajes mTAN).


Trojan que es capaz de infectar una PC con Windows conectada.


Trojan que está encriptando todos los datos personales en el dispositivo.

Descripción	Capacidades
AccuTrack Esta aplicación convierte un smartphone Android en un rastreador GPS.	
Ackposts Este troyano roba la información de contacto del dispositivo comprometido y los sube a un servidor remoto.	
Acnetdoor Este troyano abre una puerta trasera en el dispositivo infectado y envía la dirección IP a un servidor remoto.	
Adsms Es un troyano al que se le permite enviar mensajes SMS. El canal de distribución de este malware es a través de un mensaje SMS que contiene el enlace de descarga.	
Airpush / StopSMS Airpush es una Ad-Network muy agresiva.	
AnServer / Answerbot Abre una puerta trasera en dispositivos Android y es capaz de robar información personal que será cargada posteriormente en un servidor remoto.	
Antares / Antammi Este es un troyano que roba información personal del dispositivo infectado.	
AVPass Esta familia de malware trata de detectar y eludir las herramientas de seguridad de Android (como las aplicaciones de AntiVirus) instaladas en el dispositivo infectado. Posteriormente, la aplicación intenta robar datos confidenciales y recibe comandos adicionales a través de SMS.	
BackFlash / Crosate Esta aplicación malintencionada instala un plugin de Flash falso que se registra como administrador de dispositivos y filtra información confidencial.	
Badaccents Este malware pretende descargar una copia de "The Interview", pero en su lugar instala un troyano bancario en dos etapas en los dispositivos de las víctimas.	
Badnews Una vez activado, BadNews hace sondeos de su C & C-Server cada cuatro horas para obtener nuevas instrucciones mientras empuja varias piezas de información confidencial incluyendo el número de teléfono del dispositivo y IMEI hasta el servidor.	
BankBot Este malware intenta robar información confidencial de los usuarios y dinero de cuentas bancarias y móviles asociadas a dispositivos infectados.	

Beita Un ladrón de información simple.	
Binv Este malware es un clásico Banking-Trojan que está dirigido a usuarios brasileños de dispositivos Android.	   
BgServ Obtiene la información del teléfono del usuario (IMEI, número de teléfono, etc.). La información se carga a una URL específica.	   
Biige Este software espía registra mensajes SMS, llamadas, ubicación, etc. y carga estos datos en un servidor remoto.	 
Booster Esta aplicación roba información personal y carga estos datos en un servidor remoto.	
Boxer Este troyano envía mensajes SMS a números premium.	
Cajino Este malware es una RAT clásica que intenta exfiltrar información sensible. Lo que hace que esta muestra sea especial es que está utilizando el servicio Baidu Cloud Push para la comunicación.	 
Carberp Intenta robar códigos confidenciales de autenticación bancaria (mensajes mTAN) enviados al dispositivo infectado.	 
Cawitt Esta aplicación roba información personal y carga estos datos en un servidor remoto.	
Cellspy Esta aplicación es un rastreador de teléfonos inteligentes.	
Chulli Esta familia de malware se utilizó dentro de un ataque dirigido. La cuenta de correo electrónico de un activista tibetano de alto perfil fue hackeada y utilizada para enviar ataques dirigidos a otros activistas y defensores de los derechos humanos. Después de que un dispositivo móvil se infecte, se conecta a un C & C-Server y espera a que los comandos de SMS arrojen datos confidenciales a este servidor.	  
Code4hk / xRAT Este malware se ha utilizado en ataques específicos en Asia e intenta exfiltrar la geolocalización de la víctima, así como grabaciones de voz. La muestra maliciosa se está propagando a través de mensajes de WhatsApp.	 
Coogos Backdoor Trojan que tiene la capacidad de recibir una conexión remota de un hacker malicioso y realizar acciones contra el sistema comprometido.	 
CopyCat es una red publicitaria agresiva y malintencionada. El objetivo principal es generar ingresos.	
Cosha Esta aplicación monitoriza el dispositivo infectado y envía datos personales a un servidor remoto.	

