Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Análisis de Herramientas de Seguridad en Android

Trabajo Fin de Máster

Presentado por: Arias Blanco, Ana María

Director/a: Bermejo Higuera, Juan Ramón

Ciudad: Gijón
Fecha: Julio 2021

Resumen

Este proyecto pretende dar soluciones de seguridad para el usuario no experto y solventar dudas de usuarios del Sistema Operativo Android. Se enfocará de cara a si es necesario o no la instalación de herramientas tipo antivirus, dar soluciones y buenas prácticas de cara a la seguridad en sus dispositivos. Dado el uso cada vez más extendido de dispositivos móviles y la cantidad de datos accesibles desde los mismos, se realizará un análisis de algunas de las herramientas de seguridad más populares para el sistema operativo Android. Por un lado, se analizará la efectividad de las herramientas en cuanto a la protección del sistema frente a malware haciendo uso de un dispositivo real, y por otro, se estudiará cómo afecta al sistema operativo la instalación de la herramienta en aspectos tales como el rendimiento de éste o duración de la batería. Para concluir el proyecto, se incluye una guía de buenas prácticas para el uso de dispositivos con SO Android.

Palabras Clave: malware**,** herramienta de seguridad, Android, protección, análisis.

Abstract

This project aims to provide security solutions for non-expert Android device users and solve security doubts. It will focus on whether or not it is necessary to install antivirus-type tools on Android devices, provide security solutions and good practices. Due to the increasingly widespread use of mobile devices and the amount of data accessible from them, an analysis of some of the most popular security tools for the Android operating system will be carried out. On one hand, the performance of the tools will be analysed in terms of protecting the system against malware using a real device, and on the other, it will analyse how the installation of the tool affects the operating system in aspects such as the performance of the same or battery life. The Project includes a guide of good practices for the use of Android devices.

Keywords: malware, security tools, Android, protection, analysis

Contenido

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1 Introducción

1.1 Motivación

En los últimos años Android se ha consolidado como el sistema operativo más utilizado en dispositivos móviles y más concretamente en Smartphone. Según Kantar, importante consultora de marca y análisis de datos, en diciembre del 2020, los dispositivos con Android representan el 84.8% frente a IOS, que dispone de una cuota del 15% en España(Kantar World Panel, n.d.). En cuanto a los datos aportados para el resto del mundo, Android sigue siendo el sistema operativo dominante, aunque en algunos países como Australia o Reino Unido, la diferencia entre ambos sistemas operativos es realmente pequeña. Este hecho, junto con el uso cada vez más incipiente de dispositivos móviles por parte de las personas y el almacenamiento de datos personales en los dispositivos, convierte Android en el blanco del mayor número de amenazas; tendencia que se ha mantenido en los últimos años.

Por otra parte, la madurez de los dispositivos móviles ha alcanzado unos niveles muy altos, si se tienen en cuenta estadísticas ofrecidas por Ditrendia, empresa especializada en estadísticas de marketing, se obtiene que el 90% de los adultos tiene un smartphone y el 95% de ellos lo utiliza a diario. Este uso de los dispositivos móviles además cada vez es más amplio, el 91% de los usuarios acceden a internet desde el móvil y los accesos desde otros dispositivos está en continuo descenso. Los hábitos han cambiado tanto que el 43% de los españoles afirma no necesitar otro dispositivo y el uso no es solo para consulta web, sino que también se realizan acciones de mayor privacidad como consultar y actualizar redes sociales, acceder a eventos o transportes o hacer transferencias de dinero y compras online (Ditrendia, 202 C.E.).

Atendiendo a datos ofrecidos por Deloitte, (Deloitte, n.d.), las tendencias españolas son la instalación de una media de 16 aplicaciones por dispositivo, y la visualización y compartición de videos, estas prácticas aumentarían la probabilidad de la instalación de malware en el smartphone. Por otra parte, el estudio manifiesta la reticencia de los usuarios en el uso de mecanismos de seguridad biométricos.

Por otro lado, debido al crecimiento del malware en el sistema operativo Android, cada vez son más las personas que, con conocimiento de estar siendo atacadas o sin él, ven vulnerados sus derechos, siendo expuestos sus datos personales almacenados en sus dispositivos o convirtiéndose en víctimas de fraudes como smishing (SMS) u otro tipo de ataques.

Debido a todos los motivos expuestos anteriormente, con este TFM se pretenden ofrecer soluciones al usuario que aporten seguridad tanto en el uso del dispositivo en su día a día como en caso de que se produzca un incidente no deseado con el dispositivo como puede ser el robo o pérdida del mismo.

1.2 Planteamiento

Con este Trabajo Fin de Máster, se pretende dar visibilidad a las medidas de seguridad existentes en el sistema operativo, así como analizar la efectividad y eficacia de algunas de las herramientas de seguridad disponibles para la instalación en los dispositivos móviles.

Con la finalidad de alcanzar el objetivo propuesto, se han de superar los hitos detallados a continuación:

1. Identificar el entorno en el que se ha de realizar el estudio. Para ello se deberán conocer tanto el sistema operativo Android, su historia y los mecanismos de seguridad implementados para él, el malware que le afecta, así como los tipos de herramientas existentes en el mercado.
2. Realizar un estudio sobre herramientas disponibles en el mercado y seleccionar de entre estas el conjunto de las soluciones para el análisis.
3. Estudiar las diferentes opciones disponibles sobre cómo obtener una batería de malware para la realización de las pruebas y una vez seleccionado el dataset, obtener las muestras de malware que participarán en el estudio.
4. Realizar el estudio sobre la muestra de herramientas seleccionada con el fin de estudiar tanto su eficacia de detección como el efecto de la instalación de éstas en el sistema operativo en aspectos como el rendimiento del dispositivo o el consumo de batería. Para la realización del estudio se ha de definir una metodología a seguir en el análisis de cada una de las herramientas.
5. Obtener y analizar los resultados obtenidos en el estudio para extraer las conclusiones del mismo.

De este modo, y gracias a la creación de una guía de buenas prácticas para usuarios de Android, se obtendrá una configuración del dispositivo minimizando así los riesgos a los que los dispositivos Android, y por ende los usuarios de estos, se ven expuestos.

1.3 Estructura del trabajo

Para comenzar el trabajo, en el capítulo dedicado al estado del arte, se realizará un estudio del Sistema Operativo, así como de las herramientas de seguridad ofrecidas por el mismo, se expondrán también los tipos de malware que le afectan y configuraciones y herramientas

antimalware existentes en el mercado, algunas de las cuales serán objeto de estudio posteriormente.

Los siguientes capítulos, versarán sobre el desarrollo del estudio del cual es objeto el proyecto. En el capítulo 3, “Herramientas analizadas en el estudio” se realizará la selección de herramientas que formarán parte del estudio de entre las analizadas en el estado del arte. En el capítulo 4, “Colecciones de malware” se tratarán distintas colecciones de malware disponibles para utilizar en el estudio, se seleccionará una de entre las distintas opciones y se realizará la extracción de la muestra de malware que participará en el estudio.

Seguidamente, en el capítulo 5, “Objetivos concretos y metodología de evaluación” se definirán los objetivos y metodologías a seguir para el desarrollo del proyecto, así como la métrica seleccionada para la realización del estudio. A grandes rasgos, la metodología a seguir será la siguiente: se partirá de una imagen de sistema operativo Android recién instalada con una aplicación de monitorización. Se realizará la instalación de una herramienta de seguridad de las del estudio y posteriormente se descargará la selección de malware al dispositivo, se seguirán una serie de pasos como la descompresión del archivo, instalación de aplicaciones no detectadas por el antivirus y ejecución de las mismas y se anotarán los resultados. El malware que vaya siendo detectado, quedará eliminado de la siguiente etapa. Con esto se obtendrán unos resultados de detección por parte de la herramienta que serán analizados en el siguiente capítulo.

A lo largo del capítulo “6. Resultados del estudio”, se presentarán en detalle los resultados obtenidos en el estudio del rendimiento de las aplicaciones, así como de su eficacia. Para cada una de las herramientas se presentará una estadística con los datos obtenidos del estudio, así como una valoración de la misma.

Con el fin de complementar el piloto experimental, en el apartado “6.5 Guía de buenas practicas” se creará una guía de buenas prácticas para usuarios de Android mediante la cual se pondrá en relieve que no solamente la seguridad reside en la instalación de herramientas de protección en los dispositivos, sino que el usuario del sistema y las acciones realizadas por el mismo juegan un papel muy importante.

Para finalizar el trabajo, a lo largo del capítulo “ 7. Conclusiones y trabajo futur” se obtendrán las conclusiones obtenidas de la realización del piloto experimental y líneas de trabajo futuras.

2 Estado del arte

A lo largo de este capítulo, se realizará un estudio de la plataforma Android teniendo en cuenta su estructura y los mecanismos de seguridad que integra. Posteriormente se pondrá en conocimiento cómo el malware afecta al Sistema Operativo y las herramientas que existen para mitigar o detectar el malware en los dispositivos que lo ejecutan.

2.1 Android

Android es un sistema operativo móvil basado en núcleo Linux. Fue diseñado inicialmente para móviles, pero su uso se ha extendido y ha sido adaptado también a otros dispositivos de pantalla táctil como tablets, relojes inteligentes (Android Wear OS), televisores y hasta automóviles (Android Auto y Android Automotive).

2.1.1 Historia

El contenido de este epígrafe se apoya principalmente en información obtenida de la web Wikipedia (Wikipedia, n.d.)

Android inicialmente era un proyecto de una empresa llamada Android Inc. en la que desarrollaban un sistema operativo para cámaras digitales hasta que, en julio del año 2005, Google realiza la compra de Android Inc.

Un par de años más tarde, en noviembre de 2007, se crea la Open Handset Alliance - alianza formada por un conjunto de fabricantes y desarrolladores de hardware, software y operadores de servicio - y se anuncia la primera versión del sistema operativo: Android 1.0. No será hasta un año más tarde, en 2008, cuando los terminales con el sistema operativo estén disponibles (Wikipedia, n.d.).

A partir de este momento, la venta de dispositivos móviles con este sistema operativo obtiene muy buenas cifras siendo en la actualidad el sistema operativo más vendido según Kantar, (Kantar World Panel, n.d.)en todo el mundo con una representación muy importante en países como España. En diciembre de 2020 Android representa un 84.8% frente a iOS que tiene un 15% y Windows 0.2%.

Android dispone de una amplia comunidad de desarrolladores que facilitan la ampliación de funcionalidad en los dispositivos que ejecutan su sistema operativo. A principios de 2018, el número de aplicaciones disponibles en Google Play Store, la tienda de aplicaciones oficial de Android, era superior a los dos millones. Actualmente, existen algo más de 2,9 millones de aplicaciones disponibles para descargar.

Debido al conflicto comercial entre EE. UU. y China, en 2019 el gobierno estadounidense incluye a Huawei en la lista de bloqueados de colaboradores y el 19 de mayo de ese mismo año, Google anuncia que deja de prestar servicio a los usuarios de móviles Huawei por lo cual no dispondrán de actualizaciones ni se les permitirá el uso de sus aplicaciones en el futuro (Gmail, Google maps, etc.).

2.1.2 Versiones

Con frecuencia al menos anual, una nueva versión del Sistema operativo es lanzada al mercado.

Un dato que siempre ha causado expectativa sobre las versiones de Android es la denominación de las mismas. Históricamente, las diferentes versiones del Sistema operativo se han apodado con nombres de dulces o postres en inglés, comenzando cada una de ellas por una letra diferente siguiendo el orden alfabético. Con el fin de facilitar a los usuarios la tarea de conocer qué versión de Android era la más actual, en el año 2009 se produjo un rediseño del logo de Android y se comenzó a denominar las versiones numéricamente ya que, el orden alfabético seguido hasta ese momento no era suficientemente intuitivo.

La última versión de Android publicada hasta la fecha es la 11. Desde febrero de 2021, está disponible el programa de Vista previa para desarrolladores de Android 12 y continuará hasta el lanzamiento de la última actualización pública para AOSP y OEM, previsto para este mismo año.

En la Tabla 1 se presentan los datos con las diferentes versiones del sistema operativo y su fecha de lanzamiento. Para complementar la información aportada, en el ANEXO I. TABLA DE VERSIONES ANDROID, se encuentra una tabla extendida con principales características incluidas en cada una de las versiones.

Esta información ha sido obtenida de la web Wikipedia (*Anexo:Historial de Versiones de Android - Wikipedia, La Enciclopedia Libre*, n.d.)

Tabla 1. Versiones de Android

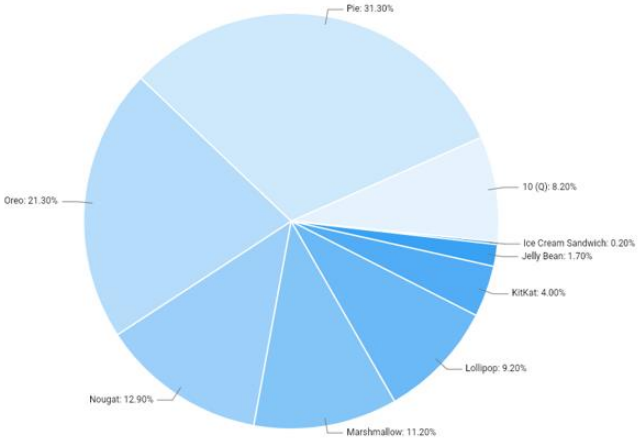
Nombre	Número de versión	Fecha de lanzamiento
Apple Pie	1.0	23 de septiembre de 2008
Banana Bread	1.1	9 de febrero de 2009
Cup cake	1.5	25 de abril de 2009
Donut	1.6	15 de septiembre de 2009
Eclair	2.0 – 2.1	26 de octubre de 2009
Froyo	2.2 – 2.2.3	20 de mayo de 2010

Nombre	Número de versión	Fecha de lanzamiento
Gingerbread	2.3 – 2.3.7	6 de diciembre de 2010
Honeycomb56	3.0 – 3.2.6	22 de febrero de 2011
Ice Cream Sandwich	4.0 – 4.0.5	18 de octubre de 2011
Jelly Bean	4.1 – 4.3.1	9 de julio de 2012
KitKat	4.4 – 4.4.4	31 de octubre de 2013
Lollipop	5.0 – 5.1.1	12 de noviembre de 2014
Marshmallow	6.0 – 6.0.1	5 de octubre de 2015
Nougat	7.0 – 7.1.2	15 de junio de 2016
Oreo	8.0 – 8.1	21 de agosto de 2017
Pie	9.0	6 de agosto de 2018
10	10.0	3 de septiembre de 2019
11	11.0	8 de septiembre de 2020
12	12.0	agosto de 2021 (Previsión)

Debido al gran número de versiones del sistema operativo y al gran número de fabricantes de dispositivos móviles Android que añaden una capa de personalización a los mismos, no todas las mejoras llegan a todos los dispositivos. Esto se debe en una parte a la limitación de hardware de los dispositivos y por otra por la no actualización de los mismos por parte del fabricante. Este es el conocido como problema de la fragmentación en Android, en la cual lleva Google trabajando un tiempo, por el que se ve afectada sobre todo la seguridad de los dispositivos.

En la siguiente figura, Ilustración 1.Distribución de versiones Android, se puede observar la segregación de versiones existente en el último estudio disponible correspondiente a abril 2020 (Bradshaw, n.d.). Como se puede observar, teniendo en cuenta las tres actualizaciones del sistema operativo más actuales, el porcentaje de dispositivos con una instalación de Android obsoleta se acerca al 50%.

Ilustración 1.Distribución de versiones Android



Version	Codename	Percentage
4.0	Ice Cream Sandwich	0.20%
4.1	Jelly Bean	0.60%
4.2	Jelly Bean	0.80%
4.3	Jelly Bean	0.30%
4.4	KitKat	4.00%
5.0	Lollipop	1.80%
5.1	Lollipop	7.40%
6.0	Marshmallow	11.20%
7.0	Nougat	7.50%
7.1	Nougat	5.40%
8.0	Oreo	7.30%
8.1	Oreo	14.00%
9.0	Pie	31.30%
10.0	10 (Q)	8.20%

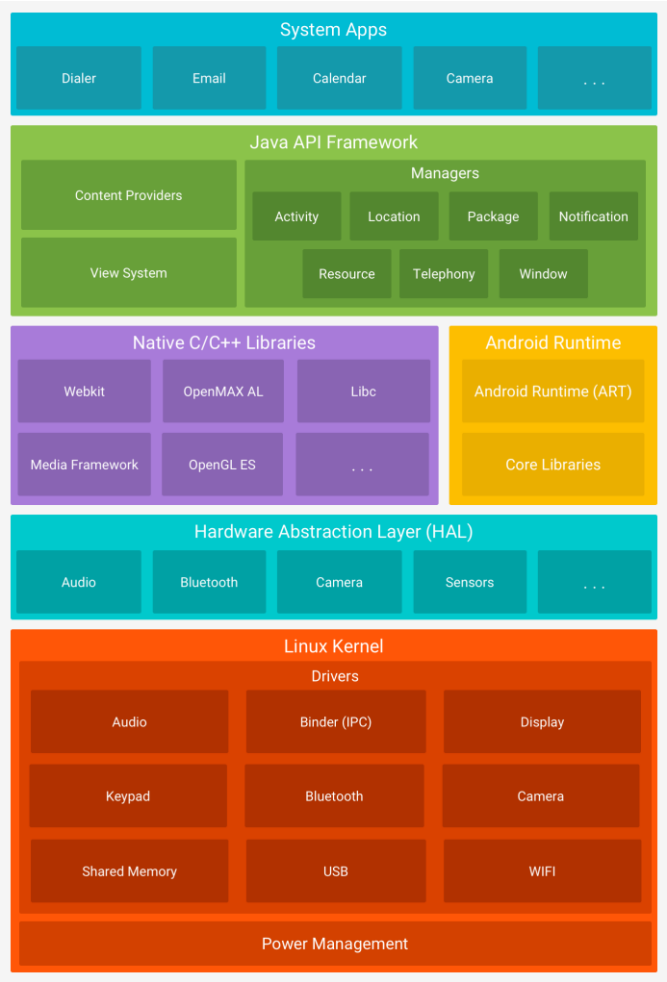
(Bradshaw, n.d.)

2.2 Arquitectura Android

Android es un sistema operativo de código abierto basado en Linux. Es compatible para una gran variedad de dispositivos y factores de forma. En el diagrama presentado en la Ilustración 1, se muestran los principales componentes de la plataforma Android.

La mayor parte del contenido de esta sección y subsecciones se ha extraído de la web oficial de Android(Android Developers, n.d.-a).

Ilustración 2.Arquitectura Android



(Android Developers, n.d.-a)

2.2.1 Kernel de Linux

Tal y como se ha comentado anteriormente, la base de la plataforma Android es el kernel de Linux, esto permite que el sistema operativo aproveche funciones de seguridad claves y, a su vez, facilita el trabajo a los fabricantes de los dispositivos haciendo que el desarrollo de los controladores de hardware se haga para un kernel conocido.

2.2.2 Capa de abstracción de hardware (HAL)

La capa de abstracción de hardware, también conocida como HAL, proporciona interfaces estándares que ponen a disposición de las capas superiores las capacidades de hardware del dispositivo. Esta capa, consta de varios módulos de biblioteca, cada uno de los cuales implementa una interfaz para un tipo particular de componente de hardware, por ejemplo, el módulo de la cámara, el bluetooth, etc. El sistema Android es el encargado de cargar el módulo de biblioteca que corresponda según la solicitud recibida por el marco de trabajo de una API para acceder a hardware del dispositivo.

2.2.3 Tiempo de ejecución de Android

Los dispositivos anteriores a Android 5.0 disponían de Dalvik. A partir de dicha versión, cada aplicación es la encargada de la ejecución de sus propios procesos y disponiendo de instancias particulares del tiempo de ejecución de Android (ART).

2.2.4 Bibliotecas C/C++ nativas

En Android, una parte importante de los componentes y servicios centrales del sistema operativo, como por ejemplo los anteriormente comentados ART y la HAL, están basados en código nativo por lo que requieren el uso de bibliotecas nativas escritas en lenguajes C y C++. Con el fin de exponer la funcionalidad de algunas de ellas, Android proporciona la API del marco de trabajo de Java.

Para tener acceso a algunas de estas bibliotecas de plataformas nativas directamente desde aplicaciones desarrolladas en C y C++ se puede hacer uso del NDK de Android.

2.2.5 Marco de trabajo de la API de Java

Todo el conjunto de funciones del sistema operativo Android está disponible mediante API escritas en Java. Estas interfaces son la base del desarrollo de aplicaciones Android, simplificando la reutilización de componentes del sistema y servicios centrales y modulares. Los desarrolladores tienen acceso total a esta colección de funciones.

2.2.6 Aplicaciones del sistema

Las aplicaciones del sistema funcionan como aplicaciones para los usuarios y además facilitan a los desarrolladores capacidades claves a las cuales pueden acceder desde las suyas propias.

En Android se incluye un conjunto de aplicaciones centrales entre las que se encuentran las aplicaciones de mensajería SMS, correo electrónico, calendario, navegador de internet, etc. Estas aplicaciones pueden ser usadas por los usuarios o sustituidas por otras de terceros salvo excepciones como la aplicación settings (ajustes).

2.3 Modelo de seguridad en Android

El modelo de seguridad de Android se implementa a lo largo de toda la arquitectura del sistema. En la presente sección, se detallan los aspectos más relevantes de dicho modelo recogidos de la web oficial de Android (Android, n.d.-c).

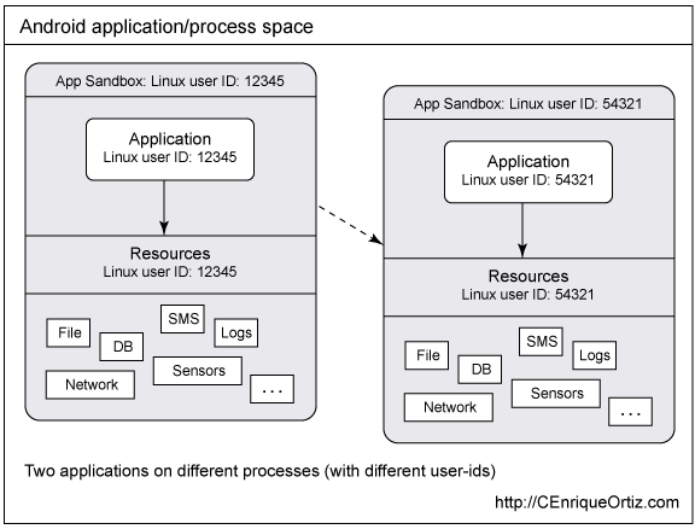
2.3.1 Sandbox de aplicaciones

El sistema operativo Android, por estar basado en Linux, implementa el principio de mínimo privilegio obligando la ejecución de cada aplicación en una sandbox. De este modo, cada aplicación solamente puede tener acceso ilimitado a sus propios recursos.

Este mecanismo se implementa a nivel de kernel, asignando a cada aplicación un identificador único de usuario UID. Los archivos existentes en el almacenamiento del sistema, por defecto, tendrán el mismo UID que la aplicación que los creó y solo podrán ser accedidos por ese UID. Aquellos que se encuentren en almacenamiento externo, podrán ser leídos o modificados por cualquier aplicación que tenga permiso para acceder a almacenamiento externo, independientemente de su UID.

La configuración es tal que ninguna aplicación de terceros puede acceder a recursos del sistema sin obtener antes el correspondiente permiso. A este tipo de aplicaciones se les asignarán UID no privilegiados. En la Ilustración 3 se representa esquemáticamente la solución implementada por el sistema operativo.

Ilustración 3. Dos aplicaciones en diferentes procesos con diferentes UID



(Programmersought, n.d.)

Adicionalmente, cada una de las aplicaciones del sistema se ejecuta como un proceso independiente al resto disponiendo de su propio espacio de direcciones. Por ello, Android garantiza gracias a los mecanismos de seguridad existentes en Linux, que por defecto ninguna aplicación puede acceder a los recursos de otra - por tener cada una de las aplicaciones distinto UID- y tampoco a los recursos del sistema - el UID que se asigna a una aplicación de terceros no dispone de privilegios para ello. Además, debido a que cada aplicación se ejecuta en un proceso diferente, el único modo de interacción entre aplicaciones será a haciendo uso de mecanismos de IPC (Inter Process Communication).

2.3.2 Partición del sistema y modo seguro

La partición del sistema es de solo lectura y contiene: el kernel, las bibliotecas del sistema operativo, las aplicaciones y el marco de trabajo y el tiempo de ejecución de las mismas. Cuando se inicia el dispositivo en modo seguro, las aplicaciones de terceros no se inician de forma predeterminada, sino que han de ser lanzadas manualmente por el propietario del dispositivo si así se desea.

2.3.3 Permisos del sistema de archivos

Como se ha indicado en la explicación de Sandbox, el sistema está basado en Linux. En un entorno tipo UNIX, se garantiza que los archivos de un usuario no podrán ser accedidos por otro mediante los permisos del sistema de archivos. Cada aplicación de terceros se ejecuta con su propio usuario y los archivos creados por ésta no pueden ser leídos o modificados por otra aplicación a menos que el desarrollador los comparta explícitamente.

2.3.4 Security-Enhanced Linux

Android utiliza Security-Enhanced Linux (SELinux) para establecer un control de acceso obligatorio en los procesos (mac) y aplicar directivas de control de acceso.

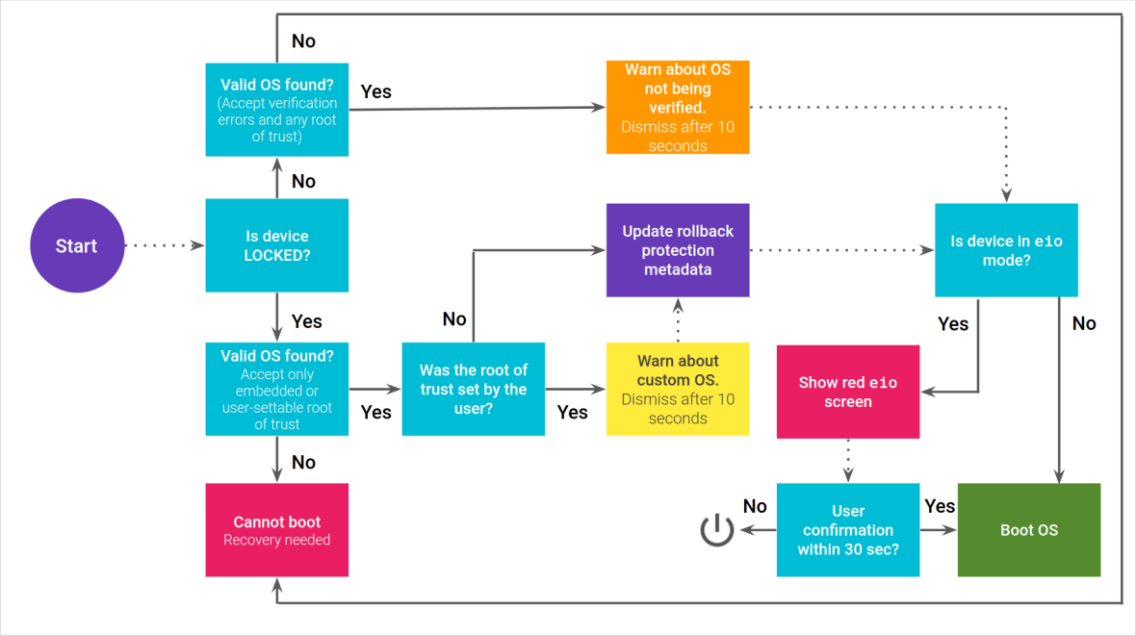
2.3.5 Arranque verificado

Desde la versión Android 6.0, el sistema operativo es compatible con verified boot y device-mapper-verity. Mediante el arranque verificado (verified boot) se garantiza la integridad del software del dispositivo partiendo de una raíz de confianza de hardware hasta la partición del sistema. Durante el arranque del dispositivo, se verifican la integridad y autenticidad de cada etapa criptográficamente antes de su ejecución.

Android 7.0 y versiones posteriores soportan strictly enforced verified boot, lo cual implica que si el dispositivo está comprometido no se podrá arrancar.

En la Ilustración 4 se presenta gráficamente el flujo de arranque seguro definido anteriormente.

Ilustración 4. Flujo de arranque seguro en Android



(Android, n.d.-a)

2.3.6 Criptografía

El sistema operativo proporciona una colección de API criptográficas para que sea usado por las aplicaciones. Estas API incluyen implementaciones de funciones criptográficas estándar como SHA, RSA, AES o DSA. También se proporcionan API para el uso de protocolos de niveles superiores como SSL y HTTPS.

En la versión Android 4.0, se introdujo la clase KeyChain con el objetivo de permitir que las aplicaciones realicen el almacenamiento de claves privadas y cadenas de certificados en el almacenamiento de credenciales del sistema.

2.3.7 Rooteo de dispositivos

La configuración por defecto del sistema operativo es tal que, únicamente el kernel del mismo y un pequeño subconjunto predefinido de las aplicaciones principales del sistema se ejecutan con permisos de administrador. Por otra parte, Android permite la modificación del sistema operativo, kernel o cualquier otra aplicación siempre y cuando el usuario o aplicación que realiza la acción disponga de permisos de superusuario. En general, root posee acceso completo a todas las aplicaciones y todos los datos de la aplicación.

Aquellos usuarios que realizan el cambio de permisos en un dispositivo Android, operación comúnmente conocida como rootear el dispositivo, para conceder acceso superusuario (root) a las aplicaciones aumentan la exposición de seguridad a aplicaciones maliciosas y posibles defectos de la aplicación.

Con el rooteo del dispositivo se obtiene una gran capacidad de modificar un dispositivo, este hecho es importante para los desarrolladores que trabajan con la plataforma Android.

En muchos dispositivos, el usuario tiene la posibilidad de desbloquear el gestor de arranque y realizar así la instalación de un sistema operativo distinto o una versión diferente a la disponible. Mediante la instalación de uno de ellos, se adquiere la capacidad de obtener acceso root. Un desarrollador puede utilizar esta capacidad con fines de depuración de aplicaciones y componentes del sistema o para acceder a características no presentadas a aplicaciones por las API de Android.

En un dispositivo rooteado, el cifrado de datos mediante clave almacenada en el dispositivo no protege los datos de la aplicación. Con la finalidad de agregar una capa de protección de datos, las aplicaciones pueden hacer uso del cifrado mediante una clave almacenada en una ubicación diferente al dispositivo, como podría ser un servidor. Esta medida de seguridad puede proporcionar protección temporal mientras la clave no está presente en el dispositivo; sin embargo, en algún momento se ha de proporcionar a la aplicación y se volverá accesible.

Mediante el uso de soluciones de hardware, se puede obtener un enfoque más sólido para proteger los datos de los usuarios root. Los fabricantes de dispositivos pueden implementar soluciones de hardware que limiten el acceso a determinados tipos de contenido como pueden ser el almacenamiento de confianza relacionado con NFC para la cartera de Google o DRM para la reproducción de vídeo.

Por último, cabe destacar que la clave de cifrado completo del sistema de archivos se protege mediante la contraseña del dispositivo. Por este motivo, la modificación del sistema operativo o el gestor de arranque del dispositivo no será suficiente para obtener acceso a los datos del usuario en caso de robo o pérdida sin disponer de la contraseña del mismo.

2.3.8 Cifrado del sistema de ficheros

A partir de la versión Android 3, se proporciona la capacidad de cifrado completo del sistema de archivos, por lo que todos los datos de usuario se pueden cifrar en el kernel.

De la versión Android 5.0 en adelante, se permite el cifrado de disco completo. Este tipo de cifrado utiliza una sola clave para proteger toda la partición de usuario (userdata) de un dispositivo, esta clave se protege mediante la contraseña del dispositivo. En el arranque del dispositivo, se solicitará la contraseña del mismo con la finalidad de proporcionar acceso al disco, de otra manera, no será accesible.

En Android 7.0, se incluye una mejora sobre el cifrado del sistema de ficheros incluyendo la posibilidad de cifrado basado en archivos. Esta funcionalidad permite que archivos diferentes

sean cifrados con distintas claves pudiendo así bloquearse y desbloquearse de modo independiente.

2.3.9 Protección con contraseña

La protección mediante contraseña es otra de las medidas de seguridad del sistema operativo, mediante la activación de esta funcionalidad, el sistema verificará una contraseña proporcionada por el usuario antes de permitir el acceso al dispositivo. Esta contraseña será, además, la que proteja la clave criptográfica usada para el cifrado del sistema de ficheros.

Para aumentar el nivel de seguridad, es posible la configuración del administrador del dispositivo para requerir el uso de contraseña y/o definir reglas de complejidad de la misma.

2.3.10 Administración de dispositivos

Android incluye asistencia para aplicaciones empresariales. Android 2.2 y versiones posteriores incluyen la API de administración de dispositivos Android (Android Device Administration API,). Esta API proporciona características de administración de dispositivos a nivel de sistema. Gracias a esta API, aplicación de correo del sistema operativo mejora la compatibilidad con Exchange posibilitando aplicar directivas de contraseñas (incluyendo tanto contraseñas alfanuméricas como PIN) en todos los dispositivos. Además, los administradores adquieren la facultad de borrado remoto (restauración los valores predeterminados de fábrica) para teléfonos perdidos o robados.

Estas API también están disponibles para su uso por parte de proveedores de aplicaciones de terceros dedicadas a soluciones de administración de dispositivos.

2.3.11 Seguridad en las aplicaciones - Elementos de aplicaciones

Tal y como se ha comentado anteriormente, Android es un sistema operativo para dispositivos móviles basado en kernel de Linux que proporciona una plataforma de código abierto.

Las aplicaciones de Android están desarrolladas sobre la plataforma Java en su mayor parte, para su ejecución se hace uso de la máquina virtual Java. Sin embargo, también es posible el desarrollo de aplicaciones para el sistema operativo en código nativo (C o C++). En ambos casos, para la instalación de las mismas se realizará a partir de un archivo con la extensión .apk.

Los principales aspectos a tener en cuenta en la creación de aplicaciones para Android son:

- **AndroidManifest.xml**: El fichero AndroidManifest.xml es el archivo de control que proporciona al sistema información acerca de qué hacer con los componentes de nivel superior - específicamente servicios, receptores de difusión y proveedores de

contenido descritos a continuación - en una aplicación. En este fichero se especifica qué permisos son necesarios para la aplicación. La consulta de este fichero es de vital importancia desde el punto de vista de la seguridad ya que se pueden observar comportamientos inadecuados como la solicitud de permisos que no procedan para algún tipo de aplicación.

