Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

Sandra del Rocío Montúfar Rivera

Alex Johao Segovia Moreno

Emilio Israel Mayorga Campoverde

Luis Angel Yepez Intriago

TUTORES:

Alejandro Cortés

Iván Reyes Chacón

TEMA:

Análisis de un malware Android tipo Spyware en un entorno virtual seguro Android

REINVENTEMOS EL FUTURO

Certificación de autoría

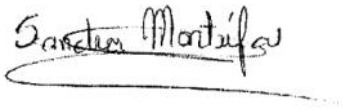
Nosotros, **Alex Johao Segovia Moreno, Emilio Israel Mayorga Campoverde, Luis Angel Yepez Intriago y Sandra del Rocío Montúfar Rivera,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firma
Alex Johao Segovia Moreno

Firma
Emilio Israel Mayorga Campoverde

Firma
Luis Angel Yépez Intriago



Firma
Sandra del Rocío Montúfar Rivera

Autorización de Derechos de Propiedad Intelectual

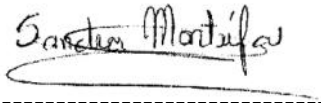
Nosotros, **Alex Johao Segovia Moreno, Emilio Israel Mayorga Campoverde, Luis Angel Yepez Intriago y Sandra del Rocío Montúfar Rivera**, en calidad de autores del trabajo de investigación titulado ***Análisis de un malware Android tipo Spyware en un entorno virtual seguro Android***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, enero 2026

Firma
Alex Johao Segovia Moreno

Firma
Emilio Israel Mayorga Campoverde

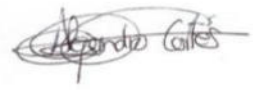
Firma
Luis Angel Yépez Intriago



Firma
Sandra del Rocío Montúfar Rivera

Aprobación de dirección y coordinación del programa

Nosotros, **Alejandro Cortés y Iván Reyes,** declaramos que: **Alex Johao Segovia Moreno, Emilio Israel Mayorga Campoverde, Luis Angel Yepez Intriago y Sandra del Rocío Montúfar Rivera** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés L.

Maestría en Ciberseguridad

Iván Reyes Ch.

Maestría en Ciberseguridad

DEDICATORIA

A Dios por ser la guía en mi camino, en los momentos difíciles por ser mi soporte para levantarme con mayor ímpetu y propósito.

A mi **madre** con su infinito amor, sacrificio incondicional ha sido pilar fundamental en mi vida, a mi **padre** (+)que está gozando de la vida eterna quien me inculco los valores fundamentales de la vida como la responsabilidad, integridad; por enseñarme que con esfuerzo y dedicación todo se puede lograr y a mi hermano por su apoyo profesional, para ellos infinita gratitud, este logro alcanzado es de ellos.

Sandra del Rocío Montúfar Rivera

A **Dayanara Egas**, mi compañera, mi inspiración y el motor que impulsa cada uno de mis pasos. Este trabajo es una muestra más de lo que construimos juntos: un futuro lleno de metas, esfuerzo, amor y crecimiento. Gracias por ser mi refugio, mi fuerza y el amor más grande que la vida me ha dado. Que todo lo que soñamos siga cumpliéndose de la mano.

A **mi madre, Delia Campoverde**, porque en cada logro mío hay un pedazo de su sacrificio, de sus consejos y de ese amor incondicional que siempre me levanta, incluso en los momentos más duros. Gracias por enseñarme a no rendirme y por ser el corazón de mi vida.

A **mis hermanos, Sophyanne Mayorga y Joed Mayorga**, quienes han sido ejemplo, guía y sostén. A ustedes les debo gran parte de mi camino: mis papás me criaron, pero ustedes me mimaron, me acompañaron y me empujaron a soñar más alto. Su apoyo y complicidad han hecho mi vida más ligera y llena de abundancia.

A todos ustedes, con amor y gratitud, dedico este trabajo.

Emilio Israel Mayorga Campoverde

A **mi madre**, por su paciencia, apoyo incondicional y cuidado diario, que me permitió dedicarme plenamente a este proceso.

A **mi padre**, cuyo respaldo fue fundamental para alcanzar mi pregrado y continuar con la maestría.

A mis compañeros de maestría, por la motivación compartida y el aprendizaje conjunto.

A **mis profesores y a la universidad,** por los conocimientos, la guía y las oportunidades que hicieron posible este logro.

Luis Ángel Yépez Intriago

Dedico este trabajo de titulación en primera instancia a Dios quién supo guiarme por el buen camino, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional; y supo darme fuerzas en los momentos de debilidad y nunca me dejo desmayar en los problemas que se presentaban, enseñándome a enfrentar las adversidades con humildad y nunca decaer en el intento.

Para mis **padres Galo, Gladys** y hermanos Katherine y Jairo por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar.

A mis abuelitos Emma(+) y Estuardo que han sido como unos segundos padres aportando cariño y comprensión en cada instante de mi vida y mi formación.

Gracias a mis compañeros de trabajo de grado, porque han sido un gran apoyo durante este tiempo de clases.

Alex Johao Segovia Moreno

AGRADECIMIENTOS

A Dios por darme la fortaleza para seguir adelante convirtiendo los obstáculos en oportunidades, por darme la vida.

A mis padres con su ejemplo me enseñaron el amor a Dios y que con esfuerzo y trabajo se pueden conseguir los objetivos, a mi hermano por su apoyo profesional cuando lo necesite.

A mis instructores de la maestría que me brindaron sus valiosos conocimientos y experiencias, más allá de la teoría.

A mis compañeros de grupo Alex, Luis y Emilio por su apoyo incondicional a lo largo de la maestría y del proyecto.

Sandra del Rocío Montúfar Rivera.

Agradezco profundamente a todos quienes hicieron posible la culminación de este proyecto. A mis docentes y tutores, por su guía académica y su compromiso con mi formación profesional.

Mi gratitud también para mis compañeros de la maestría, **Sandra, Alex y Luis**, con quienes compartí desafíos, debates, proyectos colaborativos y largas jornadas de trabajo. Gracias

por su compañerismo, apoyo constante y por ser parte esencial del desarrollo de este proyecto y de mi crecimiento académico.

A mi familia, especialmente a mi madre **Delia Campoverde**, por su apoyo constante y sus palabras de aliento en cada etapa de mi vida académica. A mis hermanos **Sophyanne Mayorga y Joed Mayorga**, por ser guía e inspiración, y por acompañarme siempre con cariño y respaldo.

De manera especial, a mi novia **Dayanara Egas**, por su amor, motivación y por ser un pilar fundamental en mi crecimiento personal y profesional. Gracias por creer en mí y caminar a mi lado en cada meta.

A todos ustedes, mi sincero agradecimiento por ser parte de este logro.

Emilio Israel Mayorga Campoverde.

Expreso mi más profundo agradecimiento a quienes hicieron posible la culminación de este proyecto.

A mis docentes y tutores, por su orientación y compromiso en mi formación.

A la universidad, por brindarme las herramientas necesarias para crecer académica y profesionalmente.

A mis compañeros, por su apoyo, colaboración y amistad durante este camino.

Finalmente, a mi familia, por ser el pilar que me sostuvo en cada etapa de este recorrido.

Luis Ángel Yépez Intriago

A nuestros docentes, quienes siempre estuvieron dispuestos a ayudarnos con nuestras inquietudes y, más allá de impartir una cátedra nos enseñaron muchas lecciones de vida.

Son muchas las personas que han formado parte de la vida profesional a las que nos encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de nuestra vida quiero darles las gracias por formar parte de este camino, por todo lo que nos han brindado y por todas sus bendiciones.

Alex Johao Segovia Moreno

RESUMEN

El incremento global de aplicaciones maliciosas dirigidas a dispositivos Android ha situado a los *spyware* como una de las amenazas más críticas para la privacidad y la seguridad de los usuarios. En este contexto, el presente proyecto tiene como finalidad analizar el comportamiento de un malware Android tipo *spyware* dentro de un entorno virtual seguro, empleando exclusivamente técnicas de análisis estático mediante la herramienta *Mobile Security Framework* (MobSF). El estudio se desarrolla sobre una arquitectura controlada que integra Android Studio, ADB y un emulador configurado específicamente para ejecutar aplicaciones sospechosas sin comprometer sistemas reales.

El análisis estático permitió identificar permisos abusivos, posibles filtraciones de información sensible, uso de APIs peligrosas, comunicación con recursos externos y patrones

comunes de vigilancia digital. Asimismo, se detallan los procesos de preparación del entorno, instalación de dependencias, manejo del emulador y ejecución de las herramientas necesarias, describiendo cada paso de forma metodológica para asegurar la reproducibilidad del estudio.

Los resultados evidencian que el *spyware* evaluado presenta características propias de aplicaciones diseñadas para recolectar datos personales, manipular funciones del dispositivo y mantenerse oculto ante el usuario. Se discuten además implicaciones de seguridad para organizaciones y usuarios, y se reflexiona sobre la importancia de la concientización en el uso responsable de dispositivos móviles.

Este trabajo contribuye a la comprensión técnica del análisis de *spyware* Android, proporcionando una guía práctica para investigaciones futuras y fortaleciendo las capacidades de detección en entornos educativos y profesionales.

Palabras Claves: Android, spyware, análisis estático, MobSF, ciberseguridad, malware, privacidad, emulador.

ABSTRACT

The global increase in malicious applications targeting Android devices has positioned spyware as one of the most critical threats to user privacy and device security. In this context, the present project aims to analyze the behavior of an Android spyware sample within a secure virtual environment, using exclusively static analysis techniques through the Mobile Security Framework (MobSF). The study is conducted within a controlled architecture that integrates Android Studio, ADB, and a custom-configured emulator designed to execute suspicious applications without compromising real systems.

Static analysis enabled the identification of abusive permissions, potential leakage of sensitive information, the use of dangerous APIs, communication with external resources, and

common patterns associated with digital surveillance. Additionally, this work details the procedures for environment configuration, dependency installation, emulator setup, and execution of the required tools, ensuring methodological clarity and reproducibility.

Results indicate that the evaluated spyware exhibits behaviors characteristic of applications designed to collect personal data, perform device manipulation, and remain concealed from the user. Security implications for organizations and individuals are discussed, and emphasis is placed on the importance of awareness regarding safe mobile device usage.

This project contributes to the technical understanding of Android spyware analysis, offering a practical guide for future research while strengthening detection capabilities in educational and professional settings.

Keywords: Android, spyware, static analysis, MobSF, cybersecurity, malware, privacy, emulator.

TABLA DE CONTENIDOS (Índice)

LISTA DE TABLAS (Índice de tablas)

LISTA DE FIGURAS (Índice de figuras)

Capítulo 1

1. Introducción

1.1. Definición del proyecto

El presente proyecto consiste en realizar un análisis estático exhaustivo de un archivo APK clasificado como spyware utilizando un entorno de laboratorio seguro basado en máquinas virtuales y la herramienta Mobile Security Framework (MobSF). A través de este análisis se estudian los componentes internos del APK, su estructura, permisos, librerías, uso de APIs sensibles, cadenas codificadas, rutas de comunicación, certificados digitales y posibles mecanismos de ofuscación o persistencia.

El proyecto adopta una aproximación metodológica, sistematizada y replicable, permitiendo que otros investigadores puedan reproducir el experimento sin comprometer la seguridad de sus sistemas personales o corporativos. Asimismo, el análisis estático permite evitar la ejecución directa del malware, mitigando riesgos inherentes y asegurando un proceso controlado.

De esta manera, el proyecto contribuye al entendimiento técnico de las amenazas dirigidas al sistema operativo Android, a la formación profesional del analista en ciberseguridad y al desarrollo de estrategias de mitigación basadas en evidencia empírica obtenida de la ingeniería inversa del APK.

1.2. Justificación e importancia del trabajo de investigación

El malware móvil ha dejado de ser un fenómeno aislado para convertirse en una problemática global que afecta tanto a usuarios individuales como a organizaciones públicas y

privadas. Diversos estudios (Kaspersky Lab, 2023; Check Point Research, 2024) muestran que el número de variantes de spyware y stalkerware ha aumentado exponencialmente en los últimos años, debido a la facilidad con la que pueden distribuirse mediante aplicaciones falsas, phishing móvil, repositorios alternativos o procesos engañosos de actualización.

La justificación del presente trabajo se fundamenta en seis ejes principales:

Relevancia Tecnológica. Android posee una arquitectura abierta y flexible, lo que facilita el desarrollo de aplicaciones, pero también aumenta la probabilidad de abuso. Comprender cómo funcionan internamente los APK maliciosos es esencial para anticipar nuevas campañas de ataque y para evaluar vulnerabilidades persistentes en el ecosistema.

Necesidad de Investigación Aplicada. Gran parte de los estudios sobre malware se enfocan en análisis dinámicos complejos o en infraestructuras empresariales. Sin embargo, existe limitada documentación sobre metodologías prácticas que estudiantes, investigadores y equipos pequeños puedan replicar en entornos controlados utilizando herramientas accesibles como MobSF.

Fortalecimiento de Habilidades en ciberseguridad. El análisis estático de malware contribuye directamente al desarrollo de competencias clave como:

- ingeniería inversa básica;
- análisis de permisos peligrosos;
- comprensión del modelo de seguridad de Android;
- manejo de frameworks de análisis automatizado;

- interpretación de resultados desde una perspectiva forense.

Estas capacidades son indispensables para profesionales de ciberseguridad, pentesters, analistas SOC y equipos CERT.

Impacto en la Protección del Usuario Final. Los spyware son particularmente peligrosos porque se orientan al espionaje personal, violencia digital, chantaje, extorsión y robo de identidad. Un análisis técnico profundo permite identificar patrones comunes que pueden alimentar sistemas de detección temprana en organizaciones y mejorar la gestión de riesgos.

Contribución Académica. Este trabajo aporta conocimiento científico y técnico sobre el comportamiento interno del malware móvil, constituyendo un insumo para investigaciones futuras sobre:

- análisis dinámico,
- instrumentación avanzada con Frida,
- detección basada en machine learning,
- análisis comparativo entre diferentes familias de spyware.

Ética y responsabilidad profesional. Finalmente, estudiar malware no solo exige conocimientos técnicos, sino también una responsabilidad ética. El análisis en un entorno seguro evita daños a terceros y promueve prácticas profesionales responsables.

1.3. Alcance

El presente proyecto posee un alcance claramente delimitado para asegurar rigurosidad metodológica y evitar riesgos inherentes a la ejecución del malware. A continuación, se especifican los límites del estudio:

Tipo de Análisis. El trabajo se enfoca exclusivamente en el análisis estático, entendiendo este como el proceso de examinar el archivo APK sin ejecutarlo. No se incluyen análisis dinámicos, hooking, instrumentación, tráfico de red ni ejecución en sistemas reales.

Herramientas Utilizadas. La herramienta principal es Mobile Security Framework (MobSF), seleccionada por su capacidad de:

- desensamblar el APK,
- extraer e interpretar el AndroidManifest.xml,
- analizar permisos peligrosos,
- detectar comportamientos sospechosos mediante reglas integradas,
- generar reportes automatizados,
- identificar strings codificados, certificados y rutas.

Complementariamente, se utilizaron herramientas de apoyo como:

- ADB para comunicación con emuladores,
- Android Studio para manipulación del entorno virtual,
- Máquinas virtuales Ubuntu en VMware para aislamiento total.

Límites del análisis. No se contempla:

- análisis dinámico;
- explotación de vulnerabilidades;
- ingeniería inversa avanzada con desensambladores complejos;
- pruebas sobre dispositivos físicos;
- comparación entre múltiples familias de malware;

El análisis se circunscribe a una muestra representativa única seleccionada desde un repositorio confiable como MalwareBazaar.

Resultados Esperados. Se espera obtener:

- un perfil técnico del spyware;
- la identificación de datos que intenta acceder;
- patrones de comportamiento malicioso;
- riesgos asociados al usuario final;
- recomendaciones preventivas;

1.4. Objetivos

1.4.1. Objetivo general

Desarrollar un análisis estático integral de un spyware para Android mediante herramientas de laboratorio seguro, con el fin de identificar sus características internas, riesgos asociados y mecanismos potenciales de espionaje.

1.4.2. Objetivo especifico

- Evaluar los permisos declarados en el APK para determinar el nivel de acceso que

solicita;

- Identificar librerías, clases y métodos que indiquen comportamientos maliciosos;
- Analizar cadenas de texto, rutas y URLs incrustadas en el código;
- Examinar el certificado digital y metadatos de la firma;
- Detectar patrones de comportamiento definidos por las reglas internas de MobSF;
- Generar un informe técnico documentado bajo normas APA 7ma edición;
- Proponer recomendaciones de seguridad para usuarios, empresas y administradores de TI;
- Identificar el conocimiento, la percepción de riesgo y los hábitos de seguridad de los usuarios de dispositivos Android frente al spyware, para evaluar su grado de exposición, concienciación y disposición a recibir capacitación en seguridad móvil.

Capítulo 2

2. Revisión de literatura

2.1. Estado del Arte

La revisión del estado del arte permite comprender la evolución de las amenazas móviles, su comportamiento técnico, las técnicas modernas de análisis y la relevancia creciente del sistema operativo Android en la superficie global de ciberataques. Este apartado integra estudios recientes, reportes de laboratorios de ciberseguridad y literatura científica publicada entre 2020 y 2024, con énfasis en investigaciones que analizan spyware, análisis estático y frameworks orientados al estudio seguro de malware.