Counterclank No es un verdadero malware, sino una red de anuncios muy agresiva con la capacidad de robar información relacionada con la privacidad.	
Crusewind Intercepta mensajes SMS entrantes y los envía a un servidor remoto incluyendo información como IMSI e IMEI.	
Dogowar Este troyano envía mensajes SMS de spam a todos los contactos.	
Dougalek Esta aplicación roba información personal y carga estos datos en un servidor remoto.	
DroidDeluxe Explota el dispositivo para obtener privilegios de root. Posteriormente modifica el permiso de acceso de algunos archivos de base de datos del sistema e intenta recopilar información de la cuenta.	
DroidDream Utiliza dos herramientas diferentes (rageagainstthecage y exploid) para arraigar el smartphone.	
DroidDreamLight Recopila información de un teléfono móvil infectado (dispositivo, IMEI, IMSI, país, lista de aplicaciones instaladas) y se conecta a varias URL para cargar estos datos.	
DroidJack / SandoRAT Este malware tiene características similares a otras RATs Android. Algunas de estas características incluyen lo siguiente: Instalar cualquier APK, ver todos los mensajes en el dispositivo, escuchar conversaciones de llamadas realizadas en el dispositivo, etc.	
DroidKungfu Recoge una gran variedad de información sobre el teléfono infectado (IMEI, dispositivo, versión del sistema operativo, etc.). La información recopilada se descarga en un archivo local que se envía a un servidor remoto posteriormente.	
DroidSheep Esta aplicación puede capturar y secuestrar sesiones web sin cifrar.	
DSEncrypt Roba información confidencial (mensajes SMS, certificados y claves privadas, etc.) de smartphones infectados y carga los datos en un servidor remoto.	
Extensión / Mónada Este troyano puede interceptar llamadas telefónicas entrantes y salientes, abrir un navegador y visitar sitios web específicos, ejecutar clics en anuncios y puede actualizar su propio código malicioso. Además, la aplicación correspondiente puede realizar llamadas telefónicas, enviar mensajes SMS y recopilar información relacionada con la privacidad, como el historial de llamadas, los contactos, la ubicación GPS y la ID del dispositivo, que se cargarán en un servidor remoto.	
FaceNiff Esta aplicación puede capturar y secuestrar sesiones web sin cifrar.	

FakeAngry Backdoor Trojan que tiene la capacidad de recibir una conexión remota de un hacker malicioso y realizar acciones contra el sistema comprometido.	
FakeApp.AL Un Adware clásico para Android.	
FakeAV El malware engaña a los usuarios a pagar por la limpieza de otras infecciones inexistentes en su dispositivo. Además de mostrar falsos mensajes de infección, el APK también tiene la funcionalidad de interceptar llamadas telefónicas entrantes y salientes, así como mensajes.	
FakeBank Esta aplicación es un troyano para dispositivos Android que abre una puerta trasera y roba información del dispositivo comprometido. Además, es capaz de infectar una PC conectada de Windows y engaña al usuario para intercambiar aplicaciones bancarias legítimas contra las maliciosas.	
FakeDaum / vmwol El troyano recoge la siguiente información del dispositivo comprometido: mensajes SMS, número de teléfono y el IMEI del dispositivo infectado.	
FakeDefender Esta aplicación es un caballo de Troya para dispositivos Android que muestra falsas alertas de seguridad en un intento de convencer al usuario de que compre una aplicación para eliminar el malware inexistente o los riesgos de seguridad del dispositivo.	
FakeDoc Este troyano instala aplicaciones adicionales.	
FakeFlash Este troyano redirecciona al usuario a través de proxies pagados.	
FakeInst El **Fraudware** más común. Estas aplicaciones envían mensajes SMS premium.	
FakeJobOffer El malware muestra un mensaje de estafa que intenta hacer que las víctimas crean que han sido seleccionadas como candidatas. Con el fin de asegurar su colocación en la empresa, deben hacer un depósito en una cuenta bancaria.	
FakeMarket El objetivo general de esta aplicación maliciosa es simplemente aumentar fraudulentamente el número de visitas a unos 20 sitios web diferentes dentro de la búsqueda de google.	
FakeMart El troyano puede realizar las siguientes acciones mientras se está ocultando como una aplicación de blackmarket: Borre el contenido XMBPSP.xml en la preferencia compartida y vuelva a configurarlo para enviar mensajes SMS de alta calidad a 81211 ó 81308, configurar el dispositivo en modo silencioso, eliminar SMS recibido de 81211, etc.	
FakeNefix Esta aplicación roba credenciales de usuario.	
FakeNotify Esta aplicación envía mensajes SMS de calidad premium mientras utiliza técnicas de obfuscación y detección para moverse por las herramientas AV.	