- **Actividades:** Una actividad se describe generalmente como el código de una sola tarea centrada en el usuario. Normalmente incluye mostrar una interfaz al usuario, pero no es estrictamente necesario, algunas actividades nunca muestran interfaces de usuario. Normalmente, una de las actividades de la aplicación es el punto de entrada a una aplicación.
- **Servicios**: Un servicio es un cuerpo de código que se ejecuta en segundo plano. La ejecución del mismo se puede realizar en su propio proceso o bien en el contexto del proceso de otra aplicación. A través de llamadas a procedimientos remotos, otros componentes tienen la posibilidad de "enlazar" a un servicio e invocar sus métodos.
  Un ejemplo de servicio podría ser un reproductor multimedia: incluso cuando el usuario abandona la interfaz del reproductor, es muy probable que desee que la música siga reproduciéndose. La funcionalidad de mantener la música en marcha incluso cuando se ha completado la interfaz de usuario se implementa a través de un servicio.
- **Receptor de difusión** (**BroadcastReceiver):** Un BroadcastReceiver es un objeto que se crea una instancia cuando el sistema operativo u otra aplicación emite un mecanismo IPC conocido como intención. Gracias a esta funcionalidad, se hace posible que una aplicación registre un receptor para un mensaje y cambie su funcionamiento. Por ejemplo, una aplicación podría registrar un receptor de mensaje cuando el sistema entre en batería baja y activar su modo de ahorro de energía.

2.3.12 El modelo de permisos de Android: acceso a APIS protegidas

Todas las aplicaciones en Android se ejecutan en una Sandbox que ya ha sido objeto de estudio en apartados anteriores. Por defecto, una aplicación en Android solamente tiene acceso a un conjunto limitado de recursos del sistema. El sistema administra el acceso de las aplicaciones a los recursos, si se usan de un modo incorrecto o malicioso, podrían afectar negativamente a la experiencia de usuario, a la red o a los datos en el dispositivo.

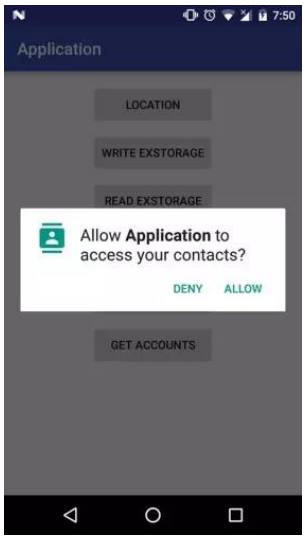
Las restricciones anteriores, se implementan de muchos modos diferentes. En algunos casos, existe limitación de acceso a algunas funcionalidades por la falta de una API que proporcione acceso a la funcionalidad sensible. Por ejemplo, no existe API que permita una manipulación directa de la SIM. La separación de roles, así como el aislamiento de aplicaciones, proporcionan una medida de seguridad en algunos casos. En otros casos, las API

confidenciales están diseñadas para ser usadas por aplicaciones de confianza y protegidas a través de permisos.

Las API protegidas incluyen: Datos de ubicación (GPS), conexiones de red/datos y funciones de la cámara, bluetooth, de telefonía y SMS/MMS.

Los recursos anteriores solamente son accesibles a través del sistema operativo. Para usar las APIS protegidas en el dispositivo, la aplicación debe definir los recursos que necesita en su manifiesto. Todas las versiones a partir de Android 6.0 utilizan un modelo de permisos en tiempo de ejecución. Si un usuario solicita una característica de una aplicación que requiere una API protegida, el sistema muestra un cuadro de diálogo solicitando al usuario que deniegue o permita el permiso. En la Ilustración 5 se muestra el modo a través del cual Android solicita un permiso concreto.

Ilustración 5. Solicitud de permisos Android



(Pandeli, 2016)

Un usuario puede ver y modificar, si así lo desea, los permisos asignados a una aplicación a través de la configuración del dispositivo.

Las aplicaciones no podrán hacer uso de una característica protegida no declarada en el manifiesto de la aplicación, ya que, de ser así, el sistema lanzará una excepción de seguridad. Para evitar evadir la comprobación de permisos, esta se aplica en el nivel más bajo posible de la estructura Android.

Los permisos predeterminados del sistema se pueden consultar a través de la página oficial de desarrolladores Android (Android Developers, n.d.-b). Las aplicaciones también tienen la

posibilidad de declarar sus propios permisos para que otras los usen, estos permisos no se enumeran en la ubicación anterior.

Al definir un permiso, el atributo protectionLevel indica al sistema cómo se debe informar al usuario de las aplicaciones que requieren el permiso o quién puede tenerlo. Los detalles acerca de la creación y el uso de permisos específicos de la aplicación se describen en la página oficial de desarrolladores Android.(Android Developers, n.d.-c)

Existe una serie de capacidades del dispositivo, como la capacidad de enviar intenciones de difusión por SMS, que no son accesibles por aplicaciones de terceros, pero pueden ser utilizadas por aplicaciones preinstaladas por el fabricante. Estos permisos utilizan el permiso signatureOrSystem.

2.3.13 Cómo entienden los usuarios las aplicaciones de terceros

Android se esfuerza por dejar claro a los usuarios cuando están interactuando con aplicaciones de terceros e informar al usuario de las capacidades o permisos que tienen esas aplicaciones. Antes de que una aplicación sea instalada, el usuario puede conocer los permisos que ésta solicita posibilitándole además su aceptación o denegación. Una vez la aplicación se encuentra instalada en el sistema, no se vuelve a solicitar al usuario que confirme ningún permiso.

Existen muchas razones para mostrar los permisos de una aplicación antes de su instalación, por ejemplo, cuando el usuario desea revisar la información de ésta obteniendo datos del desarrollador y las funcionalidades que ofrece para poder así determinar si se adecúa a sus necesidades y expectativas y compararla fácilmente con otras alternativas.

2.3.14 Comunicación entre procesos

Los procesos se pueden comunicar haciendo uso de cualquiera de los mecanismos tradicionales de tipo UNIX como pueden ser los sockets locales o las señales. Es importante tener en cuenta que, aun así, los permisos de Linux seguirán siendo de aplicación.

Android también proporciona nuevos mecanismos IPC:

- **Enlazador(binder)**: Un mecanismo ligero de llamada a procedimientos remotos basado en capacidades diseñado para un alto rendimiento al realizar llamadas dentro de un proceso y entre procesos.
- **Servicios:** Los servicios (discutidos anteriormente) pueden proporcionar interfaces directamente accesibles mediante enlazador.
- **Intenciones:** Una intención es un objeto de mensaje simple que representa el deseo o "intención" de hacer algo. Un ejemplo de intención podría ser el siguiente: una

aplicación desea mostrar una página web, por lo que expresa su "Intención" de ver la dirección URL creando una instancia de Intención y entregándola al sistema. El sistema localiza algún otro fragmento de código (en este caso, el navegador) que sabe cómo controlar esa intención y la ejecuta. Las intenciones también se pueden utilizar para transmitir eventos interesantes (como una notificación) en todo el sistema.

- **ContentProviders**: Un ContentProvider es un almacén de datos que proporciona acceso a los datos del dispositivo. El ejemplo más utilizado para este concepto es el ContentProvider que proporciona acceso al listado de contactos. Mediante el uso de un ContentProvider, una aplicación puede acceder a los datos expuestos por otras, del mismo modo, una aplicación puede exponer sus propios datos mediante la definición de sus propios ContentProviders

Si bien es posible implementar IPC utilizando otros mecanismos como sockets de red, estos son los marcos IPC de Android recomendados. Se ha de promover que los desarrolladores de Android sigan las buenas prácticas con la finalidad de proteger los datos de los usuarios y evitar la introducción de vulnerabilidades de seguridad.

2.3.15 APIs sensibles a los costos

Una API sensible a los costes es cualquier función que puede generar un coste al usuario o la red. Android ha colocado API sensibles a los costos en el listado de API protegidas controladas por el sistema operativo. Las aplicaciones de terceros que soliciten el uso de estas APIs han de obtener permiso explícito por parte del usuario, entre estas APIs se encuentran: SMS/MMS, telefonía, red/datos, facturación dentro de la aplicación, acceso NFC, etc.

Android 4.2 añade más control sobre el uso de SMS. Si una aplicación intenta enviar SMS a un código corto que hace uso de servicios premium y por lo tanto podría causar cargos adicionales al usuario, el sistema mostrará una notificación y será el usuario el que permita o deniegue la acción.

2.3.16 Acceso a la tarjeta SIM

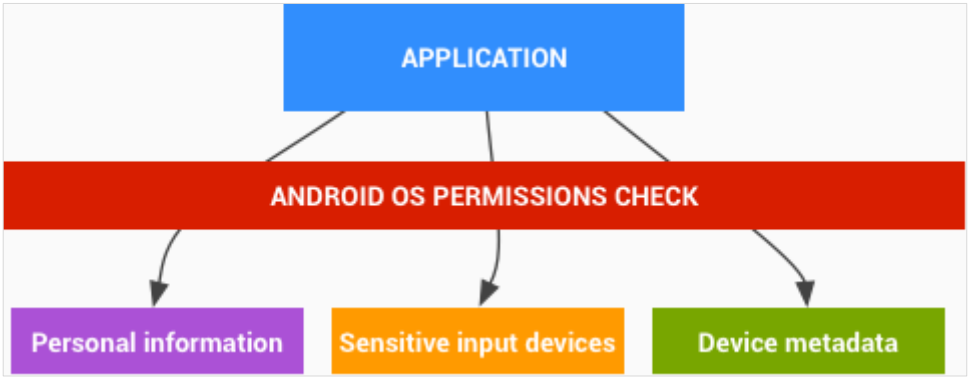
Las aplicaciones de terceros no disponen de acceso de bajo nivel a la tarjeta SIM. El sistema operativo es el encargado de la gestión de todas las comunicaciones con la tarjeta SIM, incluido el acceso los contactos almacenados en la misma.

Tampoco está permitido el acceso por parte de aplicaciones de terceros a los comandos AT, ya que éstos son manejados exclusivamente por la capa de interfaz de radio (RIL). El RIL no proporciona API de alto nivel para estos comandos.

2.3.17 Información personal

Entre el conjunto de API protegidas de Android también se encuentran aquellas que proporcionan acceso a los datos de usuario. Con el uso de un dispositivo, las aplicaciones de terceros acumulan datos de usuario entre sus datos. Tal y como se pone de manifiesto en la Ilustración 6, las aplicaciones que decidan compartir esta información han de hacerlo a través de API protegidas.

Ilustración 6. El acceso a los datos confidenciales de los usuarios solo está disponible a través de API protegidas



(Android, n.d.-b)

Los proveedores de contenido del sistema que sean susceptibles de contener datos personales o datos identificables de personas como por ejemplo contactos o calendario, se han de crear con permisos claramente identificables. Esta granularidad proporciona al usuario información clara acerca de la información proporcionada a la aplicación. Si una aplicación de terceros desea acceder a estos recursos, debe recabar el consentimiento correspondiente durante su instalación. Si el permiso es asignado, la aplicación podrá ser instalada y dispondrá de acceso a los datos solicitados durante el tiempo que esté instalada en el dispositivo.

Aquellas aplicaciones que recojan datos personales, por defecto deben tener restringido el acceso a esos datos a su aplicación. Si una aplicación comparte datos con otra a través de IPC, puede facilitar permisos al mecanismo IPC aplicado por el sistema operativo.

2.3.18 Dispositivos de entrada de datos confidenciales

Los dispositivos Android normalmente disponen de funcionalidades de entrada que manejan datos confidenciales y permiten a las aplicaciones interactuar con el entorno, algunos ejemplos de estos pueden ser el micrófono, la cámara o el GPS. El usuario ha de proporcionar su deseo explícito de uso de estos mecanismos mediante el uso de permisos del sistema operativo si desea que los mismos sean accesibles por aplicaciones de terceros. Tras la instalación de una aplicación de terceros, el instalador solicitará al usuario que solicite permiso al sensor por su nombre.

2.3.19 Metadatos del dispositivo

Otra de las líneas de trabajo en cuanto a la seguridad proporcionada por el sistema operativo, es la restricción de acceso a datos que, no siendo intrínsicamente sensibles, son susceptibles de revelar indirectamente datos o sesgos del usuario, sus preferencias y el modo en el que hacen uso de sus dispositivos.

Para la implementación de la medida descrita, se restringe el acceso por parte de las aplicaciones a los registros del sistema operativo, el historial de navegación, el número de teléfono o la información de identificación de hardware / red. En el caso de que una aplicación desee acceder a alguno de estos datos, necesita permiso explícito para ello.

2.3.20 Autoridades de certificación

Android incluye un conjunto de entidades de certificación del sistema instalado, que son de confianza en todo el sistema. Antes de Android 7.0, los fabricantes de dispositivos podrían modificar el conjunto de CA enviados en sus dispositivos. Sin embargo, los dispositivos que funcionen 7.0 y superiores tendrán un conjunto uniforme de CA del sistema, ya que ya no se permite la modificación por parte de los fabricantes de dispositivos.

Para agregarse como una nueva CA pública al conjunto de acciones de Android, la CA debe completar el proceso de inclusión de Mozilla CA y, a continuación, presentar una solicitud de característica contra para que la CA se agregue a la CA de Android de stock establecida en el proyecto de código abierto (AOSP) de Android.

Todavía hay CA que son específicos del dispositivo y no deben incluirse en el conjunto principal de CA AOSP, como los CA privados de los operadores que pueden ser necesarios para acceder de forma segura a los componentes de la infraestructura del operador, como las puertas de enlace SMS/MMS. Se recomienda a los fabricantes de dispositivos que incluyan los CA privados solo en los componentes/aplicaciones que necesitan confiar en estos CA.

2.3.21 Firma de aplicaciones

Mediante la firma de código, los desarrolladores pueden identificarse como autor de la aplicación y realizar actualizaciones de la misma sin crear interfaces y permisos complicados. Todas las aplicaciones que se ejecuten en la plataforma Android deben estar firmadas por el desarrollador. El almacén de aplicaciones Google Play rechazará la subida de aplicaciones que estén sin firmar, así mismo, el instalador de paquetes denegará la instalación el dispositivo Android.

La firma de aplicaciones es un contrato que cierra por una parte la confianza que Google tiene con el desarrollador y por otra la confianza que el desarrollador tiene con su aplicación. Por

una parte, los desarrolladores pueden garantizar mediante la firma la integridad en la distribución de su aplicación y pueden rendir cuentas por el comportamiento de su aplicación.

Para colocar una aplicación en el espacio aislado de aplicaciones Android, esta ha de estar firmada. El certificado de firma define qué id de usuario está asociado a qué aplicación; diferentes aplicaciones se ejecutan bajo diferentes ID de usuario. Además, la firma garantiza que una aplicación no puede tener acceso a ninguna otra excepto a través de IPC bien definido.

Cuando se instala una aplicación (.apk) en un dispositivo, el administrador de paquetes comprueba que el fichero se ha firmado correctamente con el certificado incluido en ese apk. En el caso de que el certificado (concretamente, la clave pública del certificado) coincida con la clave utilizada para firmar cualquier otro apk en el dispositivo, el nuevo apk tiene la opción de especificar en su archivo manifest que compartirá un UID con las otras apk firmadas con ese certificado.

Las solicitudes pueden ser firmadas por un tercero (OEM, operador, mercado alternativo) o autofirmadas.

Android proporciona a los desarrolladores la generación de certificados autofirmados de firma de código. Las solicitudes no tienen que ser firmadas por una autoridad central. Según se facilita en la documentación oficial, en el momento de desarrollo de este estudio, no realiza la verificación de CA para certificados de aplicación.

Las aplicaciones también tienen la posibilidad de declarar permisos de seguridad en el nivel de protección signature, restringiendo el acceso solo a las aplicaciones firmadas con la misma clave mientras mantienen distintos UIDs y entornos limitados de aplicaciones.

2.3.22 Verificación de aplicaciones

Android 4.2 y posteriores versiones, admiten la verificación de la aplicación. Esta funcionalidad permite al usuario habilitar "Verificar aplicaciones" y de este modo forzar que las aplicaciones sean evaluadas antes de la instalación por un verificador de aplicaciones. Mediante este mecanismo, el usuario será advertido si intenta la instalación una aplicación que potencialmente perjudicial. La verificación de aplicaciones puede bloquear la instalación de las mismas en el caso de que el comportamiento de la misma sea calificado como potencialmente dañino.

2.3.23 Gestión de derechos digitales

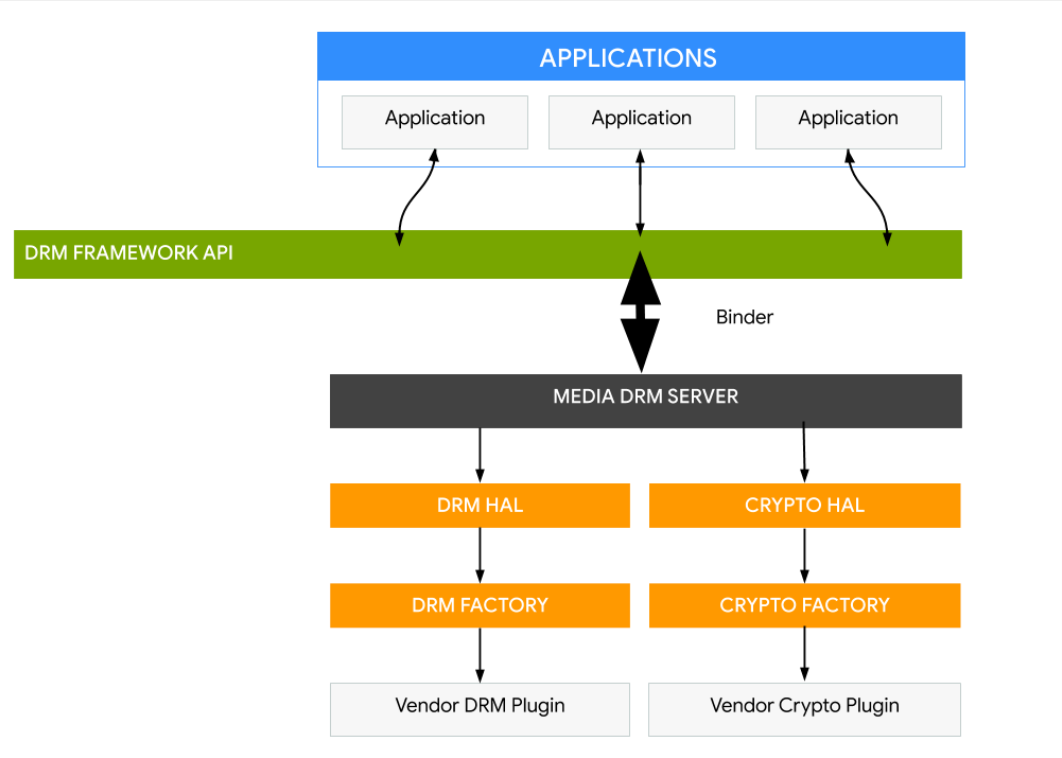
El sistema operativo proporciona un framework DRM que provee a las aplicaciones de un mecanismo para la administración de contenido protegido por derechos de autor de acuerdo

con la licencia que tengan asociada. Este framework soporta gran variedad de esquemas DRM, el fabricante del dispositivo será el que establezca los esquemas soportados por el mismo. En la Ilustración 7 se muestra la arquitectura de gestión de derechos digitales.

El marco DRM de Android se implementa en dos capas arquitectónicas:

- La API de DRM framework, que está disponible a las aplicaciones a través del framework de aplicaciones de Android y, para las aplicaciones estándar, se ejecuta en la máquina Java.
- Un mánager nativo de DRM, que implementa el framework DRM y expone una interfaz para DRM plugins con la finalidad del manejo de derechos y el descifrado e interpretación de varios esquemas DRM.

Ilustración 7. Arquitectura de gestión de derechos digitales en la plataforma Android



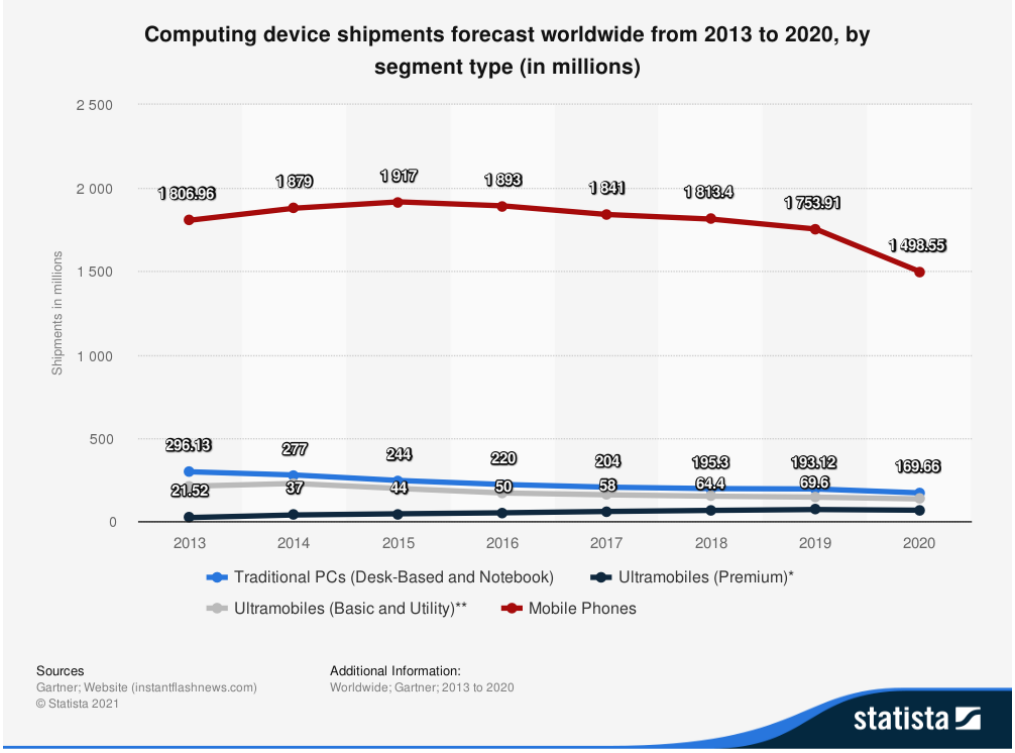
(Android, n.d.-b)

2.4 Malware en Android

Android es uno de los sistemas operativos con mayor presencia en los dispositivos a nivel mundial. Visto anteriormente la representación del sistema Android frente a otros sistemas operativos móviles y dados los datos de ventas de dispositivos por tipo presentes en la

siguiente gráfica obtenida de un estudio de Gartner, una de las consultoras de TI más conocidas a nivel global, y realizada por Statista, Android será presumiblemente el sistema operativo con mayor presencia a nivel mundial (Alsop, n.d.). En la Ilustración 8 se facilitan los datos facilitados de ventas de dispositivos a nivel mundial.

Ilustración 8. Ventas de dispositivos a nivel mundial

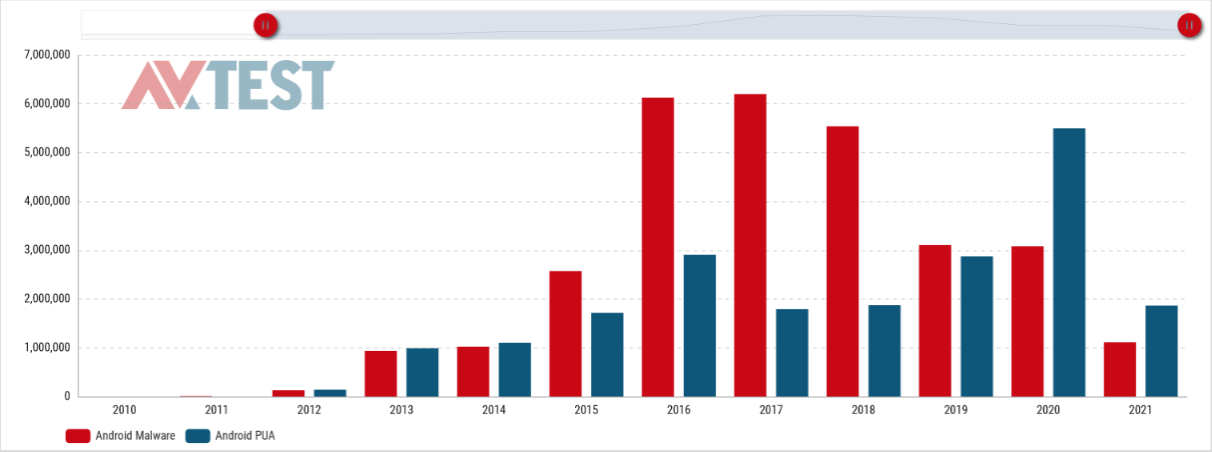


(Alsop, n.d.)

El alto número de dispositivos con este sistema operativo, lo hace muy atractivo para los desarrolladores de malware ya que se puede acceder a un gran número de dispositivos muy fácilmente. Si a esto le sumamos la facilidad de programar en lenguajes como Java o C++, nos encontramos ante un caldo de cultivo para el malware.

La presencia de malware en Android se representa en el siguiente gráfico gracias a datos ofrecidos por el portal Av-Atlas de Av-Test, (AV-TEST, n.d.). En la Ilustración 9, se representan el malware detectado en Android en los últimos 11 años, así como las aplicaciones potencialmente no deseadas. El malware detectado ha caído estos dos últimos años siendo aún muy significativo, mientras que las PUA han sufrido un incremento progresivo que se ha visto enormemente afectado en el año 2020 seguramente por el efecto COVID19.

Ilustración 9. Malware y PUAs en Android



(AV-TEST, n.d.)

Si se estudian otros datos ofrecidos por la compañía, las tendencias de las últimas dos semanas, tal y como se muestra en se puede observar que las aplicaciones no deseadas representan un porcentaje importantísimo frente al malware (Ilustración 10 e Ilustración 11).

Ilustración 10. Familias de malware Android

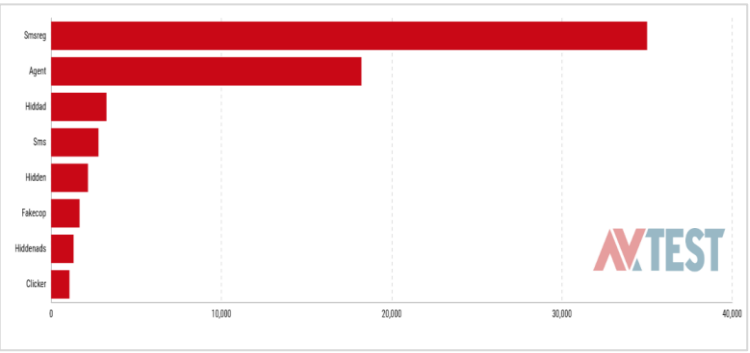
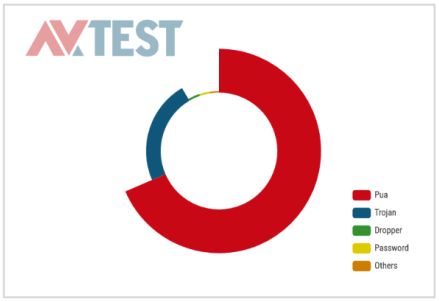


Ilustración 11. Categorías de malware



(AV-TEST, n.d.)

2.4.1 Definición y objetivos

En una de las webs oficiales relacionadas con el sistema operativo(*Google Play*, n.d.), se ofrece una definición precisa y simple del concepto malware.

El malware como cualquier programa que podría poner en riesgo a un usuario, los datos de un usuario o un dispositivo. El malware incluye, pero no se limita a, aplicaciones potencialmente dañinas (PHAs), binarios, o modificaciones del marco de trabajo.

Por lo general, tiene uno de los siguientes objetivos:

- Comprometer la integridad de un dispositivo.
- Obtener el control de un dispositivo.
- Habilitar el acceso por control remoto para que un atacante acceda, use o explote de otro modo un dispositivo infectado.
- Obtener datos personales o credenciales.
- Difundir spam o comandos desde el dispositivo infectado con la finalidad de afectar a otros dispositivos o redes.
- Defraudar al usuario

2.4.2 Protecciones en el dispositivo Android

Google Play Protect incluye capacidades en el dispositivo que ayudan a mantener seguros los dispositivos y los datos. Estos servicios en el dispositivo se integran con componentes basados en la nube que permiten a Google insertar actualizaciones que mejoran constantemente su funcionalidad.

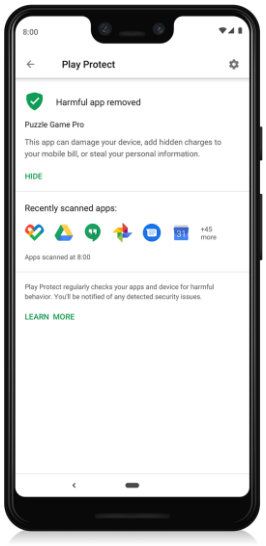
Servicios de escaneo de aplicaciones potencialmente dañinas

Google Play Protect hace uso de los servicios de verificación de aplicaciones basados en la nube para analizar y determinar si las aplicaciones son o no potencialmente dañinas (PHAs). En su propósito de facilitar seguridad al usuario, Google Play Protect también realiza análisis a los dispositivos Android en busca de pruebas de PHAs.

Play Protect dispone de distintos tipos de escaneo:

Escaneo diario de PHA

Los dispositivos son escaneados una vez al día, si se encuentra una PHA, una notificación pide al usuario que la quite. En los casos en que la PHA no tenga ningún beneficio para los usuarios, Google Play Protect puede eliminar la PHA de los dispositivos afectados y bloquear futuras instalaciones. Mediante este tipo de escaneo se descubre el 93% de las PHAs. Mediante Google Play se puede ver el histórico de ejecuciones de este tipo de escaneo en el dispositivo



Análisis de PHA bajo demanda

A petición del usuario, el dispositivo se pone en contacto con los servidores de Google para obtener la información más reciente y escanea todas las aplicaciones del dispositivo. Si se descubre una aplicación dañina, Google Play Protect notifica al usuario que tome medidas o tome medidas en su nombre.

Escaneo PHA sin conexión

Un poco más de una cuarta parte de las nuevas instalaciones de PHA se producen cuando un dispositivo está sin conexión o ha perdido conectividad de red. Para abordar esto, Google Play Protect tiene un análisis sin conexión, lo que ayuda a evitar que se instalen aplicaciones potencialmente dañinas conocidos sin conexión. Cuando el dispositivo recupera la conectividad de red, se somete a un análisis completo.

Más de 300 millones de instalaciones de PHA están bloqueadas anualmente por el escaneo sin conexión de Google Play Protect.

Desactivar automáticamente las PHAs

Algunas PHAs son más dañinas que otras y se tratan de manera diferente dependiendo de la clasificación PHA. Los PHAs más dañinos se eliminan automáticamente del dispositivo, mientras que las PHAs menos graves se desactivan. Una aplicación deshabilitada es inutilizable, pero permanece en el dispositivo haciendo que se puedan recuperar los datos asociados a ella. Cuando una aplicación se deshabilita automáticamente, se notifica al usuario de modo que pueda eliminarla o habilitarla de nuevo.

Apelación para desarrolladores de PHA

Los desarrolladores de aplicaciones Google pueden apelar el bloqueo de sus aplicaciones si Google Play Protect las ha marcado como dañinas, antes deberá revisar las directrices de Google para desarrollar aplicaciones móviles y la política de Google sobre software no deseado.

Buscar mi dispositivo

La función “buscar mi dispositivo” está habilitada de forma predeterminada en todos los dispositivos Android con Android 4.4 y superior y requiere instalaciones adicionales. Ayuda a los usuarios a mantener sus dispositivos seguros incluso cuando el dispositivo se pierde. Esta opción permite la localización, el uso e incluso el bloqueo o borrado remoto de los datos de dispositivo.

Si el dispositivo no está conectado a internet y no puede reportar su localización, se mostrará la última conocida. Además, mediante el timeline de localización los usuarios pueden ver el historial de localizaciones de su dispositivo.

SafetyNet APIs

SafetyNet permite a los dispositivos aportar información relacionada con la seguridad a los servicios basados en la nube de Google. Esto puede incluir información sobre eventos de seguridad, registros, configuraciones y otros detalles relacionados con la seguridad.

Las API de SafetyNet permiten a los desarrolladores mejorar la seguridad de las aplicaciones al proporcionar un conjunto de servicios que ayudan a proteger las aplicaciones contra amenazas de seguridad, incluida la manipulación de dispositivos, direcciones URL incorrectas, aplicaciones potencialmente dañinas y usuarios falsos.

Certificado

La API de Certificado ayuda a evaluar la seguridad y compatibilidad de los entornos Android en los que se ejecutan las aplicaciones. Puede usar esta API para analizar los dispositivos que han instalado la aplicación.

reCAPTCHA

reCAPTCHA es un servicio gratuito que utiliza un motor avanzado de análisis de riesgos para proteger su aplicación del spam y otras acciones abusivas.

Navegación segura

La API de navegación segura protege a los usuarios contra las amenazas al permitir que las aplicaciones comprueben las URL con listas de recursos web no seguros, como sitios de ingeniería social (sitios de phishing y engañosos), y sitios que alojan PHAs o software no deseado. Cuando los usuarios intentan visitar un recurso web no seguro, su navegador compatible con navegación segura muestra una advertencia.

Navegación segura es una característica de suscripción que los desarrolladores pueden usar para proteger a los usuarios de sitios host de phishing y PHA en la aplicación.

2.4.3 Categorías de malware

Google Play Protect categoriza el malware atendiendo a la siguiente clasificación.

Backdoor o puerta trasera.

Código o programa que habilita la ejecución de operaciones no deseadas, potencialmente dañinas y controladas a distancia en un dispositivo.

Fraude de facturación

Código o programa que realiza cargos económicos automáticamente al usuario de forma deliberadamente engañosa. Este tipo de malware se divide en tres grandes grupos:

- **Fraude por SMS (SMS fraud):** programa que se ejecuta en el dispositivo y realiza cargos a los usuarios por enviar SMS premium sin consentimiento. Este tipo de malware disfraza sus actividades de SMS imposibilitando al usuario la visualización de las advertencias de divulgación o mensajes SMS del operador móvil notificando al usuario de cargos o confirmando suscripciones.

  Algunos códigos, a pesar de que técnicamente revelan el comportamiento de envío de SMS, introducen comportamientos adicionales que se adaptan al fraude de SMS. Algunos ejemplos son ocultar partes de un acuerdo de divulgación al usuario, hacerlas ilegibles y suprimir condicionalmente los mensajes SMS del operador móvil informando al usuario de los cargos o confirmando una suscripción.

- **Fraude de llamadas (Call fraud):** programa que realiza cobros a los usuarios haciendo llamadas a números de tarificación especial sin el consentimiento del usuario.
- **Fraude de peaje (Toll fraud):** Código que engaña a los usuarios para que suscriban o compren contenido a través de su factura de teléfono móvil.

  En esta categoría se incluyen cualquier tipo de facturación a excepción de los definidos anteriormente SMS y llamadas premium. Algunos ejemplos de este tipo de malware incluyen la facturación directa del operador, el punto de acceso inalámbrico (WAP) y la transferencia de tiempo de transmisión móvil. El fraude WAP es uno de los tipos más frecuentes de fraude de peaje, puede incluir el engaño a los usuarios para que hagan clic en botón cargado en una ventana transparente en segundo plano. Al realizar

la acción, se iniciará una suscripción periódica y el SMS o email de confirmación se oculta o secuestra para evitar que el usuario sea consciente de la transacción financiera.