Evolución del Malware Móvil en Android. Diversos informes de Kaspersky Lab (2023), ESET (2024) y Check Point Research (2024) coinciden en que Android continúa siendo el sistema operativo móvil más atacado del mundo debido a:

- Su cuota de mercado global, que supera el 70 %;
- Su arquitectura abierta, que permite instalación desde repositorios de terceros;
- La fragmentación del ecosistema, que complica la aplicación homogénea de parches de seguridad;
- La existencia de centros de desarrolladores independientes, donde apps maliciosas pueden ocultarse entre paquetes legítimos;

Según Statista (2023), el número de variantes de malware móvil detectadas anualmente supera los 5,5 millones, siendo los spyware una de las familias con mayor crecimiento debido a su capacidad de recopilar datos personales, monitoreo constante y fines de espionaje.

Estas amenazas incluyen:

- Stalkerware: utilizado para vigilancia privada;

- Spyware bancario: enfocado en capturar contraseñas o tokens;
- Remote Access Trojans (RATs): permiten control remoto completo;
- Apps impersonadas: como versiones falsas de TikTok, Facebook o WhatsApp que contienen payloads maliciosos;

***Spyware, Tendencias de Investigación*.** Las investigaciones de malware spyware destacan:

- Técnicas avanzadas de ofuscación, como DexProtector, ProGuard o cadenas XOR;
- Uso de permisos peligrosos: ACCESS_FINE_LOCATION, READ_SMS, RECORD_AUDIO, CAMERA;
- Comunicación con servidores C2 (Command and Control) mediante HTTP/S, WebSockets o MQTT;
- Persistencia mediante servicios en segundo plano, broadcast receivers y abuso del archivo Manifest;
- Suplantación de aplicaciones legítimas, especialmente comerciales o de entretenimiento;

Artículos recientes (Liu et al., 2022; Kumar & Shinde, 2023) evidencian que el spyware moderno combina técnicas forenses anti-análisis para evadir entornos virtualizados, lo que incrementa la importancia del análisis estático antes de la ejecución.

Herramientas para Análisis de Malware en Android. En investigaciones académicas y forenses se mencionan diversas herramientas; sin embargo, tres destacan por su uso extendido:

***MobSF (Mobile Security Framework*).** Framework que permite análisis estático y dinámico de APKs. Es recomendado en múltiples trabajos científicos debido a:

- su automatización;
- facilidad de uso;
- capacidad de detección basada en reglas;
- integración con análisis de firmas y permisos;

Es la herramienta utilizada en este proyecto.

JADX. Descompilador para ingeniería inversa, útil para revisar clases Java y métodos. Aunque no es el eje principal de este estudio, se reconoce en la literatura.

ADB (Android Debug Bridge). Permite comunicación entre el dispositivo/emulador y el analista. Se emplea principalmente para:

- listar procesos;
- instalar APKs de prueba;
- verificar acceso a sistemas de archivos;

Uso de emuladores en investigación de malware. Los emuladores se han convertido en una alternativa común dentro de laboratorios académicos debido a su seguridad y bajo costo. La literatura clasifica los entornos más utilizados;

- Android Studio Emulator: flexible, gratuito, ideal para pruebas básicas;
- Genymotion: reconocido en investigación por su rendimiento y soporte para múltiples versiones;
- Corellium: plataforma profesional orientada a análisis avanzado (aunque de acceso restringido) ;

En investigaciones recientes (Yu et al., 2023; Rastegari, 2024), se confirma que el análisis estático puede realizarse de manera segura sin necesidad de ejecutar el malware, reduciendo significativamente riesgos operativos.

2.2. Marco Teórico

Seguridad Informática y Ciberseguridad La seguridad informática constituye una disciplina fundamental dentro del campo de las ciencias de la computación, cuyo objetivo principal es proteger los sistemas de información frente a accesos no autorizados, alteraciones, destrucción o divulgación indebida de datos. En un contexto global marcado por la digitalización acelerada, la seguridad informática ha evolucionado hacia un enfoque más amplio conocido como ciberseguridad, el cual abarca no solo la protección de sistemas computacionales tradicionales, sino también redes, dispositivos móviles, servicios en la nube y entornos virtualizados.

Malware definición y clasificación. El término malware proviene de la contracción de las palabras malicious software y se utiliza para describir cualquier programa o código diseñado con fines maliciosos. El malware tiene como objetivo principal comprometer la seguridad de un sistema, causar daños, robar información o permitir el control remoto del dispositivo afectado.

La clasificación del malware se realiza generalmente en función de su comportamiento y propósito. Entre las principales categorías se encuentran los virus, gusanos (worms), troyanos, ransomware, adware y spyware. Cada una de estas categorías presenta características específicas y niveles de impacto distintos sobre los sistemas afectados.

En el contexto de los dispositivos móviles, el malware ha evolucionado significativamente, adaptándose a las particularidades de los sistemas operativos móviles y a los mecanismos de seguridad implementados por los fabricantes. Esta evolución ha dado lugar a

variantes más sofisticadas que combinan múltiples funcionalidades maliciosas, dificultando su detección mediante métodos tradicionales.

adsMalware en Android. Android es susceptible a múltiples categorías de malware:

Tabla 1

Categorías de Malware

Categoría	Descripción
Spyware	Captura datos privados sin autorización.
Ransomware	Bloquea archivos y exige pago.
Adware	Muestra publicidad invasiva.
Trojan	Finge ser app legítima.
Botnet malware	Controla dispositivos infectados de forma remota.

Elaborado por: Integrantes del grupo

Spyware Características y Riesgos. El spyware es una categoría de malware diseñada para recopilar información del usuario de manera encubierta, sin su conocimiento o consentimiento explícito. A diferencia de otros tipos de malware que buscan causar daños inmediatos, el spyware se caracteriza por su comportamiento sigiloso y persistente, lo que le permite operar durante largos periodos de tiempo sin ser detectado.

Entre las principales características del spyware Android se encuentran la recopilación de datos personales, el acceso a mensajes de texto, contactos, registros de llamadas, información de ubicación y, en algunos casos, la activación de sensores como el micrófono o la cámara. Estas capacidades representan una amenaza significativa para la privacidad de los usuarios y pueden ser utilizadas con fines de espionaje, fraude o extorsión.

Los riesgos asociados al spyware no se limitan únicamente al ámbito personal. En entornos corporativos, la presencia de spyware en dispositivos móviles puede comprometer información confidencial, facilitar ataques dirigidos y generar pérdidas económicas y reputacionales para las organizaciones.

Arquitectura del Sistema Operativo Android. Android es un sistema operativo basado en el núcleo Linux, diseñado principalmente para dispositivos móviles. Su arquitectura se organiza en múltiples capas, cada una con funciones específicas que contribuyen al funcionamiento y seguridad del sistema.

Las principales capas de la arquitectura Android incluyen el kernel Linux, las bibliotecas nativas, el entorno de ejecución de Android (*Android Runtime*), el marco de aplicaciones (*Application Framework*) y las aplicaciones. Esta estructura modular permite un alto grado de flexibilidad, pero también introduce desafíos en términos de seguridad, especialmente cuando las aplicaciones solicitan permisos excesivos o utilizan componentes de manera indebida.

El modelo de seguridad de Android se basa en el aislamiento de aplicaciones mediante sandboxes, lo que impide que una aplicación acceda directamente a los recursos de otra. Sin embargo, el uso inadecuado de permisos y la explotación de vulnerabilidades pueden permitir que aplicaciones maliciosas, como el spyware, superen estas barreras de seguridad.

Sistema de Permisos en Android. El sistema de permisos de Android constituye uno de los principales mecanismos de control de acceso a los recursos del dispositivo. A partir de versiones recientes del sistema operativo, los permisos se clasifican en categorías según su nivel de riesgo, incluyendo permisos normales y permisos peligrosos.

Los permisos peligrosos permiten el acceso a información sensible o a funciones críticas del dispositivo, como la ubicación, la cámara, el micrófono o el almacenamiento. El spyware

suele aprovechar estos permisos para recopilar información del usuario, por lo que su análisis resulta fundamental en estudios de seguridad móvil.

El análisis estático de los permisos solicitados por una aplicación permite identificar posibles comportamientos maliciosos antes de su ejecución. Herramientas como MobSF facilitan este proceso al proporcionar evaluaciones automáticas del nivel de riesgo asociado a cada permiso.

Análisis de mMalware Enfoques Generales. El análisis de malware puede abordarse desde diferentes enfoques, entre los cuales destacan el análisis estático y el análisis dinámico. El análisis estático consiste en examinar el código y los recursos de una aplicación sin ejecutarla, mientras que el análisis dinámico implica observar su comportamiento durante la ejecución en un entorno controlado.

En el contexto académico y formativo, el análisis estático se presenta como una técnica inicial segura y eficaz, especialmente cuando se trabaja con malware móvil. Este enfoque permite identificar indicadores de compromiso, configuraciones inseguras y patrones de comportamiento malicioso sin exponer el sistema a riesgos innecesarios.

Análisis Estático de Aplicaciones Android. El análisis estático de aplicaciones Android se centra en la inspección del archivo APK, que contiene el código, los recursos y la configuración de la aplicación. Este proceso incluye el análisis del archivo *AndroidManifest.xml*, donde se declaran los permisos, componentes y configuraciones de la aplicación.

Además, el análisis estático permite examinar el código descompilado, identificar técnicas de ofuscación, detectar el uso de bibliotecas sospechosas y evaluar posibles vulnerabilidades de seguridad. Estas actividades resultan especialmente relevantes en el estudio

del spyware, ya que este tipo de malware suele ocultar sus funcionalidades maliciosas mediante técnicas avanzadas de evasión.

Mobile Security Framework (MobSF). El Mobile Security Framework (MobSF) es una herramienta de código abierto ampliamente utilizada para el análisis de seguridad de aplicaciones móviles. MobSF soporta el análisis estático de aplicaciones Android, iOS y Windows, proporcionando informes detallados sobre permisos, configuraciones, vulnerabilidades y riesgos potenciales.

En el ámbito del análisis estático de malware Android, MobSF destaca por su capacidad para automatizar tareas complejas, generar reportes estructurados y facilitar la interpretación de resultados. La herramienta analiza aspectos clave como permisos peligrosos, componentes exportados, uso de criptografía insegura y posibles indicadores de spyware.

La utilización de MobSF en entornos académicos permite estandarizar los procesos de análisis y garantiza la reproducibilidad de los resultados, lo cual constituye un aspecto fundamental en investigaciones científicas.

MobSF es un framework libre para análisis de seguridad móvil. Para el análisis estático, permite:

- extraer *AndroidManifest.xml*,
- analizar permisos peligrosos,
- identificar endpoints de red,
- clasificar riesgos,
- explorar metadatos de firma,
- detectar código potencialmente malicioso.

MobSF utiliza reglas basadas en el modelo Common Weakness Enumeration (CWE) para evaluar riesgos.

Permisos Peligrosos en Android. Google clasifica los permisos en:

- Normales (riesgo bajo)
- Peligrosos (riesgo alto)
- Firma (solo para apps de sistema)

Tabla *2*

Solicitud de Permisos

Permiso	**Riesgo asociado**
READ_SMS	Lectura de mensajes privados
RECORD_AUDIO	Espionaje mediante micrófono
CAMERA	Toma de fotos sin consentimiento
READ_CONTACTS	Robo de contactos
ACCESS_FINE_LOCATION	Rastreo de ubicación

Elaborado por: Integrantes del grupo

Los spyware dependen fuertemente de estos permisos.

Emulación como Entorno Seguro. El uso de máquinas virtuales es fundamental para evitar infección real. Android Studio fue seleccionado para:

- crear un ambiente aislado;
- cargar APKs sin comprometer el sistema;
- usar ADB para inspección básica;

Entornos Virtuales Seguros para el Análisis de Malware. Los entornos virtuales seguros desempeñan un papel crucial en el análisis de malware, ya que permiten ejecutar y examinar aplicaciones maliciosas sin comprometer sistemas reales. En el caso del análisis estático, estos entornos proporcionan una plataforma controlada para la instalación de herramientas especializadas y la gestión de muestras de malware.

El uso de máquinas virtuales basadas en sistemas operativos Linux, como Ubuntu, facilita la integración de herramientas de análisis y reduce el riesgo de propagación de malware. Asimismo, la virtualización permite replicar configuraciones específicas del sistema, como versiones recientes de Android, garantizando la validez de los resultados obtenidos.

Estudios recientes sobre spyware Android. Diversas investigaciones recientes han abordado el análisis de spyware Android, destacando la necesidad de utilizar enfoques actualizados y herramientas especializadas. Estudios publicados a partir de 2023 resaltan el incremento de variantes de spyware que emplean técnicas de ofuscación avanzada y solicitan permisos aparentemente legítimos para ocultar su comportamiento malicioso.

Estos estudios coinciden en la importancia del análisis estático como etapa inicial del proceso de investigación, especialmente en contextos académicos y de formación. Asimismo, enfatizan la necesidad de utilizar versiones recientes del sistema operativo Android para reflejar con mayor precisión el entorno actual de amenazas.

Relación del Marco Teórico con la Investigación. El marco teórico desarrollado en este capítulo proporciona los fundamentos conceptuales necesarios para la comprensión del análisis realizado en los capítulos posteriores. Los conceptos de malware, spyware, arquitectura Android, sistema de permisos y análisis estático constituyen la base teórica que sustenta la metodología y el análisis de resultados presentados en este estudio.

La integración de estos elementos teóricos permite contextualizar los hallazgos obtenidos mediante MobSF y facilita la interpretación de los riesgos asociados al malware Android analizado, contribuyendo así al cumplimiento de los objetivos planteados en la investigación.

Malware Móvil Moderno (2023–2025). En los últimos años, el panorama del malware móvil ha experimentado una evolución significativa, impulsada por el crecimiento sostenido del uso de dispositivos inteligentes y la ampliación de los servicios digitales accesibles desde plataformas móviles. Entre los años 2023 y 2025, se ha observado un incremento notable tanto en la cantidad como en la sofisticación del malware dirigido específicamente a sistemas operativos móviles, siendo Android el principal objetivo de estas amenazas debido a su amplia cuota de mercado y a la diversidad de dispositivos que lo implementan.

El malware móvil moderno se caracteriza por la incorporación de técnicas avanzadas que buscan evadir los mecanismos de seguridad tradicionales del sistema operativo. A diferencia de las primeras generaciones de malware, que presentaban comportamientos evidentes y fácilmente detectables, las variantes actuales priorizan la persistencia, el sigilo y la adaptación dinámica al entorno del dispositivo. Estas características permiten que las aplicaciones maliciosas permanezcan activas durante periodos prolongados sin levantar sospechas por parte del usuario ni de los sistemas de detección básicos.

Uno de los factores que ha contribuido a la expansión del malware móvil en el periodo 2023–2025 es la creciente dependencia de los dispositivos Android para la realización de actividades sensibles, como transacciones financieras, autenticación de servicios, comunicación empresarial y almacenamiento de información personal. Esta concentración de datos de alto valor ha convertido a los dispositivos móviles en objetivos estratégicos para actores maliciosos, quienes desarrollan malware específicamente diseñado para explotar estas oportunidades.

Dentro de este contexto, el spyware ha consolidado su presencia como una de las categorías de malware más relevantes. A diferencia de otras amenazas que buscan un impacto inmediato, como el ransomware, el spyware opera de forma silenciosa, recopilando información de manera continua y transmitiéndola a servidores externos controlados por los atacantes. Este comportamiento resulta especialmente peligroso, ya que permite la construcción de perfiles detallados de los usuarios sin que estos sean conscientes de la intrusión.

Las investigaciones recientes destacan que el malware móvil moderno suele presentarse camuflado como aplicaciones legítimas, tales como herramientas de productividad, utilidades del sistema o aplicaciones de entretenimiento. Esta estrategia de engaño se ve reforzada por el uso de interfaces visuales atractivas y descripciones funcionales aparentemente inocuas, lo que incrementa la probabilidad de instalación por parte de los usuarios. En muchos casos, estas aplicaciones solicitan permisos que, aunque parecen justificados según la funcionalidad declarada, permiten en realidad la recopilación de información sensible.

Otro aspecto relevante del malware móvil contemporáneo es el uso de técnicas de ofuscación del código. Estas técnicas dificultan el análisis manual y automatizado del software malicioso, ocultando la lógica interna de la aplicación y complicando la identificación de funciones críticas relacionadas con el espionaje. La ofuscación se ha convertido en una práctica común entre los desarrolladores de spyware, quienes buscan evadir herramientas de detección estática y retrasar la respuesta de los analistas de seguridad.

Asimismo, el malware móvil moderno ha demostrado una notable capacidad de adaptación a las actualizaciones del sistema operativo Android. A medida que Google introduce mejoras en los mecanismos de seguridad, los desarrolladores de malware ajustan sus técnicas para mantener la efectividad de sus ataques. Esto incluye la explotación de configuraciones

incorrectas, el abuso de permisos legítimos y el uso de componentes del sistema que permiten la ejecución de tareas en segundo plano.

Desde una perspectiva académica, el análisis del malware móvil moderno resulta fundamental para comprender las tendencias actuales en ciberamenazas y para desarrollar estrategias de mitigación efectivas. El periodo comprendido entre 2023 y 2025 representa una etapa particularmente relevante, ya que coincide con la adopción de versiones recientes de Android que incorporan cambios significativos en la gestión de permisos y en el aislamiento de aplicaciones. Analizar malware compatible con estas versiones permite obtener resultados más representativos del estado actual de la seguridad móvil.

En este sentido, el análisis estático se consolida como una técnica inicial esencial para el estudio del malware móvil moderno. A través del examen del código, los permisos y las configuraciones de las aplicaciones, es posible identificar indicadores tempranos de comportamiento malicioso sin necesidad de ejecutar el software en un entorno real. Herramientas como el Mobile Security Framework (MobSF) facilitan este proceso, proporcionando una visión integral de los riesgos asociados a las aplicaciones analizadas.