FakePlay La aplicación se ejecutará en segundo plano, recopilando actividad de SMS y periódicamente la enviará a una dirección de correo electrónico de proxy. Una vez ejecutado, el troyano solicita privilegios de administrador de dispositivos.	
FakePlayer Envía mensajes SMS a números preestablecidos.	
FakeRegSMS Envía mensajes SMS a números premium e intenta ocultar esta acción de los investigadores de malware usando algún tipo de esteganografía.	
FakeTaoBao Este malware intenta robar las credenciales de usuario de TaoBao and ZhifuBao. Combinado con otra aplicación del mismo desarrollador también es capaz de enviar mensajes SMS.	
FakeTimer Envía información personal a un servidor remoto y abre sitios pornográficos	
FakeUpdate / Apkqug Esta familia de malware actúa como descargador automatizado para otras aplicaciones.	
FakeVertu SMS Trojan dirigido a los consumidores de Vertu en Japón. Este troyano recibe todos los mensajes SMS entrantes y los sube a un servidor remoto.	
Buscar y llamar / Fidall Envía información personal (libreta de direcciones) a un servidor remoto.	
Finspy Este troyano es un componente de un producto de vigilancia comercial que supervisa la actividad del usuario.	
Fjcon Este troyano se conecta a un C & C-Server y tiene la capacidad de instalar paquetes adicionales y enviar mensajes premium de mensajes SMS.	
Flexispy Este malware rastrea las llamadas telefónicas, los mensajes SMS, la actividad de Internet y la localización GPS.	
Foncy Este troyano envía mensajes SMS de alta calidad.	
Fonefee / Feejar Este troyano envía mensajes SMS de alta calidad.	
Fokange / Fokonge Es un malware de robo de información que carga los datos robados a un servidor remoto.	
Gamex Abre una puerta trasera e instala aplicaciones adicionales.	
Gazon Este malware intenta exfiltrar la información sensible y está mostrando anuncios. La muestra maliciosa se está propagando a través de mensajes WhatsApp y SMS.	

Geinimi Abre una puerta trasera y transmite información desde el dispositivo (IMEI, IMSI, etc.) a una URL específica.	
GGTracker Envía varios mensajes SMS a un número premium. También roba información del dispositivo.	
GingerBreak GingerBreak es una explotación de root para Android 2.2 y 2.3	
GingerMaster / GingerBreaker Obtiene acceso root y está recolectando datos en smartphones infectados. Estos datos se envían a un servidor remoto posteriormente.	
Godwon Esta aplicación intenta robar datos de contacto y personales de la libreta de direcciones local y la aplicación de Skype.	
GoldenEagle / GlodEagl Este troyano roba información personal y recibe comandos a través de SMS.	
GoneIn60Seconds Roba información (mensajes SMS, IMEI, IMSI, etc.) desde smartphone infectado y carga los datos en una URL específica.	
GPspy Rastrea la ubicación del dispositivo infectado.	
HeHe Este troyano roba mensajes de texto e intercepta llamadas telefónicas.	
HideIcon Roba información (mensajes SMS, IMEI, IMSI, etc.) desde teléfonos inteligentes infectados y carga los datos en un servidor remoto. Adcionalmente, muestra anuncios en pantalla completa al usuario.	
HippoSMS Envía varios mensajes SMS a un número premium y elimina los mensajes SMS entrantes de estos números.	
HongTouTou / Adrd Es un malware de robo de información que carga los datos robados a través de un proxy local a un servidor remoto. Los datos se cifran de antemano.	
Iconosys Esta aplicación roba datos personales.	
Imlog Esta aplicación roba datos personales.	
Jifake Esta aplicación envía mensajes SMS de calidad superior.	
JollyServ El troyano puede enviar mensajes SMS de calidad superior, enviar mensajes SMS a todos los contactos del usuario infectado e interceptar mensajes SMS entrantes.	
Jsmshider / Xsider Abre una puerta trasera y envía información a una URL específica.	
Kidlogger Este troyano roba información personal y la envía a un servidor remoto.	
KMIN Intenta enviar datos de dispositivos Android a un servidor remoto.	
Ksapp Este troyano tiene las capacidades para manejar la conexión de acceso remoto, realizar DoS o DDoS, capturar entradas de teclado, eliminar archivos u objetos, o terminar procesos.	