Stalkerware (Spyware comercial)

Código o programa que transmite información personal desde el dispositivo sin previo aviso o consentimiento y no muestra una notificación persistente de que esto está sucediendo.

Las aplicaciones de stalkerware suelen transmitir datos a una entidad distinta del proveedor PHA. Formas legítimas aceptables de estas aplicaciones pueden ser las utilizadas por los padres para rastrear a sus hijos. Sin embargo, estas aplicaciones no se pueden usar para realizar un seguimiento de un adulto (un cónyuge, por ejemplo) sin su conocimiento o permiso a menos que se muestre una notificación persistente mientras se transmiten los datos.

Denegación de servicio (DoS)

Código o programa que, sin el conocimiento del usuario, ejecuta ataques del tipo denegación de servicio (DoS) o forma parte de un ataque de denegación de servicio distribuido contra otros sistemas o recursos.

Aplicaciones que descargan código malicioso

Código o programa que en sí mismo no es potencialmente dañino, pero descarga otros PHAs. Se puede clasificar una aplicación en este tipo si el código puede ser un descargador hostil si:

- Hay razones para creer que fue creado para difundir PHAs y ha descargado PHAs o contiene código que podría descargar e instalar aplicaciones; o al menos el 5% de las aplicaciones descargadas por ella son PHAs con un umbral mínimo de 500 descargas de aplicaciones observadas (25 descargas PHA observadas).
- Los principales navegadores y aplicaciones para compartir archivos se consideran descargadores hostiles si impulsan las descargas sin intervención del usuario o las descargas PHA se inician por sí mismas.

Amenazas para dispositivos no Android (Non-Android threat)

Código que contiene non-Android threats. Estas aplicaciones no pueden causar daño al usuario o dispositivo Android, pero contienen componentes que son potencialmente dañinos para otras plataformas.

Phishing

Código o programa que se hace pasar por ser un origen confiable, solicita las credenciales de autenticación o información de facturación o de tarjetas de crédito de un usuario y envía los datos obtenidos a un tercero.

Esta categoría de malware también es aplicable se aplica al código que intercepta la transmisión de credenciales de usuario en tránsito.

Los objetivos comunes de phishing incluyen números de tarjetas de crédito, credenciales bancarias y credenciales de cuentas online como pueden ser las correspondientes a redes sociales y juegos.

Abuso de privilegios

Este tipo de código o programas comprometen la integridad del sistema rompiendo el entorno limitado de la aplicación, obteniendo privilegios elevados o cambiando o deshabilitando el acceso a las funciones principales relacionadas con la seguridad.

Algunos ejemplos son:

- Una aplicación que infringe el modelo de permisos de Android o roba credenciales (como tokens de OAuth) de otras aplicaciones.
- Aplicaciones que impiden la detención de ejecución o desinstalación.
- Una aplicación que deshabilita SELinux.
- Las aplicaciones de escalada de privilegios que rootean los dispositivos sin autorización.

Ramsomware

Código o programa que actúa tomando el control parcial o total de un dispositivo o datos existentes en un dispositivo y exige al usuario la realización de un pago o acción para liberar el control.

Algunos son conocidos por cifrar los datos existentes en el dispositivo y exigir el pago para descifrar los datos y / o aprovechar las características de administración del dispositivo para que no pueda ser eliminado por un usuario sin privilegios. Algunos ejemplos son:

- Bloquear a un usuario en el dispositivo y exigir dinero para restaurar el control del usuario.
- Cifrar datos en el dispositivo y exigir el pago, aparentemente para descifrar los datos.

- Aprovechar las características del administrador de directivas de dispositivos y bloquear la eliminación por parte del usuario.

Aplicaciones de rooteo

Pertenecen a esta categoría aquellas aplicaciones que rootean el dispositivo. Existe una diferencia los programas de rooteo no malicioso y los que sí lo son: los de rooteo malintencionado no informan al usuario de la acción que van a realizar, sino que además también es posible que ejecuten adicionalmente otras acciones que se aplican a diferentes categorías de PHA.

Spam

Código o programa que realiza el envío de mensajes no solicitados a los contactos del usuario o hace uso del dispositivo como retransmisor de spam por correo electrónico.

Spyware

Código o programa que transmite datos personales a un tercero fuera del dispositivo sin previo aviso o consentimiento.

La transmisión de cualquiera de los siguientes datos de una manera inesperada para el usuario es suficiente para que una aplicación sea considerada spyware:

- Lista de contactos
- Fotos u otros archivos de la tarjeta SD o que no son propiedad de la aplicación
- Contenido del correo electrónico del usuario
- Registro de llamadas
- Registro de SMS
- Historial web o marcadores de navegador del navegador predeterminado
- Información de los directorios /data/ de otras aplicaciones.

Aquellas acciones que se puedan considerar como espionaje al usuario, también pueden catalogarse como spyware. Por ejemplo, grabar llamadas de audio o grabación realizadas al teléfono o robar datos de la aplicación.

Troyanos

Código que parece ser benigno, pero que en realidad realiza acciones indeseables contra el usuario.

Este tipo de malware se utiliza normalmente en combinación con otras categorías de PHA. Un troyano consta de dos componentes: uno inocuo y el otro dañino que además permanece oculto. Un ejemplo sencillo de este tipo de malware sería un juego instalado en el dispositivo que, en segundo plano y sin el consentimiento del usuario, envía mensajes SMS premium.

Poco comunes (Uncommon)

Si una aplicación es nueva y rara, puede ser clasificada como uncommon si Google Play Protect en el caso de que no disponga de suficiente información para marcarla como seguras. Este hecho no quiere decir que la aplicación sea necesariamente dañina, pero sin más revisión tampoco se pueden clasificar como seguras.

Software no deseado móvil (MUwS)

Google define el software no deseado (MUwS) como aplicaciones que no son estrictamente malware, pero son perjudiciales para el ecosistema de software. El software no deseado (MUwS) se hace pasar por otras aplicaciones o recopila al menos una de las siguientes opciones sin el consentimiento del usuario:

- Dirección de correo electrónico principal
- Número de teléfono del dispositivo
- Información sobre las aplicaciones instaladas
- Información sobre cuentas de terceros

2.4.4 Familias de malware

Las distintas categorías de malware son a su vez clasificadas en familias. En la **¡Error! No se encuentra el origen de la referencia.**, se proporciona una tabla con las diferentes categorías de código y algunas de las familias más comunes de malware de cada una de ellas (Gurdip Kaur & Arash Habibi Lashkari, 2021).

Tabla 2. Familias más comunes de malware por categoría

Categoría	Descripción / comportamiento	Familias más comunes
Adware	Muestra ventanas emergentes no deseadas o molestas al usuario.	gexin, batmobi, ewind, shedun, pandaad, appad, dianjin, gmobi, hummingbird, mobisec, loki, kyhub, y adcolony
Backdoor (Puerta trasera)	Explota el dispositivo de forma encubierta ocultándose en segundo plano.	mobby, kapuser, hiddad, dendroid, levida, fobus, moavt, androrat, kmin, pyls, y droidkungfu
File Infector	Contamina todo tipo de ficheros especialmente las apk.	leech, tachi, commplat, gudex, y aqplay

Categoría	Descripción / comportamiento	Familias más comunes
PUA (Aplicación potencialmente maliciosa)	Actúa como una interrupción no deseada de las actividades normales realizadas por el dispositivo.	apptrack, secapk, wiyun, youmi, scamapp, utchi, cauly y umpay
Ransomware	Encripta ficheros y directorios del dispositivo y pide una recompensa para poder obtener la clave de descifrado de los archivos.	congur, masnu, fusob, jisut, koler, lockscreen, slocker y smsspy
Riskware	Supone un riesgo para explotar vulnerabilidades existentes en el dispositivo.	badpac, mobilepay, wificrack, triada, skymobi, deng, jiagu, smspay, smsreg, y tordow
Scareware	Hace que el usuario descargue aplicaciones maliciosas sembrando en él el miedo e incitándole a descargarlas	avpass, mobwin y fakeapp
Spyware	Roba información del dispositivo y la envía a un servidor remoto.	spynote, qqspy, spydealer, smsthief, spyagent, spyoo, smszombie y smforw
Trojan	Se comporta como un suplantador en segundo plano que sigue robando información del dispositivo. Se representa de varias formas, como trojan-banker, trojan-dropper, trojan-sms y trojan-spy.	gluper, lotoor, rootnik, guerrilla, gugi, hqwar, obtes, y hypay

2.5 Configuraciones seguras en Android

En la red existen multitud de páginas disponibles para los usuarios Android en las cuales se facilitan indicaciones para securizar los dispositivos Android. Algunas de ellas, como la guía de Innoves, (Innoves, 2021) facilitan al usuario una serie de pinceladas básicas sobre la seguridad en el sistema operativo. También el conocido portal Andro4All dispone de una guía con este fin, lo más interesante de esta guía es que destaca la importancia de las acciones del usuario a la hora de mantener la seguridad “El mejor antivirus para Android eres tú” (Alcántara, 2020)

Además de las anteriormente citadas, para el estudio de configuraciones seguras del sistema operativo, se ha realizado una selección de guías publicadas para este fin por diversas empresas y organismos de seguridad como el CCN-CERT, ESET o el CIS.

Cabe destacar que la mayoría de ellas sugieren al usuario las mismas acciones a configurar para securizar sus dispositivos, si bien es cierto, algunas de ellas tienen propuestas individuales que resultan de gran interés, como por ejemplo la guía ESET que destaca la importancia del borrado completo de los datos del dispositivo en caso de darle una segunda vida tras una venta o cambio de usuario. O la guía de CCN - STIC 453 G, que a pesar de

especializarse para Android 9 se puede extender a otras versiones del sistema operativo, destaca la importancia del uso de gestores de contraseñas para poder mantener contraseñas de calidad.

Entre las medidas de seguridad más destacables se encuentran:

- Descargar aplicaciones solamente desde repositorios confiables, sospechar de las aplicaciones que exigen demasiados permisos, pueden tener objetivos maliciosos / limitar los permisos asignados a las aplicaciones y desinstalar aquellas aplicaciones que no se usen. Revisar periódicamente los permisos de las aplicaciones instaladas.
- Configurar acceso y bloqueo del dispositivo mediante contraseña, PIN, patrón o medidas biométricas usando cuando corresponda contraseñas de calidad y con una longitud mínima de 8 caracteres. En el caso de usar patrón para el desbloqueo, deshabilitar el trazado del este.
- Mantener el dispositivo actualizado sistema operativo/aplicaciones
- Proteger mediante PIN la tarjeta SIM
- Crear copias de seguridad: contactos, agenda, calendario y activar el cifrado de la información en el dispositivo
- Activar opciones de administración remota o usar programas como Android Device Manager (encontrar teléfono, borrado remoto, etc.)
- Desactivar los mecanismos como WiFi, Bluetooth, NFC cuando no se necesite
- Establecer bloqueo automático del dispositivo cuando no esté en uso y configurar el botón de encendido para tal fin.
- Evitar conexión a redes abiertas, en caso de utilizarlas, hacer que el dispositivo la elimine de la lista de redes.
- Configurar la cuenta de usuario de Google con contraseña robusta y única y habilitar un segundo factor de autenticación
- No rootear el dispositivo y deshabilitar las opciones de desarrollador.
- Activar el escaneo del dispositivo en busca de amenazas de seguridad
- Eliminar perfiles de invitado, no permitir añadir usuarios desde la pantalla de bloqueo y eliminar de ajustes rápidos opciones sensibles como WiFi, zona WiFi, Bluetooth, NFC

En el ANEXO III. COMPARATIVA GUIAS DE SEGURIDAD ANDROID se especifica una tabla con las propuestas de cada una de las guías.

2.6 Herramientas de seguridad antimalware en Android

Debido al incipiente uso de dispositivos Android y la cantidad de malware a la que está sometido el sistema operativo, muchas empresas, algunas de ellas dedicadas desde hace año a ofrecer soluciones de seguridad para otros sistemas operativos, han visto un nicho de mercado y han comenzado a ofrecer soluciones de seguridad para Android.

El primer antivirus para Android salió al mercado en 2008, poco después del lanzamiento del primer dispositivo con Android instalado. SMobile Systems, un desarrollador de soluciones de seguridad móvil fue el pionero con su producto VirusGuard. Sucesivamente, otras empresas fueron lanzando sus productos, algunas de ellas nuevas y otras viejas conocidas del mundo de la seguridad que decidieron especializarse o ampliar su abanico de productos ofreciendo también soluciones para este sistema operativo. Algunas de las empresas más conocidas que disponen de soluciones para móviles pueden ser McAfee, Kaspersky, AVG

El uso de este tipo de herramientas siempre ha sido un tema controvertido, pues existen retractores que argumentan que este tipo de herramientas únicamente fomenta el uso de recursos del sistema operativo y el consumo de batería, pero dudan de su eficacia de protección. Entre los detractores de los antivirus en Android, se encuentra Adrián Ludwig, el jefe de seguridad de Android, quien afirma en Julio de 2014 que los smartphones y tablets Android no necesitan un antivirus. Para él, el 99% de los usuarios no hallarán beneficio en instalar un antivirus en un smartphone o un tablet Android. El sistema operativo de Google ya cuenta con diferentes sistemas de seguridad que hacen que instalar un antivirus sea innecesario. Uno de estos sistemas es la propia tienda de aplicaciones Google Play.

Con este trabajo, se pretende aportar un grano de arena a esta decisión por lo que, en las conclusiones de este trabajo, se extraerá la opinión resultante del estudio realizado.

2.6.1 Técnicas de detección

El objetivo principal de este tipo de herramientas es detectar el malware para notificar al usuario y eliminarlo del dispositivo. Para la detección de amenazas se usan las siguientes técnicas: Verificación de firmas, verificación heurística y bloqueo de comportamiento.

Verificación de firmas

Mediante esta técnica, se establecen las características que llevan a un archivo a ser considerado o no un malware. Se verifican aspectos como: tamaño, secuencias binarias, etc. Cuando el archivo cumple con los criterios para considerarse malware, este se reconoce como tal y recibe una identidad con su firma respectiva. De este modo, la firma pasará a la lista de la herramienta.

Esta técnica de detección no siempre es la más eficiente, ya que no está incluido el malware 0-day y, por lo tanto, éste no se detectará.

Verificación Heurística

Se refiere a la capacidad de la herramienta de reconocer un malware sin contar con la "vacuna" específica en su contra. En el caso de la verificación heurística, se anticipa la aparición del virus, su acción es similar a los programas antispam. Este método de detección tiene una gran desventaja y es que genera una cantidad alta de falsos positivos.

La verificación por medio de esta técnica es más lenta. El proceso para buscar archivos con rasgos comunes al malware es completamente diferente a buscar elementos que ya se reconocen como virus en una base de datos y tampoco aporta detección de malware 0-day.

Bloqueo de Comportamiento

El bloqueo de comportamiento es la técnica que consiste en analizar las acciones sospechosas ejecutadas por algunos programas, con el objetivo de identificar posibles infecciones. De acuerdo con el modo de actuación de una aplicación, puede ser considerado malware y no permitir que su ejecución.

2.6.2 Características de las herramientas antimalware

Un programa antimalware está compuesto por dos módulos principales, el de control y el de respuesta, divididos a su vez cada uno de ellos en varias partes.

Módulo de control: proporciona a la herramienta la técnica verificación de integridad que hace posible el registro de cambios en los archivos ejecutables y las zonas críticas de almacenamiento interno. Se trata, de una herramienta preventiva que tiene como objetivo mantener y controlar los componentes de información de que no son modificados a menos que el usuario lo requiera.

Módulo de respuesta: este módulo proporciona la función de alarma. Siempre está presente y su trabajo es detener la acción del sistema ante la sospecha de la presencia de un virus informático. Además, informará de la situación a través de un aviso en pantalla. Algunos programas ofrecen la funcionalidad de erradicación del programa malicioso una vez detectado.

2.6.3 Funcionalidades

Las herramientas cada día son más sofisticadas y aportan una suite de funcionalidades más completa. Entre las funcionalidades que ofrecen este tipo de herramientas se pueden encontrar:

- **Control de aplicaciones**: función para la autorización, bloqueo o restricción del acceso de determinadas aplicaciones.
- **Copia de seguridad**: salvaguarda de datos personales en la tarjeta SD o mediante almacenamiento en la nube.
- **Bloqueo de llamadas**: posibilidad de bloquear llamadas de números desconocidos o de determinados números.
- **Asesor de privacidad (Privacy Advisor):** funciones para evaluar los datos recopilados por las aplicaciones basándose en autorizaciones, tráfico de datos y confianza merecida
- **Navegación segura**: protección contra páginas web maliciosas y/o contra páginas web de phishing
- **VPN**: utilización de una red privada virtual (Virtual Private Network) para proteger el tráfico de datos y navegar de forma anónima
- **Asesor/control de wifi**: Comprobación para detectar conexiones de wifi seguras o inseguras
- **Escáner de red**: ofreciendo qué otros dispositivos están conectados al mismo WiFi que el usuario.
- **Sistemas antirrobo**: con funcionalidades como el borrado remoto de datos o la localización del dispositivo.
- **Protección de identidad**: Comprueba si las direcciones de correo electrónico o cuentas del usuario han sido filtradas por terceros.

Algunas de las herramientas también incluyen funcionalidades más exclusivas como pueden ser la conexión con Android Wear OS para la conexión con los relojes inteligentes, monitorización de filtración de datos en la Dar Web u otras funciones como borrado seguro de ficheros.

Cabe indicar que la mayoría de las herramientas de protección, a pesar de ser gratuitas, tienen parte de sus funcionalidades bajo suscripción.

2.6.4 Herramientas antimalware en el mercado

Con objeto de realizar el estudio del que tiene propósito este TFM, se ha analizado el mercado de herramientas antimalware y se ha elegido un conjunto para realizar el análisis.

En la *Tabla 3. Características de herramientas comerciales* se puede encontrar la selección de herramientas antimalware seleccionadas para el estudio. Para la búsqueda y selección se han utilizado tanto páginas web de análisis de este tipo de herramientas, como análisis oficiales como los de la empresa AV Test(AV-TEST, n.d.).

En el ANEXO II. TABLA HERRAMIENTAS COMERCIALES ANTI-MALWARE se facilita una tabla equivalente a la presentada a continuación que aporta más datos como información de Play Store, versión necesaria de Android o si la herramienta dispone de características premium.

Como se puede observar la mayoría de las soluciones comerciales ofrecidas hoy en día proporcionan servicios adicionales como pueden ser sistemas antirrobo, control de aplicaciones, copias de seguridad, control parental o incluso VPN.

Tabla 3. Características de herramientas comerciales

Herramienta	Antirrobo	Asesor de privacidad	Asesor/control de wifi	Bloqueo de llamadas	Control de aplicaciones	Copia de seguridad	Navegación segura	VPN	Otros
Ahnlab V3 Mobile Security	No	Sí	Sí	No	Sí	No	Sí	No	Borrado seguro de ficheros
AVAST Mobile Security	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	
AVG Antivirus free	No	No	No	Sí	No	No	No	No	
Avira Antivirus Security	No	Sí	No	No	No	No	Sí	No	
AVL Mobile Security	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Filtro de mensajes
Bitdefender Mobile Security	No	Sí	No	Sí	Sí	Sí	Sí	No	Filtro de mensajes
ESET Mobile Security & Antivirus	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	
F-Secure Safe	Sí	Sí	No	No	Sí	No	Sí	Sí	Bloqueo de aplicaciones, Escáner de red, Protección de cámara y micrófono
GDATA Mobile Security	Sí	No	Sí	No	Sí	No	Sí	Sí	Salvaguarda de identidad, Privacidad de cuenta, Asesor de seguridad, WearON
Google Play Protect	Sí	Sí	No	No	Sí	No	Sí	No	Control parental
IKARUS mobile security	Sí	Sí	No	No	Sí	No	Sí	No	
Kaspersky internet security	No	No	No	No	Sí	No	No	No	
LINE Antivirus	Sí	Sí	No	No	No	No	Sí	No	Alertas de seguridad
Malwarebytes	Sí	No	No	Sí	Sí	No	Sí	No	
McAfee Mobile Security	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	
Norton 360	No	Sí	Sí	Sí	No	No	Sí	No	Monitorización Dark Web
SECURION OnAV	No	No	Sí	No	Sí	No	Sí	Sí	Navegador de incognito
Total, AV	No	No	No	No	No	No	No	No	Detección de rooteo, protección de mensajes, protección de red y control parental
Trend Micro Mobile Security	Sí	Sí	Sí	Sí	Sí	No	Sí	No	

2.7 Trabajos relacionados

Uno de los trabajos con mayor nivel de similitud al que se está desarrollando es el realizado como TFM en 2016 por Oscar Villanueva Pascual “Malware en Android y medidas de protección”(Villanova Pascual, 2016). En este trabajo, con el fin de alcanzar el objetivo principal, se infecta una máquina virtual con software dañino para obtener la eficacia de una serie de herramientas.

Relacionados con el malware existen infinidad de artículos y proyectos que estudian el malware para este sistema operativo e incluso tratan temas como los distintos métodos de análisis del mismo (estático, heurístico, uso de machine learning, etc.). Este tipo de proyectos ha sido clave en el desarrollo de la parte de malware, así como de la obtención de distintos proyectos que pudiesen facilitar una base de datos de malware con la que desarrollar el estudio y aportar distintos puntos de vista de cómo afrontar el análisis de malware o diseñar la metodología a seguir. Algunos ejemplos son los citados a continuación;

- Android malware family classification and analysis: Current status and future directions(Alswaina & Elleithy, 2020): este ha sido uno de los artículos de más provecho para el desarrollo del presente TFM ya que ha aportado una información valiosa en cuanto a diferentes datasets de malware. En este artículo, se clasifica una selección de trabajos existentes sobre análisis de malware en base a tres dimensiones: tipo de análisis, características y metodologías y técnicas. Además, facilita información de los conjuntos de datos que se utilizan habitualmente y destaca las limitaciones identificadas en el conjunto de artículos y publicaciones estudiados, los retos y las futuras direcciones de investigación en relación con familias de malware Android
- Kharon dataset: Android malware under a microscope (Kiss et al., 2016): el trabajo define una colección de malware para Android llamada Kharon que ofrece una representación de la diversidad de tipos de malware. Con este conjunto de datos, se disecciona manualmente cada malware invirtiendo su código, se ejecuta en un smartphone controlado y monitorizado para extraer su comportamiento preciso y finalmente se resume su comportamiento mediante representaciones gráficas obteniendo un conocimiento preciso de su código y acciones maliciosas.
- Drebin: Effective and Explainable Detection of Android Malware in Your Pocket (Arp et al., 2014): en el artículo se propone un método ligero de detección de malware para Android que opera directamente en el smartphone denominado

Drebin. El método realiza análisis estático de las aplicaciones de Android e identifica automáticamente patrones típicos de actividades maliciosas que pueden presentarse al usuario.

Siguiendo la misma línea anterior se encuentra el trabajo de un compañero de Unir "Detección y Clasificación de Malware con el sistema de Análisis de Malware Cuckoo"(Rivera, 2018) : el trabajo desarrolla un piloto experimental con el fin de evaluar la exactitud que presenta un enfoque de clasificación de malware utilizando Cuckoo SandBox. De él se han obtenido sobre todo datos generales sobre el malware y herramientas.

El presente trabajo sigue la misma línea que el primero de los citados en esta sección. Desde la publicación del trabajo de Oscar Villanueva Pascual hasta el momento han surgido grandes cambios en la arquitectura del sistema, muchos de ellos mejorando la línea de seguridad del sistema operativo que son reflejados en este TFM. Además, se tienen en cuenta todas las actualizaciones disponibles del sistema operativo hasta la fecha. Por otra parte, se plantea un modelo de análisis de las herramientas seleccionadas distinto incluyendo en el estudio por una parte análisis del momento en el que el malware es detectado por las herramientas facilitadas y, por otra parte, teniendo en cuenta un enfoque innovador en cuanto a la selección y segmentación al dataset de malware tratado, en este caso el dataset estará segmentado por niveles de dificultad de detección y siempre se tratará de malware actual y disponible en la Play Store. Así mismo, se facilita una comparativa de guías de configuraciones seguras en Android y un análisis de colecciones de malware disponibles para la realización de estudios similares.

3 Herramientas analizadas en el estudio

De las herramientas analizadas en el capítulo anterior, se realizará un estudio de un conjunto de ellas. Debido a que las valoraciones de las aplicaciones son muy similares en la mayoría de los casos y no existen valoraciones extremas, se seleccionarán aquellas participantes en el estudio atendiendo a los siguientes criterios:

- Aquellas en las que su porcentaje de reseñas con respecto a las descargas realizadas se encuentre en los extremos, seleccionando los casos extremos tanto por arriba como por abajo, 5 de cada extremo. Con este criterio entrarían en el análisis: ESET Mobile Security & Antivirus, Trend Micro Mobile Security, Kaspersky internet security, AVG Antivirus free, AVAST Mobile Security, Avira Antivirus Security, Total AV, LINE Antivirus, McAfee Mobile Security y AVL Mobile Security.
- Atendiendo al número de componentes o mejoras adicionales, aquellas que mayor y menor número de ellos tengan. Al igual que en el caso anterior se seleccionan 5 de cada uno de los extremos obteniendo como subconjunto muestra el siguiente: F-Secure Safe, GDATA Mobile Security, Ahnlab V3 Mobile Security, ESET Mobile Security & Antivirus, Trend Micro Mobile Security, Kaspersky internet security, AVG Antivirus free, AVAST Mobile Security, McAfee Mobile Security, AVL Mobile Security.

Combinando los dos conjuntos obtenidos con los criterios anteriormente citados, se tiene el conjunto de las trece herramientas que participarán en el estudio. En la Ilustración 12, se muestran los nombres y logos de las herramientas que participarán en el estudio.

Ilustración 12. Herramientas de seguridad a estudiar

4 Malware utilizado en el estudio

En este capítulo se muestra el conjunto de malware que se utilizará para el desarrollo del estudio, así como las consideraciones tenidas en cuenta para su selección.

4.1 Colecciones de malware

Existen diversas colecciones de malware recopiladas por diferentes compañías que pueden ser utilizadas para la realización de estudios(Kouliaridis et al., 2020):

- Contagio mobile mini-dump (Contagio, n.d.): Es un repositorio de muestras de malware móvil. Contiene unas 189 muestras de malware recopiladas en 2010.
- MalGenome (Zhou & Jiang, 2012): disponible desde 2012, contiene 1.260 muestras de malware recopilado entre agosto 2010 y octubre de 2011 categorizado en 49 familias. Este proyecto ha sido discontinuado en diciembre de 2015.
- VirusShare (VirusShare, n.d.): Contiene muestras de malware para Android desde 2012 y se actualiza regularmente. Es muy utilizado en el mundo de la investigación y el acceso es por invitación.
- Drebin (Arp et al., 2014): Comprende al menos 5.560 muestras de malware de 179 familias diferentes recogidas entre agosto de 2010 y octubre de 2012. Drebin es uno de los conjuntos de datos más populares en los estudios de malware a pesar de no haber sido actualizado desde hace casi 10 años.
- DroidBench (DroidBench, n.d.): Es un conjunto de aplicaciones que implementan diferentes tipos de fugas de datos. Las muestras no son casos reales de malware, solamente están pensadas para evaluar el análisis de herramientas. Actualmente, el repositorio consta de 120 aplicaciones cuya tarea principal es la fuga de datos.
- PRAGuard (Maiorca et al., 2015): Colección de 10.479 muestras de malware recopiladas entre 2010 y 2011
- AndroZoo (Allix et al., 2016): es una colección de aplicaciones recopiladas de diferentes fuentes entre las que se encuentra Google Play. El proyecto se encuentra en actualización continúa contando en la actualidad con más de 12 millones de muestras.
- Kharon (Kiss et al., 2016): Comprende sólo 7 casos de malware de entre 2012 y 2016.
- Android Adware and General Malware Dataset (AAGM) (Tsiatsikas et al., 2015): Se compone de a más de 1.900 aplicaciones (250 aplicaciones de adware, 150

malware en general y 1.500 aplicaciones benignas). Los datos se han recogido entre 2015 y 2016 aunque no existen datos claros sobre el malware ni adware.

- AMD (*Android Malware Dataset*, n.d.): El sitio web en el momento del desarrollo de este TFM se encuentra sin disponibilidad. Es un conjunto de datos público que contiene 24.553 muestras categorizadas en 135 variedades entre 71 familias de malware. Las muestras están fechadas desde 2010 hasta 2016.
- Curated Android for Researching Malware APK Set (CARMA) de ElevenPaths(*CARMA*, n.d.): Proporciona un conjunto gratuito de muestras de malware, adware y otros archivos potencialmente peligrosos para el sistema operativo Android. Solamente puede ser utilizado con fines de investigación o académicos previa aceptación por parte de la empresa. La última actualización es de 2019

Debido principalmente a la cantidad de datos, así como a la actualización de los mismos, las dos mejores opciones para el desarrollo del piloto serían VirusShare y AndroZoo. Se usará una muestra AndroZoo para el desarrollo del proyecto por ser esta la más actualizada.

4.2 Selección de malware para el estudio

Haciendo uso del proyecto elegido para la realización del trabajo, AndroZoo, se ha obtenido la lista de posibles apk. El formato del listado de aplicaciones ofrecidas por el proyecto, así como el detalle del mismo se detalla en el ANEXO IV. PROYECTO ANDROZOO.

Sobre este listado inicial, se ha obtenido un subconjunto suficientemente significativo para el trabajo teniendo en cuenta las apk introducidas desde el 1 de enero de este año hasta la fecha de extracción (25 de mayo) obteniendo un listado de 56960 elementos susceptibles de análisis. Se reducirá aún más este subconjunto seleccionando aquellas aplicaciones descargadas de Play Store, que hayan sido analizadas y marcadas como malware por al menos un antivirus en este año, con estos nuevos datos, los registros descienden hasta 6583 muestras.

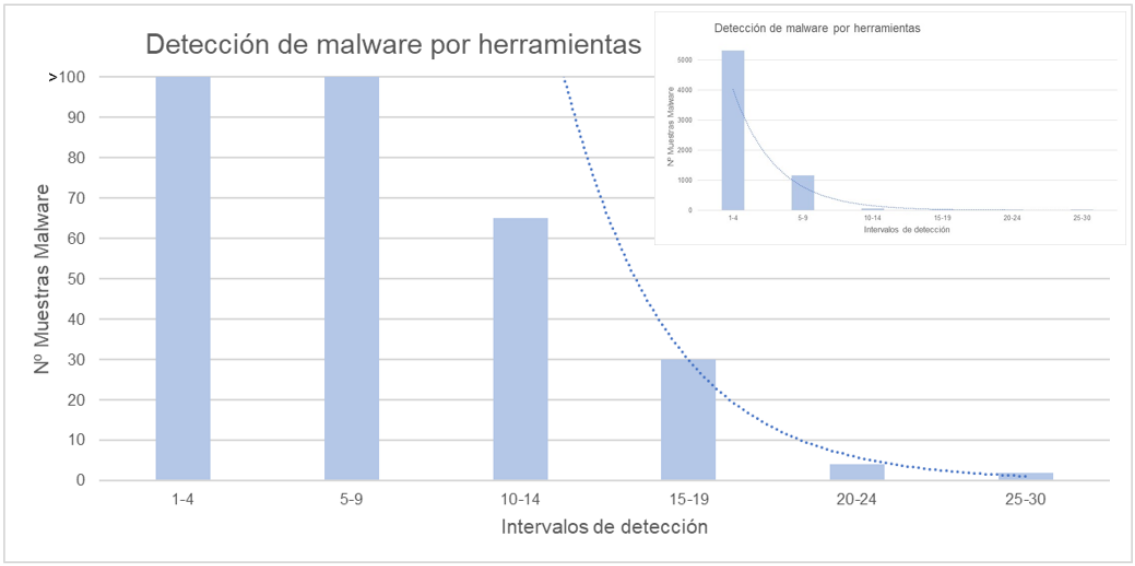
Como todavía existe una cantidad muy elevada de muestras para realizar el estudio – se pretende utilizar unas 30 muestras – el siguiente paso es extraer un subconjunto de ellas. Para ello, se va a utilizar un criterio que tiene relación directa con la eficacia de una herramienta antimalware y es la capacidad de detección. Se usa el campo vt_detection de la base de datos para la selección del malware. Tras un estudio del subconjunto de las más de seis mil muestras, se divide el campo detección en intervalos y se obtiene el

número de muestras de malware detectados por ese número de herramientas. Los datos obtenidos son los mostrados en la Tabla 4 y gráfico (Ilustración 13. Gráfico de análisis de detección de malware AndroZOO) facilitados a continuación.

Tabla 4. Intervalos de herramientas que detectan malware AndroZOO

Intervalos de detección (malware detectado por nº herramientas)	Nº muestras detectadas
1-4	5325
5-9	1157
10-14	65
15-19	30
20-24	4
>=25	2

Ilustración 13. Gráfico de análisis de detección de malware AndroZOO



Tal y como se puede observar en el gráfico, los datos siguen una tendencia invertida asimétrica positiva. Con esto extrapolamos también que la mayor parte de muestras de programas maliciosos son detectadas por únicamente de 1 a 4 herramientas de malware, lo cual saca a la luz el gran problema de seguridad existente.

Para la selección del malware, teniendo en cuenta el objetivo de obtener una muestra para el estudio que sea útil para probar la eficacia de las herramientas, se agruparán los intervalos anteriores de modo que se obtengan tres conjuntos, cada uno de ellos contiene la agrupación de dos de los intervalos anteriores:

- **Malware fácilmente detectable**: contendrá aquellas muestras de malware detectadas por un gran número de herramientas (más de 20 herramientas). Este conjunto contiene 6482 muestras
- **Malware difícilmente detectable**: detectado por un número medio de herramientas (entre 10 y 20 herramientas). Este conjunto contiene 95 muestras
- **Malware prácticamente indetectable**: detectado por muy pocas herramientas (de 1 a 9). Constaría de 6 muestras de malware.

Para la realización del estudio se ha fijado un número de muestras de 30 por lo que se elegirán 12 muestras de los dos intervalos de mayor numero de muestras y la totalidad de las muestras disponibles, seis, en el malware prácticamente indetectable. La selección de muestras dentro de los intervalos es totalmente aleatoria. El conjunto definitivo viene representado en la tabla del ANEXO V- MALWARE SELECCIONADO.

Dado que el proyecto proporciona además aplicaciones no maliciosas, se aprovechará para seleccionar una muestra de ellas e introducirlas en los test, de este modo, se podrían obtener falsos positivos o nuevos positivos, en caso de que una muestra diese positivo en uno de los test habría que realizar el análisis para ver si realmente se trata de un falso positivo o no

5 Objetivos concretos y metodología de evaluación

A lo largo de este capítulo, se define el objetivo del trabajo, así como la metodología que se ha de seguir para el correcto desarrollo del piloto experimental del cual es objeto este TFM.