Finalmente, el estudio del malware móvil moderno no solo contribuye al avance del conocimiento técnico, sino que también desempeña un papel clave en la concientización sobre los riesgos de seguridad en dispositivos Android. Comprender cómo evolucionan estas amenazas permite a usuarios, desarrolladores y organizaciones adoptar medidas preventivas más eficaces, reduciendo la probabilidad de infecciones y fortaleciendo la seguridad del ecosistema móvil en su conjunto.

Spyware Android frente a otras Familias de Malware. El spyware Android constituye una de las familias de malware más relevantes dentro del ecosistema de amenazas móviles

contemporáneas, especialmente cuando se lo compara con otras categorías de software malicioso como el ransomware, los troyanos bancarios, el adware y los backdoors. Aunque todas estas amenazas comparten el objetivo común de comprometer la seguridad del dispositivo, difieren significativamente en cuanto a su propósito, técnicas de operación y nivel de impacto sobre el usuario.

A diferencia del ransomware, cuyo objetivo principal es la extorsión mediante el cifrado de datos y la exigencia de un rescate económico, el spyware se caracteriza por su enfoque en la vigilancia silenciosa. El spyware busca recopilar información personal, credenciales, mensajes, ubicaciones y otros datos sensibles sin alertar al usuario ni interferir de forma evidente con el funcionamiento del sistema. Esta discreción convierte al spyware en una amenaza particularmente peligrosa, ya que puede permanecer activo durante largos periodos sin ser detectado.

En comparación con los troyanos bancarios, el spyware presenta un alcance más amplio en términos de recopilación de información. Mientras que los troyanos bancarios se centran en el robo de credenciales financieras y la manipulación de aplicaciones bancarias, el spyware Android suele abarcar múltiples vectores de información, incluyendo registros de llamadas, mensajes SMS, contenido de aplicaciones de mensajería, archivos multimedia y datos de localización. Esta versatilidad permite a los atacantes construir perfiles detallados de las víctimas.

El adware, otra familia común de malware móvil, se diferencia del spyware principalmente por su finalidad comercial. Aunque el adware también puede recopilar información del usuario, su objetivo principal es la generación de ingresos mediante la visualización forzada de anuncios. En contraste, el spyware prioriza la recopilación de datos

confidenciales para su uso en actividades de espionaje, fraude o venta en mercados clandestinos. No obstante, en el periodo reciente se ha observado una convergencia entre ambas categorías, dando lugar a aplicaciones híbridas que combinan publicidad intrusiva con funcionalidades de espionaje.

Los backdoors móviles representan otra amenaza relevante dentro del ecosistema Android. Estas aplicaciones maliciosas permiten a los atacantes mantener acceso remoto al dispositivo comprometido, facilitando la ejecución de comandos, la descarga de cargas adicionales y el control persistente del sistema. Aunque el spyware puede incorporar funcionalidades de acceso remoto, su enfoque principal sigue siendo la recolección pasiva de información, mientras que los backdoors priorizan el control activo del dispositivo.

Una diferencia clave entre el spyware Android y otras familias de malware radica en su modelo de persistencia. El spyware suele aprovechar permisos legítimos del sistema para mantenerse activo en segundo plano, utilizando servicios de accesibilidad, permisos de notificaciones o acceso a almacenamiento. Este uso de componentes oficiales del sistema operativo dificulta su detección, ya que no siempre requiere vulnerabilidades explícitas. Por el contrario, otras familias de malware pueden depender de exploits específicos o de configuraciones inseguras para garantizar su persistencia.

Desde el punto de vista del análisis de seguridad, el spyware Android plantea desafíos particulares. Su comportamiento discreto y su dependencia de permisos aparentemente legítimos complican tanto el análisis estático como el dinámico. A diferencia del ransomware, cuyos indicadores de compromiso son evidentes, el spyware puede requerir un análisis detallado del código, los permisos solicitados y las comunicaciones de red para identificar su verdadera

naturaleza. En este contexto, herramientas como MobSF resultan fundamentales para detectar patrones sospechosos en aplicaciones que, a simple vista, parecen inofensivas.

Otra diferencia significativa se observa en el impacto percibido por el usuario. Mientras que el ransomware o el adware suelen generar molestias inmediatas que alertan a la víctima, el spyware opera sin generar síntomas visibles. Esta ausencia de señales evidentes incrementa el riesgo, ya que los usuarios pueden continuar utilizando el dispositivo comprometido sin tomar medidas correctivas, permitiendo la exfiltración continua de información sensible.

En el periodo comprendido entre 2023 y 2025, diversos estudios han señalado un aumento en el uso de spyware Android como herramienta de espionaje tanto a nivel individual como organizacional. Esta tendencia refleja un cambio en las prioridades de los atacantes, quienes buscan maximizar la obtención de información en lugar de beneficios económicos inmediatos. En este sentido, el spyware se posiciona como una amenaza estratégica dentro del panorama del malware móvil moderno.

Finalmente, la comparación entre el spyware Android y otras familias de malware pone de manifiesto la necesidad de enfoques de análisis diferenciados. Mientras que algunas amenazas pueden ser mitigadas mediante soluciones de seguridad tradicionales, el spyware requiere un análisis profundo y contextualizado, que considere no solo el comportamiento técnico de la aplicación, sino también el uso indebido de permisos y la interacción con el usuario. Este enfoque resulta esencial para el desarrollo de estrategias efectivas de detección y prevención en entornos Android actuales.

Impacto del Spyware Android en Usuarios y Organizaciones. El impacto del spyware Android se manifiesta de forma significativa tanto en usuarios individuales como en organizaciones, convirtiéndose en una de las amenazas más críticas dentro del ecosistema móvil

actual. A diferencia de otros tipos de malware que generan efectos inmediatos y visibles, el spyware opera de manera silenciosa, lo que amplifica sus consecuencias a largo plazo y dificulta su detección temprana.

En el ámbito del usuario individual, el spyware Android compromete directamente la privacidad personal. La recopilación no autorizada de mensajes, llamadas, ubicaciones geográficas, contactos y contenido multimedia permite a los atacantes reconstruir patrones de comportamiento, hábitos diarios y relaciones sociales. Esta información puede ser utilizada con fines de extorsión, suplantación de identidad o vigilancia prolongada, afectando gravemente la seguridad personal del usuario.

Uno de los impactos más relevantes del spyware es la pérdida de control sobre la información privada. En muchos casos, los usuarios desconocen que han otorgado permisos excesivos a aplicaciones aparentemente legítimas, lo que facilita la explotación de servicios del sistema como accesibilidad, notificaciones o almacenamiento. Esta situación genera una falsa sensación de seguridad y expone al usuario a riesgos continuos sin que exista una percepción clara del problema.

Desde una perspectiva psicológica, la exposición a spyware puede generar consecuencias significativas. La revelación de información personal, conversaciones privadas o datos sensibles puede provocar estrés, ansiedad y pérdida de confianza en el uso de tecnologías móviles. En escenarios más graves, el spyware ha sido vinculado a casos de acoso digital, vigilancia abusiva y violencia tecnológica, lo que amplía su impacto más allá del ámbito técnico.

En el contexto organizacional, el spyware Android representa una amenaza estratégica para la seguridad de la información. El uso de dispositivos móviles personales o corporativos para acceder a correos electrónicos, plataformas internas y aplicaciones empresariales convierte a

estos dispositivos en objetivos de alto valor. Un solo dispositivo comprometido puede actuar como punto de entrada para la filtración de información confidencial o estratégica.

Las organizaciones enfrentan riesgos relacionados con la fuga de datos corporativos, la pérdida de propiedad intelectual y la exposición de credenciales de acceso. El spyware puede capturar contraseñas, tokens de autenticación y mensajes corporativos, facilitando ataques posteriores más sofisticados. En sectores regulados como la banca, la salud o la educación, estas filtraciones pueden derivar en sanciones legales y daños reputacionales significativos.

Otro impacto relevante del spyware en las organizaciones es la afectación a la continuidad operativa. La recopilación de información sensible puede ser utilizada para ataques dirigidos, ingeniería social avanzada o sabotaje interno. Además, la necesidad de investigar y mitigar incidentes relacionados con spyware implica costos adicionales en términos de recursos humanos, tiempo y tecnología.

Desde el punto de vista económico, el spyware Android genera costos directos e indirectos. Los costos directos incluyen la implementación de medidas de seguridad, auditorías, herramientas de análisis y capacitación del personal. Los costos indirectos abarcan la pérdida de confianza de clientes, la interrupción de servicios y el deterioro de la imagen institucional. En muchos casos, estos costos superan ampliamente el valor de la información inicialmente comprometida.

El impacto del spyware también se extiende al cumplimiento normativo. Regulaciones internacionales y nacionales sobre protección de datos personales, como el Reglamento General de Protección de Datos (GDPR), exigen a las organizaciones garantizar la seguridad de la información. La presencia de spyware en dispositivos corporativos puede implicar incumplimientos normativos, sanciones económicas y responsabilidades legales.

En el periodo reciente, la creciente adopción del teletrabajo y el uso intensivo de dispositivos móviles han incrementado la superficie de ataque. Los entornos híbridos, donde dispositivos personales acceden a recursos corporativos, facilitan la propagación de spyware y dificultan la aplicación de controles de seguridad centralizados. Este contexto refuerza la necesidad de enfoques preventivos y de análisis riguroso del software móvil.

Desde una perspectiva de ciberseguridad, el impacto del spyware Android subraya la importancia del análisis estático como herramienta fundamental para la detección temprana de amenazas. El análisis de permisos, bibliotecas, componentes y configuraciones permite identificar comportamientos sospechosos antes de que la aplicación sea desplegada en entornos productivos. Herramientas como MobSF se convierten en aliadas clave para mitigar los riesgos asociados al spyware.

Finalmente, el impacto del spyware Android en usuarios y organizaciones evidencia la necesidad de una mayor concienciación y educación en seguridad digital. La combinación de buenas prácticas, herramientas de análisis y políticas de seguridad adecuadas resulta esencial para reducir la exposición a este tipo de amenazas. Comprender el alcance y las consecuencias del spyware es un paso fundamental para fortalecer la resiliencia frente a un panorama de amenazas móviles cada vez más complejo.

Desafíos Actuales en la Detección de Spyware Android. La detección de spyware Android constituye uno de los principales retos dentro del ámbito de la ciberseguridad móvil contemporánea. A pesar del avance significativo de las herramientas de análisis y de las soluciones de seguridad, el spyware continúa evolucionando y adaptándose a los mecanismos de defensa existentes, lo que dificulta su identificación temprana y su mitigación efectiva. Este desafío se intensifica en un ecosistema tan amplio y heterogéneo como Android, donde la

diversidad de dispositivos, versiones del sistema operativo y modelos de distribución de aplicaciones amplía considerablemente la superficie de ataque.

Uno de los desafíos más relevantes en la detección de spyware Android es su capacidad para camuflarse como aplicaciones legítimas. Muchas muestras de spyware se presentan bajo la apariencia de utilidades comunes, aplicaciones de productividad, herramientas de mensajería o servicios de personalización. Estas aplicaciones suelen solicitar permisos que, aunque extensos, pueden parecer coherentes con su funcionalidad aparente, lo que reduce la sospecha tanto del usuario como de los sistemas automáticos de detección.

El uso de permisos legítimos del sistema representa otro obstáculo significativo. El spyware Android aprovecha componentes oficiales del sistema operativo, como los servicios de accesibilidad, el acceso a notificaciones, el almacenamiento externo o la lectura de registros del sistema. Debido a que estos permisos están diseñados para mejorar la experiencia del usuario o la accesibilidad, su utilización no implica necesariamente un comportamiento malicioso, lo que dificulta la diferenciación entre aplicaciones legítimas y spyware mediante análisis superficiales.

La ofuscación del código fuente es una técnica ampliamente utilizada por los desarrolladores de spyware para evadir la detección. Mediante el uso de cifrado, renombrado de clases y métodos, empaquetado dinámico y ocultamiento de cadenas sensibles, los atacantes logran dificultar el análisis estático del código. Estas técnicas reducen la eficacia de los mecanismos tradicionales de detección basados en firmas y obligan a emplear herramientas más avanzadas para identificar patrones sospechosos.

Otro desafío importante es la modularidad del spyware moderno. Muchas aplicaciones maliciosas no contienen toda su funcionalidad dentro del archivo APK inicial, sino que descargan componentes adicionales desde servidores remotos una vez instaladas. Esta estrategia

limita la capacidad del análisis estático para detectar comportamientos maliciosos completos, ya que parte de la lógica del spyware no se encuentra presente en el paquete original analizado.

La comunicación cifrada con servidores de comando y control (C2) constituye un obstáculo adicional en la detección del spyware Android. El uso de protocolos seguros, certificados personalizados y técnicas de ocultamiento del tráfico dificulta la identificación de comunicaciones sospechosas mediante análisis de red. Aunque el análisis estático puede revelar la presencia de endpoints o bibliotecas de red, no siempre permite determinar con precisión la naturaleza de las comunicaciones establecidas.

La fragmentación del ecosistema Android también complica la detección del spyware. La coexistencia de múltiples versiones del sistema operativo, diferentes fabricantes y capas de personalización implica que una misma aplicación puede comportarse de manera distinta según el entorno en el que se ejecute. Esta variabilidad dificulta la creación de modelos de detección universales y obliga a adaptar las estrategias de análisis a contextos específicos.

Desde la perspectiva del análisis estático, uno de los principales desafíos radica en la interpretación contextual de los resultados. Herramientas como MobSF generan una gran cantidad de información relacionada con permisos, APIs utilizadas, configuraciones y posibles vulnerabilidades. Sin embargo, no todos los hallazgos indican necesariamente un comportamiento malicioso. La correcta interpretación de estos resultados requiere conocimiento especializado y un análisis crítico que considere el contexto funcional de la aplicación.

La velocidad de aparición de nuevas variantes de spyware representa otro reto significativo. Los desarrolladores de malware actualizan constantemente sus aplicaciones para evadir las detecciones existentes, introduciendo cambios menores pero efectivos que alteran los

indicadores conocidos. Esta dinámica obliga a una actualización continua de las herramientas de análisis y a la revisión constante de los criterios de detección utilizados.

Asimismo, la distribución del spyware fuera de las tiendas oficiales dificulta su monitoreo. Plataformas de terceros, repositorios alternativos y campañas de ingeniería social facilitan la propagación de aplicaciones maliciosas sin pasar por los controles de seguridad de las tiendas oficiales. Esta situación incrementa la necesidad de análisis preventivos antes de la instalación de aplicaciones en dispositivos personales o corporativos.

Finalmente, los desafíos actuales en la detección de spyware Android ponen de manifiesto la importancia de adoptar un enfoque integral de seguridad. Si bien el análisis estático constituye una herramienta fundamental para la identificación temprana de amenazas, su eficacia depende de la combinación con buenas prácticas de desarrollo, concienciación del usuario y políticas de seguridad adecuadas. En este contexto, la detección del spyware no debe entenderse como un proceso aislado, sino como parte de una estrategia global orientada a la protección de la información y la privacidad en entornos móviles.

Buenas Prácticas para la Prevención del Spyware Android. La prevención del spyware Android constituye un elemento fundamental dentro de las estrategias de ciberseguridad móvil, tanto en el ámbito personal como organizacional. Considerando la creciente sofisticación de este tipo de malware y su capacidad para operar de forma silenciosa, resulta imprescindible adoptar un conjunto de buenas prácticas orientadas a reducir el riesgo de infección, minimizar la exposición a amenazas y fortalecer la protección de la información sensible.

Una de las primeras buenas prácticas consiste en el control riguroso de las fuentes de instalación de aplicaciones. Aunque el spyware puede encontrarse incluso en repositorios aparentemente confiables, la mayoría de las campañas maliciosas se distribuyen a través de

tiendas de aplicaciones no oficiales, enlaces fraudulentos o archivos compartidos mediante mensajería instantánea. Limitar la instalación de aplicaciones a fuentes verificadas reduce significativamente la probabilidad de exposición a spyware.

El análisis previo de aplicaciones antes de su instalación representa otra práctica esencial. En entornos académicos y organizacionales, el uso de herramientas de análisis estático como Mobile Security Framework (MobSF) permite evaluar el comportamiento potencial de una aplicación sin necesidad de ejecutarla. El análisis de permisos solicitados, bibliotecas utilizadas, configuraciones del manifiesto y posibles vulnerabilidades proporciona información valiosa para identificar riesgos asociados al spyware.

La gestión adecuada de permisos es una de las medidas más efectivas para prevenir el espionaje digital. Muchas aplicaciones solicitan permisos excesivos que no guardan relación directa con su funcionalidad principal. Revisar cuidadosamente los permisos otorgados y revocar aquellos innecesarios reduce la superficie de ataque y limita las capacidades del spyware en caso de que una aplicación maliciosa logre instalarse en el dispositivo.

Otra buena práctica fundamental es mantener el sistema operativo y las aplicaciones actualizadas. Las actualizaciones de Android incluyen parches de seguridad que corrigen vulnerabilidades conocidas y mejoran los mecanismos de protección del sistema. El uso de versiones recientes del sistema operativo, como aquellas posteriores a API 35, incrementa la resistencia del dispositivo frente a técnicas de explotación utilizadas por el spyware.

Desde el punto de vista organizacional, la implementación de políticas de seguridad móvil resulta indispensable. Estas políticas deben establecer criterios claros sobre el uso de dispositivos personales y corporativos, la instalación de aplicaciones, el acceso a información

sensible y la respuesta ante incidentes de seguridad. La definición de normas claras contribuye a reducir comportamientos de riesgo y a fortalecer la postura de seguridad institucional.

La concienciación y formación de los usuarios desempeñan un papel clave en la prevención del spyware Android. Muchos ataques se basan en técnicas de ingeniería social que explotan el desconocimiento o la confianza del usuario. Programas de capacitación orientados a identificar aplicaciones sospechosas, permisos excesivos y comportamientos anómalos permiten reducir significativamente la efectividad de estas campañas.