LeNa LeNa necesita un dispositivo enraizado para las siguientes acciones: Comunicación con un C & C-Server, descarga e instalación de otras aplicaciones, inicio de la actividad del navegador web, actualización de binarios instalados y muchos más	   
Lien / Después de la instalación, la aplicación recopilará información confidencial del usuario, como número de teléfono, SMS entrante y saliente y audio grabado en una dirección de correo electrónico. A continuación, hace uso de servidores SMTP para enviar los datos robados de nuevo al atacante.	 
Locker / SLocker Ransomware Este troyano es el primer casillero criptográfico para Android.	
Loicdos Este troyano tiene la capacidad de realizar DoS o DDoS.	
Loozfon Este troyano roba datos personales.	
Lovetrap / Luvrtrap Envía mensajes SMS a números premium y roba información de teléfonos inteligentes.	
Luckycat Abre una puerta trasera y está escuchando comandos desde un servidor remoto.	 
Mástealer Este troyano roba datos personales	
Malap Otro ladrón de información simple.	
Mania Este troyano envía mensajes SMS a números premium.	
MMarketPay Este troyano puede comprar automáticamente aplicaciones en los mercados chinos de Android.	
MobiDash Clásico Adware que muestra anuncios de pantalla completa para el usuario.	
MobileSpy / Godwon Este troyano roba datos personales.	
MobileTx Este troyano roba datos personales y los envía a través de mensajes SMS o HTTP.	
Mobinauten Esta aplicación rastrea la ubicación del smartphone infectado.	
Moghava Compromete todas las imágenes del teléfono inteligente fusionándolas con una imagen del ayatolá Jomeini.	
Nandrobox Este troyano roba datos personales y elimina ciertos mensajes SMS.	
Netisend Reúne información de smartphones infectados y carga los datos en una URL específica.	
Nickispy Recopila información de teléfonos inteligentes infectados (IMSI, IMEI, ubicación GPS, etc.) y carga los datos en una URL específica.	  

Obad Una de las familias de malware más sofisticadas hasta 2013. Un análisis detallado se puede encontrar aquí .	
Oldboot / MouaBad Obtiene el permiso de root por vulnerabilidades del sistema y reflashing la partición del sistema. También intenta ejecutar código malicioso en las primeras etapas del arranque del sistema para evitar que las aplicaciones AV las limpien. Posteriormente, algunas versiones de esta familia envían mensajes SMS de alta calidad y actúan como bot.	
OpFake El segundo **Fraudware** más común. Estas aplicaciones envían mensajes SMS premium.	
PDAspy Este troyano roba datos personales e información de ubicación.	
Penetho Esta aplicación es una herramienta hack para romper contraseñas WiFi.	
Photsy / Phopsy Este malware intenta **vaciar** todos los archivos jpg y mp4 de un dispositivo infectado.	
Pincer Este malware es capaz de reenviar mensajes SMS y realizar otras acciones basadas en los comandos que recibe de su servidor remoto.	
Pjapps Abre una puerta trasera y roba información del dispositivo. Este malware tiene las capacidades de un bot implementado.	
Placms Este troyano tiene la capacidad de manejar la conexión de acceso remoto, realizar DoS o DDoS, capturar entradas de teclado, eliminar archivos u objetos, o terminar procesos.	
Plankton Este malware tiene la capacidad de comunicarse con un servidor remoto, descargar e instalar otras aplicaciones, enviar mensajes SMS de alta calidad y muchos más	
Podec Este troyano envía mensajes SMS a números premium y es capaz de evitar el sistema de asesoramiento que Android muestra al usuario normalmente cuando envía mensajes con clasificación superior.	