5.1 Objetivo general

El objetivo del presente trabajo es la evaluación de herramientas de seguridad antimalware, teniendo en cuenta tanto la efectividad de las mismas - en cuanto a la detección de malware - como la no afectación de las mismas sobre el rendimiento del dispositivo con la finalidad de poder dar una respuesta sobre si merece o no la pena la instalación de las mismas al usuario final de los dispositivos Android. La instalación de este tipo de herramientas siempre ha sido un asunto muy controvertido por lo que se pretende estudiar si es realmente beneficioso para un usuario su instalación o, por el contrario, la aportación es mínima.

Para la realización de la evaluación, se han de definir por un lado las herramientas de estudio, las cuales serán un subconjunto de las presentadas en el capítulo dedicado a tal fin. Por otra parte, se definirá un conjunto de malware con el que se infectará el dispositivo y seguidamente se aplicarán las metodologías definidas a continuación con el objetivo de obtener los resultados de la evaluación.

5.2 Objetivos específicos

Se fijan dos objetivos específicos que ayudarán a formar la valoración general de cada una de las herramientas seleccionadas para el estudio:

- Valorar su efectividad en cuanto a la detección. Esta tarea se llevará a cabo mediante la ejecución de la metodología de análisis de efectividad que se definirá más adelante.
- Valorar su rendimiento haciendo uso de la metodología de valoración de rendimiento definida a continuación.

5.3 Metodología del trabajo

Como ya se ha comentado anteriormente, dado que son dos los aspectos a tener en cuenta sobre las herramientas estudiadas, se definirá una metodología híbrida que aunará tanto el estudio de la eficacia de las herramientas como el estudio de la eficiencia de las mismas en cuando a consumo de recursos del dispositivo.

Antes de comenzar se ha de disponer de un entorno de trabajo, se trabajará con un dispositivo real, en concreto se tratará de un Xiaomi Redmi Note 5 pro que será únicamente utilizado para el fin del estudio. El dispositivo no dispondrá de tarjeta SIM, aunque sí que tendrá conexión a internet para el posible uso por parte de los motores antivirus instalados mediante WiFi.

En la Tabla 5 se detallan las especificaciones técnicas del dispositivo utilizado para el estudio.

Tabla 5. Especificaciones del dispositivo

Nombre del dispositivo	Xiaomi Redmi
Modelo	Redmi Note 5
Versión MIUI	MIUI Global 11.0.3
Versión de Android	Android 9 (Pie)
RAM	4 GB
Almacenamiento interno	64 GB
CPU	Octa-core Max 1.8 GHz

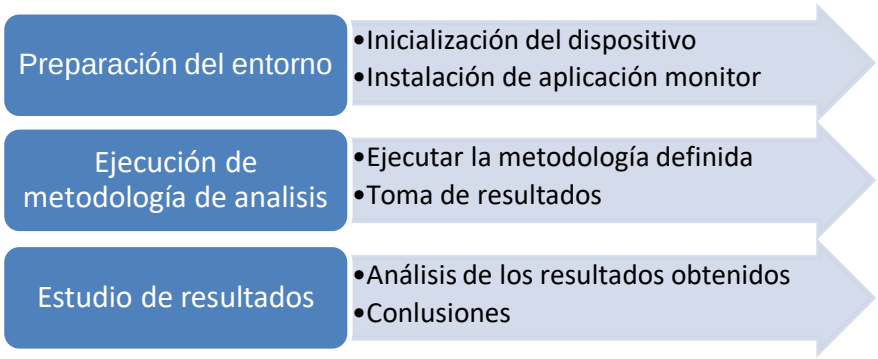
Tal y como se puede observar, el dispositivo cuenta con una capa de personalización propia del fabricante (MIUI 11) que corre una versión 9 de Android. A pesar de no tratarse de un dispositivo de última generación, pues ya tiene unos 3 años, es un dispositivo que a día de hoy sigue contando con unas prestaciones aceptables y con mecanismos de seguridad actuales como la huella de seguridad. Por otra parte, corre una versión de Android muy habitual pues según el estudio presentado en de abril 2020 estaba presente en el 31,30% de los dispositivos mientras que la siguiente versión solamente lo estaba en el 8% de ellos (Ilustración 1.Distribución de versiones Android). Además, esta versión se correspondería con la más actual en el caso de utilizar una máquina virtualizada como OsBoxes.

Se instalará una aplicación de análisis de rendimiento y se realizará una prueba de análisis de rendimiento que servirá como referencia. Después de haber valorado varias alternativas, se ha decidido utilizar 3C All-in-One Toolbox (3C, n.d.) por ser una de las más completas teniendo disponibles todos los controles necesarios para el estudio del piloto – dispone tanto de monitor de CPU, de RAM, de batería.

Antes de la prueba de cada una de las herramientas estudiadas, se volverá el equipo a valores de fábrica con la finalidad de que antiguas instalaciones de otras herramientas no afecten negativamente a los datos obtenidos en la muestra.

En la Ilustración 14, se representa gráficamente el proceso definido anteriormente.

Ilustración 14. Trabajos a realizar



5.3.1 Metodología de análisis de herramienta

La eficacia de la herramienta se medirá usando la tasa de aciertos (verdaderos positivos detectados). Para el análisis se tendrá en cuenta el número de resultados obtenidos tanto en tiempo real como en otros momentos. Inicialmente se descomprimirá el malware en el dispositivo, si la herramienta no es capaz de realizar esta detección se realizará un análisis manual que determine de nuevo la tasa de aciertos obtenida. Si aun así el malware no es detectado, se realizará la instalación del malware en el sistema y se obtendrán los resultados de detección. Posteriormente con la aplicación instalada en el dispositivo se lanzará un nuevo análisis para complementar la estadística si fuese necesario. En cada una de las detecciones, se anotarán los resultados teniendo en cuenta el momento en el que se producen.

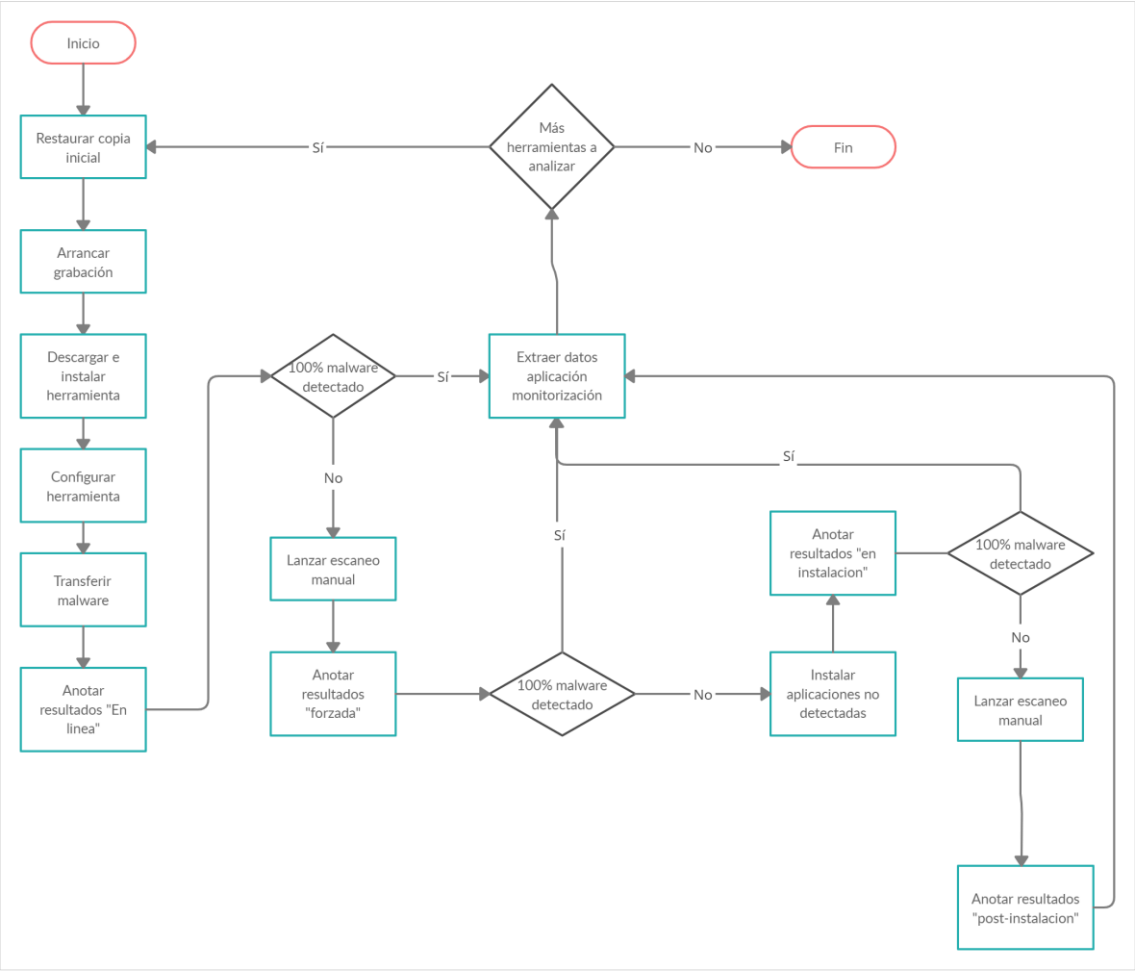
La metodología a utilizar para el análisis de efectividad de cada una de las herramientas a estudiar será la que sigue.

1. Restaurar sistema de fábrica e instalar las herramientas necesarias instaladas.
2. Arrancar la grabación del entorno de ejecución
3. Descargar e instalar la herramienta a analizar
4. Configurar la herramienta a analizar activando la protección.
5. Transferir el conjunto de prueba de malware.
6. Anotar resultados de detección “en línea”
7. Si se ha detectado el 100% del malware, ir a paso 16.
8. Realizar un escaneo manual
9. Anotar resultados de detección “forzada”
10. Si se ha detectado el 100% del malware, ir a paso 16.
11. Instalar las aplicaciones que no hayan sido detectadas.
12. Anotar los resultados de alertas “en instalación”
13. Si se ha detectado el 100% del malware, ir a paso 16.

14. Realizar un escaneo
15. Anotar resultados de detección post-instalación.
16. Extraer los datos obtenidos por la aplicación de rendimiento.
17. Si no es la última herramienta a analizar, volver al paso 1

La Ilustración 15 representa el diagrama de flujo para la metodología definida.

Ilustración 15. Metodología de análisis de herramientas



5.4 Métricas o Indicadores

Los indicadores de rendimiento a utilizar para realizar el estudio de las distintas herramientas a evaluar serán los siguientes:

- CPU utilizada.
- Batería consumida.

Para la valoración de la eficacia de las distintas herramientas se utilizarán los siguientes indicadores:

- Porcentaje de verdaderos positivos detectado en tiempo real
- Porcentaje de verdaderos positivos detectado en escaneo forzado
- Porcentaje de verdaderos positivos detectado en instalación
- Porcentaje de verdaderos positivos detectado en post-instalación

6 Resultados del estudio

A lo largo de este capítulo se presentan los resultados obtenidos en el estudio del comportamiento de las 13 herramientas seleccionadas ante la detección de los programas maliciosos elegidos para participar en el estudio. Se mostrará así mismo, el impacto en el rendimiento del sistema de la instalación de una herramienta de este tipo.

6.1 Efectividad de las herramientas

En el ANEXO VI. RESULTADOS EFICACIA se encuentran los resultados obtenidos del estudio realizado.

Cabe destacar, que la herramienta Total AV ha tenido que ser eliminada del estudio al no ofrecer ningún tipo de protección antimalware de modo gratuito.

A continuación, se presentan los análisis realizados de los datos obtenidos en el estudio.

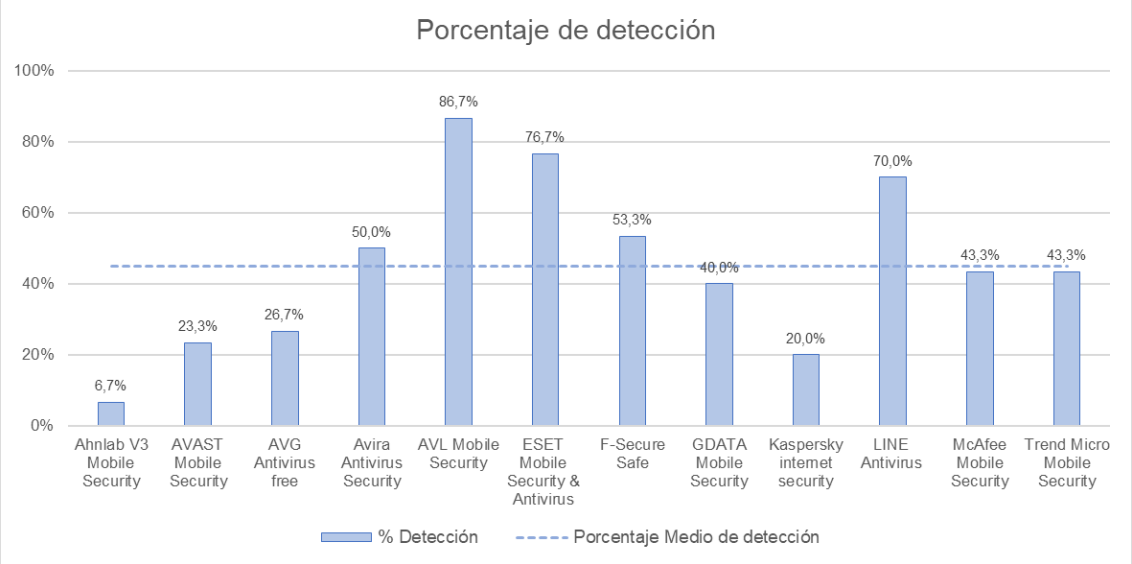
Como era de esperar, debido a las muestras elegidas para el estudio, ninguna de las herramientas participantes ha sido capaz de obtener el 100% de detección. Si bien es cierto que algunas de las herramientas han obtenido valores notables (iguales o superiores al 70%), como pueden ser AVL Mobile, ESET o Line, otras han arrojado unos resultados muy por debajo de la media de detección frente a sus competidoras, como pueden ser Ahnlab o Kaspersky ambas con porcentajes de detección del malware inferiores o iguales al 20%. La media de detección por parte de las herramientas es del 45%.

A continuación, en la Tabla 6, se presentan de manera simplificada los datos obtenidos del estudio en cuanto a número de muestras detectadas y porcentaje de detección. Se muestran tanto resultados totales como los obtenidos en cada uno de los intervalos definidos. La Ilustración 16, ofrece una representación gráfica de los porcentajes totales de detección de cada una de las herramientas participantes teniendo como punto de referencia el porcentaje medio de detección obtenido en el estudio.

Tabla 6. Datos de detección de herramientas en el estudio

	Número de muestras detectadas				% detección sobre total de muestras			
	Detectado	Malware prácticamente indetectable	Malware difícilmente detectable	Malware Facilmente detectable	Detectado	Malware prácticamente indetectable	Malware difícilmente detectable	Malware Facilmente detectable
Ahnlab V3 Mobile Security	2	0	0	2	7%	0%	0%	33%
AVAST Mobile Security	7	1	1	5	23%	8%	8%	83%
AVG Antivirus free	8	1	1	6	27%	8%	8%	100%
Avira Antivirus Security	15	1	8	6	50%	8%	67%	100%
AVL Mobile Security	26	10	10	6	87%	83%	83%	100%
ESET Mobile Security & Antivirus	23	7	10	6	77%	58%	83%	100%
F-Secure Safe	16	1	9	6	53%	8%	75%	100%
GDATA Mobile Security	12	2	4	6	40%	17%	33%	100%
Kaspersky internet security	6	0	4	2	20%	0%	33%	33%
LINE Antivirus	21	5	12	4	70%	42%	100%	67%
McAfee Mobile Security	13	0	7	6	43%	0%	58%	100%
Trend Micro Mobile Security	13	1	8	4	43%	8%	67%	67%

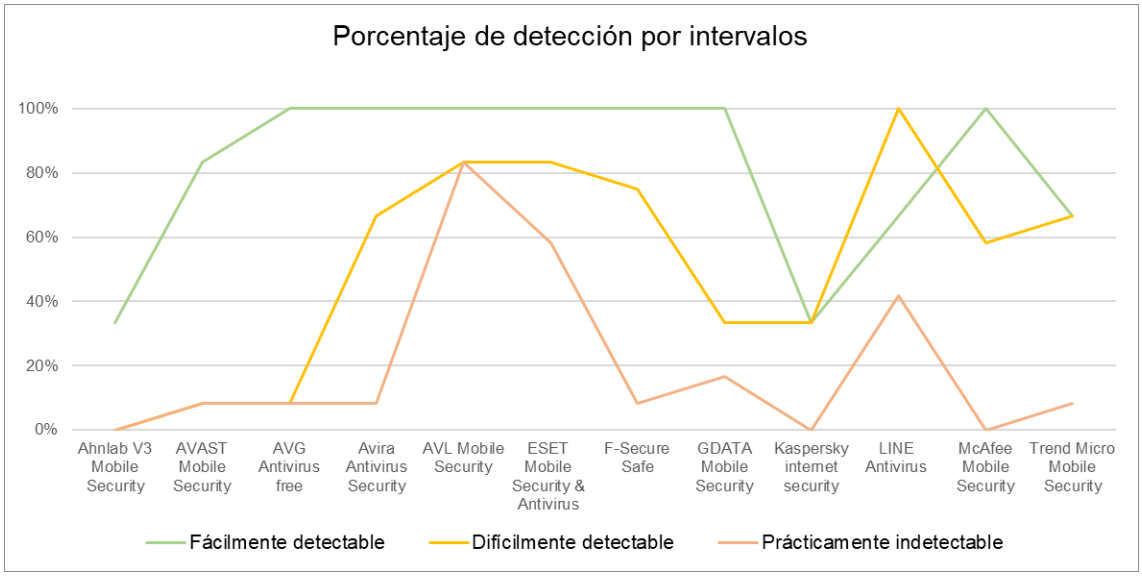
Ilustración 16. Porcentaje de detección de herramientas en el estudio



Por otra parte, tal y como representa gráficamente la Ilustración 17, si se tienen en cuenta los intervalos o rangos en los que ha sido clasificado el malware seleccionado para el estudio, se obtiene que la mayor parte de las herramientas han detectado todo el malware del intervalo fácilmente detectable y más de la mitad de ellas han detectado al menos la mitad del malware perteneciente al rango difícilmente detectable. Cabe destacar la eficiencia de AVL Mobile Security y ESET Mobile Security en la detección del malware del intervalo prácticamente indetectable ya que ambas han conseguido porcentajes de detección superiores al 50% obteniendo la primera de ellas un porcentaje de detección del 83,3%. Además, en todos los

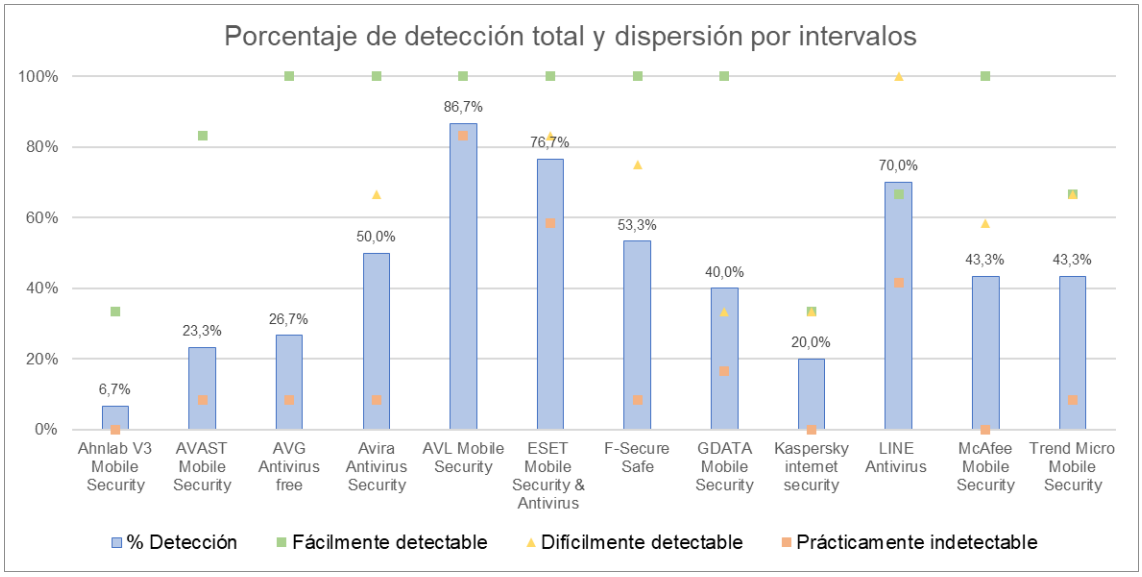
casos de detección se cumplen que los porcentajes van acorde a los rangos a excepción de la herramienta LINE antivirus, la cual es capaz de detectar más herramientas del intervalo intermedio que del fácilmente detectable.

Ilustración 17. Porcentaje de detección por intervalos de herramientas en el estudio



Teniendo en cuenta todos los datos presentados anteriormente, la Ilustración 18 muestra gráficamente los porcentajes de detección de cada una de las 13 herramientas finalmente analizadas y la dispersión de las detecciones en cada uno de los intervalos.

Ilustración 18. Porcentaje de detección total y dispersión por intervalos



Otras consideraciones generales obtenidas del estudio son las siguientes:

- Todas las muestras han sido reconocidas por al menos una de las soluciones participantes en el estudio. Este dato corrobora la validez de la muestra de malware considerada para el estudio a pesar de estar ya avalada por las detecciones de VirusTotal aportadas por la base de datos AndroZoo.
- Ninguna de las herramientas ha conseguido la etiqueta de óptima, ya que no ha podido detectar el 100% de las detecciones.
- A pesar de lo que se podría esperar, los resultados obtenidos de herramientas comerciales o de mayor nombre no han sido mejores a las demás, destacando alguna de ellas negativamente. Es posible que las tasas mejorasen si se utilizase para el estudio la versión de pago, aunque es un dato desconocido.

En cuanto al ranking de herramientas, tal y como se puede observar en la Ilustración 18. Porcentaje de detección total y dispersión por intervalos, existen tres soluciones que satisfacen los objetivos en cuanto a efectividad de las mismas. Las tres soluciones mejores para el análisis del conjunto de malware seleccionado son las indicadas en la Tabla 7.

Tabla 7. Eficiencia top 3 herramientas analizadas

	Total Muestras		Malware prácticamente indetectable		Malware difícilmente detectable		Malware Facilmente detectable	
	Nº Muestras	% detección	Nº Muestras	% detección	Nº Muestras	% detección	Nº Muestras	% detección
AVL Mobile Security	26	86,67%	10	83,33%	10	83,33%	6	100,00%
ESET Mobile Security & Antivirus	23	76,67%	7	58,33%	10	83,33%	6	100,00%
LINE Antivirus	21	70,00%	5	41,67%	12	100,00%	4	66,67%

1. AVL Mobile Security: resulta la vencedora del estudio con un porcentaje de detección del 86,67% obteniendo además unos buenos resultados en los análisis por intervalos definidos para el estudio.
2. ESET Mobile Security & Antivirus: obtiene el segundo puesto en la clasificación con un 76.6% de detección. Además, obtiene los mismos porcentajes de detección en los tramos más simples de detección. Cabe destacar que, en este caso, la detección de malware de más difícil detección baja del 60% lo cual penaliza su puesto en la clasificación notablemente.
3. LINE Antivirus: frente a todo pronóstico inicial, esta herramienta consigue un tercer puesto en la clasificación gracias a la gran capacidad de detección de malware en el nivel intermedio del estudio, siendo la única de las herramientas participantes en el mismo que obtiene un 100% de detección.

Otras consideraciones importantes obtenidas del estudio es que, en el caso en el que la herramienta proporciona una denominación al programa malicioso o datos adicionales sobre

el malware detectado, esta nomenclatura es independiente de la empresa, aunque sí que suele ser aportadora de información sobre el malware en sí. Aunque este dato de información no ha sido añadido en el ANEXO VI. RESULTADOS EFICACIA, se muestra un ejemplo de los datos ofrecidos por algunas de las herramientas para cuatro de las muestras de malware participantes en el estudio. De la Tabla 8. Denominación de malware por las soluciones se puede extrapolar fácilmente que cada una de las herramientas selecciona una nomenclatura diferente, de la cual, en ocasiones, es posible la obtención de datos sobre el malware detectado. Como, por ejemplo:

- El sistema operativo para el que está diseñado o que infecta el programa malicioso (Android)
- Tipo de malware: Adware, troyano (Trojan, Adware, G-Ware, PUA, etc.)
- Familia a la que pertenece, por ejemplo, FakeAV
- Variante: s, a, etc.

Estos datos son muy fácilmente detectables por ejemplo en la solución AVL Mobile Security G-Ware/Android.FakeAV.s[fra.smf] o Adware/Android.UnityAds.a[ads,gen].

En la Tabla 8 se muestra algún ejemplo de las categorizaciones de malware realizadas por una muestra de las herramientas para determinadas aplicaciones malware analizadas.

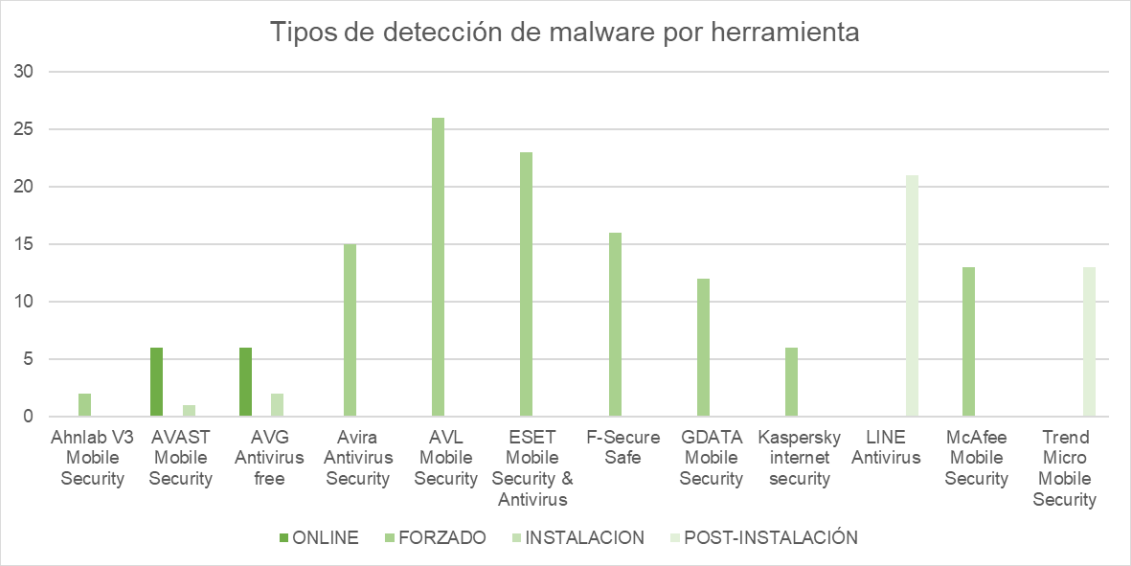
Tabla 8. Denominación de malware por las soluciones

Nombre aplicación	Mystery Luck	Antivirus	Story Teller with Cute Layout	Nombre en árabe
Nombre del archivo	5DC494E30640524EB216D17D07CEA4B077140FF5BD86AE5646A3BEF9A9F9CC05.apk	9DC1D72168B148AAB3838078B11E0391388853F9ECFA6B6377DBF0F879A48351.apk	4254769325279B84CF2F6E68D648C87E45D40A754D71480AE580875D558B05E8.apk	B8C9C2B67DE9793C5394587D834365C1D12E799452DEBA03604B102EADC3FECE.apk
Ahnlab V3 Mobile Security	-	-	Troyano	-
Avira Antivirus Security	-	Fake	Android jocker Android agent	Android packed
AVL Mobile Security	Adware/Android.other.k [ads.gen]	G-Ware/Android.FakeAV.s[fra.smf]	Trojan/Android.Joker2.bm[prv, pay,exp,crt]	Adware/Android.UnityAds.a[ads,gen]
ESET Mobile Security & Antivirus	Android/Packed.Jiagu.D	Android/Blacklister.B	Android/Agent.CHT	Android/Packed.Agent.DMJ
F-Secure Safe	-	Infeccion	Infeccion	Infeccion
GDATA Mobile Security	-	-	Android.Trojan.Agent.CHT (1-QXYYXT)	Android.Trojan.Agent.DUI (1-0q3h10)
Kaspersky internet security	AdWare.AndroidOS.HiddenAd.rr	-	Trojan.AndroidOS.Jocker.jd	-
LINE Antivirus	Trojan.Jiagu	Trojan.Blacklister	Trojan.Jocker	Trojan.Agent
McAfee Mobile Security	-	Android/FakeAVQ	Artemis!5f7701879f13	Artemis!ff944cd9ae49
Trend Micro Mobile Security	PUA	PUA	PUA	-

Para finalizar el estudio general de las soluciones, cabe destacar que cada una de ellas a, pesar de tener las ratios de detección mostradas anteriormente, la tarea ha sido realizada en momentos diferentes. Cabe destacar, que solamente AVAST Mobile Security y AVG Antivirus

han sido capaces de la detección de algunas de los programas maliciosos en tiempo real (simplemente con la descompresión del archivo zip contenedor del malware), si bien es cierto que este tipo de detección en algunas de ellas pertenece a la versión de pago. En el otro extremo de la balanza se encuentra LINE Antivirus, solución entre las 3 de mayor efectividad de las participantes que ha detectado el malware en el peor de los escenarios posibles, post-instalación del programa, lo cual quiere decir que, a pesar de ser detectada la actividad maliciosa, habría podido causar daños en el caso de no haberse producido la infección en un entorno controlado. La Ilustración 19 representa gráficamente esta casuística.

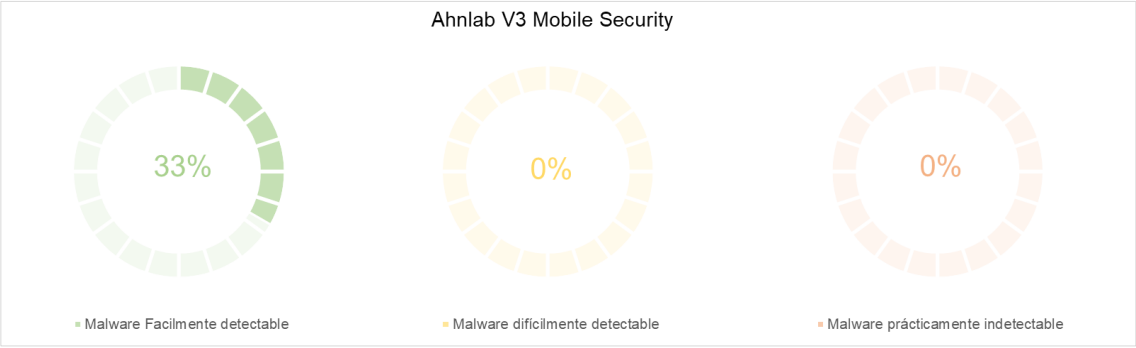
Ilustración 19.Tipos de detección de malware por solución



6.2 Análisis de las herramientas

6.2.1 Ahnlab V3 Mobile Security

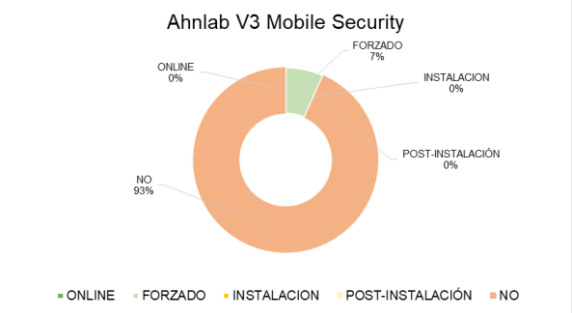
Ilustración 20. Porcentajes de detección Ahnlab V3 Mobile

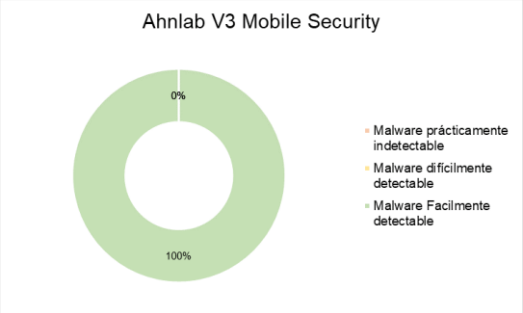


Esta herramienta ha obtenido unos resultados de detección de los peores entre las soluciones que han participado en el estudio. Su porcentaje de detección de malware total es tan solo del

6,7%, además, tal y como se puede observar en los gráficos anteriores, “Ilustración 20. Porcentajes de detección Ahnlab V3 Mobile”, todos los programas maliciosos detectados pertenecen al intervalo de fácil detección.

Ilustración 21. Tipos de detección Ahnlab V3





En cuanto al momento de la detección, todos los programas maliciosos detectados fueron realizados por análisis forzado tal y como se puede observar en los gráficos representados en “Ilustración 21. Tipos de detección Ahnlab V3”.

Rendimiento

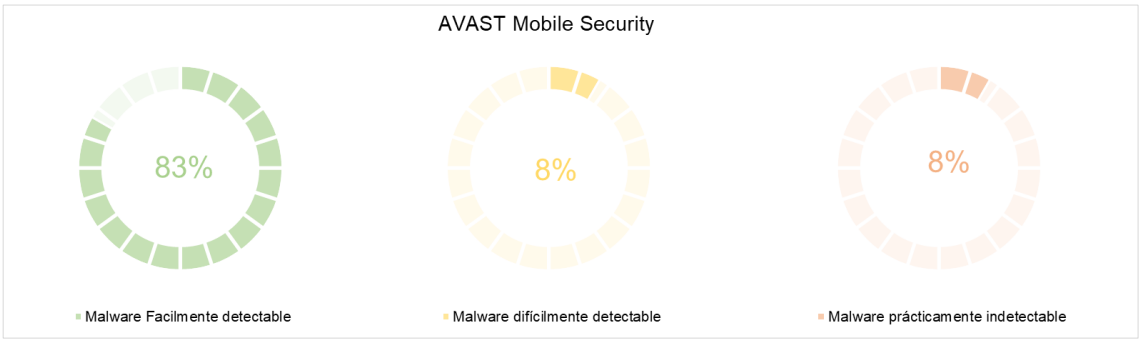
Desde el punto de vista del rendimiento del sistema con la aplicación instalada, no se aprecia descenso en el rendimiento del mismo y tampoco se muestran alertas o avisos que incomoden el uso del mismo o lo interrumpan de alguna manera.