El uso de soluciones de seguridad móvil complementarias también forma parte de las buenas prácticas preventivas. Aunque ninguna herramienta garantiza una protección absoluta, las soluciones de seguridad pueden ofrecer detección adicional basada en reputación, análisis de comportamiento y monitoreo de aplicaciones instaladas. Estas herramientas deben considerarse como un complemento al análisis manual y no como un sustituto del criterio humano.

Otra medida preventiva importante es la segmentación de la información sensible. Evitar el almacenamiento innecesario de datos confidenciales en dispositivos móviles limita el impacto potencial del spyware. En entornos corporativos, la separación de perfiles personales y profesionales contribuye a reducir el riesgo de exposición de información estratégica en caso de compromiso del dispositivo.

La auditoría periódica de aplicaciones instaladas representa una práctica recomendable tanto para usuarios como para organizaciones. Revisar regularmente las aplicaciones presentes en el dispositivo, identificar aquellas que ya no se utilizan y evaluar su legitimidad permite detectar posibles amenazas que hayan pasado desapercibidas en el momento de la instalación.

En el contexto del análisis académico y profesional, documentar los resultados obtenidos mediante herramientas como MobSF constituye una buena práctica adicional. La generación de

informes detallados facilita la toma de decisiones, el seguimiento de riesgos y la mejora continua de los procesos de seguridad. Además, esta documentación contribuye a la transferencia de conocimientos y a la concienciación sobre las amenazas existentes.

Finalmente, la prevención del spyware Android debe entenderse como un proceso continuo y evolutivo. La rápida evolución de las técnicas de ataque exige una actualización constante de conocimientos, herramientas y estrategias. La combinación de análisis estático, buenas prácticas de uso, políticas de seguridad y formación continua constituye la base para reducir de manera efectiva los riesgos asociados al spyware en entornos Android modernos.

Capítulo 3

3. Desarrollo

3.1. Desarrollo del Trabajo

Arquitectura del Laboratorio. El presente trabajo está compuesto por un laboratorio con las siguientes características:

PC físico(host)

Procesador: Intel core i9 de 14 cores

Memoria RAM: 32 GB

Disco SSD (NVMe): 1 TB

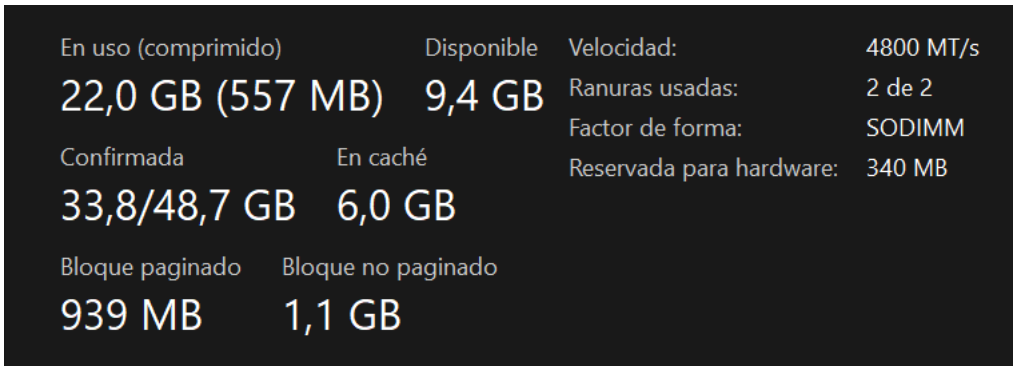
Figura 1

Recursos Procesador

Nota: Detalle del CPU de la máquina física.

Figura 2

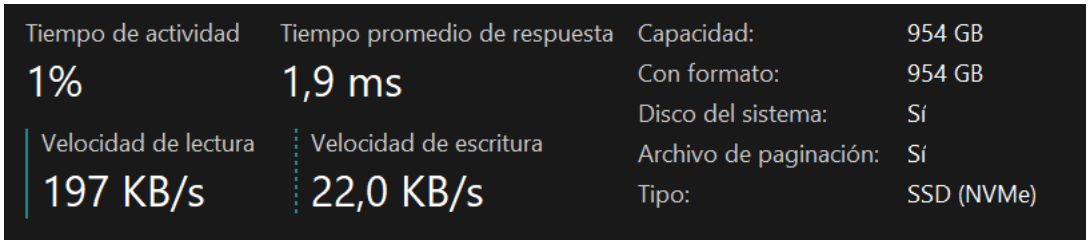
Recursos Memoria RAM



Nota: Detalle de la memoria de la máquina física.

Figura 3

Recursos Disco SSD



Nota: Detalle del Disco SSD (NVMe) de la máquina física.

Máquina virtual (VM)

Sistema Operativo: Ubuntu 22.04 LTS

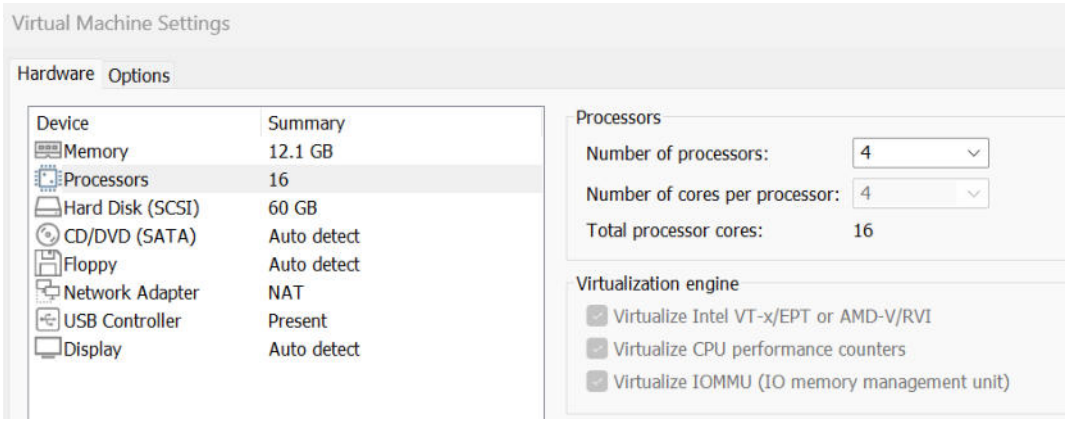
Disco: 60 GB

RAM: 12 GB

CPU: 16 cores

Figura 4

Recursos Máquina Virtual



Nota: Detalle de la configuración de la máquina virtual.

Entorno Virtual Seguro. El análisis del malware se llevó a cabo en un entorno virtual seguro basado en una máquina virtual con sistema operativo Linux (Ubuntu). La virtualización permite aislar el entorno de análisis del sistema anfitrión, reduciendo el riesgo de infección y facilitando la gestión de herramientas especializadas.

El uso de una máquina virtual garantiza la reproducibilidad del estudio y permite controlar variables como la configuración del sistema, la instalación de dependencias y el

almacenamiento seguro de muestras de malware. Este enfoque es ampliamente recomendado en investigaciones de ciberseguridad y análisis de malware.

Android Studio + Emulador Android 15 (API 35). Para la implementación del emulador que nos servirá de entorno seguro para realizar el análisis del malware se utilizó Android Studio que al ser instalado sobre un ambiente linux nos brinda un mejor rendimiento y compatibilidad para emular sistemas Android.

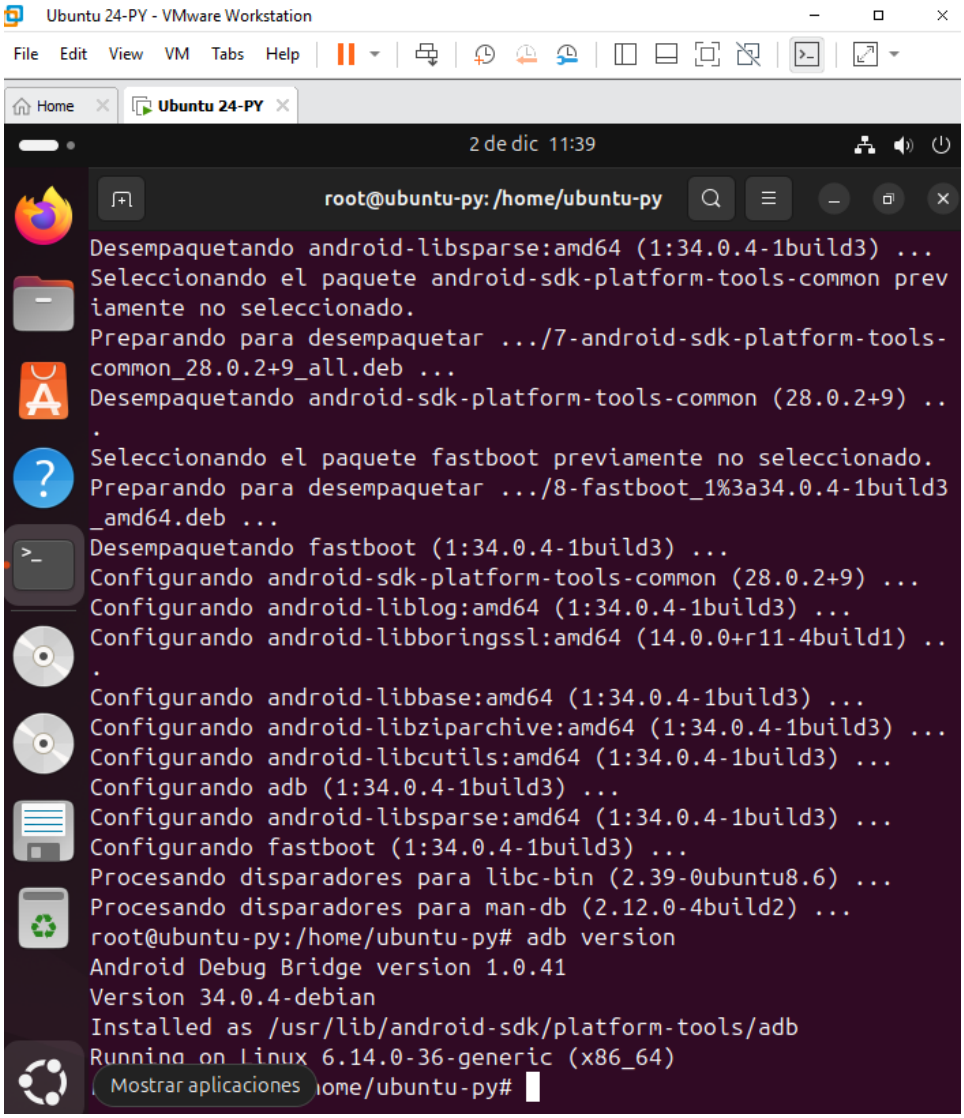
Android Debug Bridge (ADB). Fue utilizado como herramienta complementaria para la interacción con el entorno Android virtual. ADB permitió verificar la conectividad del entorno,

gestionar archivos y realizar comprobaciones básicas relacionadas con la estructura de la aplicación analizada.

Su uso se limitó a tareas de soporte técnico, evitando la ejecución directa del malware y manteniendo el enfoque metodológico centrado en el análisis estático.

Figura 5

Instalación Android tools y tools ADB

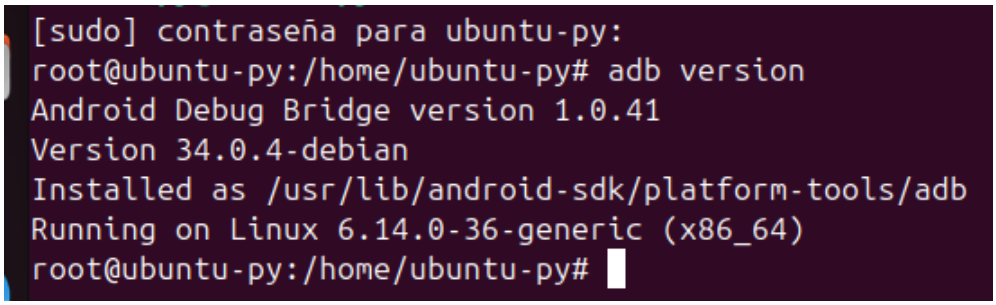


Nota: Comando utilizado para la instalación de Android tools y tools ADB

```
sudo apt install android-tools-adb android-tools-fastboot -y
```

Figura 6

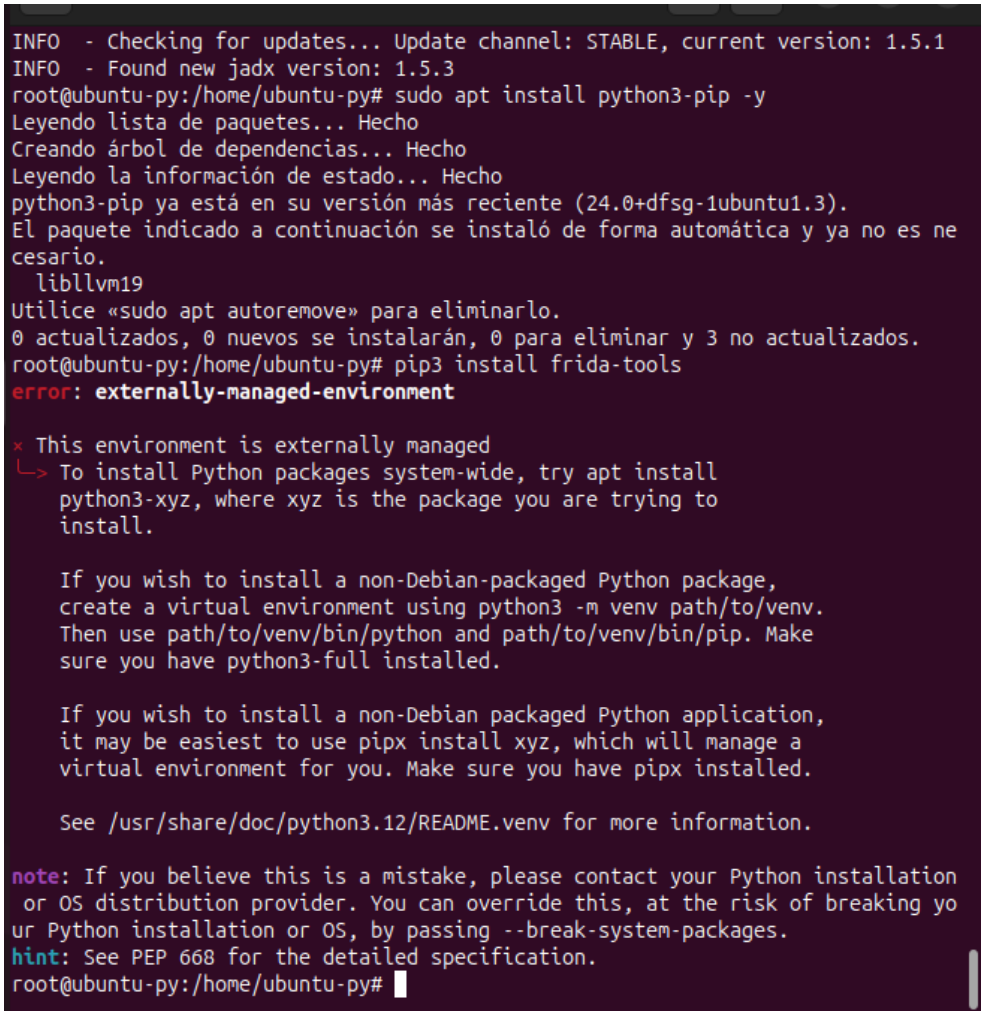
Instalación Android tools y tools ADB



Nota: Comprobamos La instalación y la versión con el comando "`adb version`"

Figura 7

Instalación de FRIDA



Nota: Instalamos con los siguientes comandos

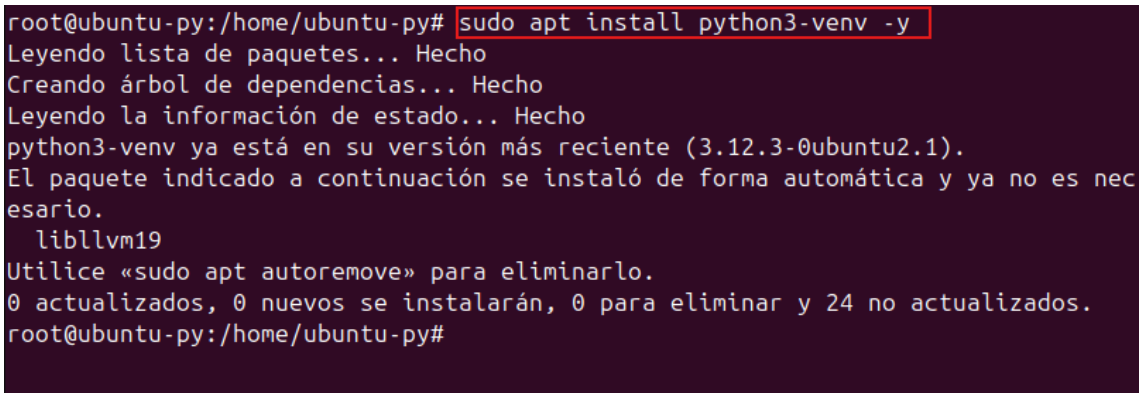
```
sudo apt install python3-pip -y
pip3 install frida-tools
```

Al probar la versión se observa un “error: externally-managed-environment” el cual es resultado de “no dejo usar pip3 directamente sobre el Python del sistema, porque lo maneja Ubuntu” (PEP 668)”

Para el cual la solución fue realizar un entorno virtual para que funcionara y se instalara correctamente FRIDA