PoisonCake Este malware puede instalarse, descifrar y soltar otras cargas, crear servicios de fondo y es capaz de realizar las siguientes acciones maliciosas: Inject com.android.phone, enviar e interceptar SMS, visitar el sitio WAP, recopilar información del teléfono y subirlas a un servidor remoto	
ProxyTrojan / NotCompatible / NioServ Este troyano roba datos personales.	
Qicsomos Envía mensajes SMS a números premium.	
Raden Este malware está enviando un mensaje SMS a un número premium chino.	
Repane Un ladrón de información simple.	
Roidsec / Sinpon Un simple ladrón de información de Android.	
RootSmart / Bmaster Este malware está aprovechando el exploit de GingerBreak para obtener privilegios de root. Este exploit no está incrustado en la aplicación, sino que se descarga dinámicamente desde un servidor remoto junto con otras aplicaciones malintencionadas.	
RuFraud Envía mensajes SMS de alta calidad. Esta es la primera aplicación maliciosa de este tipo que fue construida especialmente para los países europeos.	
Saiva Este troyano tiene la capacidad de manejar conexiones de acceso remoto, realizar DoS o DDoS, capturar entradas de teclado, eliminar archivos u objetos, o terminar procesos.	
Samsapo Este malware se propaga mediante mensajes SMS maliciosos y se comunica con C & C-Server. Las muestras correspondientes tienen la capacidad de instalar paquetes adicionales y enviar mensajes SMS de calidad superior.	

SaveMe / SocialPath Este malware roba mensajes SMS, registros de llamadas de contactos, así como información de dispositivos y carga estos en un servidor remoto.	
Scavir Envía mensajes SMS a números nominales premium.	
Scipiex Un ladrón de información simple.	
SeaWeth Este troyano tiene las capacidades para manejar conexiones de acceso remoto, realizar DoS o DDoS, capturar entradas de teclado, eliminar archivos u objetos, o terminar procesos.	
Selfmite Este gusano SMS utilizó una plataforma de publicidad legal y pago por instalación para la monetización y se está difundiendo a través de mensajes SMS.	
Skullkey El troyano se oculta utilizando la vulnerabilidad de la **clave principal de** Android para mantener válida la firma de la aplicación legítima. Permite a los atacantes realizar las siguientes acciones: Abrir una puerta trasera, robar datos sensibles (como IMEI y número de teléfono) y enviarlos a un servidor remoto, enviar mensajes SMS de calidad superior, etc.	
Smack El spyware se basa en XMPP Smack Openfire y tiene las siguientes capacidades: Cargar la información de contacto de los usuarios, mensajes cortos, registros telefónicos, ubicación GPS y fecha, ocultar su icono e interceptar mensajes cortos especificados.	
SMSpacem Recopila información del smartphone y carga estos datos en una URL específica. Este malware también envía mensajes SMS.	
SMSreg Registra el smartphone infectado a servicios no libres.	
SMSilence / SMSCatcher SMS Trojan dirigido a los consumidores de Starbucks en Corea del Sur. Este troyano recibe todos los mensajes SMS entrantes y los sube a un servidor remoto.	
SMSspy Banking Trojan dirigido a los consumidores en España.	
SMSsniffer Envía copias de mensajes SMS a otros dispositivos.	
Sndapps / Snadapps El malware puede acceder a varias informaciones desde el dispositivo: la compañía y el país, el ID del dispositivo, la dirección de correo electrónico y el número de teléfono y carga esta información en un servidor remoto.	
SpamBot Envía mensajes de spam SMS. La aplicación obtiene el contenido del mensaje de spam y los números del receptor a través de un C & C-Server.	
Spitmo Es una de las primeras versiones de los troyanos SpyEye para el sistema operativo Android que roba información del teléfono inteligente infectado. El troyano también monitorea e intercepta los mensajes SMS de los bancos (mensajes mTAN) y los sube a un servidor remoto.	
SPPush Este malware está enviando mensajes SMS premium y está enviando información relacionada con la privacidad a un servidor remoto. Desde el mismo servidor, el malware está descargando nuevas aplicaciones.	