Tal y como se pone de manifiesto en Ilustración 22. Rendimiento Ahnlab V3, los datos ofrecidos por la herramienta de monitorización representan un pico de uso de la CPU correspondiente al forzado del análisis y detección de malware. En cuanto al uso de batería no se aprecia una disminución significativa de la misma debido a su uso.

Ilustración 22. Rendimiento Ahnlab V3

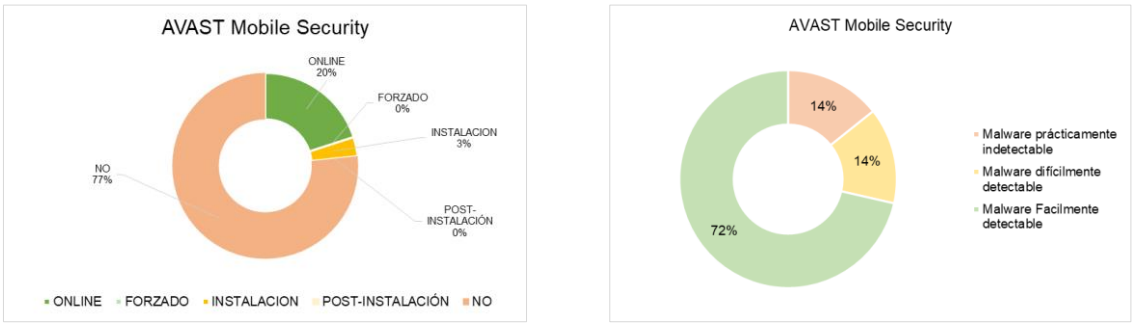
6.2.2 AVAST Mobile Security

Ilustración 23. Porcentajes de detección AVAST



AVAST es otra de las herramientas colistas en cuanto a los resultados de detección obtenidos con un porcentaje de detección total de las muestras de malware del 23,3%. Del análisis de los gráficos representados en Ilustración 23. Porcentajes de detección AVAST, se obtiene que, la detección de malware en el intervalo fácil es bueno, sin embargo, para los otros dos resultados el porcentaje de detección es solo de un 8% lo que hace bajar mucho su valoración final.

Ilustración 24. Tipos de detección AVAST



La Ilustración 24. Tipos de detección AVAST, ofrece datos sobre el momento en el que la herramienta realiza la detección de malware, así como los porcentajes de detección frente a malware detectado de la misma. En cuanto al momento de la detección, cabe destacar que es una de las pocas herramientas que ha detectado malware en tiempo real, de hecho, un 20% del malware se ha detectado solo descomprimiendo el archivo zip que contenía el malware. La detección del resto de malware se ha realizado durante la instalación de las aplicaciones restantes en el dispositivo.

Rendimiento

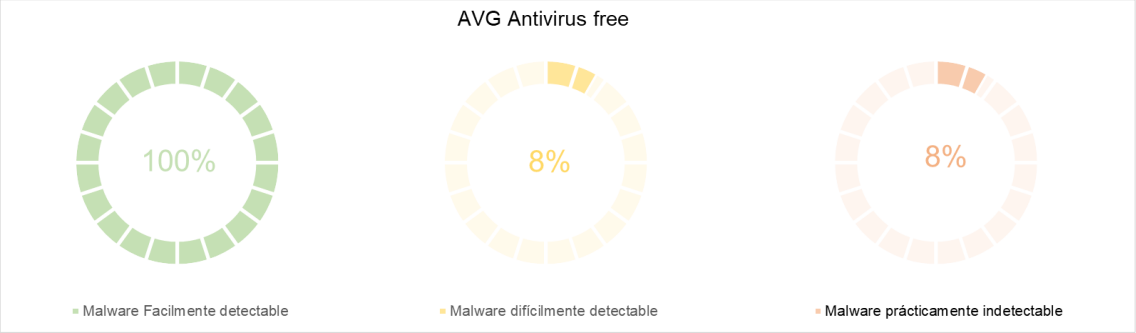
Desde el punto de vista del rendimiento del sistema con la aplicación instalada, no se aprecia descenso en el rendimiento del mismo y tampoco se muestran alertas o avisos que incomoden el uso del mismo o lo interrumpan de alguna manera.

Los datos ofrecidos por la herramienta de monitorización representan un pico de uso de la CPU, ver Ilustración 25. Rendimiento Avast, correspondiente la descompresión del zip y mostrado de alertas de seguridad en el sistema, sin embargo, en posteriores análisis forzados no se aprecia un uso excesivo de la CPU. En cuanto al uso de batería no se aprecia una disminución significativa de la misma debido a su uso.

Ilustración 25. Rendimiento Avast

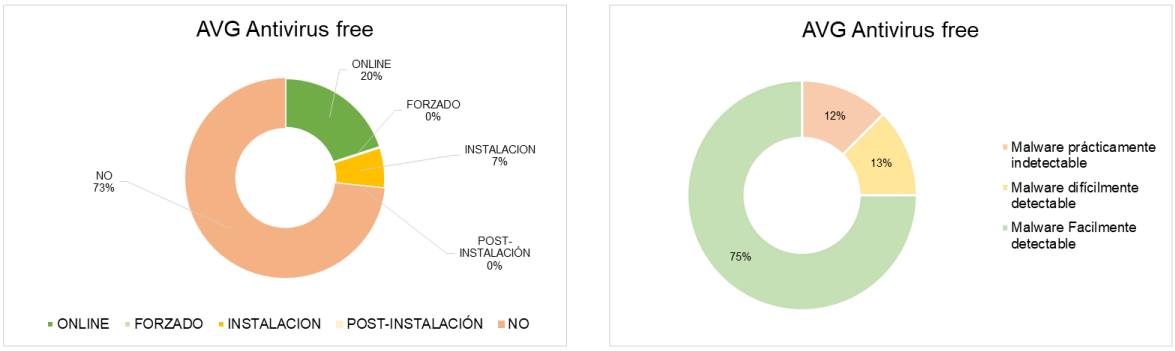
6.2.3 AVG Antivirus free

Ilustración 26.Porcentajes de detección AVG



AVG es otra de las herramientas colistas en cuanto a los resultados de detección obtenidos con un porcentaje de detección total de las muestras de malware del 26,7%. Al analizar los datos obtenidos en el estudio y representados en la Ilustración 26.Porcentajes de detección AVG, la detección de malware en el intervalo fácil es óptimo. Sin embargo, al igual que ocurre con AVAST, en los otros dos intervalos el porcentaje de detección es solo de un 8%.

Ilustración 27. Tipos de detección AVG



En cuanto al momento de la detección, al igual que ocurría con AVAST, hay que destacar su poder de detección en línea solo con la descompresión del zip contenedor del malware. Al igual que en el caso anterior, la detección del resto de malware se ha realizado durante la instalación de las aplicaciones restantes en el dispositivo. Del malware detectado por la aplicación, el 75% pertenecía al intervalo de fácilmente detectable, mientras el 13 y el 12% pertenecían a los tramos de dificultad intermedia y alta respectivamente. La Ilustración 27. Tipos de detección AVG representa el anterior análisis gráficamente.

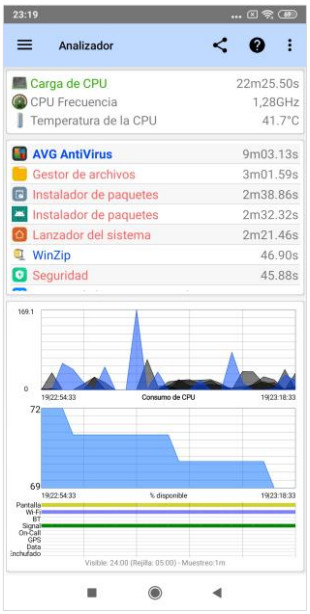
Esta herramienta y la anterior disponen de grandes similitudes, no solamente en cuanto a resultados obtenidos sino a información arrojada sobre el malware y modo de trabajo.

Rendimiento

Al igual que en casos anteriores, el rendimiento del sistema con la aplicación instalada, no se aprecia descenso en el rendimiento del mismo y tampoco se muestran alertas o avisos que incomoden el uso del mismo o lo interrumpan de alguna manera.

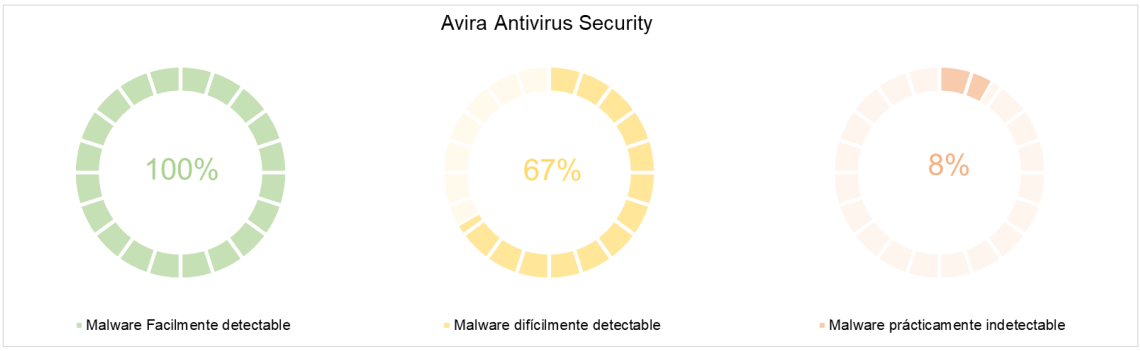
Los datos ofrecidos por la herramienta de monitorización, Ilustración 28. Rendimiento AVG, representan un pico de uso de la CPU correspondiente la descompresión del zip y mostrado de alertas de seguridad en el sistema. En todos los análisis realizados se aprecia un uso intensivo de CPU representado por picos en la gráfica de monitorización. En cuanto al uso de batería no se aprecia una disminución significativa de la misma debido a su uso.

Ilustración 28. Rendimiento AVG



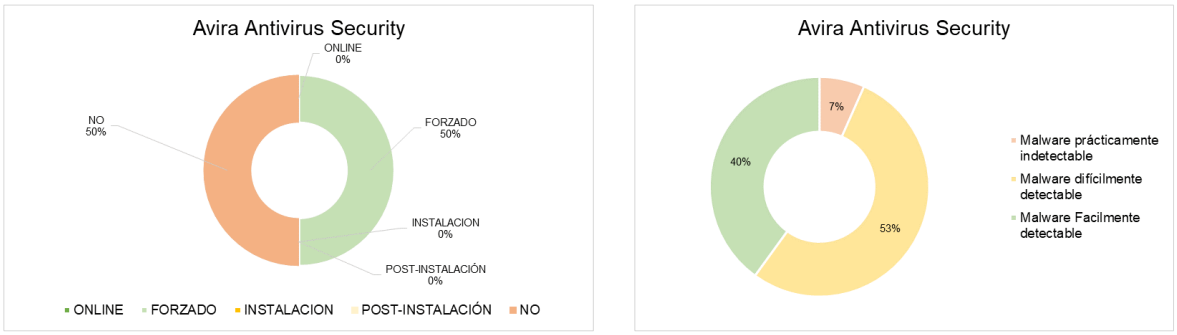
6.2.4 Avira Antivirus Security

Ilustración 29. Porcentajes de detección Avira



Esta solución ha sido capaz de detectar 15 programas maliciosos, lo cual se corresponde con un porcentaje de detección total del 50%. En cuanto al trabajo por intervalos, se puede decir que su comportamiento es excelente en el fácil, aceptable en el segundo y malo en el intervalo de malware prácticamente indetectable. Los porcentajes, tal y como se puede observar en los gráficos de Ilustración 29. Porcentajes de detección Avira, son del 100%, 67% y 8% respectivamente.

Ilustración 30. Tipos de detección Avira



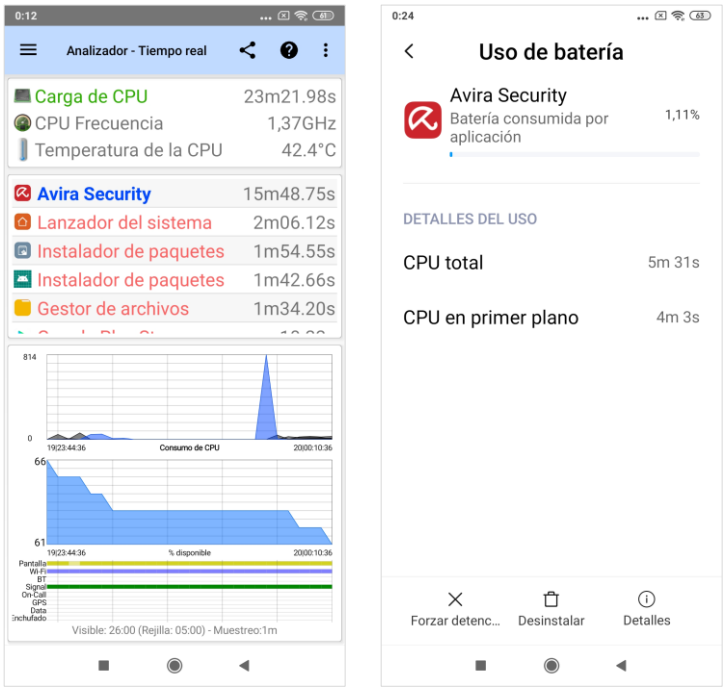
Esta solución solamente ha arrojado alertas de detección en el análisis forzado tras la descompresión del zip, tal y como se representa en el gráfico Ilustración 30. Tipos de detección Avira, la herramienta ha realizado una detección forzada del 50% mientras que el otro 50% del malware no ha sido detectada por ella. En los siguientes análisis ejecutados o durante la instalación de las aplicaciones maliciosas no ha detectado nuevos positivos.

Rendimiento

La instalación de la solución no ralentiza el sistema ni muestra alertas o avisos que puedan incordiar al usuario.

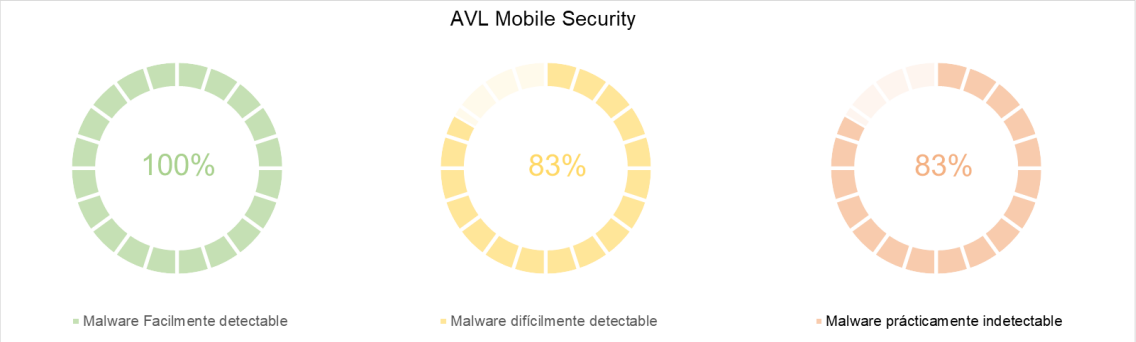
Los datos ofrecidos por la herramienta de monitorización representan pequeños picos a lo largo del desarrollo del estudio mostrando un uso de la CPU mucho mayor durante la instalación de las aplicaciones maliciosas en el sistema, lo cual indica el análisis de las mismas. En cuanto al uso de batería no se aprecia una disminución significativa de la misma debido a su uso siendo el porcentaje de consumo de la misma muy inferior al de otras aplicaciones utilizadas en el estudio. En la Ilustración 31. Rendimiento Avira se ilustran los datos comentados anteriormente.

Ilustración 31. Rendimiento Avira



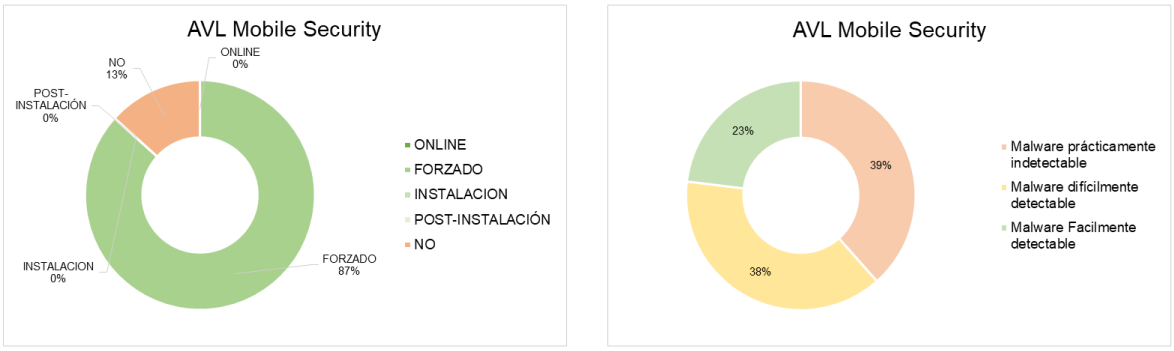
6.2.5 AVL Mobile Security

Ilustración 32. Porcentajes de detección AVL Mobile Security



Esta es la herramienta que mejores resultados ha obtenido en el análisis de malware. Su porcentaje total de detección fue de un 86,7% obteniendo en los intervalos intermedio y más complicado de detección un 83% de tasa de aciertos y en el simple un 100% de efectividad, tal y como se representa gráficamente en la Ilustración 32. Porcentajes de detección AVL Mobile Security.

Ilustración 33. Tipos de detección AVL Mobile Security



En cuanto al momento de la detección, todo el malware que activó los sistemas de alarma de la herramienta (26 programas maliciosos) fue detectado mediante el primer análisis forzado, teniendo las apk presentes en el sistema simplemente, sin ejecutar. Este hecho favorece también la recomendación de la herramienta ya que, a pesar de no haberse detectado el malware al almacenarse en el sistema en tiempo real, al menos se ha detectado antes de la ejecución y posible infección del sistema. Los datos comentados anteriormente se presentan en los gráficos representados en Ilustración 33. Tipos de detección AVL Mobile Security.

Rendimiento

Al igual que en los demás casos, el sistema no influye en el uso normal del dispositivo.

Cabe destacar que los análisis del sistema son muchos más lentos en comparación con las otras herramientas, si bien es cierto que los resultados obtenidos de los mismos han sido los mejores del estudio.

Como curiosidad, es la única herramienta que en análisis inicial del sistema detecta la herramienta mi remote preinstalada en el sistema como PUA.

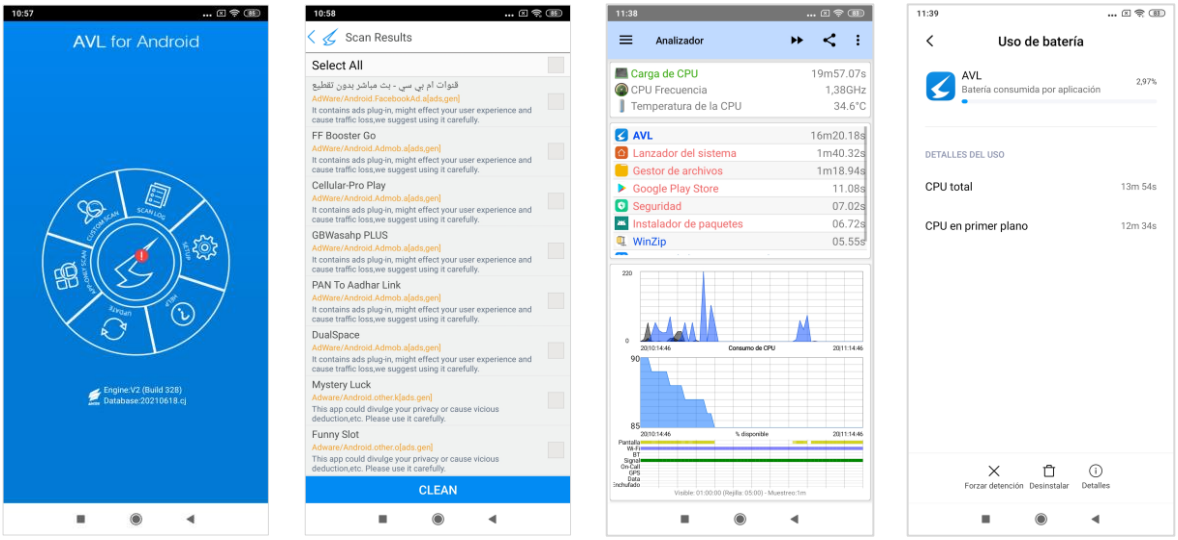
En cuanto a los resultados de las alertas de malware ofrecidas por la aplicación cabe destacar que son de las más completas aportando mucha información sobre el malware detectado.

En cuanto a su aspecto visual quizás esté entre las más complicadas o menos amigables.

El uso de CPU de la herramienta es bastante elevado, así como el de batería que llega a duplicar los porcentajes de uso durante el estudio comparado con otras herramientas utilizadas.

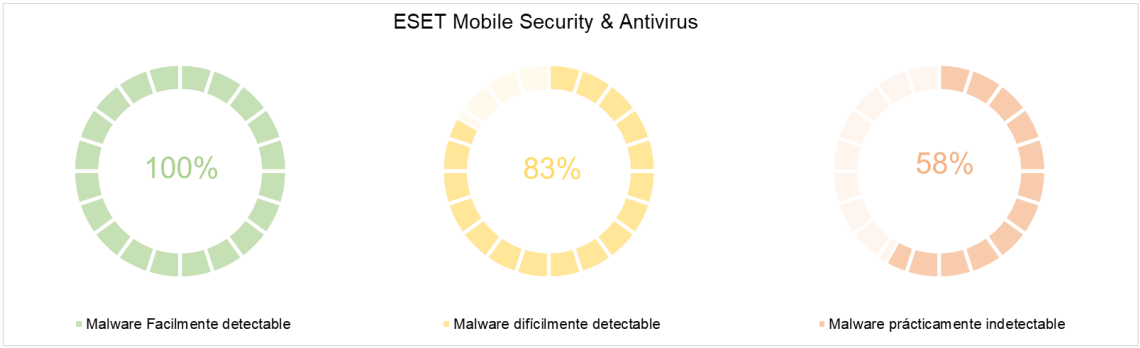
La Ilustración 34. Rendimiento AVL Mobile Security ilustra los aspectos comentados en este apartado.

Ilustración 34. Rendimiento AVL Mobile Security



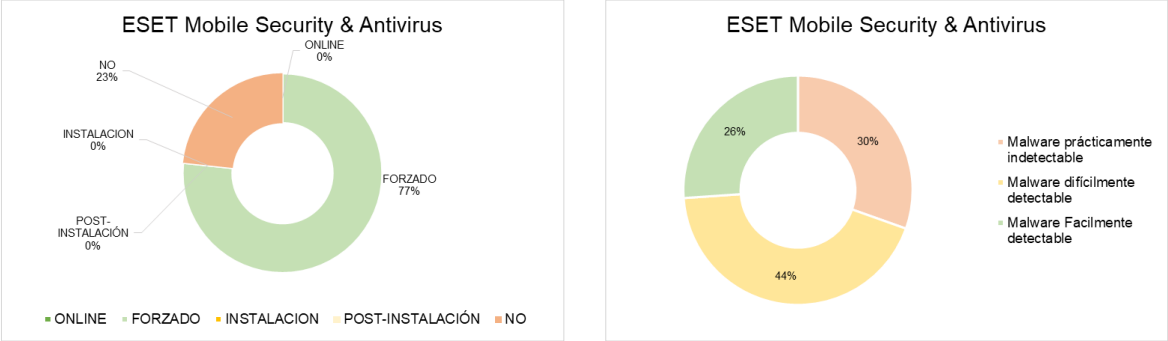
6.2.6 ESET Mobile Security & Antivirus

Ilustración 35. Porcentajes de detección ESET Mobile Security



ESET es la segunda herramienta en el ranking de detección de malware obteniendo resultados por intervalos peores que AVL únicamente en la detección de malware en el intervalo prácticamente indetectable. La Ilustración 35. Porcentajes de detección ESET Mobile Security representa gráficamente los resultados de análisis por intervalos de la herramienta. Cabe destacar que, aun teniendo un porcentaje de detección malware en el intervalo de mayor dificultad poco superior al 50%, su porcentaje total de detección total es del 76,7%.

Ilustración 36. Tipos de detección ESET Mobile Security



El momento en el que la herramienta detecta el malware no es el óptimo, pero es de los mejores, detectando el 100% de los casos detectados en el análisis forzado posterior a la descompresión del zip con malware en el sistema. Como se representa en Ilustración 36. Tipos de detección ESET Mobile Security, el 77% del malware detectado ha sido en la etapa denominada en el estudio como “forzada”.

Rendimiento

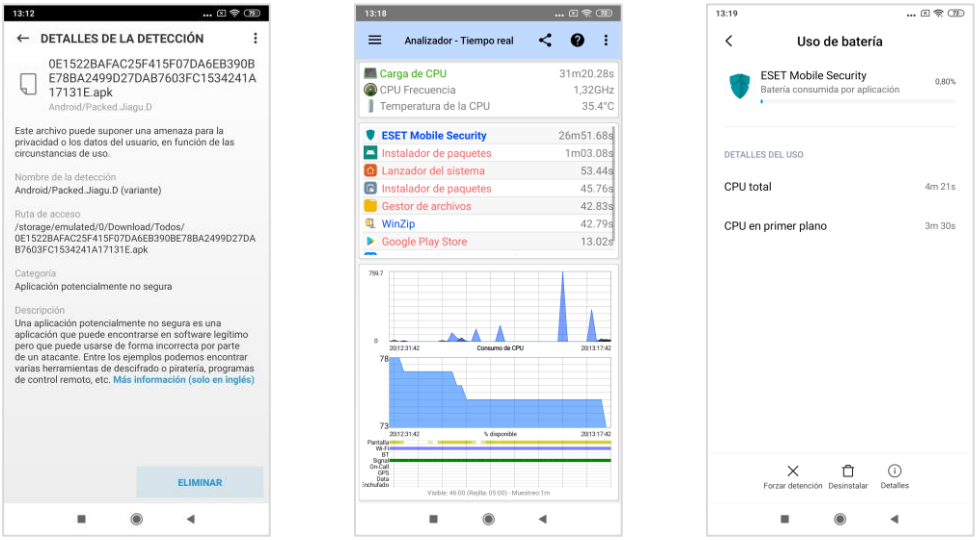
La Ilustración 37. Rendimiento ESET Mobile Security pone de manifiesto los resultados de rendimiento de la herramienta que se analizan a continuación.

El entorno de la solución es muy simple y favorece su uso. Así mismo, la información ofrecida por la herramienta en el caso de detecciones es muy amplia y fácilmente comprensible.

Cabe destacar también que el consumo de CPU de la herramienta es bastante notable con respecto a otras de las participantes en el estudio. Aun así, el uso de batería es de los más bajos obtenidos.

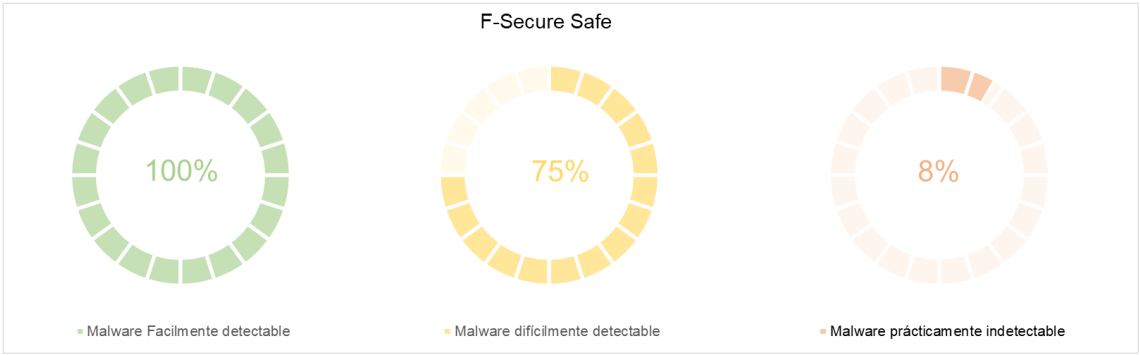
Como elemento diferenciador a otras herramientas, y de cara a la captación de clientes, la herramienta solicita en la configuración de la misma un email para poder hacer uso de la misma.

Ilustración 37. Rendimiento ESET Mobile Security



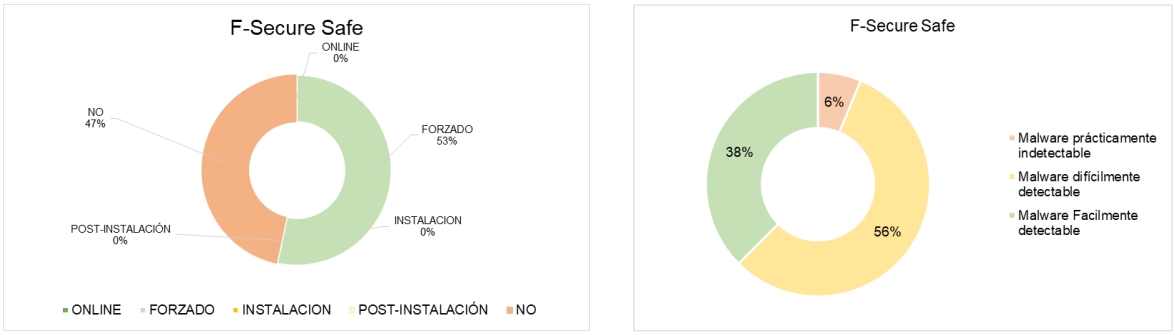
6.2.7 F-Secure Safe

Ilustración 38. Porcentajes de detección F-Secure Safe



Tal y como evidencia la Ilustración 38. Porcentajes de detección F-Secure Safe, esta herramienta consigue buenos resultados de detección en dos de los intervalos definidos pero su detección es mala para el conjunto de malware perteneciente al intervalo prácticamente indetectable, solo un 8% del malware en este tramo ha sido detectado por la herramienta. Aun así, y gracias a su buena detección en los otros tramos consigue detectar más de la mitad del malware de la prueba, un 53,3%.

Ilustración 39. Tipos de detección F-Secure Safe



El 100% del malware que hizo saltar las alarmas de la herramienta (53% de las muestras), fue detectado solamente con la presencia de la apk maliciosa en el sistema. La Ilustración 39. Tipos de detección F-Secure Safe pone de manifiesto este hecho.

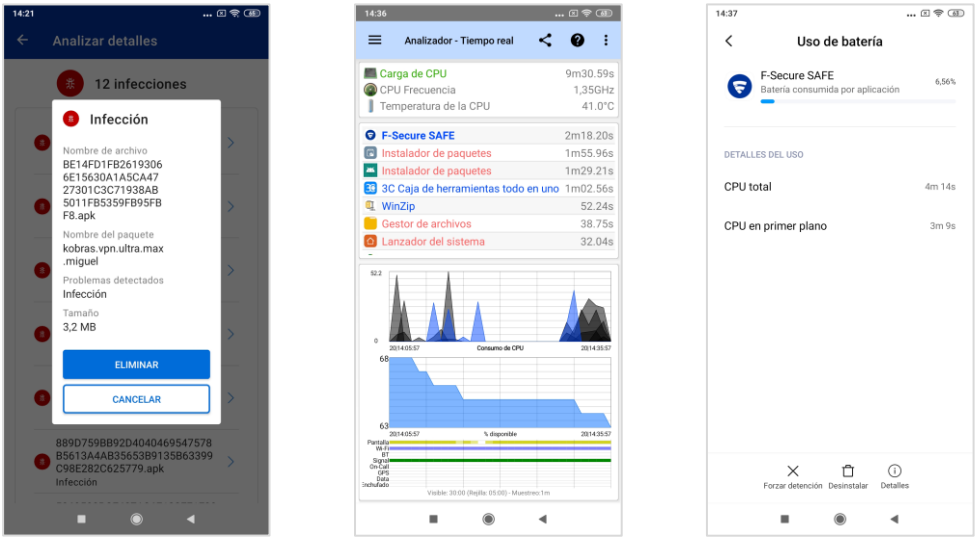
Rendimiento

En cuanto a rendimiento se refiere – ver Ilustración 40. Rendimiento F-Secure Safe – la herramienta no hace que el sistema se vuelva inestable o se vea ralentizado. Tampoco resulta molesta la existencia de la herramienta en el sistema desde el punto de vista de que muestre alertas innecesarias o similar.

Otro punto positivo de la herramienta es que las alertas muestran algo de detalle sobre el malware detectado a contraposición de otras que simplemente muestran la alerta.

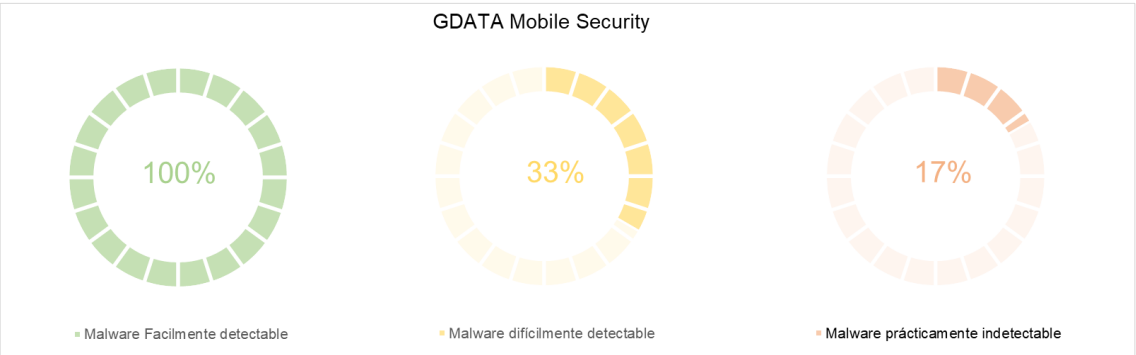
En las estadísticas de uso de CPU y batería, cabe destacar que el a pesar de no consumir demasiados recursos de CPU, el consumo de batería de la herramienta durante el estudio ha sido considerable.

Ilustración 40. Rendimiento F-Secure Safe



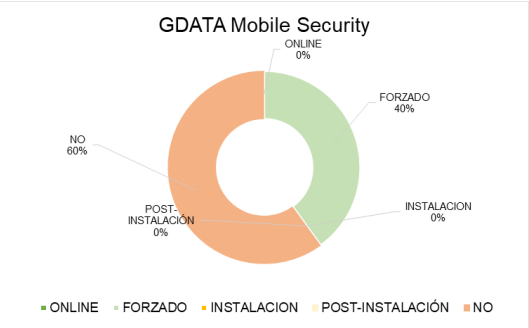
6.2.8 GDATA Mobile Security

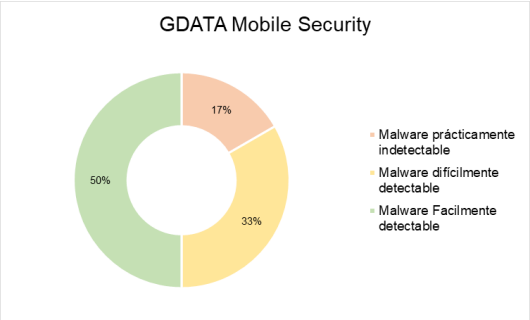
Ilustración 41. Porcentajes de detección GDATA Mobile Security



Esta herramienta ha arrojado excelentes resultados en la detección de malware en el intervalo fácilmente detectable, no obstante, los resultados obtenidos en los dos intervalos restantes no son satisfactorios, siendo ambos inferiores al 40%. Así mismo, el porcentaje general de la detección por parte de la herramienta ha sido muy pobre obteniendo un 40,0% con solamente 12 muestras detectadas de las 30 participantes en el estudio. Los datos comentados son los representados en la Ilustración 41. Porcentajes de detección GDATA Mobile Security.