Figura 8

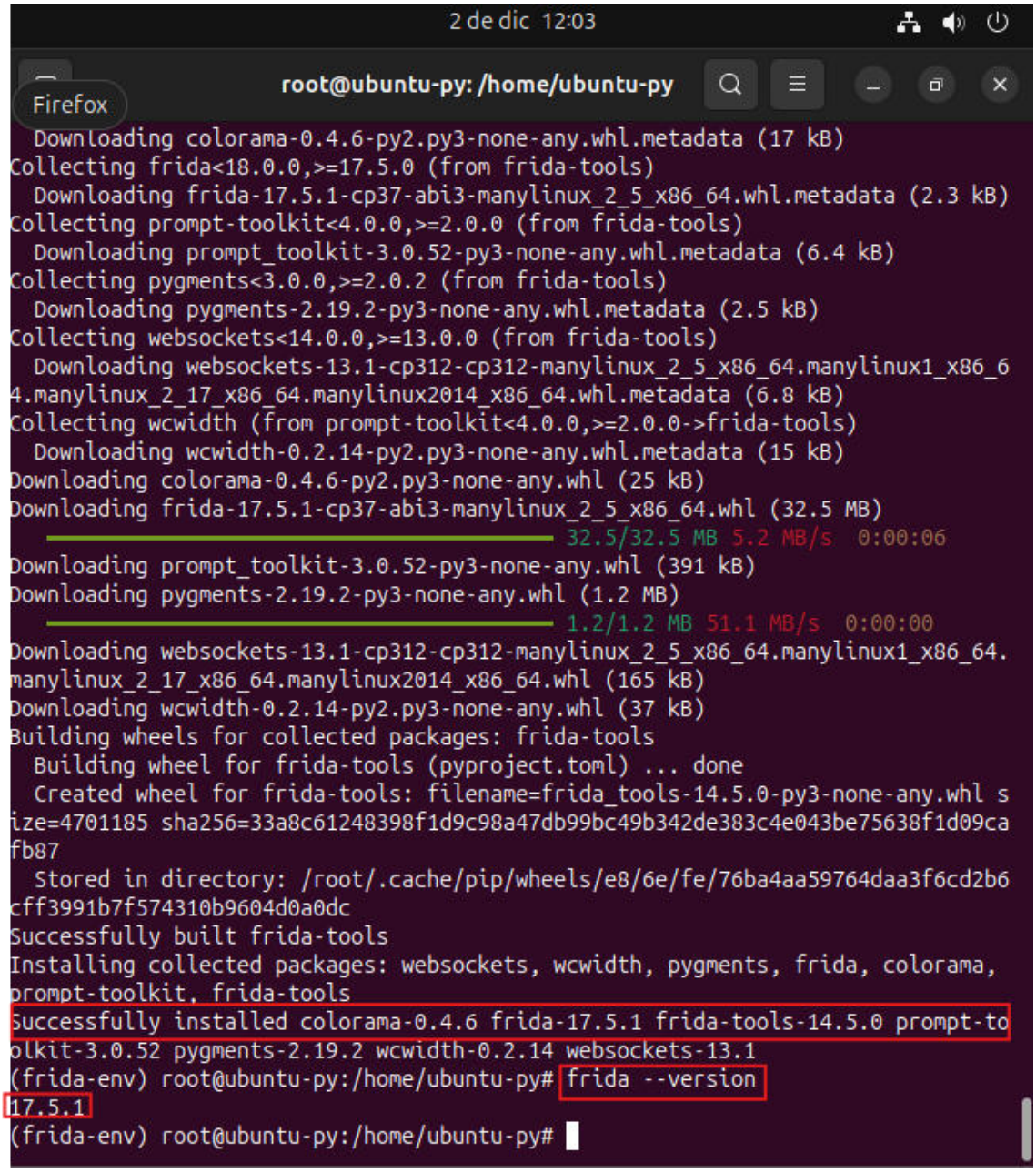
Instalación de FRIDA



Nota: Se utilizó el comando "`sudo apt install python3-venv -y`" creando un entorno en el HOME con los comandos "`cd /home/ubuntu-py | python3 -m venv frida-env`"

Figura 9

Instalación de FRIDA



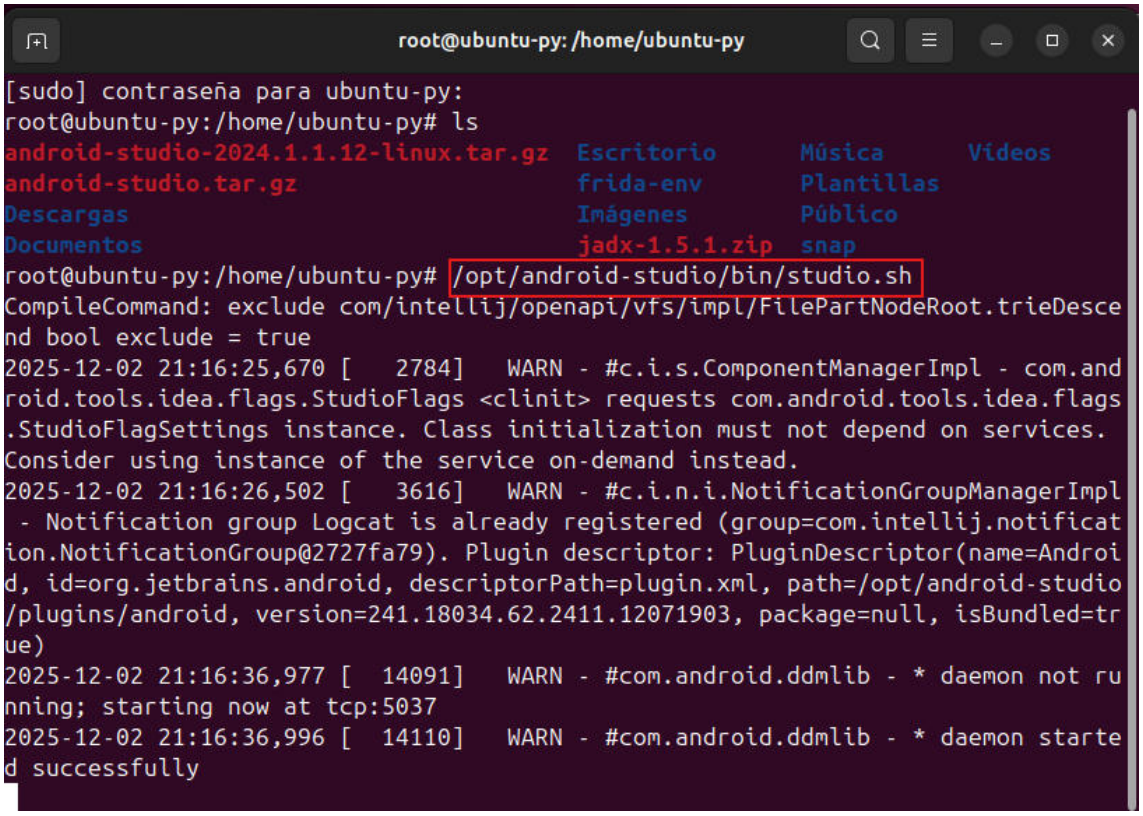
Nota: Utilizamos los siguientes comandos "`cd /home/ubuntu-py | source frida-env/bin/actívate | frida –versión`" los cuales nos ayudan activar Frida y verificar la

versión y todo este correctamente instalado en el entorno virtual y funcionando para realizar análisis

Instalación Android Studio. Android Studio fue utilizado como entorno de apoyo para la gestión de versiones de Android y la simulación del ecosistema Android. Aunque no se empleó para la ejecución dinámica del malware, Android Studio permitió verificar la compatibilidad de la aplicación con versiones recientes del sistema operativo y gestionar los componentes necesarios para el análisis estático.

Figura 10

Instalación de Android Studio

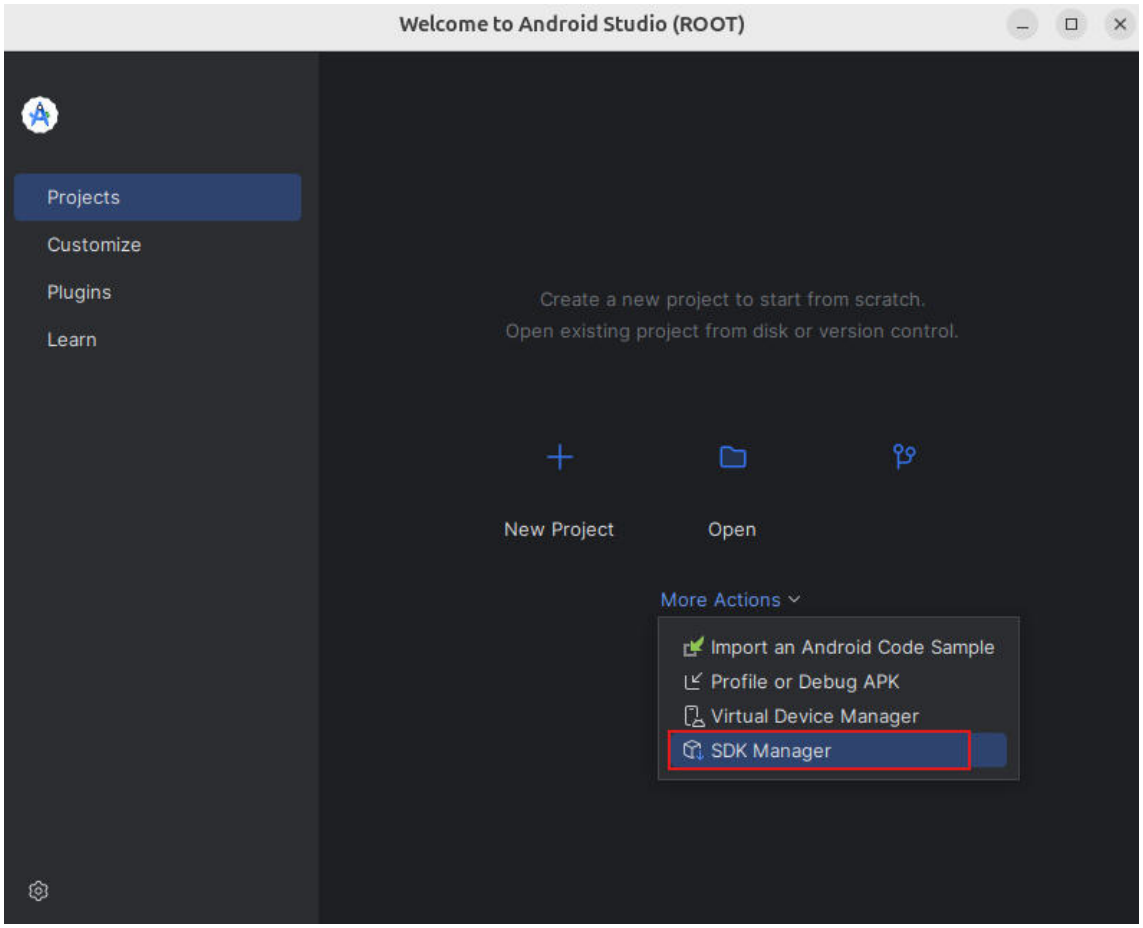


Nota: Comando para iniciar Android estudio

`/opt/android-studio/bin/studio.sh`

Figura 11

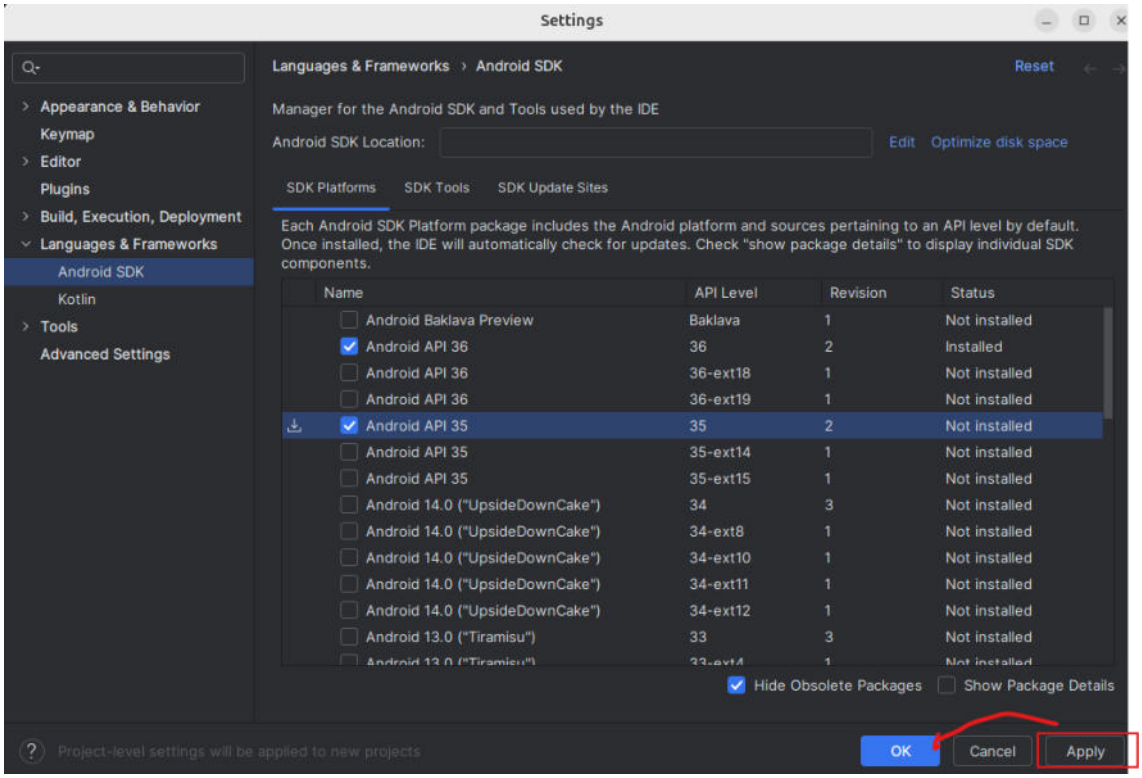
Instalación de Android Studio



Nota: Ejecutamos Android Studio y escogemos la SDK manager para congigura que imagen de Android usaremos.

Figura 12

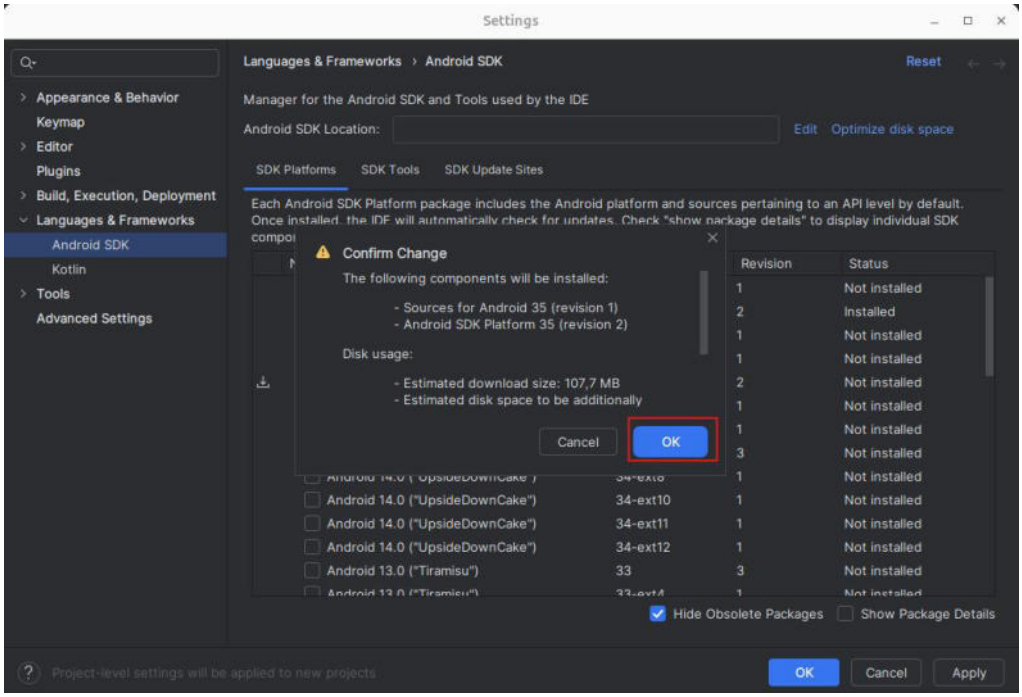
Instalación de Android Studio



Nota: Escogemos Android API 35 que equivale a la versión 15.