SpyBubble Este troyano roba datos personales.	
SpyOO Este troyano registra y roba datos personales.	
Ssucl Este troyano es el primer troyano de Android que puede infectar una PC con Windows conectada. Además, es capaz de enviar mensajes SMS, habilitar Wi-Fi, recopilar información sobre el dispositivo y su usuario (como contactos, fotos, datos GPS) que se carga en un servidor remoto. Además, este troyano puede cargar toda la tarjeta SD y todos los mensajes SMS almacenados en el dispositivo.	    
Steek / Fatakr Es una aplicación fraudulenta que anuncia una solución de ingresos en línea. Algunas de las muestras tienen la capacidad de robar información relacionada con la privacidad y enviar mensajes SMS.	  
TapSnake / Droisnake Asigna la ubicación del teléfono a un servicio web.	
Tascudap Esta aplicación se conecta a un servidor remoto (gzqtmtsnidcdwxoborizslk.com) y monitorea los mensajes SMS entrantes para comandos. El dispositivo infectado puede utilizarse para ataques DDoS.	 
Tetus Este troyano recibe todos los mensajes SMS entrantes y los sube a un servidor remoto. La aplicación correspondiente también se permite eliminar mensajes SMS en el dispositivo infectado y es capaz de enviar mensajes SMS. Además, el troyano envía una lista de todas las aplicaciones instaladas a un servidor remoto.	 
TigerBot Este malware se comunica con un C & C-Server a través de mensajes SMS, es capaz de descargar e instalar otras aplicaciones, iniciar actividades de navegador web, actualizar binarios instalados, y muchos más	   
Titan Este malware ha sido utilizado en ataques específicos en Asia y trata de exfiltrar información sensible. La muestra maliciosa se está propagando a través de mensajes SMS.	 
Tonclank Abre una puerta trasera y descarga archivos en los dispositivos infectados. También roba información del teléfono inteligente.	
TGloader / Stiniter Escucha un C & C-Server para comandos. Este troyano puede instalar aplicaciones adicionales y enviar mensajes SMS de alta calidad.	  

Tracer Commercial Spyware - ver http://killermobile.com/manuals/TRa.pdf para más información	
TypStu Este troyano roba datos personales.	
UpdtBot Este malware se propaga a través de mensajes SMS malintencionados y se comunica con un C & C-Server. Las muestras correspondientes tienen la capacidad de instalar paquetes adicionales y enviar mensajes SMS de calidad superior.	
UpdtKiller Este troyano detecta y desactiva las aplicaciones AV instaladas.	
Uracto Este malware se utiliza para engañar a las madres, a los fanáticos del anime, a los jugadores y más para instalar las aplicaciones maliciosas y robar los datos confidenciales después.	
USBcleaver Cuando el dispositivo está conectado a un equipo con Windows que no está deshabilitado, el troyano intenta recopilar un montón de información del equipo, incluyendo: Puerta de enlace predeterminada, contraseña de Google Chrome, dirección IP, contraseña de Microsoft Internet Explorer, contraseñas WiFi, etc	
Uten Cuando se ejecuta el troyano, informa del estado del dispositivo al atacante y descarga un archivo de configuración que contiene listas de números de teléfono. Posteriormente, el troyano envía mensajes SMS a los números de teléfono enumerados en este archivo de configuración. También puede realizar las siguientes acciones adicionales: modificar la configuración del dispositivo, descargar e instalar nuevos paquetes, intentar obtener privilegios de root, etc.	
Uxipp Este malware intenta enviar mensajes SMS de alta calificación.	
Vdloader Este malware abre una puerta trasera en el dispositivo infectado y roba datos personales.	
Walkinwat / Pirater Envía mensajes SMS a todos los números de la guía telefónica y roba información del dispositivo infectado.	
Waps / Simhosy Esta aplicación maliciosa trata de robar mensajes SMS y entradas de contacto de un dispositivo infectado.	
Wroba / HijackRAT Esta aplicación maliciosa trata de filtrar datos relacionados con la privacidad o credenciales bancarias de un dispositivo infectado y lo combina con una RAT.	

YZHC Este malware está enviando mensajes SMS premium y bloquea cualquier mensaje de entrada que informe al usuario acerca de estos servicios. Como otra conducta malintencionada, el malware está cargando información crítica de privacidad a un servidor remoto.	
Zeahache Abre una puerta trasera y carga la información robada en una URL específica. También envía mensajes SMS.	
ZergRush ZergRush es una explotación de root para Android 2.2 y 2.3	
ZertSecurity Esta aplicación maliciosa trata de engañar a un usuario comprometido para que inserte los detalles de su cuenta bancaria que luego se enviarán a los atacantes.	
Zitmo / Citmo Trata de robar códigos confidenciales de autenticación bancaria (mensajes mTAN) enviados al dispositivo infectado.	
Zsone Envía mensajes SMS a los números nominales premium relacionados con la suscripción para servicios basados en SMS.	

Fuente: https://forensics.spreitzenbarth.de/android-malware/

Última actualización: enero de 2016

Universidad de Alcalá

Escuela Politécnica Superior

Universidad de Alcalá