Ilustración 42. Tipos de detección GDATA Mobile Security





Como en la mayoría de los casos, tal y como representan los gráficos de Ilustración 42. Tipos de detección GDATA Mobile Security, la detección del malware se ha realizado en el análisis forzado una vez transferido el mismo al sistema.

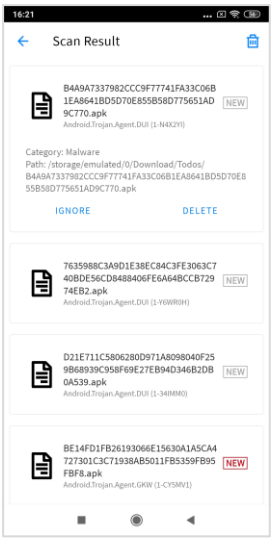
Rendimiento

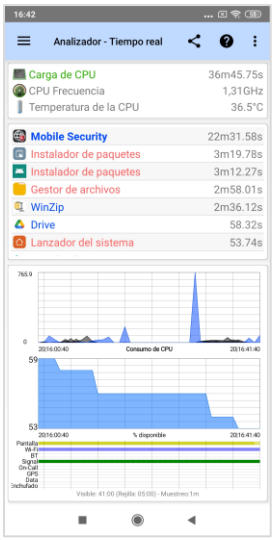
La aplicación no usa excesivamente la CPU, aunque en el gráfico de monitorización se puede observar que el pico de mayor valor es el correspondiente a la instalación del malware en la máquina. En cuanto al consumo de batería, destaca su bajo consumo en el tiempo utilizado para el estudio.

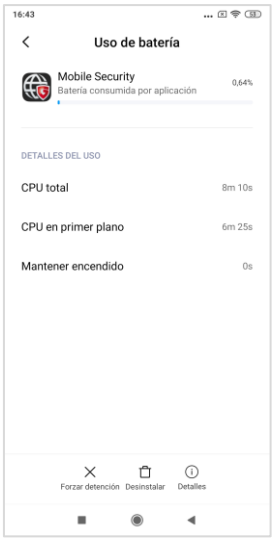
Al igual que otras herramientas, la sensación al usuario con la herramienta instalada no ofrece puntos negativos. La apariencia de la herramienta es sencilla y fácil de utilizar. Además, las alertas ofrecidas al usuario, aunque muy simples, arrojan más información que otras herramientas participantes en el estudio.

Estos datos se ilustran en la Ilustración 43. Rendimiento GDATA Mobile Security.

Ilustración 43. Rendimiento GDATA Mobile Security

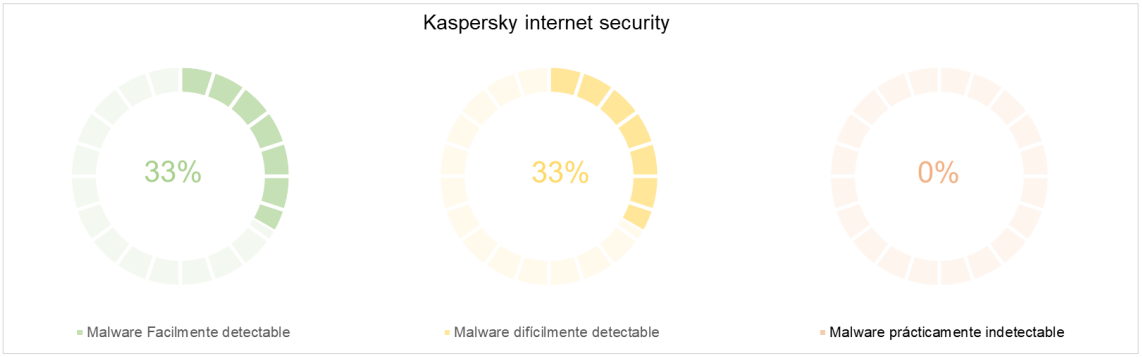






6.2.9 Kaspersky internet security

Ilustración 44. Porcentajes de detección Kaspersky internet security



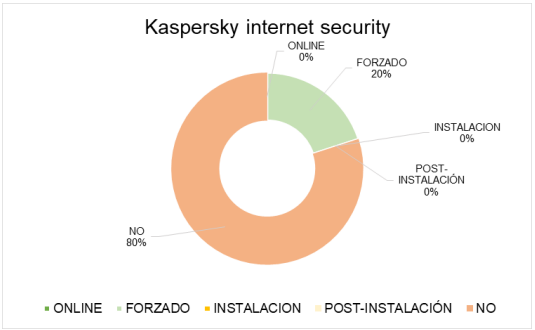
Kaspersky es una marca con un gran prestigio en el mundo de la protección de sistemas, las expectativas depositadas en esta herramienta antes de comenzar el estudio eran altas, sin embargo, los resultados obtenidos se encuentran entre los peores del conjunto de soluciones.

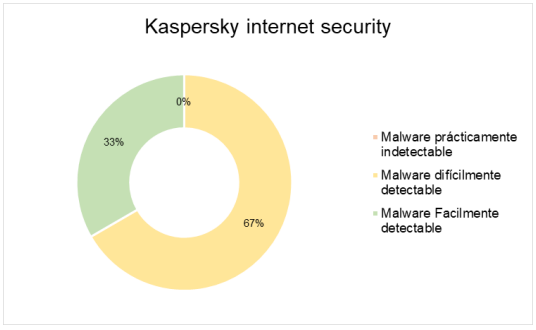
Si bien es cierto que la herramienta consta de una versión de pago, se desconoce si los resultados de este estudio podrían mejorar en caso de disponer de la misma.

La Ilustración 44. Porcentajes de detección Kaspersky internet security, refleja los datos del análisis por intervalos de la herramienta.

La herramienta solamente ha sido capaz de detectar el 20,0% de malware con el que se ha infectado la máquina objetivo. Además, en las detecciones por intervalos, no ha sido capaz de detectar ninguna de las muestras pertenecientes al tramo prácticamente indetectable. En los otros dos intervalos ha obtenido una detección del 33%, valor bastante malo.

Ilustración 45. Tipos de detección Kaspersky internet security





El modo de detección del malware, ver Ilustración 45. Tipos de detección Kaspersky internet security, no arroja sorpresas detectándose todos los positivos obtenidos en el primer escaneo realizado con las apk en el sistema.

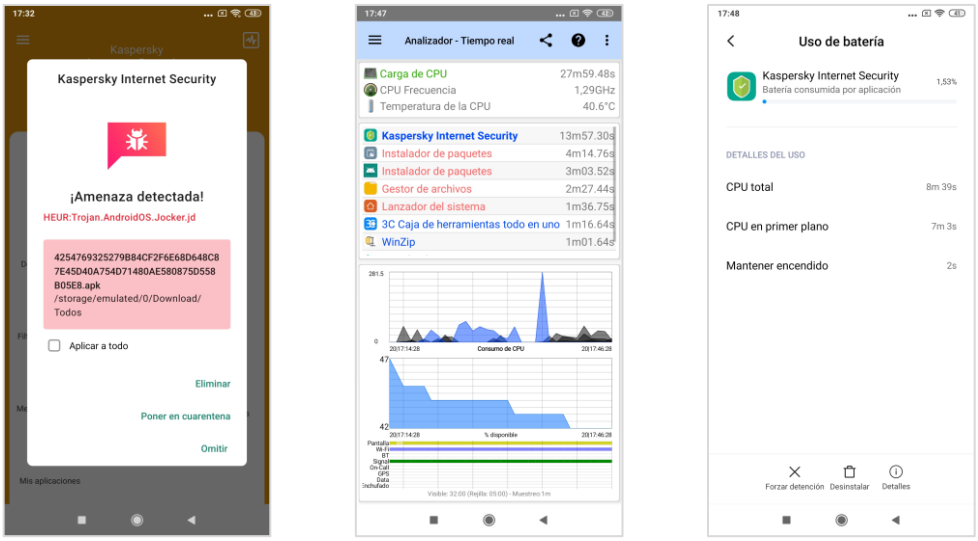
Rendimiento

En cuanto al consumo de CPU se observa un pico notable, al igual que en otras ocasiones durante la instalación de las aplicaciones en el dispositivo. En lo que se refiere al porcentaje de batería consumido durante el estudio, se encuentra en valores de consumo intermedios con respecto a las demás herramientas.

La interfaz de usuario de la herramienta es actual, visual e intuitivo. Así mismo, las alertas facilitadas por la herramienta son claras y las acciones a tomar aparecen bien detalladas, incluso se facilitan con código de colores atendiendo a su gravedad.

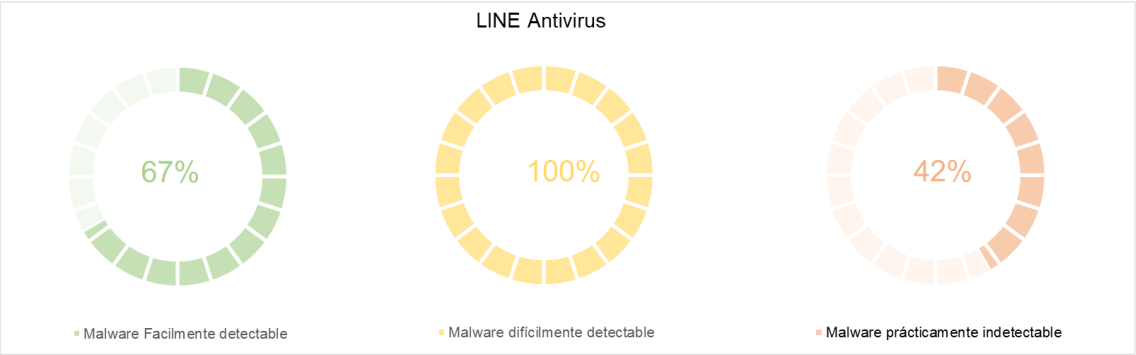
La Ilustración 46. Rendimiento Kaspersky internet security, ilustra una alerta de infección mostrada por la herramienta, los datos arrojados por la aplicación de rendimiento de la CPU y la batería.

Ilustración 46. Rendimiento Kaspersky internet security



6.2.10 LINE Antivirus

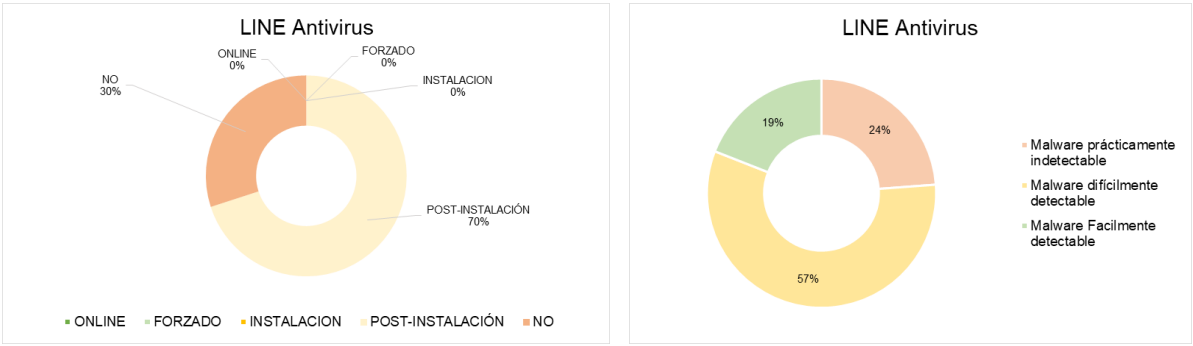
Ilustración 47. Porcentajes de detección LINE Antivirus



La empresa que se encuentra detrás de esta solución es la misma que la de la conocida aplicación de mensajería. Frente a todo pronóstico inicial, la herramienta ha conseguido el tercer porcentaje de detección general de malware mejor del estudio obteniendo un 70,0% de detección.

Un aspecto destacable en el análisis por intervalos y representado en Ilustración 47. Porcentajes de detección LINE Antivirus, es que, esta herramienta se sale de lo común detectando el 100% del malware en el rango intermedio y siendo capaz de detectar solamente 4 de las 6 muestras de malware existentes en el intervalo de malware fácilmente detectable.

Ilustración 48. Tipos de detección LINE Antivirus



En el modo de detección de malware, también consta de una peculiaridad frente a las demás herramientas y es que la detección se realiza en el peor de los escenarios posibles, cuando la aplicación ya está instalada en el sistema, por lo que, las consecuencias podrían ser nefastas para el dispositivo. La Ilustración 48. Tipos de detección LINE Antivirus, analiza tanto los momentos de detección como el intervalo al que pertenecen las muestras calificadas como malware.

Rendimiento

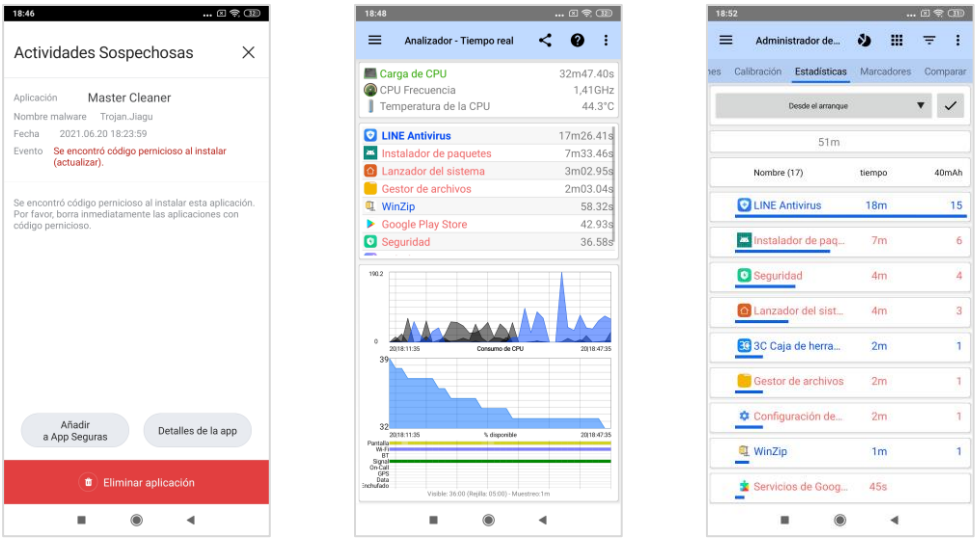
Los datos que se comentan en este apartado se apoyan con las imágenes de la Ilustración 49. Rendimiento LINE Antivirus. La herramienta dispone de una interfaz de usuario simplificada y con diseño desenfadado, sin embargo, personalmente, me parece una de las de más difícil manejo por tener que configurar el tipo de escaneo a realizar en un apartado de configuración separado.

En cuanto a las alertas mostradas, no son demasiado exhaustivas, pero muestran algo de información.

La carga de CPU de la herramienta, así como el uso de batería de la misma, es bastante elevado. Además, el sistema Android no muestra el porcentaje de batería consumido por la aplicación por lo que se ha tenido que obtener por otros medios.

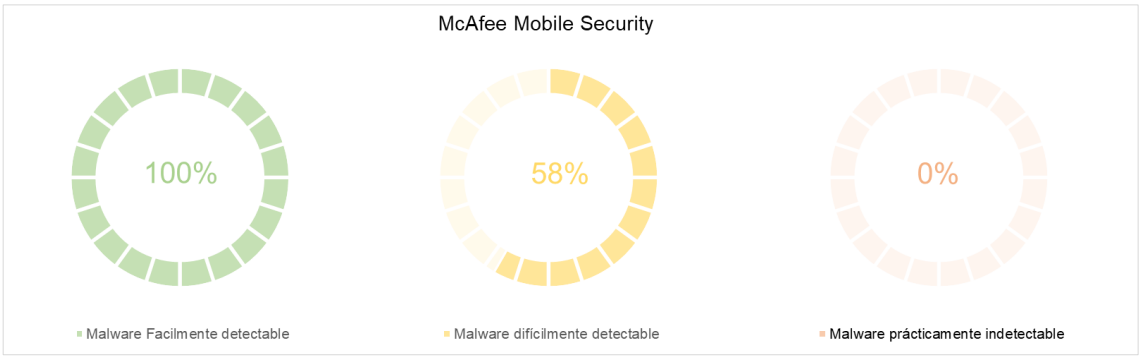
Como resumen a esta aplicación, a pesar de tener un porcentaje de detección bastante bueno, su modo de detección, así como el consumo de recursos del sistema no resulta del todo óptimo por lo que no sería una de las grandes candidatas a uso.

Ilustración 49. Rendimiento LINE Antivirus



6.2.11 McAfee Mobile Security

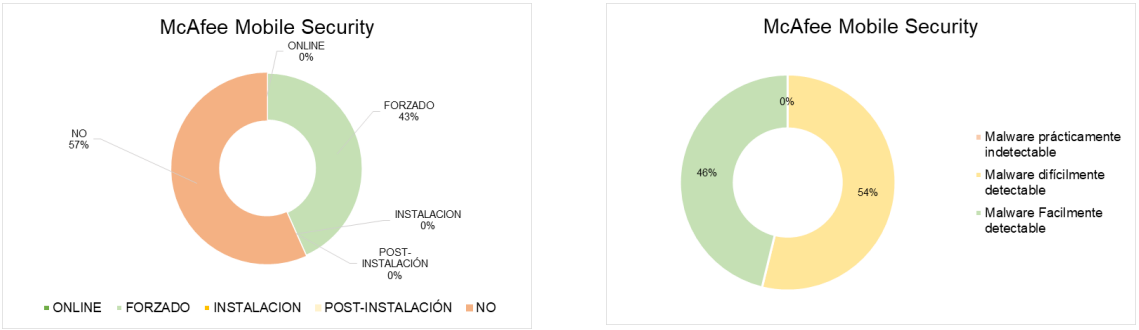
Ilustración 50. Porcentajes de detección McAfee Mobile Security



McAfee es una empresa de gran prestigio en el sector, la herramienta dispone de una versión de pago por la cual, como en otras ocasiones, se desconocen los resultados que se podrían obtener con ella.

Según demuestran los gráficos de la Ilustración 50. Porcentajes de detección McAfee Mobile Security, si bien es cierto que en los porcentajes de detección por intervalos el primero de los tramos tiene la mejor de las puntuaciones, en el segundo los resultados caen casi a la mitad y se desploman en el caso del intervalo de malware prácticamente indetectable no siendo posible la detección de ninguna muestra.

Ilustración 51. Tipos de detección McAfee Mobile Security



Según muestra la Ilustración 51. Tipos de detección McAfee Mobile Security, en cuanto al momento de detección de la infección, no hay sorpresas y, como en la mayor parte de los casos, los programas maliciosos son detectados con la simple presencia del archivo .apk en el sistema.

Rendimiento

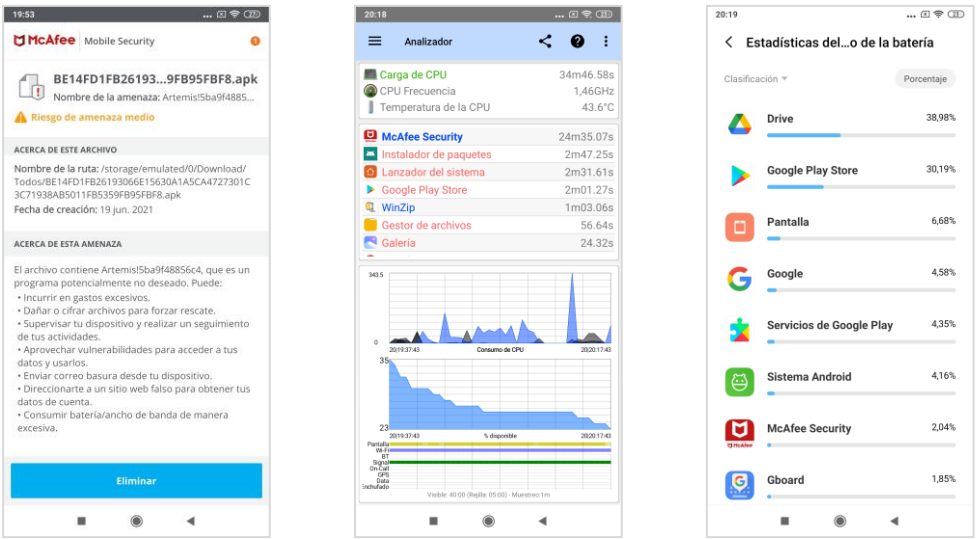
Tanto el porcentaje de uso de la CPU como la batería consumida por la herramienta, está por encima de la de muchas de las herramientas participantes en el estudio.

Un punto reseñable de la solución es que la información aportada por la herramienta es de las mejores de entre las que han participado en el estudio.

Al igual que en otros casos, se desconoce si con la instalación de la versión de pago de la herramienta los resultados de detección podrían mejorar.

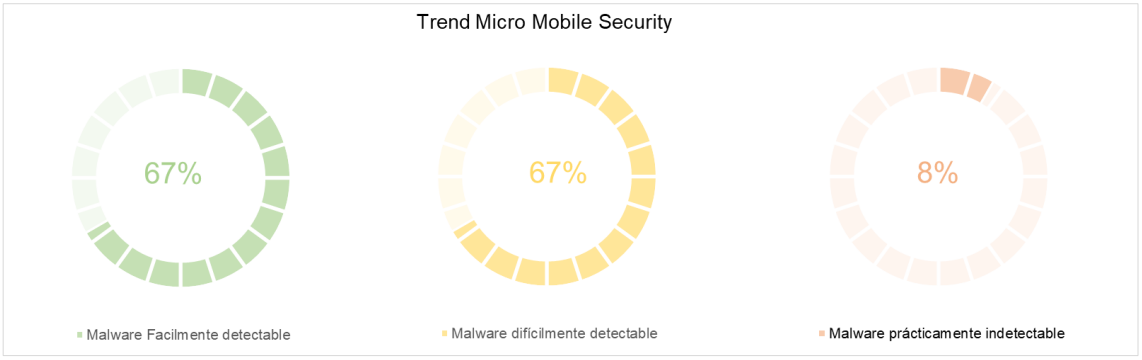
La Ilustración 52. Rendimiento McAfee Mobile Security pretende aportar una solución visual a los datos comentados en este apartado.

Ilustración 52. Rendimiento McAfee Mobile Security



6.2.12 Trend Micro Mobile Security

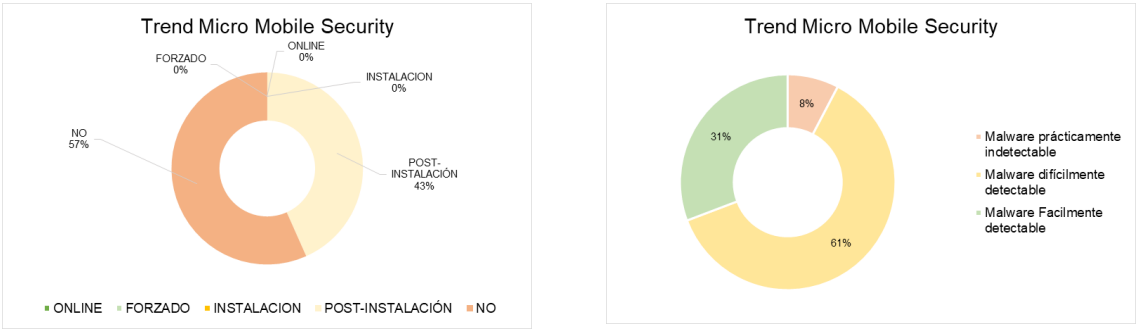
Ilustración 53. Porcentajes de detección Trend Micro Mobile



Trend Micro es una empresa de renombre en el sector, por lo que se había depositado en ella una confianza mayor de la obtenida en los resultados finales.

La herramienta ha conseguido solamente un 43,3% de porcentaje de detección del malware seleccionado para el estudio. En el estudio por intervalos, la apreciación mejora un poco obteniendo un 67% de detección en los dos más simples y solo un 8 % para el intervalo de mayor complejidad. Estos resultados se manifiestan en la Ilustración 53. Porcentajes de detección Trend Micro Mobile.

Ilustración 54. Tipos de detección Trend Micro Mobile



Mediante el análisis de la Ilustración 54. Tipos de detección Trend Micro Mobile, cabe destacar, que tal y como ha ocurrido con otras herramientas, esta dispone de una versión de pago y la que se ha utilizado para el estudio es realmente limitada, ya que no se dispone a penas de mecanismos de detección.

Por ello, el 100% del malware detectado ha sido en la fase de post-instalación de la herramienta.

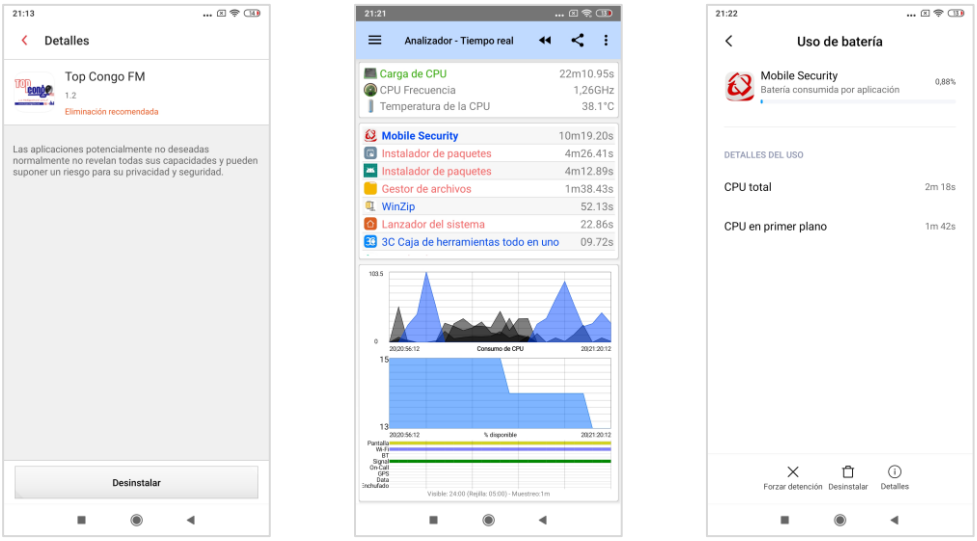
Rendimiento

La aplicación muestra alertas sobre las aplicaciones instaladas y la jerga utilizada es tal que su comprensión está a nivel de cualquier tipo de usuario.

El consumo de CPU es bastante elevado, no obstante, el consumo de batería por parte de la aplicación se encuentra en el rango bajo frente a las demás herramientas participantes en el estudio.

Los datos comentados en este apartado se representan mediante una muestra de capturas realizadas en el análisis en la Ilustración 55. Rendimiento Trend Micro Mobile.

Ilustración 55. Rendimiento Trend Micro Mobile



6.3 Rendimiento de las herramientas

Los valores presentados anteriormente referentes a la batería o CPU se corresponden con datos extraídos durante la ejecución definida para el desarrollo del estudio. No obstante, como estos valores pueden estar condicionados por los picos de análisis forzados y además el tiempo de medición de los valores es muy bajo, se ha realizado una segunda prueba de rendimiento de las soluciones para ver su comportamiento en un entorno normal de uso de un dispositivo móvil. Para la realización de este análisis, se ha realizado la instalación en el dispositivo utilizado para el estudio cada una de las herramientas analizadas y se ha utilizado normalmente el teléfono.

En cuanto a los datos de consumo de CPU son tan irrelevantes que no son mostrados ni por el sistema operativo Android ni por la herramienta de monitorización instalada en el dispositivo.

En cuanto a la batería consumida por las herramientas, el sistema operativo desprecia los valores consumidos por las mismas incluyéndolos en el apartado otros. Sin embargo, de la herramienta de monitorización se obtienen los mAh consumidos por cada una de las aplicaciones del estudio en dos momentos denominados toma1 y toma 2. Para el cálculo de

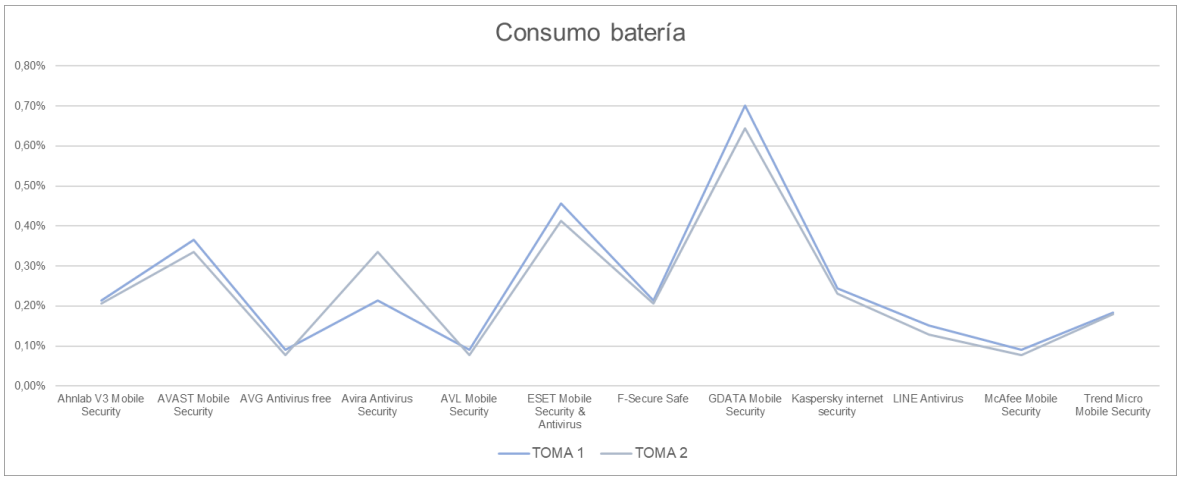
los porcentajes consumidos por la herramienta se consideran los mAh totales consumidos que son 3280 y 3880.

Los datos obtenidos se representan en la Tabla 9. Resultados estudio consumo de batería.

Tabla 9. Resultados estudio consumo de batería

	TOMA 1		TOMA 2	
	Batería %	Batería mAh	Batería %	Batería mAh
Ahnlab V3 Mobile Security	0,21%	7	0,21%	8
AVAST Mobile Security	0,37%	12	0,34%	13
AVG Antivirus free	0,09%	3	0,08%	3
Avira Antivirus Security	0,21%	7	0,34%	13
AVL Mobile Security	0,09%	3	0,08%	3
ESET Mobile Security & Antivirus	0,46%	15	0,41%	16
F-Secure Safe	0,21%	7	0,21%	8
GDATA Mobile Security	0,70%	23	0,64%	25
Kaspersky internet security	0,24%	8	0,23%	9
LINE Antivirus	0,15%	5	0,13%	5
McAfee Mobile Security	0,09%	3	0,08%	3
Trend Micro Mobile Security	0,18%	6	0,18%	7

Ilustración 56. Gráfico consumo de batería



Analizando los resultados obtenidos (ver Ilustración 56. Gráfico consumo de batería) se obtiene que el consumo de batería por las herramientas en un uso normal del dispositivo es constante dado que los porcentajes de las dos tomas son dos líneas que prácticamente se superponen. Por otra parte, si se realiza el análisis del total de batería consumida, se tiene el consumo de todas las herramientas está por debajo del 1% de la batería del dispositivo, por lo que, es un consumo realmente bajo. A pesar de que alguna herramienta tiene un consumo

muy superior a otras – por ejemplo, GDATA (0,70%) consume mucho más que AVL Mobile Security (0,09%) pero el rango de consumo total es tan pequeño que apenas será apreciable en la descarga total de batería del dispositivo.

Por lo tanto, del análisis de rendimiento de las aplicaciones analizadas se obtiene que todas ellas tienen un gran rendimiento y no afectan negativamente a la experiencia de usuario en el uso de su dispositivo móvil.

6.4 Evaluación de los resultados

La instalación de una herramienta de seguridad en el dispositivo aporta una capa más a la protección del mismo.

Los resultados obtenidos en el estudio no han sido del todo reveladores de cara a favorecer la instalación de una de estas herramientas ya que los resultados de eficacia obtenidos han sido muy dispares obteniendo porcentajes de detección de un 86,7% en el mejor de los casos o de un 6,7% en el peor de los mismos.

Por parte del rendimiento de las mismas, en ninguno de los casos se ha detectado un consumo de batería excesivo, notificaciones constantes que impidan o molesten el uso normal del dispositivo o cambios significativos en el rendimiento del teléfono móvil utilizado para el estudio.

Es por lo anterior por lo que, se recomienda el uso de una herramienta de seguridad en el dispositivo móvil. Lo óptimo sería elegir de todas ellas la más eficiente, en este estudio se han obtenido las mejores para la muestra de malware del estudio, si bien es cierto que no es posible saber si el resultado de rendimiento obtenido de este trabajo es extrapolable a todos los programas maliciosos existentes y por ende existen herramientas muy superiores a otras y solamente algunas serían merecedoras de ser instaladas como barrera de seguridad en el dispositivo.

6.5 Guía de buenas practicas

A continuación, se presenta una guía de buenas prácticas para el sistema operativo Android extraídas de la información tratada para el desarrollo del presente trabajo.

- **Actualizar el sistema operativo y las aplicaciones instaladas**. Se han puesto de manifiesto las mejoras de seguridad que se han ido introduciendo a lo largo de la vida del sistema operativo. Además, es importante siempre la actualización del software de cara a la solución de posibles vulnerabilidades descubiertas. En Android la problemática de la actualización de versiones es que además éste depende también

de la marca del dispositivo, por lo que, también sería un punto a tener en cuenta en el momento de adquirir dispositivos el compromiso de la marca con la distribución de actualizaciones.