Figura 13

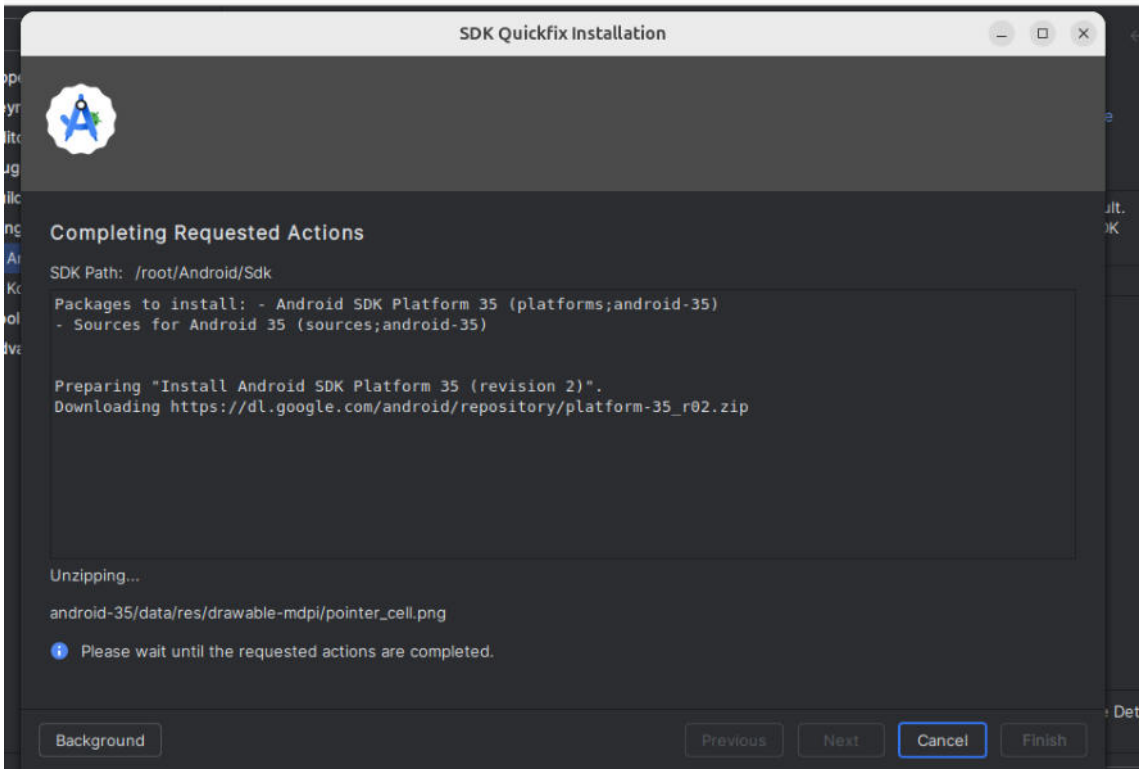
Instalación de Android Studio



Nota: Confirmamos lo que escogimos en la figura anterior para continuar con la configuración.

Figura 14

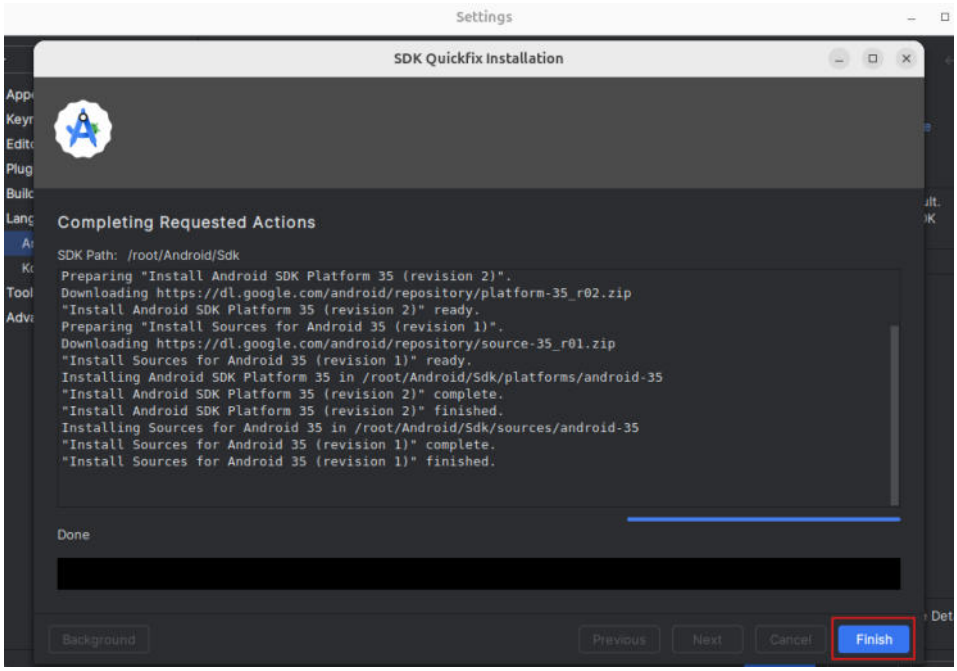
Instalación de Android Studio



Nota: A continuación, inicia la descargar de la imagen de Android 15 que estamos configurando.

Figura 15

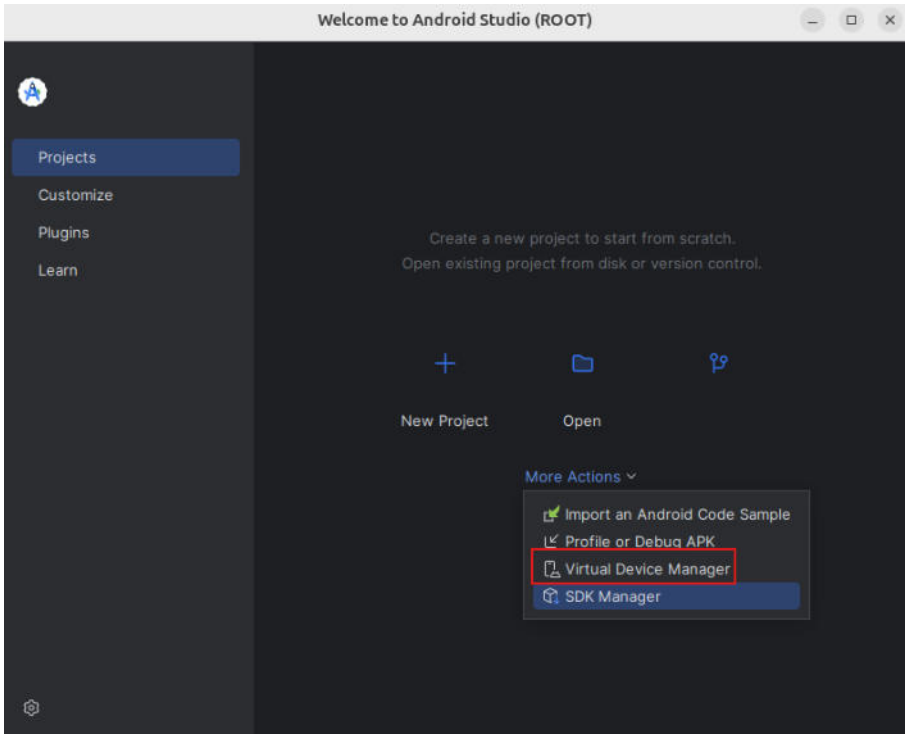
Instalación de Android Studio



Nota: Una vez que termina la descarga procedemos a dar clic en el botón Finish.

Figura 16

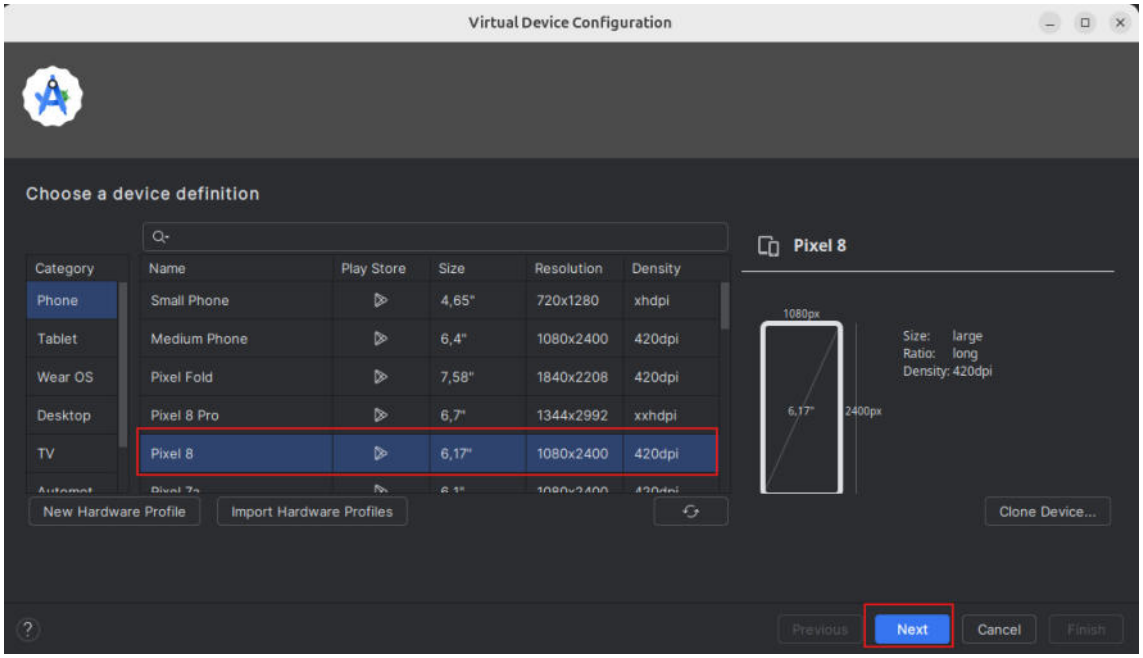
Creación dispositivo virtual en Android Studio



Nota: Seleccionamos Virtual Device Manager para crear el dispositivo virtual.

Figura 17

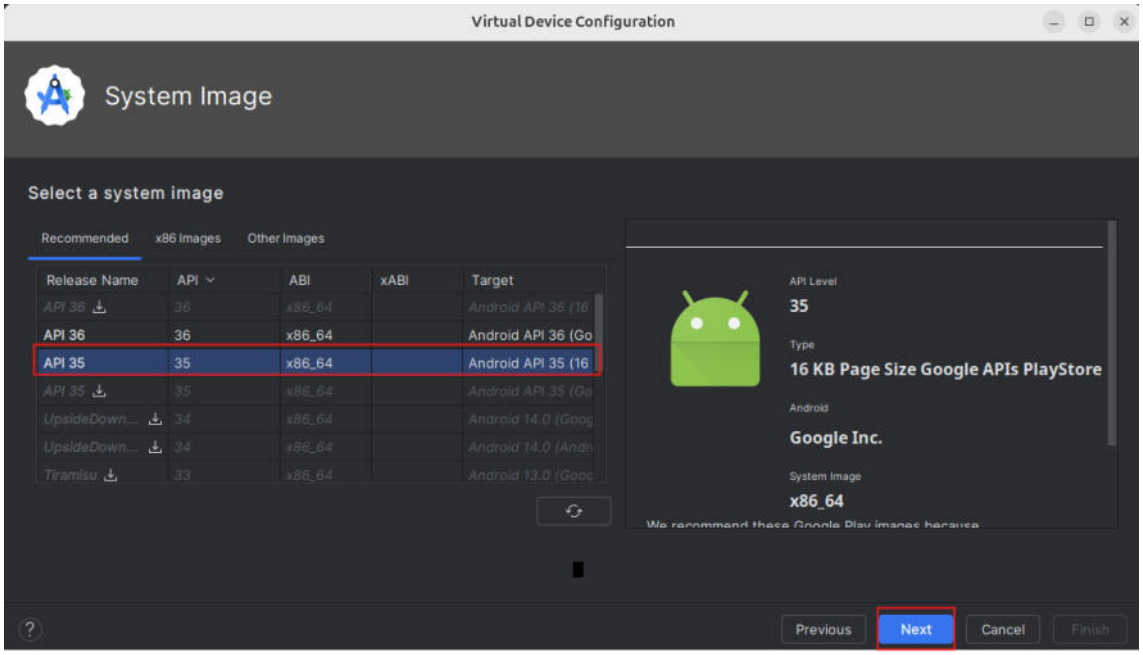
Creación dispositivo virtual en Android Studio



Nota: Seleccionamos el tipo de celular virtual que queremos crear en este caso un Pixel 8.

Figura 18

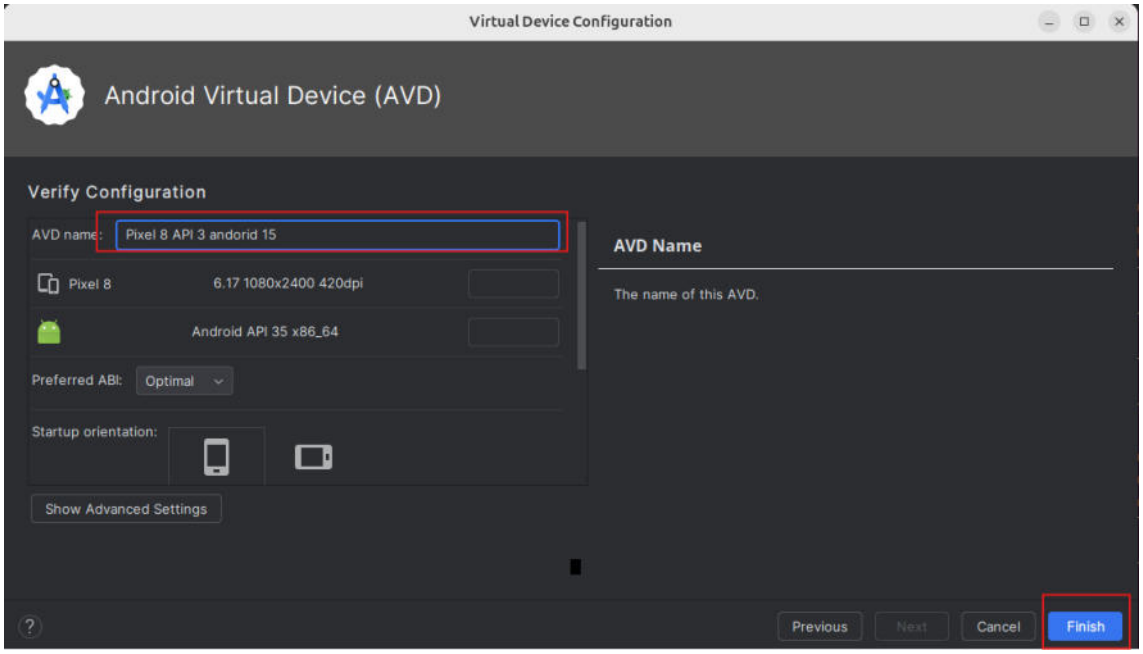
Creación dispositivo virtual en Android Studio



Nota: Seleccionamos la versión de Android en este caso la API 35 que es la equivalente a Android 15.

Figura 19

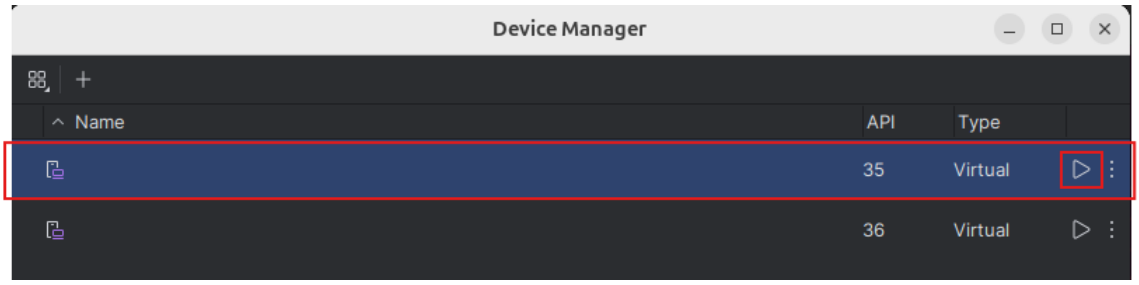
Creación dispositivo virtual en Android Studio



Nota: Colocamos un nombre para identificar a nuestro dispositivo virtual.

Figura 20

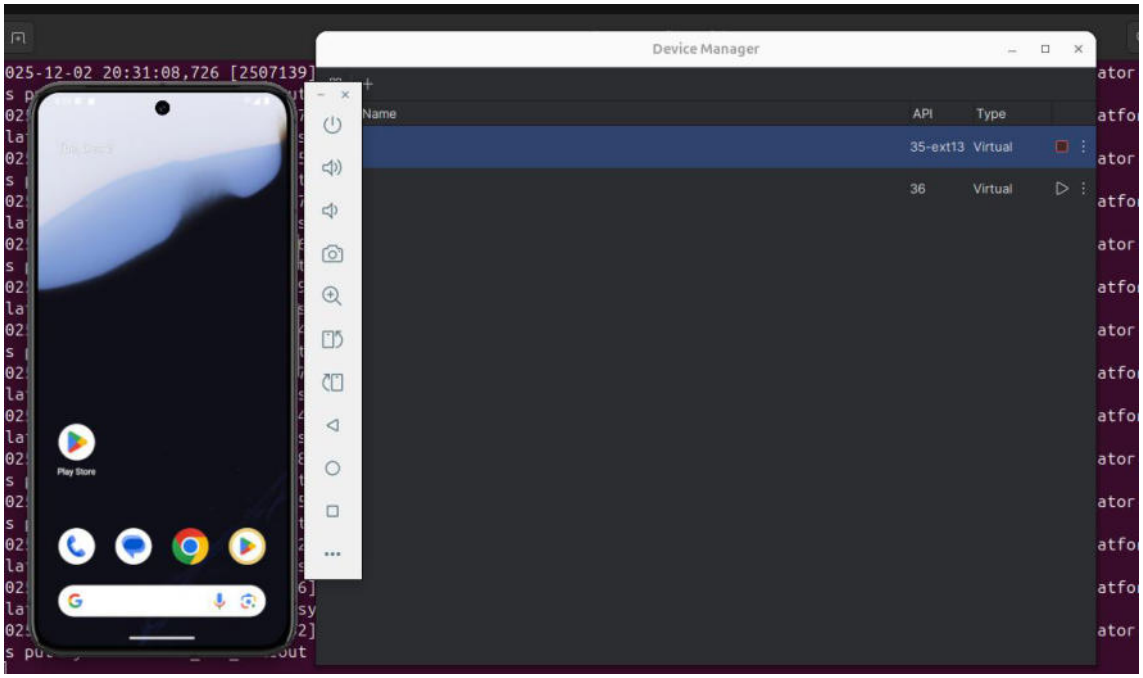
Creación dispositivo virtual en Android Studio