- **Utilizar los mecanismos de bloqueo facilitados**. Hacer uso de los mecanismos de bloqueo del dispositivo, ya sean biométricos o de contraseña. En el caso de uso de mecanismos de seguridad por contraseña, PIN o patrón, seleccionar los mismos con la mayor seguridad posible haciendo uso de contraseñas largas, con mayúsculas y minúsculas en el caso que corresponda y no utilizar datos triviales o que se puedan descubrir fácilmente. Es importante también reducir al mínimo el tiempo de bloqueo de pantalla del dispositivo.
- **Hacer uso de los mecanismos de seguridad remota y cifrado.** Es muy importante hacer uso de todos los mecanismos facilitados por la plataforma activando la localización y borrado remoto de datos, así como el cifrado de los datos contenidos en el dispositivo. Esto facilitará la no revelación de los datos en caso de robo o pérdida.
- **Instalación de aplicaciones.** Mantener el dispositivo con el permiso para la instalación de aplicaciones de terceros desactivada. En caso de tener que instalar una aplicación no disponible en un market, instalar solamente aplicaciones de confianza y restablecer el permiso. Siempre que sea posible utilizar solamente los market oficiales para la descarga e instalación de aplicaciones y revisar los permisos de las mismas tanto antes de su instalación como periódicamente. Además, se puede hacer uso de plataformas como Virus Total para el análisis de aplicaciones antes de su instalación.
- **Menos es más en seguridad.** Se debe mantener el menor número de aplicaciones instaladas en el dispositivo de cara a tener el control en seguridad, cualquier instalación o actualización de una aplicación puede convertir el dispositivo en un foco no seguro.
- **No rootear el dispositivo.** Aunque es una práctica relativamente habitual, es muy insegura ya que se pierde la garantía de ejecución en sandbox ofrecida por el sistema operativo y, además, cualquier aplicación podría ser ejecutada con los permisos de superusuario con los problemas de seguridad que esto conlleva.
- **Desactivar los elementos de conectividad no utilizados.** Desactivar cuando no se utilicen los elementos de conectividad del dispositivo como pueden ser el bluetooth, WiFi y sobre todo NFC de cara a no facilitar ataques por esas vías. Además, es importante que estas funcionalidades no estén disponibles para activar o desactivar en el menú superior desplegable ya que éste es accesible hasta el momento de redacción de este TFM con el dispositivo bloqueado, por lo que, un atacante podría habilitarlos si así lo desea.

- **Conexiones WIFI.** No utilizar conexiones no cifradas para el transporte de datos, sobre todo no realizar acciones importantes en redes abiertas. No utilizar redes ocultas ya que puede dar lugar a problemas de seguridad igualmente. De ser posible, activar la aleatoriedad de MAC en la configuración de WIFI. En caso de utilizar este tipo de redes, eliminar el historial de WiFi para que el dispositivo no las recuerde.
- **Copias de seguridad.** De cara a minimizar el impacto de un robo, pérdida o destrucción de información en el dispositivo, siendo además este tipo más vulnerable a estos riesgos que otros, es importante hacer uso de las copias de seguridad. Se deben realizar copias de seguridad del dispositivo de modo regular y almacenarlas en un lugar seguro. Google proporciona herramientas integradas para ello.
- **Deshabitar servicios premium.** De cara a minimizar el impacto ante un ataque o infección, es importante deshabilitar las llamadas a números premium, así como los mensajes con el operador de telefonía móvil.
- **Instalar herramienta de seguridad.** En este estudio se ha concluido que la instalación de una herramienta de seguridad aporta en todos los casos valor, por lo que es recomendable el uso de una de ellas en el dispositivo.
- **Hacer uso responsable del dispositivo.** Para concluir, se aporta la más importante de todas las recomendaciones, es muy importante hacer un uso responsable del dispositivo y que el usuario esté concienciado en materia de seguridad. Se han de aplicar también a los dispositivos móviles otras recomendaciones generales de seguridad como pueden ser la navegación segura (https), prestar especial atención en los email y SMS, sobre todo en links o adjuntos, para no ser objeto de campañas de phishing que puedan desencadenar en una infección o compromiso de nuestros datos. Prestar atención a las llamadas recibidas por si pudieran ser maliciosas.

Es muy importante que el usuario de un dispositivo tome consciencia de la cantidad de datos personales y accesos comprometidos que hoy por hoy tiene en su él, de cara a que sea consciente de lo importante que es la seguridad en los teléfonos móviles. Además, se ha de tener en cuenta lo especialmente vulnerables que son los mismos simplemente por su propia naturaleza. Por ello, cualquier medida de seguridad es poca y como siempre, el uso responsable y el conocimiento de los problemas y puesta en práctica de las mitigaciones existentes serán los mayores aliados a la hora de mantener un sistema seguro.

7 Conclusiones y trabajo futuro

A lo largo de este capítulo se darán a conocer las limitaciones existentes o eventos que han supuesto un cambio de planteamiento a la hora de realizar el trabajo, así como las conclusiones obtenidas del mismo y posibles líneas de trabajo futuras.

7.1 Desarrollo del trabajo

Durante el Desarrollo del piloto han surgido una serie de limitaciones en el camino que han desviado un poco el desarrollo del mismo de su planteamiento inicial.

Por una parte, la idea inicial era la ejecución del piloto en una máquina Android virtualizada haciendo uso de la aplicación VirtualBox como contenedor de la máquina virtual proporcionada por Android-x86 (Android-x86, n.d.) . Debido a la importancia de un sistema operativo actualizado, se haría uso de la última versión disponible del sistema operativo en el momento que es Android 9.0-R2 Pie. Para facilitar el trabajo de instalación, se usaría la imagen preinstalada de la máquina disponible a través de la web de OsBoxes (OsBoxes, n.d.). Finalmente, y debido a los problemas causados por la inestabilidad de la máquina, a la dificultad de controlarla en algunas ocasiones y a problemas con la aplicación de monitorización utilizada la cual tenía bastantes problemas en las grabaciones, se optó por utilizar el dispositivo físico Xiaomi Redmi Note 5 para el estudio.

Por otro lado, la idea inicial de muestras de malware para el estudio era basada en familias de malware, conforme iba avanzando en el mismo, la dificultad de realizar esta segmentación sobre una base de datos de programas maliciosos era más latente. Tras diversas pesquisas y consultas no se pudo obtener la segmentación de la base de datos de AndroZoo con las familias o tipologías de malware. Dado que la base de datos utilizada ofrecía la segmentación de la misma por otros campos como pueden ser el market del que se obtuvo la apk o el nivel de detección por antivirus, se optó por realizar este estudio que podría resultar atractivo y novedoso.

7.2 Conclusiones

La principal conclusión que se obtiene del trabajo realizado es la problemática existente con el malware en el sistema operativo Android. Existe multitud de malware para la plataforma Android y ésta se ve afectada por multitud de familias de programas malicioso, desde el simplemente molesto adware a infecciones más peligrosas como pueden ser troyanos.

Más allá de lo que se pueda pensar, el malware no viene dado solamente por descargas de apk desde páginas desconocidas u otras actividades peligrosas realizadas desde un dispositivo móvil, sino que, tal y como se ha podido comprobar en este estudio, existe una

gran cantidad de malware existente en el Play Store de Google. La problemática de la descarga de aplicaciones maliciosas desde market oficiales es todavía mayor ya que el usuario no es consciente de ello y además se ve protegido por el Play Protect el cual está generando una falsa seguridad en el usuario. Tal y como se pudo comprobar en el dataset descargado para el estudio, existen multitud de programas maliciosos que han estado disponibles para la descarga en markets oficiales.

Google trabaja día a día para mejorar la seguridad de su sistema operativo, hecho que se ha puesto en evidencia a lo largo de este trabajo, el sistema operativo ha mejorado con el paso de los años introduciendo controles o mejoras de seguridad a todos los niveles con la finalidad de hacer el sistema Android cada vez más seguro. Algunas de ellas son:

- Ejecución de aplicaciones en sandbox y sistema de permisos de las mismas.
- Google Play Protect analiza las aplicaciones del market con la finalidad de detectar malware.
- Cifrado de dispositivo por defecto.
- Posibilidad de localizar el dispositivo y eliminar los datos del mismo de forma remota.
- Bloqueo del dispositivo mediante contraseñas y controles biométricos.

Con el conocimiento de la problemática existente, multitud de empresas basan su negocio en aportar soluciones para intentar minimizar o paliar este problema. A lo largo de este estudio se han analizado un conjunto de ellas, en base a él, se concluye que aportan otra capa más de seguridad o protección al dispositivo a pesar de no ser infalibles, además su instalación no supone una carga en el rendimiento del dispositivo. Es necesario conocer que, pese a disponer de una de estas aplicaciones instaladas en el dispositivo, la seguridad total no se obtendrá nunca. Hay que destacar que la mayor seguridad reside en las personas y en el control de sus actos, cada usuario debe conocer y actuar con seguridad en el uso de los dispositivos y por supuesto, siempre poner las máximas capas de seguridad posibles.

7.3 Trabajo futuro

Respecto a trabajos futuros que complementen o continúen el estudio desarrollado en el presente TFM. A continuación, se presentan algunos posibles trabajos siguiendo las líneas de herramientas de seguridad o malware en Android.

En el presente trabajo se segmenta el dataset obteniendo malware reciente descargable de Google Play Store y se selecciona la muestra en relación a las estadísticas de detectabilidad del mismo ofrecidas por la base de datos. Para complementar este trabajo, se podría trabajar sobre otro segmento diferente y realizar comparaciones de los resultados obtenidos en ambos

estudios. Así mismo, también se podría realizar la selección de malware por familias y estudiar la efectividad de las herramientas, pudiendo incluso llegar a obtener resultados de si existen herramientas especializadas en la detección de ciertas familias de malware.

Otro posible trabajo sería un estudio más exhaustivo de los datos de rendimiento de las diferentes aplicaciones analizadas en una serie de dispositivos.

Se podría trabajar también en la línea de la automatización de la metodología utilizada para el estudio de modo que fuese posible realizar el mismo con un número mucho mayor de aplicaciones, de muestras de malware o de ambas.

Realizar el estudio en distintos dispositivos con diferentes versiones del sistema operativo o con capacidades de hardware dispares para ver si los resultados obtenidos del mismo se encuentran alineados o no.

8 Referencias bibliográficas y enlaces

3C. (n.d.). *3C All-in-One Toolbox | 3C portal*. Retrieved May 20, 2021, from http://www.3c71.com/android/?q=node/916

AhnLab. (n.d.). *Leader in Cyber Threat Analysis and Response | AhnLab*. Retrieved May 16, 2021, from https://global.ahnlab.com/site/main.do

Alcántara, B. (2020). *La mejor guía de seguridad en Android para un móvil 100% seguro*. https://andro4all.com/2019/04/guia-seguridad-android

Allix, K., Bissyandé, T. F., Klein, J., & Traon, Y. L. (2016). AndroZoo: Collecting Millions of Android Apps for the Research Community. *2016 IEEE/ACM 13th Working Conference on Mining Software Repositories (MSR)*, 468–471.

Alsop, T. (n.d.). *Global device shipments 2013-2020 | Statista*. Retrieved April 24, 2021, from https://www.statista.com/statistics/265878/global-shipments-of-pcs-tablets-ultra-mobiles-mobile-phones/

Alswaina, F., & Elleithy, K. (2020). Android malware family classification and analysis: Current status and future directions. In *Electronics (Switzerland)* (Vol. 9, Issue 6, pp. 1–20). MDPI AG. https://doi.org/10.3390/electronics9060942

Android. (n.d.-a). *Flujo de arranque | Android Open Source Project*. Retrieved May 8, 2021, from https://source.android.com/security/verifiedboot/boot-flow

Android. (n.d.-b). *Seguridad de la aplicación | Android Open Source Project*. Retrieved May 15, 2021, from https://source.android.com/security/overview/app-security

Android. (n.d.-c). *Seguridad del sistema y del kernel | Android Open Source Project*. Retrieved May 9, 2021, from https://source.android.com/security/overview/kernel-security

Android Developers. (n.d.-a). *Arquitectura de la plataforma | Desarrolladores de Android*. Retrieved April 17, 2021, from https://developer.android.com/guide/platform?hl=es-419

Android Developers. (n.d.-b). *Manifest.permission | Desarrolladores de Android | Android Developers*. Retrieved April 18, 2021, from https://developer.android.com/reference/android/Manifest.permission.html

Android Developers. (n.d.-c). *Sugerencias de seguridad | Desarrolladores de Android*. Retrieved May 6, 2021, from https://developer.android.com/training/articles/security-tips

Android Malware Dataset. (n.d.). Retrieved May 23, 2021, from http://amd.arguslab.org/

Android-x86. (n.d.). *Android-x86 - Porting Android to x86*. Retrieved May 18, 2021, from https://www.android-x86.org/

Androzoo home. (n.d.). Retrieved May 27, 2021, from https://androzoo.uni.lu/

Anexo:Historial de versiones de Android - Wikipedia, la enciclopedia libre. (n.d.). Retrieved July 11, 2021, from https://es.wikipedia.org/wiki/Anexo:Historial_de_versiones_de_Android

Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H., & Rieck, K. (2014, May 12). *Drebin: Effective and Explainable Detection of Android Malware in Your Pocket*. https://doi.org/10.14722/ndss.2014.23247

Avast. (n.d.). *Aplicación antivirus gratuita para Android | Avast Mobile Security*. Retrieved May 16, 2021, from https://www.avast.com/es-es/free-mobile-security

AVG. (n.d.). *Tienda AVG | Conozca los productos y precios | Compre ya AVG*. Retrieved May 16, 2021, from https://www.avg.com/es-es/store#mobile

Avira. (n.d.). *Descargar Avira Free Security*. Retrieved May 16, 2021, from https://www.avira.com/es/acq-free-security?x-c-channel=sem6&x-a-source=Media&x-a-medium=SEM&x-a-network=Search&gclid=CjwKCAjwhYOFBhBkEiwASF3KGUBYx0hp5Y0Q_YQjsIU8wDPXQyj6M2wv6iVuYVu_U6ONpWenaS7E4BoCtYsQAvD_BwE

AVL. (n.d.). *AVL Mobile Security | Guarding the Security of Mobile Intelligence Era | Superior Anti-virus Engine, AV-Test Best Protection*. Retrieved May 16, 2021, from https://www.avlsec.com/en/main/about

AV-TEST. (n.d.). *AV-TEST | Ensayos independientes de software antivirus*. Retrieved May 15, 2021, from https://www.av-test.org/es/?r=1

Beatriz Alcántara. (n.d.). *La mejor guía de seguridad en Android para un móvil 100% seguro*. Retrieved May 16, 2021, from https://andro4all.com/2019/04/guia-seguridad-android

Bitdefender. (n.d.). *Bitdefender Mobile Security - Buscar con Google*. Retrieved May 16, 2021, from https://www.google.com/search?client=firefox-b-d&q=Bitdefender+Mobile+Security

Bradshaw, K. (n.d.). *Distribution data for Android*. Retrieved April 17, 2021, from https://androiddistribution.io/#/

CARMA. (n.d.). Retrieved May 23, 2021, from https://tacyt.elevenpaths.com/carma

CCN. (2016). *CCN-CERT BP/03 Dispositivos Móviles 2 Centro Criptológico Nacional*. www.ccn-cert.cni.es

CCN. (2019). *Guía de Seguridad de las TIC Guía práctica de seguridad en dispositivos móviles Android 9*.

CIS. (2018). *CIS Google Android Benchmark*.

Contagio. (n.d.). *contagio mobile*. Retrieved May 23, 2021, from http://contagiominidump.blogspot.com/

Deloitte. (n.d.). *Global Mobile Consumer Survey, 2017 España*.

Ditrendia. (202 C.E.). *Todas las estadísticas sobre móviles que deberías conocer en 2020*. https://mktefa.ditrendia.es/blog/estadisticas-moviles-2020

DroidBench. (n.d.). *GitHub - secure-software-engineering/DroidBench: A micro-benchmark suite to assess the stability of taint-analysis tools for Android*. Retrieved May 23, 2021, from https://github.com/secure-software-engineering/DroidBench

ESET. (n.d.). *ESET Mobile Security: Antivirus para Android | ESET*. Retrieved May 16, 2021, from https://www.eset.com/es/hogar/mobile-security-android/

ESET. (2014). *¿Cómo configurar tu Android de la forma más segura?* 22. https://www.welivesecurity.com/wp-content/uploads/2014/07/guia_seguridad_android_eset.pdf

F-Secure. (n.d.). *F-Secure SAFE — Seguridad en Internet para todos los dispositivos | F-Secure*. Retrieved May 16, 2021, from https://www.f-secure.com/es/home/products/safe

Google. (n.d.). *Una mayor protección contra las aplicaciones dañinas con Google Play Protect - Ayuda de Google Play*. Retrieved May 16, 2021, from https://support.google.com/googleplay/answer/2812853?hl=es

Google Play. (n.d.). Retrieved July 11, 2021, from https://play.google.com

Gurdip Kaur, & Arash Habibi Lashkari. (2021). *Understanding Android Malware Families (UAMF) – The Foundations (Article 1) | IT World Canada Blog*. https://www.itworldcanada.com/blog/understanding-android-malware-families-uamf-the-foundations-article-1/441562

IKARUS Security Sofware. (n.d.). *IKARUS mobile.security – IKARUS Security Software*. Retrieved May 16, 2021, from https://www.ikarussecurity.com/en/private-customers/ikarus-mobile-security/

Innoves. (n.d.). *[PASO A PASO] Guía de seguridad en móvil Android 2021 - INNOVES.ES*. Retrieved May 16, 2021, from https://innoves.es/guia-seguridad-movil-android-2021/

Innoves. (2021). *[PASO A PASO] Guía de seguridad en móvil Android 2021 - INNOVES.ES*. https://innoves.es/guia-seguridad-movil-android-2021/

Kantar World Panel. (n.d.). *Android vs. iOS – Smartphone OS sales market share evolution*. Retrieved April 11, 2021, from https://www.kantarworldpanel.com/global/smartphone-os-market-share/

Kaspersky. (n.d.). *Kaspersky Total Security 2021 | Protección de equipos PC, Mac y Android | Kaspersky*. Retrieved May 16, 2021, from https://www.kaspersky.es/total-security

Kiss, N., Lalande, J.-F., Leslous, M., & Viet Triem Tong, V. (2016). *Kharon dataset: Android malware under a microscope*.

Kouliaridis, V., Kambourakis, G., & Peng, T. (2020). Feature importance in Android malware detection. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 1449–1454. https://doi.org/10.1109/TrustCom50675.2020.00195

Maiorca, D., Ariu, D., Corona, I., Aresu, M., & Giacinto, G. (2015). Stealth attacks: An extended insight into the obfuscation effects on Android malware. *Computers and Security*, *51*, 16–31. https://doi.org/10.1016/j.cose.2015.02.007

Malwarebytes. (n.d.). *Malwarebytes: seguridad informática para usuarios domésticos y empresas | Malwarebytes*. Retrieved May 16, 2021, from https://es.malwarebytes.com/

McAfee. (n.d.). *McAfee Mobile Security, el servicio de seguridad móvil líder para Android, BlackBerry y Symbian | Inicio*. Retrieved May 16, 2021, from https://www.mcafeemobilesecurity.com/

Norton. (n.d.). *Norton 360 |Seguridad para PC,Mac,Android y iOS*. https://es.norton.com/360

OnAv. (n.d.). *OnAV*. Retrieved May 15, 2021, from https://www.onvaccine.com/

OsBoxes. (n.d.). *Android x86 Virtual Machine images for VMware and VirtualBox*. Retrieved May 24, 2021, from https://www.osboxes.org/android-x86/#android-x86-9-0-r2-info

Pandeli, T. (2016). *Requesting Runtime Permissions in Android M and N - SitePoint*. https://www.sitepoint.com/requesting-runtime-permissions-in-android-m-and-n/

Programmersought. (n.d.). *Explanation of UID, GID and PID in Android - Programmer Sought*. Retrieved May 8, 2021, from https://www.programmersought.com/article/78426619502/

Rivera, R. (2018). *Detección y Clasificación de Malware con el sistema de Análisis de Malware Cuckoo*.

Total AV. (n.d.). *Gratis Antivirus 2021 - Download Gratis Antivirus & Sistema Seguridad - TotalAV*. Retrieved May 15, 2021, from https://www.totalav.com/es/antivirus-gratis

Tsiatsikas, Z., Geneiatakis, D., Kambourakis, G., & Keromytis, A. D. (2015). An efficient and easily deployable method for dealing with DoS in SIP services. *Computer Communications*, *57*, 50–63. https://doi.org/10.1016/j.comcom.2014.11.002

Villanova Pascual, O. (2016). *Malware en Android y medidas de*.

VirusShare. (n.d.). *VirusShare.com*. Retrieved May 23, 2021, from https://virusshare.com/about

Wikipedia. (n.d.). *Android - Wikipedia, la enciclopedia libre*. Retrieved April 17, 2021, from https://es.wikipedia.org/wiki/Android#Referencias

Zhou, Y., & Jiang, X. (2012). Dissecting Android malware: Characterization and evolution. *Proceedings - IEEE Symposium on Security and Privacy*, 95–109. https://doi.org/10.1109/SP.2012.16

ANEXO I. TABLA DE VERSIONES ANDROID

En la siguiente tabla (Tabla 10) se presenta la evolución del sistema operativo aportando nombre de la versión, número, fecha de lanzamiento, así como las novedades más relevantes introducidas por cada una de las versiones.

Tabla 10. Versiones de Android con principales características

Nombre	Número de versión	Fecha de lanzamiento	Principales novedades
Apple Pie	1.0	23 de septiembre de 2008	Contiene muchos de los componentes básicos que aparecen en Android, ejemplo de ello son la pestaña de notificaciones en la parte superior de la pantalla, posibilidad de añadir widgets en la pantalla de inicio o el Android Marquet, no obstante, el listado de aplicaciones es menor. Posee una excelente integración con Gmail e incluye las principales aplicaciones como, por ejemplo, el navegador, el reloj o la calculadora.
Banana Bread	1.1	9 de febrero de 2009	Considerada la única actualización de Android 1. Proporciona una solución a una gran lista de errores. El modo de realización de esta actualización es la única característica revolucionaria, *over the air* (OTA), puesto que hasta el momento no había existido otro sistema operativo con tal particularidad.
Cupcake	1.5	25 de abril de 2009	Dos años después del lanzamiento de Android 1.1 aparece esta actualización, la cual muestra algunas pequeñas mejoras en el diseño (sobre todo sombras o transparencias), lo que la hace más atractiva. También se incluye soporte para teclados virtuales y la posibilidad de añadir *widgets* de otras aplicaciones. Se añade también la posibilidad de copiar y pegar en el navegador, crear transiciones de pantalla animadas, rotar la pantalla de forma automática y subir vídeos a YouTube.
Donut	1.6	15 de septiembre de 2009	De esta actualización destaca sobre todo la introducción del cuadro de búsqueda rápida. Android Market comienza a destacar y también lo hacen la cantidad de aplicaciones disponibles. Esta versión permite adaptar tanto el tamaño como la resolución de la pantalla, dando lugar de esta forma a las innumerables configuraciones posibilitan el uso de Android en dispositivos muy diferentes. Entre las novedades se incluyen también el sintetizador de voz disponible en diferentes idiomas, diversas mejoras en la cámara fotográfica y en la galería, tales como la selección múltiple de fotos para su borrado. En cuanto a la conectividad, se integra soporte para conexiones VPN y redes CDMA.
Eclair	2.0 – 2.1	26 de octubre de 2009	Esta versión incluye novedades como Google Maps, el soporte multicuenta (posibilidad de disponer de más de una cuenta en el mismo dispositivo) y la sincronización con cuentas de terceros, como, es el caso de Facebook. La interfaz visual se actualiza y proporciona también un mayor número de tamaños de pantalla y de resoluciones. Además, también contiene los Live Wallpapers y la cámara se mejora a través de un soporte para flash, escenas y zoom digital. También se actualizan gran parte de las aplicaciones incluidas en el sistema operativo como por ejemplo Google Maps, el calendario, el navegador o el teclado virtual, el cual ya anteriormente incluía diccionario y proporcionaba sugerencias de nombres de contactos.
Froyo	2.2 – 2.2.3	20 de mayo de 2010	En cuanto a los cambios destacan: la creación de puntos de acceso Wi-Fi y el soporte para comandos de voz. Además, también contiene una primera versión de Google Assistant; anteriormente, ya se podían realizar acciones como buscar, programar alarmas, escribir notas u obtener direcciones a través de la voz. Cabe también mencionar el gran impulso de velocidad y rendimiento. El navegador mejora gracias a la integración del motor V8 de Javascript de Chrome, además añade soporte para GIF animados y para la subida de archivos Tras esto llegan las notificaciones push a través del servicio Android Cloud to Device Messaging (C2DM) y, por primera vez, es posible mover aplicaciones a la tarjeta SD.

Nombre	Número de versión	Fecha de lanzamiento	Principales novedades
Gingerbread	2.3 – 2.3.7	6 de diciembre de 2010	Puesto que ya poseía un excelente sistema operativo, las novedades simplemente fueron mejoras. En él se incluye soporte para NFC, API para juegos o el soporte para el uso de diversas cámaras en un mismo dispositivo. Además, también se crea la posibilidad de seleccionar fragmentos dentro de un texto en lugar de la selección del texto completo y se mejora una vez más el teclado virtual. Esta versión fue revisada hasta 7 veces antes de pasar a la siguiente versión, en la 2.3.4 se incluyen las videollamadas en Hangouts.
Honeycomb	3.0 – 3.2.6	22 de febrero de 2011	Integra System Bar, una barra inferior semejante a la barra de tareas de Windows. En ella se pueden encontrar los botones de navegación, la hora y el acceso a los ajustes rápidos (simplemente con un toque en la barra de sistema se podía ver la hora, fecha, el nivel de batería y el estado de la conexión sin necesidad de ir a los ajustes). Gingerbread también proporciona la aceleración a través de hardware, el soporte para procesadores de varios núcleos, el soporte para USB OTG, la conectividad con teclados y dispositivos señaladores externos y la posibilidad de cifrar todos los datos de usuario. Las aplicaciones solamente podrán escribir en almacenamiento secundario en su propia carpeta.
Ice Cream Sandwich	4.0 – 4.0.5	18 de octubre de 2011	Es una de las versiones que incluye el mayor cambio hasta la fecha. El sistema adoptaba el estilo Holo que dominará la plataforma hasta que llegue Material Design. La barra de sistema de Honeycomb se convertía en la barra de navegación en pantalla, y el soporte para NFC se usaba para la transferencia de datos con Android Beam. Se incluyen múltiples opciones de personalización, con las carpetas en el escritorio y el selector de widgets separados en otra pestaña. Es la primera versión en integrar el sistema de captura de pantalla nativa con la combinación volumen- y encendido y las estadísticas de uso de datos totales y por aplicación, diferenciando entre transferencias en primer y segundo plano. En esta versión se incluye también incluye el desbloqueo facial Face Unlock y la posibilidad de lanzar aplicaciones directamente desde la pantalla de bloqueo. Por lo que a las notificaciones respecta, se incluye la posibilidad de eliminar una notificación deslizándola.
Jelly Bean	4.1 – 4.3.1	9 de julio de 2012	Jelly Bean no tiene muchos cambios importantes, pero sí modifica gran parte de los componentes de Android para mejorar su funcionamiento y rendimiento. Por ejemplo, las notificaciones no solo podían descartarse individualmente, sino que ahora podían incluir acciones. También llegaban los Ajustes rápidos al panel de notificaciones. Se incluyen varias mejoras de accesibilidad, como el toque triple para usar la lupa, el deslizamiento y zoom con dos dedos o el modo hablado y la navegación por gestos para usuarios con problemas de visión.
KitKat	4.4 – 4.4.4	31 de octubre de 2013	Android KitKat es una de las versiones de Android más emblemáticas incluyendo el nuevo diseño para el marcador y "Ok Google". Se incluye una actualización de la interfaz incluyendo iconos más claros y transparencias: en el panel de notificaciones, en la barra de navegación y en Google Now, que ahora se desplegaba sobre el escritorio. El modo inmersivo llegaba también con esta versión: la barra de estado y la barra de navegación se ocultaban para dejarle todo el protagonismo a la aplicación. KitKat incluye el nuevo Android Runtime (ART) para reemplazar a la máquina virtual de Dalvik de modo experimental, pero su uso está deshabilitado de fábrica. La API de accesibilidad sigue creciendo y se otorga un nuevo aspecto de varias aplicaciones como el Reloj, Teléfono y Descargas.

Nombre	Número de versión	Fecha de lanzamiento	Principales novedades
Lollipop	5.0 – 5.1.1	12 de noviembre de 2014	El diseño de Google Now se expande, documenta y aplica a todo Android: llega Material Design.Se incluye la posibilidad de mostrar notificaciones en la pantalla de bloqueo. Vuelve a ser posible el almacenamiento externo como en tarjetas SD. El experimento de ART y su compilación de aplicaciones AOT es un éxito y reemplaza oficialmente al viejo Dalvik. Mediante el Proyecto Volta, se introducen mejoras de rendimiento y batería: modo de ahorro de energía y programación de tareas para que se ejecuten solo con WiFi para ahorrar batería al reducir el uso de los datos móviles. Se incluye la vista de aplicaciones recientes con tareas y es posible fijar aplicaciones para dificultar la salida de ellas. Otras novedades interesantes son la búsqueda dentro del menú o la aplicación linterna integrada en el sistema operativo. Con la actualización a Lollipop 5.1, llegan la protección antirrobo tras reinicio de y el soporte oficial para varias tarjetas SIM.
Marshmallow	6.0 – 6.0.1	5 de octubre de 2015	Esta versión se enfoca es seguir mejorando y cohesionando todo el sistema. Se remodela el sistema de permisos permitiendo la solicitud de permisos por parte de las aplicaciones cuando es necesario y no en su instalación. Para optimizar el rendimiento de la batería, obliga a las aplicaciones a dormir y reduce la velocidad de la CPU cuando la pantalla está apagada, para alargar la duración de la misma. Se introduce el soporte a nuevas tecnologías: USB-C, modo 4K para aplicaciones, multiventana y el soporte nativo para el lector de huellas. Desaparece el soporte para Miracast. Esta versión añade Direct Share, la forma más rápida de enviar contenido a un contacto específico y Now On Tap, botón que busca qué hay en la pantalla para ofrecer información relacionada.
Nougat	7.0 – 7.1.2	15 de junio de 2016	En esta versión de Android se refinan algunos elementos heredados que necesitaban atención. En cuanto al rendimiento, se incluyen mejoras en Doze, haciéndolo efectivo incluso cuando el teléfono está en movimiento. Además, gracias al nuevo compilador JIT, que requiere menor almacenamiento, se reduce considerablemente la instalación de las aplicaciones. De cara al usuario, se introducen mejoras como la respuesta rápida directamente desde la notificación, la plataforma VR Daydream, el modo multiventana y los gráficos de consola con Vulkan 3D. En esta versión se permite que aplicaciones de terceros añadan botones a los ajustes rápidos. Llega también Unicode 9.0 y los emojis con distintos tonos de piel, la calibración de color para la pantalla, las actualizaciones del sistema seamless, el modo de ahorro de datos y la posibilidad de elegir varios idiomas.
Oreo	8.0 – 8.1	21 de agosto de 2017	Para poner solución al problema de la fragmentación, sale a la luz Project Treble, una buena promesa de actualizaciones más rápidas. Una nueva arquitectura modular del sistema para facilitar el proceso de actualizar un terminal y, teóricamente, lograr que lleven menos trabajo y, por tanto, lleguen antes a todos los dispositivos. El modo Picture-in-Picture deja de ser exclusivo de Android TV y llega a los teléfonos, llegan también los iconos adaptativos, ya no han de ser redondos. La mayor cantidad de cambios se encuentra en las notificaciones: canales de notificación, insignias de notificación, notificaciones multimedia rediseñadas y posibilidad de silenciar notificaciones. Otra novedad importante es la API de autocompletado de formularios, que se puede usar tanto para aplicaciones como para páginas web. En cuanto al rendimiento, se reduce el uso de batería y datos de aplicaciones en segundo plano. Android Oreo 8.1 se desdoblará en una versión especial GO, para móviles con poca RAM.

Nombre	Número de versión	Fecha de lanzamiento	Principales novedades
Pie	9.0	6 de agosto de 2018	Google introducía varios cambios en el sistema que limitaban que las aplicaciones usaran la cámara de fondo, pero los cambios se centraban más en modernizar Android. Llegaban así el brillo y la batería inteligente, las aplication actions y las slices, por las cuales el sistema intentaba anticiparse a lo que necesitábamos aprendiendo de nuestras pautas de uso. El bienestar digital es otra de las grandes novedades, una serie de herramientas con las que se puede controlar el uso que se hace del móvil. Se introduce en esta versión la navegación por gestos de forma oficial.
10	10.0	3 de septiembre de 2019	Algunas de las mejoras más significativas introducidas en esta versión son: Mediante Live Caption se subtitulan automáticamente vídeos, podcasts, mensajes de audio e incluso videos grabados con el terminal. Con Sound Amplifier, el teléfono es capaz de aumentar el sonido, filtrar el ruido de fondo y ajustar el audio con el fin de que se pueda escuchar mejor. Los gestos en Android 10 son más rápidos e intuitivos. Se incluye un nuevo tema oscuro para conservar la duración de la batería durante más tiempo. Google presume de que, de momento, los dispositivos plegables y 5G solo están disponibles en Android", por lo que ha tratado de optimizar para este tipo de terminales el sistema operativo y ha introducido nuevas funcionalidades para este tipo de dispositivos. Con respecto a la privacidad, se incluyen nuevos controles inteligentes que permiten decidir cómo y cuándo se comparten los datos del dispositivo, y encontrar más fácilmente todas las configuraciones de privacidad para ajustarlas. En este sentido, es posible decidir qué datos de las aplicaciones y de la actividad web se almacenan y por cuánto tiempo, así como controlar cuándo se comparte la ubicación con las aplicaciones: todo el tiempo, mientras están en uso o nunca. También se puede la personalización de anuncios en función de los propios intereses. Un punto muy importante es que Google asegura que los dispositivos con Android 10 recibirán las actualizaciones de seguridad periódicas más rápido y fácil gracias al sistema de actualizaciones a través de Google Play. Android 10 introduce varias novedades en la herramienta Bienestar Digital, entre las que destacan los temporizadores para los sitios webs y Focus Mode, un sistema para bloquear temporalmente el acceso a las aplicaciones en las que se invierte más tiempo. Además, Family Link, permite administrar aplicaciones estableciendo restricciones de contenido y límites de tiempo de pantalla, visualizar las aplicaciones utilizadas por los y comprobar dónde están en cualquier momento.

Nombre	Número de versión	Fecha de lanzamiento	Principales novedades
11	11.0	8 de septiembre de 2020	Como en la mayoría de las nuevas versiones de Android se realizan cambios en las notificaciones, en esta versión las notificaciones se separarán en tres grupos: conversaciones, notificaciones y silenciadas. Con respecto a las notificaciones de reproducción, ahora hay una única notificación, integrada en la parte de los ajustes rápidos y las notificaciones se agrupan paginadas en el caso de tener varias reproducciones a la vez. Además, en esta versión es posible acceder al historial completo de notificaciones y en las notificaciones de conversaciones es posible cambiar la prioridad de una conversación. Se introducen también las burbujas de chat, desde un botón en el panel de notificaciones, se puede convertir una conversación en una aplicación compatible en una burbuja de chat. Se permite la grabación de la pantalla del dispositivo en video. Uno de los cambios más radicales de Android 11 llega en el menú de apagado, desde él es posible controlar multitud de dispositivos. Las respuestas inteligentes siguen integrándose en cada vez más partes del sistema operativo. Se activa la conexión inalámbrica a Android Auto. En cuanto a los permisos, llegan los permisos de un uso, que otorgan el permiso sólo para una vez concreta. Si la aplicación lo necesita más tarde, deberá volver a pedirlo. Por otro lado, el dispositivo revocará permisos automáticamente de las aplicaciones que lleven mucho tiempo sin usarse. Además, si a una aplicación se le ha denegado reiteradamente un permiso, el sistema bloqueará por sí mismo el intento, de modo que no aparecerá la ventana al usuario. Para los perfiles empresariales, será más fácil separar el perfil de trabajo del personal, además de otras novedades relacionadas como la posibilidad de que el sistema cambie de perfil de trabajo al personal a cierta hora del día. En términos de accesibilidad, se mejora Google Voice Access, se incluye el soporte para la escritura en braille en Gboard y Lookout y se incorporan dos nuevos modos: escáner de documentos y etiquetas de comida.
12	12.0	agosto de 2021 (Previsión)	Google prepara grandes cambios para Android 12. Entre ellos, llega el soporte nativo para capturas de pantalla extendidas. También llegan cambios importantes a nivel de interfaz como una barra de búsqueda de widgets. Como es habitual, se esperan nuevos emojis y cambios en la barra de notificaciones, con nuevos controles y accesos directos. A nivel de privacidad, Android 12 mostrará un ajuste para que notifique al usuario cuando una aplicación accede al portapapeles. También habrá importantes cambios en la ubicación, ya que se podrá facilitar a las aplicaciones permisos para que localicen de forma precisa o tan solo aproximada. Todas estas funciones están en desarrollo y probablemente cambien en la versión definitiva.

ANEXO II. TABLA HERRAMIENTAS COMERCIALES ANTI-MALWARE

A continuación, en la Tabla 11 se proporcionan datos relevantes sobre las funcionalidades aportadas por cada una de las herramientas participantes en el estudio, así como otros datos que pudiesen ser de interés.

Tabla 11. Características extendidas de herramientas comerciales antimalware

Herramienta	Número de descargas (>)	Número de reseñas	Calificación	Versión Android	URL Compañía / Google Play	Antirrobo	Asesor de privacidad	Asesor /control de wifi	Bloqueo de llamadas	Control de aplicaciones	Copia de seguridad	Navegación segura	VPN	Otros	Premium
Ahnlab V3 Mobile Security	10.000.000	94.707	4,6	6.0	(AhnLab, n.d.) https://play.google.com/store/apps/details?id=com.ahnlab.v3mobilesecurity.soda	No	Sí	Sí	No	Sí	No	Sí	No	Borrado seguro de ficheros	No
AVAST Mobile Security	100.000.000	6.533.717	4,7	5.0	(Avast, n.d.) https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No		Sí
AVG Antivirus free	100.000.000	7.128.885	4,7	5.0	(AVG, n.d.) https://www.av-test.org/es/antivirus/moviles/android/marzo-2021/avg-antivirus-free-6.36-213203/	No	No	No	Sí	No	No	No	No		NO
Avira Antivirus Security	10.000.000	600.352	4,6	6.0	(Avira, n.d.) https://play.google.com/store/apps/details?id=com.avira.android	No	Sí	No	No	No	No	Sí	No		Sí
AVL Mobile Security	500.000	3.119	3,9	4.0.3	(AVL, n.d.)https://play.google.com/store/apps/details?id=com.antiy.avl	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Filtro de mensajes	Sí
Bitdefender Mobile Security	10.000.000	282.586	4,7	5.0	(Bitdefender, n.d.)	No	Sí	No	Sí	Sí	Sí	Sí	No	Filtro de mensajes	
ESET Mobile Security & Antivirus	10.000.000	896.409	4,8	4.1	(ESET, n.d.) https://play.google.com/store/apps/details?id=com.eset.ems2.gp&gl=ES	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí		NO
F-Secure Safe	1.000.000	14.068	4,3	5.0	(F-Secure, n.d.) https://play.google.com/store/apps/details?id=com.fsecure.ms.safe	Sí	Sí	No	No	Sí	No	Sí	Sí	Bloqueo de aplicaciones, Escáner de red, Protección de cámara y micrófono	Sí
GDATA Mobile Security	1.000.000	10.443	3,9	5.0	https://play.google.com/store/apps/details?id=de.gdata.mobilesecurity	Sí	No	Sí	No	Sí	No	Sí	Sí	Salvaguarda de identidad, Privacidad de cuenta, Asesor de seguridad, WearON	Sí

Herramienta	Número de descargas (>)	Número de reseñas	Calificación	Versión Android	URL Compañía / Google Play	Antirrobo	Asesor de privacidad	Asesor /control de wifi	Bloqueo de llamadas	Control de aplicaciones	Copia de seguridad	Navegación segura	VPN	Otros	Premium
Google Play Protect					(Google, n.d.)	Sí	Sí	No	No	Sí	No	Sí	No	Control parental	Sí
IKARUS mobile security	100.000	3.150	3,8	4.1	(IKARUS Security Sofware, n.d.) https://play.google.com/store/apps/details?id=com.ikarus.mobile.security	Sí	Sí	No	No	Sí	No	Sí	No		Sí
Kaspersky internet security	50.000.000	3.576.572	4,8	Varía según el dispositivo.	(Kaspersky, n.d.) https://play.google.com/store/apps/details?id=com.kms.free	No	No	No	No	Sí	No	No	No		
LINE Antivirus	5.000.000	77.746	4,4	4.0.3	https://play.google.com/store/apps/details?id=jp.naver.lineantivirus.android	Sí	Sí	No	No	No	No	Sí	No	Alertas de seguridad	Sí
Malwarebytes	10.000.000	330.011	4,6	6.0	(Malwarebytes, n.d.) https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware&gl=ES	Sí	No	No	Sí	Sí	No	Sí	No		Sí
McAfee Mobile Security	50.000.000	753.189	4,5	7.0	(McAfee, n.d.) https://play.google.com/store/apps/details?id=com.wsandroid.suite	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí		Sí
Norton 360	50.000.000	1.527.336	4,6	6.0	(Norton, n.d.) https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity	No	Sí	Sí	Sí	No	No	Sí	No	Monitorización Dark Web	
SECURION OnAV				5.0	(OnAv, n.d.)	No	No	Sí	No	Sí	No	Sí	Sí	Navegador de incognito	Sí
Total AV	1.000.000	30.436	4,2	5.0	(Total AV, n.d.) https://play.google.com/store/apps/details?id=com.totalav.android	No	No	No	No	No	No	No	No	Detección de rooteo, protección de mensajes, protección de red y control parental	
Trend Micro Mobile Security	1.000.000	86.646	4,6	4.1	(AV-TEST, n.d.) https://play.google.com/store/apps/details?id=com.trendmicro.tmmspersonal	Sí	Sí	Sí	Sí	Sí	No	Sí	No		Sí

ANEXO III. COMPARATIVA GUIAS DE SEGURIDAD ANDROID

En este anexo se facilita mediante Tabla 12, una comparativa de las diferentes guías de seguridad analizadas durante este trabajo. Se tienen en cuenta aspectos como el número de páginas, el nivel técnico de las mismas, si incluyen o no explicaciones adicionales o modos de auditar la seguridad y su nivel de síntesis de la información. Se analizan también las recomendaciones aportadas por cada una de ellas en la búsqueda de sinergias.

Tabla 12. Comparativa de guías de seguridad

	ESET ¿Cómo configurar tu Android de la forma más segura?	CCN - Configuración segura de dispositivos ANDROID	CCN - STIC 453 G Guía práctica de seguridad en dispositivos móviles Android 9	CIS Google Android	Andro4All	Innoves
	(ESET, 2014)	(CCN, 2016)	(CCN, 2019)	(CIS, 2018)	(Beatriz Alcántara, n.d.)	(Innoves, n.d.)
N.º páginas	22	1	138	98		
Explicación cómo realizar las tareas propuestas	BÁSICA	NO	EXTENDIDA	EXTENDIDA	Sí	Sí
Auditoría	NO	NO	NO	SI	No	No
Síntesis	Guía sintetizada con explicaciones	Folleto visual	Guía extendida	Guía extendida	Guía muy básica	Guía muy básica
Descargar aplicaciones solamente desde repositorios confiables	Sí					Sí
Borrar el historial de Google					Sí	
Sospechar de las aplicaciones que exigen demasiados permisos, pueden tener objetivos maliciosos / limitar los permisos asignados a las aplicaciones	Sí	Sí	Sí			Sí
No permitir la instalación desde orígenes desconocidos	Sí	Sí		Sí		Sí
No permitir acceso a Geolocalización	Sí					
Ocultar aplicaciones, mensajes y archivos multimedia mediante bloqueo por huella u otros métodos					Si	
Gran parte del malware proviene de enlaces fraudulentos en Redes Sociales	Sí					
Desinstalar las aplicaciones que no se usen		Sí	Sí			
Configurar acceso y bloqueo del dispositivo	Si	Sí	Sí	Sí	Sí	
Recomendación de longitud mínima de contraseñas		Al menos 8 caracteres	Al menos 8 caracteres			
Si se usa el bloqueo por patrón, desactivar el trazado de este	Sí		Sí	Sí		
Mantener el dispositivo actualizado sistema operativo/aplicaciones	Sí	Sí	Sí	Sí		
Proteger mediante PIN la tarjeta SIM	Sí			Sí		
Crear copias de seguridad: contactos, agenda, calendario	Sí		Sí		Sí	
Activar el cifrado de la información en el dispositivo	Sí		Sí			
Activar opciones de administración remota o usar programas como Android Device Manager (encontrar teléfono, borrado remoto, etc.)	Sí			Sí	Sí	
Borrar los datos en caso de un segundo uso del dispositivo por otra persona	Sí					
Desactivar los mecanismos como WiFi, Bluetooth, NFC cuando no se necesite		Sí	Sí	Sí		

	ESET ¿Cómo configurar tu Android de la forma más segura?	CCN - Configuración segura de dispositivos ANDROID	CCN - STIC 453 G Guía práctica de seguridad en dispositivos móviles Android 9	CIS Google Android	Andro4All	Innoves
Establecer bloqueo automático del dispositivo cuando no esté en uso		Sí	Sí	Establecerlo a inmediato y configurar el botón de encendido para ello		
Evitar conexión a redes abiertas		Sí		Desactivar la conexión automática a redes abiertas		Sí
Configurar la cuenta de usuario de Google con contraseña robusta y única y habilitar un segundo factor de autenticación			Sí			
Configurar mensaje pantalla de bloqueo				Sí		
Deshabilitar la opción de mostrar contraseñas			Sí	Sí		
Deshabilitar las opciones de desarrollador			Sí	Sí		
No rootear el dispositivo				Sí		
Deshabilitar Smart Lock			Sí	Sí		
Establecer fecha y hora automática				Sí		
Activar el escaneo del dispositivo en busca de amenazas de seguridad				Sí		
Activar la mejorar la detección de aplicaciones dañinas				Sí		
No permitir añadir usuarios desde la pantalla de bloqueo			Sí	Sí		
Eliminar perfiles de invitado			Sí	Sí		
Revisar permisos de las aplicaciones periódicamente			Sí	Sí		
Deshabilitar las notificaciones en pantalla de bloqueo			Sí	Sí		
Deshabilitar los servicios de localización cuando no estén en uso				Sí		
Eliminar de ajustes rápidos opciones sensibles como WiFi, zona WiFi, Bluetooth, NFC			Sí			
Habilitar función DNS privado			Sí			
Usar un gestor de contraseñas			Sí			
Orden aleatorio de las MAC conectadas			Sí			
Contar con una solución antivirus capaz de analizar las conexiones y los archivos que se ejecutan.	Sí				Sí	Sí
Deshabilitar ejecución de Java.	Sí					
Deshabilitar ejecución de Flash.	Sí					
Asegurarse de navegar siempre en sitios confiables con HTTPS	Sí					
No visitar sitios desconocidos.	Sí					
Deshabilitar la opción Recordar contraseñas.	Sí					
Deshabilitar la opción Habilitar ubicación.	Sí					

ANEXO IV. PROYECTO ANDROZOO

El listado de aplicaciones disponibles en el proyecto es actualizado diariamente y es un fichero de más de 1.9 GB comprimido.

El fichero csv tiene los datos representados en la Ilustración 57. Extracto del listado de apks en AndroZoo

sha256	sha1	md5	dex_date	apk_size	pkg_name	vercode	vt_detection	vt_scan_date	dex_size	markets
F453C81C720A43DF	A2DBA95D76FC68F185(	C6B9CCA258EE7591B	27/02/2021 21:54	26674063	com.glitchter.vhs.vaporwave	3	1	01/04/2021 12:11	8790936	play.google.com
F454C04581A316C3	AB84BFE3A2026E69762	C19F7DF9AF8FD0351	19/02/2021 9:29	18832366	com.wNewTamilSongsHD	1555510714	3	31/03/2021 11:05	8901916	play.google.com
F4561064E09CE2E2(	1C9DDD708EDF2B8694	F96F1ADF4E54AC74B	05/01/2021 19:20	13912760	com.xchrisapps.AgSundaySchoolLesson2	39	2	08/02/2021 10:40	8548944	play.google.com
F45EE32C64C6632E	A25EED890626169D2C	3A4E00FC9BEAD9FDI	27/03/2021 5:09	11122363	com.joy4ever.sarajayapp	2	1	25/05/2021 6:10	9911928	play.google.com
F46A3D0E6994416D	D79B2BBE8F317458601	388811F8CB3328089	20/04/2021 15:45	96270517	com.superplanet.swordmaster	273	1	21/04/2021 7:41	193612	play.google.com
F47506522A6BFA67(	CFC7B559944ACD035F(	735336BC83E40FDE8	01/01/2021 19:58	2728012	com.lebassaorg.ursitech	16	1	28/03/2021 7:37	2083496	play.google.com
F48F6D86DD877A7B	2909982D5C322B9259(	598E32E374BDB056E	23/03/2021 14:05	56975757	essentionalDevotionalR.ShivaSongsTelugu	2	1	01/04/2021 9:00	4133964	play.google.com
F490C16BF8B4F8E2(	F9588089252FE394E59/	D864566EB262F0FD2	15/03/2021 15:55	15652589	com.wTruthAndDare_13398236	1555545661	7	09/05/2021 8:01	8901916	play.google.com
F4972DD45B069C46	23AD0D66FB5BA21A7A	44F5D855625A90CDA	04/04/2021 8:06	14972511	com.saharahindnews	12	1	07/05/2021 7:16	10790416	play.google.com
F4B5CB783F52EC62	69AAC72FE8E872455D/	3B55F142FEA382980	02/01/2021 15:47	5742852	com.nasir.lifetimevpn	2	14	06/05/2021 7:05	11024	play.google.com
F4B68E4CB395EACB	C39FDD73687DA6A49B	175585AE425A34FF1(	26/01/2021 14:09	11189300	com.shopgate.android.app26154	546000	1	31/03/2021 9:23	9972620	play.google.com
F4C2D8C95D8C2FF4	B220EBC6159238E8403	4D1B86242DA59C8E(	21/04/2021 20:36	7017254	com.qatar.onlineshopping.onlinestoreqatar	2	1	23/05/2021 11:46	5912156	play.google.com
F4CF22FB9B4BE302	0AC0396ECA5701FBD7(	0ECE382899948EA27	11/01/2021 2:33	11840413	com.techoragon.tunnel	5	1	21/02/2021 8:15	1558024	play.google.com
F4D8D6D168B7FC08	178B96FB7F7C7EBA477	300E0A7531724860D	18/01/2021 14:18	15098821	com.wiRazoo_13048496	1555464924	2	11/04/2021 7:52	8901916	play.google.com
F4EF35A4379B0DBE	D97E1CB2DA5E32CBFB	1D4FD8A1A2AF22685	24/03/2021 11:21	32864404	com.dicedom.mergepuzzle	28	1	26/04/2021 7:11	8108380	play.google.com
F4F4D6068375F6FCI	D7DD3640611228B78EC	C0287BFA6853D9552	28/02/2021 22:09	66092119	com.qianyan.eudic	363	4	02/03/2021 0:13	16788224	play.google.com
F50C2C0DA3797735	851DC937E8BF858BAD(	E42C68740E4F9C93A	16/04/2021 14:30	12223169	com.ns.poetry	814	1	17/05/2021 6:27	10303748	play.google.com
F50E7C3EC41194A4	12CC0F53F7B5F90CFA5	3C9AB007AED4E11FE	27/02/2021 17:02	10417249	com.cnaccountancy.ca	1	2	08/04/2021 8:07	9880544	play.google.com
F5100D2B455B859E	0AC1FED118DBDC5585	949927A0A904E867A	27/01/2021 11:25	50226926	uk.co.hsbc.hsbcukmobilebanking	23511	1	25/02/2021 17:04	10094540	play.google.com
F511F59E37E731C9(	B7E54E4F4E2DEF41828	C58FCB7981A0625C8	16/01/2021 4:56	12305711	com.technohelper.ffdiamonds	11	5	17/02/2021 8:20	6124424	play.google.com
F513A63733E1265BI	9AF7A4934905E9F33B5	57D20911A4D655410	26/01/2021 15:34	12325916	com.dreame.writer	46	5	25/02/2021 7:50	7889792	play.google.com

Ilustración 57. Extracto del listado de apks en AndroZoo

- sha256, sha1, md5: Hashes de la aplicación en los distintos formatos
- dex_size: Tamaño del fichero classes.dex
- dex_date: Fecha en la que ha sido añadido al fichero dex. En ocasiones el valor es no válido y/o manipulado como la gran mayoría de las aplicaciones de Google Play tienen un dex_date de 1980
- apk_size: Tamaño de la apk
- pkg_name: el nombre del paquete Android (tal y como indica el archivo manifest).
- vercode: código de versión (tal y como indica el archivo manifest).
- vt_detection: El número de antivirus de VirusTotal (VT) que detectaron estos apks como un malware.
- vt_scan_date: Fecha de detección de antivirus de VirusTotal (VT) que detectaron estos apks como un malware.
- markets: una lista separada por '|' de los mercados en los que se encontró el APK.

El proyecto permite la descarga de las aplicaciones disponibles en su listado mediante el uso de su API proporcionando tanto el SHA256 como el APIKEY obtenida mediante registro en el proyecto.

Para más información se puede consultar la web del proyecto en la que se detallan los distintos modos de acceso(*Androzoo Home*, n.d.)

ANEXO V. MALWARE SELECCIONADO

En la siguiente tabla, Tabla 13. Malware seleccionado para el estudio, se muestra el malware seleccionado para el estudio, se muestra, el intervalo al que pertenece de entre los definidos, el nombre del archivo descargado y el nombre del paquete de AndroZOO y los datos facilitados por VirusTotal de porcentaje de detección y fecha de detección.

Tabla 13. Malware seleccionado para el estudio

Intervalo	Nombre del archivo	Hash md5	Fecha	Nombre paquete	Detección %
01-abr	0BE524D71BD912956C8DC3019936BC938860DAD9D9825AC41F7DE28512106FEC.apk	E4C17A730624D7270DDE8C4F433D9355	12/05/2021	com.vantop.heimlink	10%
01-abr	D897E663F58436A4D557A7A0394CCB83692EDA797CA485023B10C681879A5CA9.apk	2648BA4D4D6C7D042CB2589B9CC39E66	24/04/2021	com.real.police.cop.car.transporter.truck.cargo.game	2%
01-abr	424A64066279CEE1A41C0D57B863C67E7EE753FF1ED285A0C9F59D6A10825B4F.apk	71560A036C860DD692CC40AD3D6D4EB6	06/02/2021	com.rlapclub.pan_to_aadhaar_link.update_aadhar	2%
01-abr	D93CE1C5552364F1E71572D7F57D07F67EC42D82C04075047C8C168CE34CA5F5.apk	FD74230C0A10D1B7C167147E8B7314DD	08/04/2021	com.kartun.horor.animasi	2%
01-abr	FF399FCE187F31ED6FE977125EFD8398A0B1B224C637E0585970E8C8BE7AC4D7.apk	BC9B8EC260C325AD61A6EB98B6DE2C71	18/05/2021	io.kodular.okwuvic.Radio_GPS	2%
01-abr	FFDB6693BC433E113F9ADC93ED89141515A433AD33307DE77E838AA868B2C5DD.apk	84F10FF294CCE2AD1FDF6D5D69CE5FAE	18/05/2021	com.saheadbd.browser	2%
05-sep	0E1522BAFAC25F415F07DA6EB390BE78BA2499D27DAB7603FC1534241A17131E.apk	B84F207F7A93F689D90C7DA886EAE09A	02/04/2021	make.more.r2d2.google.cellular_pro	14%
05-sep	BB9A6B2AA13BFE703821FB3FA424130D24A70A38061FFCBA1B2B70CD35018495.apk	464381A4B5AD6348572B415E10BEDB5F	26/02/2021	com.tpf.gavw.mcyzj	12%
05-sep	7D742A4DB7AFB33D0DF539125AB46CC62576FB14B95D32C1BFE0B55BCA9E2C2A.apk	719293A2B6DB080DF8E49107B786D15B	02/03/2021	com.dawenming.novelreader	12%
05-sep	C375081B521FC8CBB55BE2ECBFECB49F34734A16258D0B872F4FEFD0BE9A13A5.apk	B7BC09FCDAC334C270579A44FAEDFE81	05/03/2021	com.starrycamera.funnyeffects.makeupfilters.collage	11%
05-sep	1475318A2C04D34539A10EF3C74388D74D3E883DFD0A8554D0AE9737000401AB.apk	37F7C21C4D0C4AE293E2D2F4F034634D	11/06/2021	com.wJalnikaMoyzaOfflciel_13422040	14%
05-sep	6A61E2A57BB5D6D3342F79BAF64EFA78CD3A61DC73B74D440F94C1E537AC1A6E.apk	E9E5CD82C55DF0BEB381C2B05C29FACC	20/03/2021	com.lwcx.lw016	11%

Intervalo	Nombre del archivo	Hash md5	Fecha	Nombre paquete	Detección %
oct-14	FC2B5418BD040515952E1EA333A8E5E44FE14FAFC54C31B1D1F0BA2DA8586D88.apk	B3AACEA1F16836DC94AB1DAEE96A28C1	20/04/2021	com.dualspace.multiple.account.tool	19%
oct-14	457EEA67B622DB712DD52BEFC5595DFBDEF5C6C1E42586C68E5D683B2273B241.apk	F4F8AA77AFA53B99D06E978F64E2FA68	15/02/2021	com.hassapps.freedating	17%
oct-14	CDD62B29F2F87C17AE533DC6538694AE18C9A02CF2BA5567A2050C67B93B2140.apk	33560FB9F76EFF1EB8BCBAEC5E488D87	08/03/2021	com.appgb.gbnewpro	17%
oct-14	476C58CE904F1DA2489000DD88181829391D31C4544B455143EDBF50E4898B99.apk	5EA460874FB81BFB74B1A60F7835A925	08/04/2021	com.potter.teenpattivungo.pokergo	13%
oct-14	ACEBE3527D6D797B588380046D47BF9A09D51F66ADF2E0988EC8BF3CED7D1523.apk	D4D93EC66E49DB6E641C994FD46183CA	21/04/2021	com.sslurzbmwty.funnyslots	19%
oct-14	F6E91B5B41834A8A8EF4C534DCC1C26B40AF1FA933FB65329031AFE4CE955C9D.apk	01B1B9D052EF31D11D788AC124DF70BB	09/03/2021	tech.miidii.offscreen_android	16%
15-19	7635988C3A9D1E38EC84C3FE3063C740BDE56CD8488406FE6A64BCCB72974EB2.apk	112DB9F0E693E706F96B523EF675BD83	03/06/2021	com.fahrezone.booster.ff	33%
15-19	F1A5F37BBF8A0636B311FDA8346FDFF86017315BBB3B95EFE9A6746DBDA66FD1.apk	C3C576B7CB5968CA10F8CF90E256B865	21/04/2021	kobras.vpn.ultra.max.miguel	27%
15-19	5DC494E30640524EB216D17D07CEA4B077140FF5BD86AE5646A3BEF9A9F9CC05.apk	BA22F9FEBEB516F6A93DF238D41CE63A	14/05/2021	com.ml.mysteryluck	25%
15-19	BE14FD1FB26193066E15630A1A5CA4727301C3C71938AB5011FB5359FB95FBF8.apk	5BA9F48856C4552C1B0A73F55D5629FA	14/02/2021	kobras.vpn.ultra.max.miguel	30%
15-19	9DC1D72168B148AAB3838078B11E0391388853F9ECFA6B6377DBF0F879A48351.apk	CE42AE3094186A8B808FA86FEABAC0EE	30/04/2021	com.maticmobi.mobilesecurity.antivirus	27%
15-19	889D759BB92D4040469547578B5613A4AB35653B9135B63399C98E282C625779.apk	B3DC079694FB9F94540DD2C9CF1E9D87	15/03/2021	com.daimsights.newworld	24%
20-24	5869508BCF407A36E132FF1F39BD6B3419D2C1178155698960BA5C40638B486C.apk	4D9B0C3F5A986537D43F99C4679C64BC	16/02/2021	com.flyingbees.mbc	39%
20-24	D21E711C5806280D971A8098040F259B68939C958F69E27EB94D346B2DB0A539.apk	29150177535100F9C0A3C718168765F1	10/03/2021	com.satunnelvpn.app	40%
20-24	B4A9A7337982CCC9F77741FA33C06B1EA8641BD5D70E855B58D775651AD9C770.apk	6DDB1853EBA4441204366FA6AC59A75	23/05/2021	com.fahrezone.booster.ff	34%
20-24	BFB450534FB16E8EFF32DB67F6F0246A5A897A1B62BCE0303201AB600F059A25.apk	E8B71A644858855172EE2F95AAFBD761	03/06/2021	com.clays.topcongo	33%
25-30	4254769325279B84CF2F6E68D648C87E45D40A754D71480AE580875D558B05E8.apk	5F7701879F135904448A0678C2369CC3	25/04/2021	xa.photocc.opd_collage	39%
25-30	B8C9C2B67DE9793C5394587D834365C1D12E799452DEBA03604B102EADC3FECE.apk	FF944CD9AE49220C2BB973370539A619	04/02/2021	com.flyingbees.mbc	39%

ANEXO VI. RESULTADOS EFICACIA

En la siguiente tabla, Tabla 14. Resultados de eficacia de las herramientas, se muestran los resultados de detección del malware seleccionado para el estudio por parte de las herramientas de seguridad.

Siguiendo la metodología definida en el estudio, se ha identificado la detección de los distintos programas maliciosos atendiendo al momento de su detección. La tabla ha sido cumplimentada con distintos valores que vienen definidos del siguiente modo:

- NO: La herramienta no ha sido capaz de detectar el programa malicioso
- ONLINE: La herramienta ha detectado el malware simplemente con la descompresión del zip que lo contenía.
- FORZADO: La herramienta detecta la presencia del apk en el sistema sin falta de ejecutarlo, pero mediante la ejecución de un análisis manual.
- INSTALACIÓN: La herramienta detecta el software malicioso durante la instalación de este.
- POST-INSTALACIÓN: La herramienta detecta el software malicioso una vez que ha sido instalado en el sistema.

Tabla 14. Resultados de eficacia de las herramientas

Intervalo		Nombre del archivo	Nombre aplicación	Ahnlab V3 Mobile Security	AVAST Mobile Security	AVG Antivirus free	Avira Antivirus Security	AVL Mobile Security	ESET Mobile Security & Antivirus	F-Secure Safe	GDATA Mobile Security	Kaspersky internet security	LINE Antivirus	McAfee Mobile Security	Trend Micro Mobile Security
Prácticamente indetectable	1-4	0BE524D71BD912956C8DC3019936BC938860DAD9D9825AC41F7DE28512106FEC.apk	HeimLink	NO	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	1-4	D897E663F58436A4D557A7A0394CCB83692EDA797CA485023B10C681879A5CA9.apk	Offroad Police Transporter Truck	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	1-4	424A64066279CEE1A41C0D57B863C67E7EE753FF1ED285A0C9F59D6A10825B4F.apk	PAN To Aadhar Link	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	1-4	D93CE1C5552364F1E71572D7F57D07F67EC42D82C04075047C8C168CE34CA5F5.apk	Kartun Horor	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	1-4	FF399FCE187F31ED6FE977125EFD8398A0B1B224C637E0585970E8C8BE7AC4D7.apk	Radio GPS	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	1-4	FFDB6693BC433E113F9ADC93ED89141515A433AD33307DE77E838AA868B2C5DD.apk	Fastest browser Bd	NO	NO	NO	NO	FORZADO	NO	NO	NO	NO	NO	NO	NO
Prácticamente indetectable	5-9	0E1522BAFAC25F415F07DA6EB390BE78BA2499D27DAB7603FC1534241A17131E.apk	Cellular-Pro Play	NO	NO	NO	NO	FORZADO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO
Prácticamente indetectable	5-9	BB9A6B2AA13BFE703821FB3FA424130D24A70A38061FFCBA1B2B70CD35018495.apk	Pregnancy Tracker Pro	NO	NO	NO	NO	FORZADO	FORZADO	NO	FORZADO	NO	NO	NO	NO
Prácticamente indetectable	5-9	7D742A4DB7AFB33D0DF539125AB46CC62576FB14B95D32C1BFE0B55BCA9E2C2A.apk	Texto Chino	NO	NO	NO	NO	FORZADO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO
Prácticamente indetectable	5-9	C375081B521FC8CBB55BE2ECBFECB49F34734A16258D0B872F4FEFD0BE9A13A5.apk	Master Cleaner	NO	NO	NO	NO	FORZADO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO

Intervalo		Nombre del archivo	Nombre aplicación	Ahnlab V3 Mobile Security	AVAST Mobile Security	AVG Antivirus free	Avira Antivirus Security	AVL Mobile Security	ESET Mobile Security & Antivirus	F-Secure Safe	GDATA Mobile Security	Kaspersky internet security	LINE Antivirus	McAfee Mobile Security	Trend Micro Mobile Security
Prácticamente indetectable	5-9	1475318A2C04D34539A10EF3C74388D74D3E883DFD0A8554D0AE9737000401AB.apk	Jalnika Moyza Offlciel	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	NO	POST-INSTALACIÓN
Prácticamente indetectable	5-9	6A61E2A57BB5D6D3342F79BAF64EFA78CD3A61DC73B74D440F94C1E537AC1A6E.apk	Eachine FPV	NO	INSTALACION	INSTALACION	NO	NO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO
Difícilmente detectable	10-14	FC2B5418BD040515952E1EA333A8E5E44FE14FAFC54C31B1D1F0BA2DA8586D88.apk	DualSpace	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	10-14	457EEA67B622DB712DD52BEFC5595DFBDEF5C6C1E42586C68E5D683B2273B241.apk	GBWasahp New Version	NO	NO	NO	FORZADO	FORZADO	NO	FORZADO	NO	FORZADO	POST-INSTALACIÓN	NO	POST-INSTALACIÓN
Difícilmente detectable	10-14	CDD62B29F2F87C17AE533DC6538694AE18C9A02CF2BA5567A2050C67B93B2140.apk	GBWasahp PLUS	NO	NO	NO	FORZADO	FORZADO	NO	FORZADO	NO	FORZADO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	10-14	476C58CE904F1DA2489000DD88181829391D31C4544B455143EDBF50E4898B99.apk	TeenPatti Vungo	NO	NO	NO	NO	FORZADO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO
Difícilmente detectable	10-14	ACEBE3527D6D797B588380046D47BF9A09D51F66ADF2E0988EC8BF3CED7D1523.apk	Funny Slot	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	NO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	10-14	F6E91B5B41834A8A8EF4C534DCC1C26B40AF1FA933FB65329031AFE4CE955C9D.apk	OffScreen	NO	NO	NO	NO	NO	FORZADO	NO	NO	NO	POST-INSTALACIÓN	NO	NO
Difícilmente detectable	15-19	7635988C3A9D1E38EC84C3FE3063C740BDE56CD8488406FE6A64BCCB72974EB2.apk	FF Booster Go	NO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	15-19	F1A5F37BBF8A0636B311FDA8346FDFF86017315BBB3B95EFE9A6746DBDA66FD1.apk	Kobras Ultra Max VPN	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	NO
Difícilmente detectable	15-19	5DC494E30640524EB216D17D07CEA4B077140FF5BD86AE5646A3BEF9A9F9CC05.apk	Mystery Luck	NO	NO	NO	NO	FORZADO	FORZADO	NO	NO	FORZADO	POST-INSTALACIÓN	NO	POST-INSTALACIÓN
Difícilmente detectable	15-19	BE14FD1FB26193066E15630A1A5CA4727301C3C71938AB5011FB5359FB95FBF8.apk	Kobras Ultra Max VPN	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	15-19	9DC1D72168B148AAB3838078B11E0391388853F9ECFA6B6377DBF0F879A48351.apk	Antivirus	NO	NO	NO	FORZADO	FORZADO	FORZADO	FORZADO	NO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Difícilmente detectable	15-19	889D759BB92D4040469547578B5613A4AB35653B9135B63399C98E282C625779.apk	TikFolloers	NO	NO	NO	NO	NO	FORZADO	FORZADO	NO	FORZADO	POST-INSTALACIÓN	NO	NO
Fácilmente detectable	20-24	5869508BCF407A36E132FF1F39BD6B3419D2C11781556989 60BA5C40638B486C.apk	ARABE	NO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	NO	FORZADO	POST-INSTALACIÓN
Fácilmente detectable	20-24	D21E711C5806280D971A8098040F259B68939C958F69E27EB94D346B2DB0A539.apk	SA PRO	NO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Fácilmente detectable	20-24	B4A9A7337982CCC9F77741FA33C06B1EA8641BD5D70E855B58D775651AD9C770.apk	FF Booster Go	NO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	NO	FORZADO	NO

Intervalo		Nombre del archivo	Nombre aplicación	Ahnlab V3 Mobile Security	AVAST Mobile Security	AVG Antivirus free	Avira Antivirus Security	AVL Mobile Security	ESET Mobile Security & Antivirus	F-Secure Safe	GDATA Mobile Security	Kaspersky internet security	LINE Antivirus	McAfee Mobile Security	Trend Micro Mobile Security
Fácilmente detectable	20-24	BFB450534FB16E8EFF32DB67F6F0246A5A897A1B62BCE0303201AB600F059A25.apk	Top Congo	FORZADO	NO	INSTALACION	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Fácilmente detectable	25-30	4254769325279B84CF2F6E68D648C87E45D40A754D71480AE580875D558B05E8.apk	Story Teller with Cute Layout	FORZADO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	POST-INSTALACIÓN	FORZADO	POST-INSTALACIÓN
Fácilmente detectable	25-30	B8C9C2B67DE9793C5394587D834365C1D12E799452DEBA03604B102EADC3FECE.apk	ARABE	NO	ONLINE	ONLINE	FORZADO	FORZADO	FORZADO	FORZADO	FORZADO	NO	POST-INSTALACIÓN	FORZADO	NO