Nota: Damos clin en el botón de iniciar nuestro dispositivo virtual

Figura 21

Creación dispositivo virtual en Android Studio

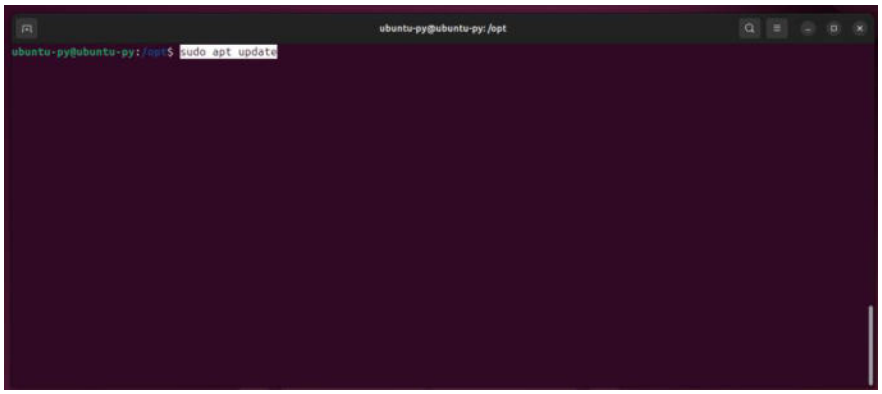


Nota: Como paso final vemos que se inicia una pantalla que es nuestro dispositivo virtual para realizar

Instalación de DOCKER

Figura 22

Instalación de Docker para MobSF

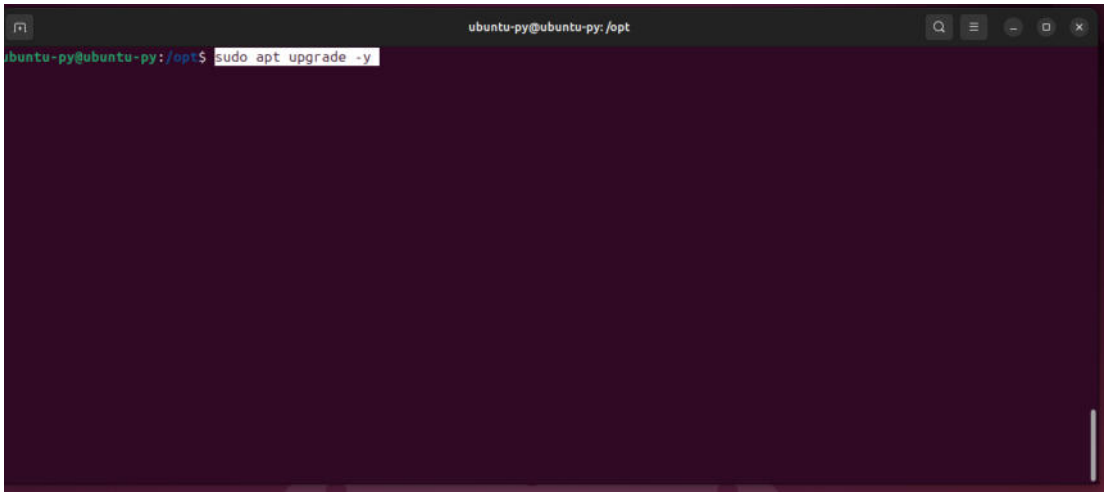


Nota: Verificamos que la lista de paquetes del sistema esté actualizada.

```
Sudo apt update
```

Figura 23

Instalación de Docker para MobSF

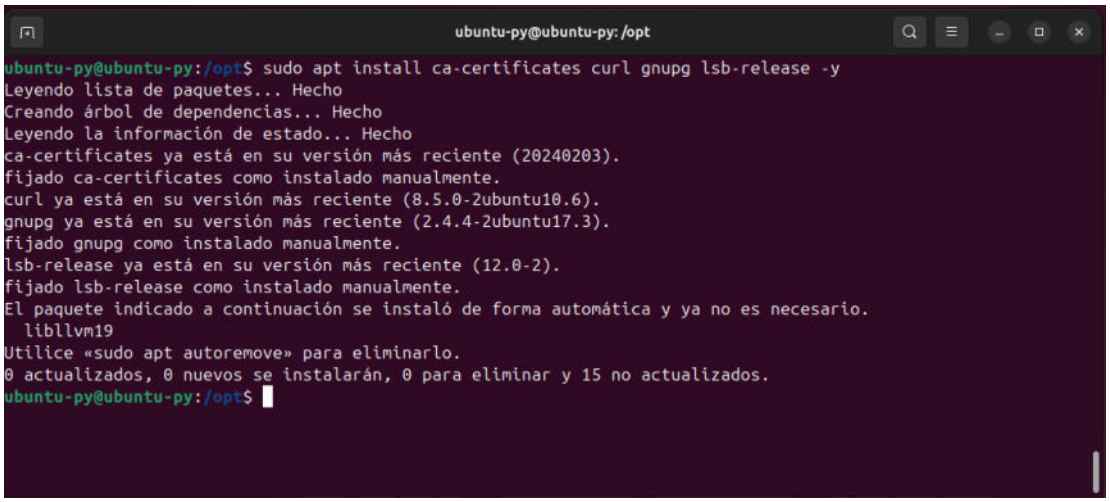


Nota: Se procede a actualizar los paquetes del Sistema operativo.

```
sudo apt upgrade -y
```

Figura 24

Instalación de Docker para MobSF

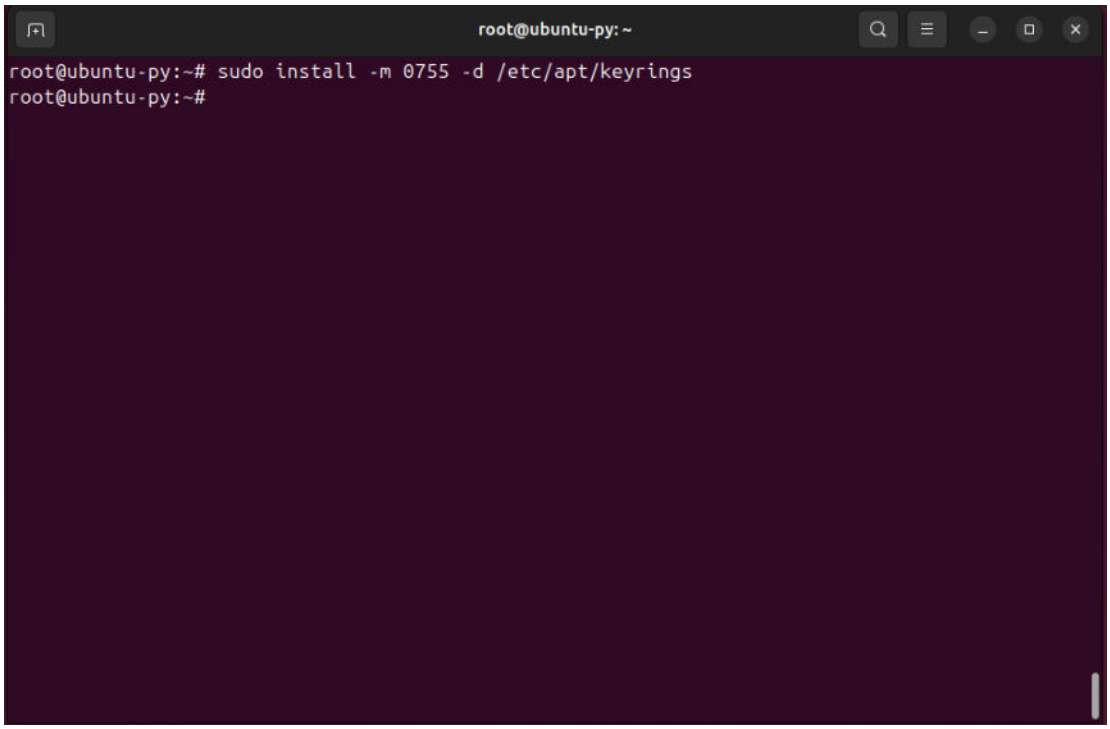


Nota: Se instala los paquetes necesarios para configurar el repositorio de Docker.

```
sudo apt install ca-certificates curl gnupg lsb-release -y
```

Figura 25

Instalación de Docker para MobSF

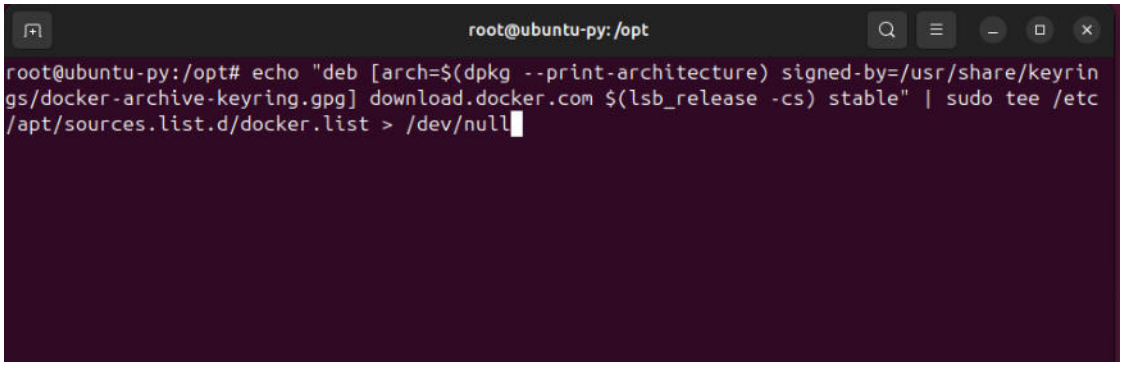


Nota: Se agrega la clave GPG de Docker al sistema.

```
sudo install -m 0755 -d /etc/apt/keyrings
```

Figura 26

Instalación de Docker para MobSF

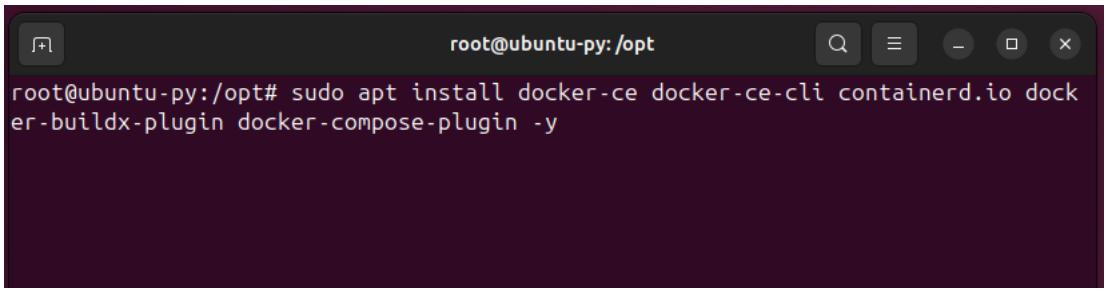


Nota: Se agrega el repositorio de Docker al sistema.

```
echo "deb [arch=$(dpkg --print-architecture) signed-
by=/usr/share/keyrings/docker-archive-keyring.gpg] download.docker.com
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list >
/dev/null
```

Figura 27

Instalación de Docker para MobSF

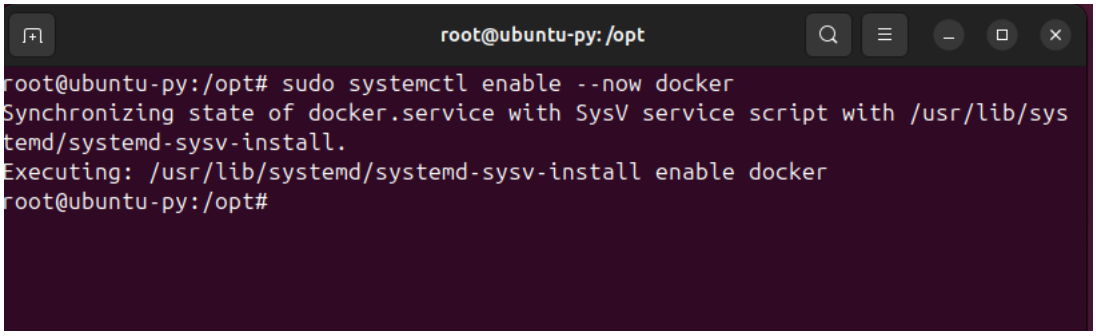


Nota: Se instala Docker Engine, CLI, containerd y el complemento Docker Compose

```
sudo apt install docker-ce docker-ce-cli containerd.io docker-
buildx-plugin docker-compose-plugin -y
```

Figura 28

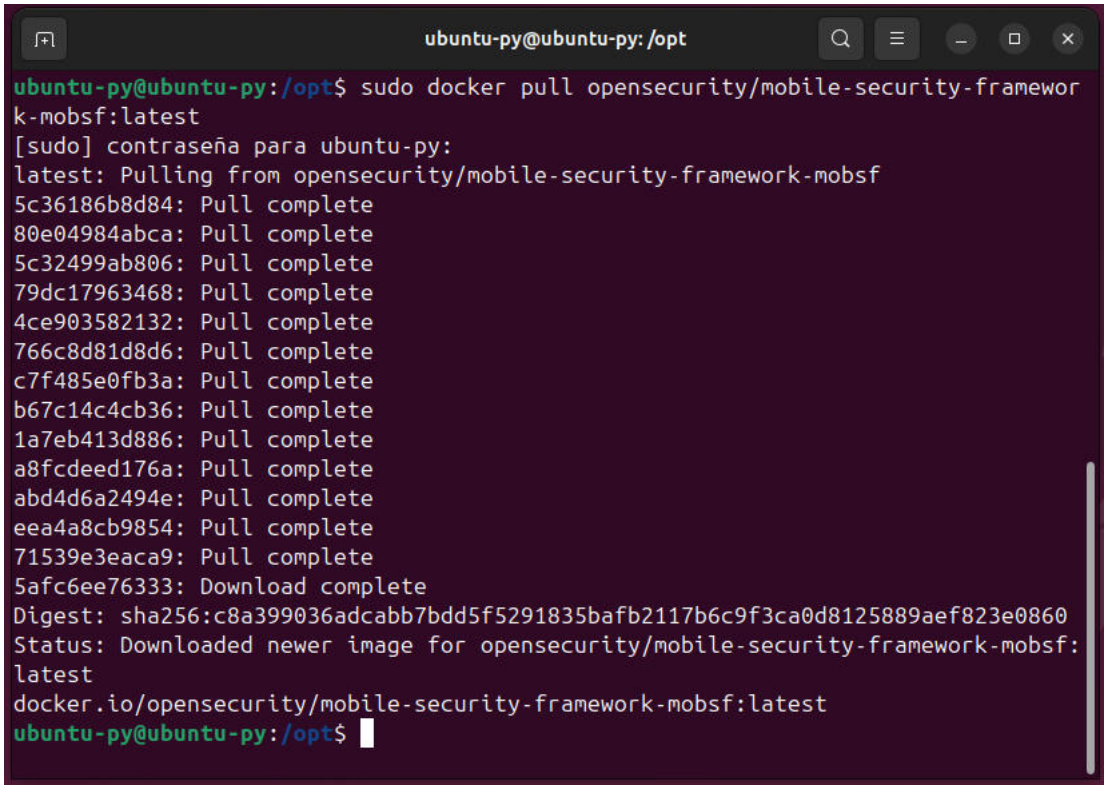
Instalación de Docker para MobSF



Nota: Se configura que el servicio Docker se inicie automáticamente al arrancar.

Figura 29

Instalación de MobSF

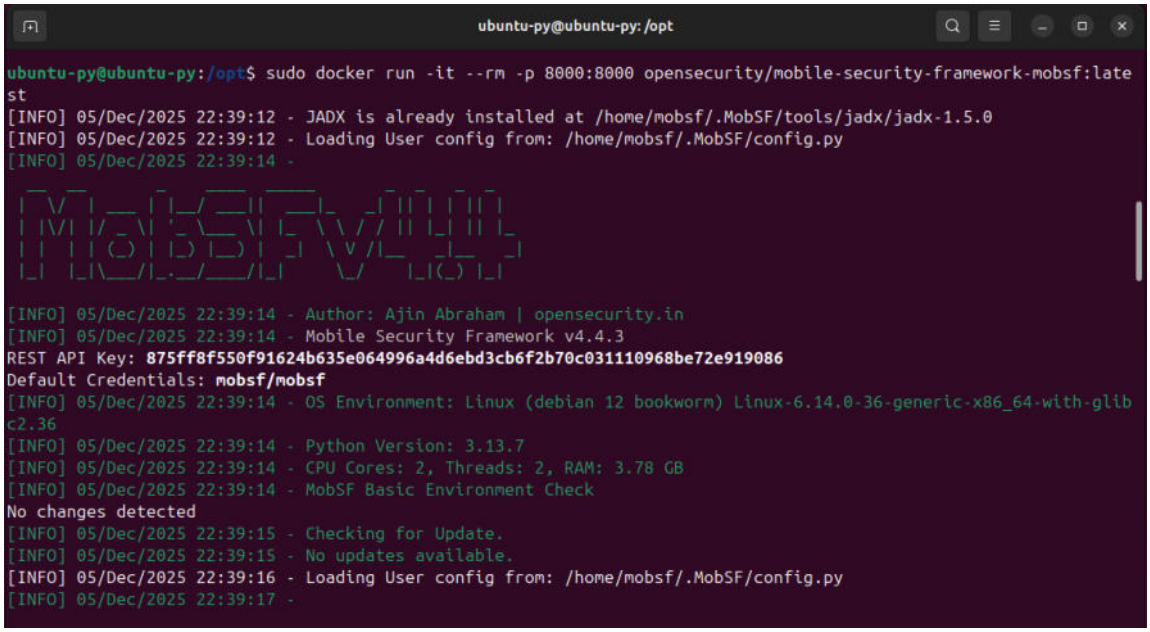


Nota: Se realiza la instalación de MobSF median su imagen de Docker

```
docker pull opensecurity/mobile-security-framework-mobsf:latest
```

Figura 30

Instalación de MobSF

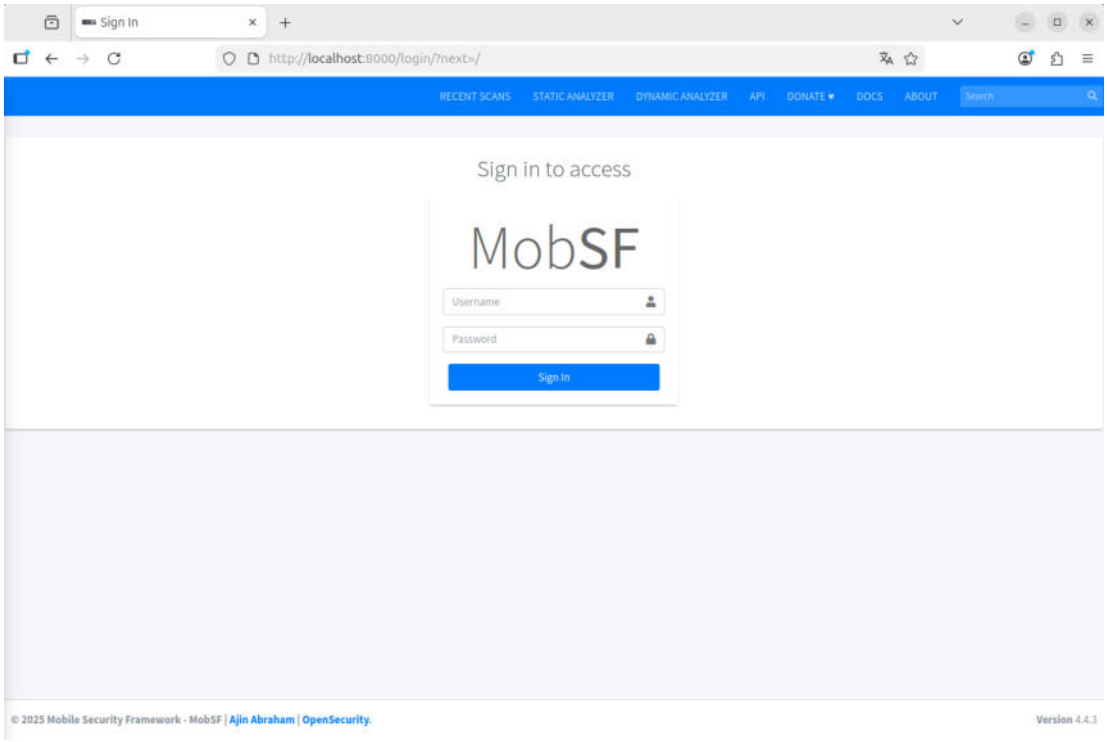


Nota: Se procede a levantar el MobSFen el puerto 8000

```
docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
```

Figura 31

Ingreso de MobSF



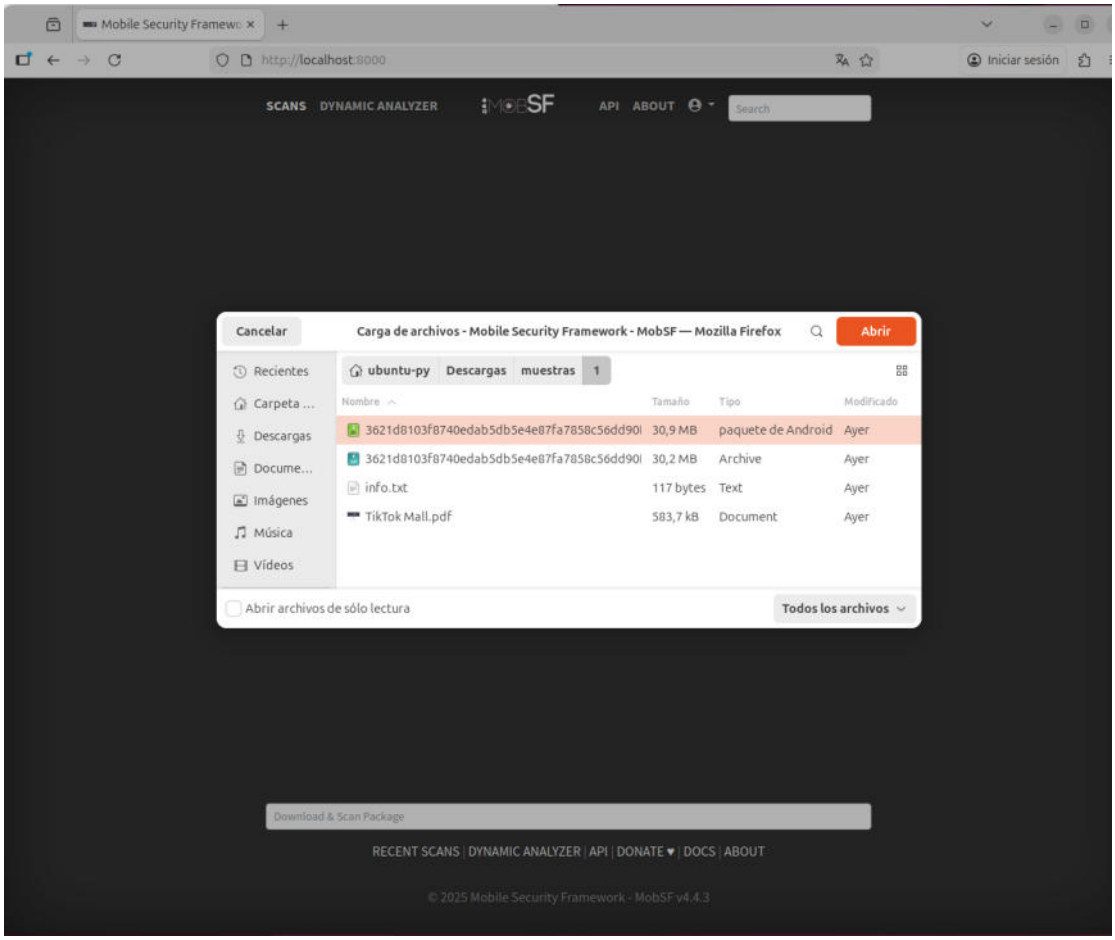
Nota: Mediante un navegador web se accede a la interfaz web colocando http://localhost:8000

Análisis Estático con MobSF.

El archivo APK fue cargado en MobSF para su análisis estático. La herramienta generó un reporte detallado que incluyó información sobre permisos, componentes, configuraciones de seguridad y posibles vulnerabilidades. Estos resultados constituyen la base principal del análisis presentado en el Capítulo IV.

Figura 32

Análisis estático con MobSF



Nota: Se selecciona el apk del malware a analizar.

Obtención de la Muestra. La muestra de malware Android tipo spyware fue obtenida desde un repositorio especializado en análisis de malware, asegurando su autenticidad y relevancia para el estudio. Antes de su análisis, el archivo APK fue almacenado en el entorno virtual seguro para evitar cualquier interacción con el sistema anfitrión.

Preparación del Entorno. Se configuró la máquina virtual con las herramientas necesarias, incluyendo MobSF, Android Studio y ADB. Asimismo, se verificó la correcta

instalación de dependencias y se establecieron medidas básicas de seguridad, como la restricción de conexiones externas innecesarias.

Consideraciones éticas

El desarrollo de esta investigación se realizó respetando principios éticos fundamentales. El análisis se llevó a cabo exclusivamente con fines académicos, utilizando muestras de malware en entornos controlados y sin afectar a usuarios reales ni a sistemas en producción.

Asimismo, no se ejecutó el malware en dispositivos físicos ni se recopiló información personal de terceros. Las herramientas utilizadas se emplearon de acuerdo con sus licencias y recomendaciones, garantizando un uso responsable de los recursos tecnológicos.

Limitaciones Metodológicas. Entre las principales limitaciones de la investigación se encuentra el enfoque exclusivo en el análisis estático, lo cual impide observar el comportamiento dinámico del malware durante su ejecución. Sin embargo, esta limitación es deliberada y responde a la necesidad de mantener un entorno seguro y alineado con los objetivos del estudio.

Otra limitación corresponde al análisis de una única muestra de spyware Android. No obstante, el nivel de detalle alcanzado permite identificar características comunes y establecer bases sólidas para investigaciones futuras.

Relación de la metodología con los objetivos. La metodología empleada en esta investigación se encuentra directamente alineada con los objetivos planteados. El uso del análisis estático y de herramientas especializadas como MobSF permite identificar las características técnicas del malware, evaluar sus riesgos y generar conclusiones fundamentadas.

Este enfoque metodológico garantiza la coherencia entre el marco teórico, los procedimientos aplicados y los resultados obtenidos, fortaleciendo la validez académica del estudio.

Capítulo 4

4. Análisis de resultados

4.1. Pruebas de Concepto

Las pruebas de concepto se realizaron mediante un análisis estático del malware "TikTok Mall", obtenido desde MalwareBazaar y posteriormente evaluado mediante la herramienta Mobile Security Framework (MobSF).

El objetivo de esta fase fue identificar comportamientos maliciosos, riesgos de seguridad, permisos abusivos, inconsistencias estructurales y cualquier evidencia que sugiriera actividad asociada a spyware.

El análisis estático fue seleccionado por su capacidad para inspeccionar el contenido del paquete APK sin necesidad de ejecución, permitiendo examinar:

- El AndroidManifest.xml;
- Los permisos declarados;
- El código descompilado (smali o Java reconstruido);
- Los componentes exportados;
- Las librerías integradas;
- Los puntos de entrada;
- La estructura interna del malware;
- Las reglas YARA y coincidencias con patrones de amenazas;
- Comportamientos internos identificados por el motor heurístico de MobSF;

Estas pruebas permitieron establecer con precisión qué capacidades posee el malware y cuáles serían los posibles vectores de ataque si el usuario lo instalara en un dispositivo real.

4.2. Análisis de Resultados

El presente capítulo expone los resultados obtenidos a partir del análisis estático del malware Android de tipo spyware, utilizando como herramienta principal el Mobile Security Framework (MobSF). Los hallazgos presentados se derivan de la inspección detallada del archivo APK analizado, sin ejecutar la aplicación en un entorno real, garantizando así la seguridad del sistema y la integridad del entorno de investigación.

Los resultados se organizan de manera sistemática, abordando aspectos clave como permisos solicitados, componentes de la aplicación, configuraciones de seguridad, riesgos identificados y posibles indicadores de comportamiento malicioso. La interpretación de estos resultados se fundamenta en el marco teórico desarrollado previamente, permitiendo establecer relaciones claras entre los hallazgos técnicos y los conceptos de spyware Android.

Descripción General de la Muestra 1 Analizada

La muestra 1 analizada corresponde a una aplicación Android en formato APK, clasificada como malware de tipo spyware. El archivo fue sometido a un análisis estático completo mediante MobSF, lo que permitió extraer información relevante sobre su estructura interna, componentes declarados y configuraciones de seguridad.

De acuerdo con el reporte generado por MobSF, la aplicación presenta características típicas de software malicioso orientado a la recopilación de información sensible. Entre estas características se destacan la solicitud de múltiples permisos peligrosos, la presencia de componentes exportados y el uso de configuraciones que podrían facilitar accesos no autorizados.

A partir del análisis generado al apk (muestra 1) “TikTok Mall”, se observa que la aplicación presenta múltiples indicadores de actividad maliciosa, clasificados por severidad.

A continuación, se detallan los hallazgos más relevantes estructurados en categorías.

Permisos Abusivos Identificados. MobSF detectó que el APK solicita permisos sensibles, típicos de spyware y aplicaciones utilizadas para exfiltrar datos o monitorear al usuario.

Entre ellos:

- **WRITE_EXTERNAL_STORAGE**

Riesgo: permite leer, copiar o eliminar archivos del usuario.

- **READ_PHONE_STATE**

Riesgo: obtiene IMEI, número telefónico y estado de llamadas.

- **INTERNET y ACCESS_NETWORK_STATE**

Riesgo: comunicación con servidores externos para exfiltración.

- **REQUEST_INSTALL_PACKAGES**

Riesgo: capacidad de instalar aplicaciones no autorizadas.

Estos permisos coinciden con las prácticas habituales observadas en troyanos bancarios, adware agresivo y spyware de nivel básico.

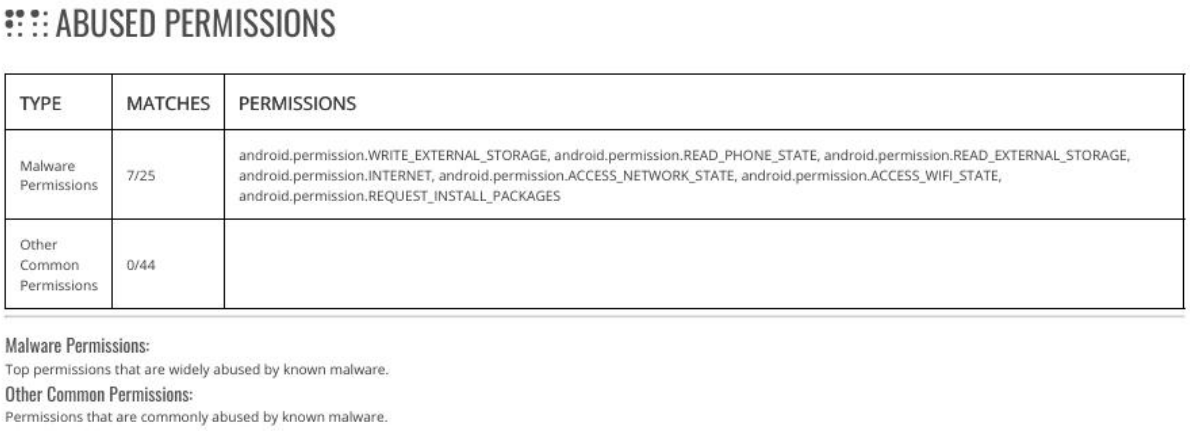
Análisis de Permisos Solicitados. Uno de los aspectos más relevantes del análisis estático corresponde a la evaluación de los permisos solicitados por la aplicación. El sistema de permisos de Android constituye un mecanismo fundamental de control de acceso a los recursos del dispositivo, por lo que el análisis de estos permisos permite identificar posibles comportamientos maliciosos.

El reporte de MobSF evidenció que la aplicación solicita varios permisos clasificados como peligrosos, los cuales permiten el acceso a información sensible del usuario. Entre estos permisos se incluyen aquellos relacionados con el acceso al almacenamiento, lectura de información personal y uso de recursos críticos del dispositivo.

La combinación y cantidad de permisos solicitados resulta inconsistente con la funcionalidad aparente de una aplicación legítima, lo que constituye un indicador claro de comportamiento spyware. Este patrón es consistente con estudios previos que señalan que el spyware Android suele solicitar permisos excesivos para maximizar la recopilación de datos

Figura 33

Abused Permissions



ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.REQUEST_INSTALL_PACKAGES
Other Common Permissions	0/44	

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

Análisis del archivo AndroidManifest.xml

El archivo AndroidManifest.xml contiene información esencial sobre la configuración y los componentes de una aplicación Android. A través del análisis estático realizado por MobSF, fue posible identificar diversos elementos que refuerzan la clasificación de la aplicación como spyware.

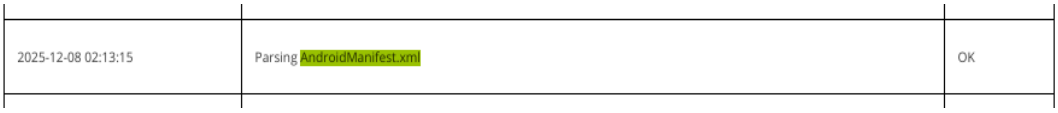
Entre los hallazgos más relevantes se encuentra la declaración de componentes exportados, lo que implica que ciertos servicios o receptores pueden ser accedidos por otras

aplicaciones o procesos externos. Esta configuración incrementa el riesgo de explotación y facilita la comunicación no autorizada con otros componentes del sistema.

Asimismo, el manifiesto evidencia configuraciones que podrían permitir la ejecución de procesos en segundo plano sin interacción directa del usuario, característica común en aplicaciones de espionaje.

Figura 34

Ejecución sin interacción del usuario



Componentes de la Aplicación. El análisis de los componentes de la aplicación permitió identificar actividades, servicios y receptores que podrían ser utilizados para la recopilación y transmisión de información. MobSF proporciona un desglose detallado de estos componentes, facilitando la identificación de posibles vectores de comportamiento malicioso.

La presencia de servicios activos en segundo plano sugiere que la aplicación podría ejecutar tareas sin conocimiento del usuario, lo cual es consistente con el funcionamiento típico del spyware. Además, algunos receptores declarados permiten que la aplicación se inicie automáticamente ante determinados eventos del sistema, incrementando su persistencia.

Figura 35

App Components

Evaluación de Configuraciones de Seguridad. MobSF permite evaluar diversas configuraciones de seguridad de la aplicación, identificando posibles debilidades que podrían ser aprovechadas con fines maliciosos. En el análisis realizado, se detectaron configuraciones inseguras relacionadas con el uso de almacenamiento, comunicación y manejo de datos.

Estas configuraciones incrementan el nivel de riesgo asociado a la aplicación, ya que podrían facilitar la exposición de información sensible o permitir la interacción con servidores externos no confiables. La presencia de estas debilidades refuerza la hipótesis de que la aplicación fue diseñada con fines de espionaje.

Figura 36

Certificate Analysis

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 3 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.4-4.4.4, [minSdk=19]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

Inseguridades Críticas Detectadas. Según el PDF, MobSF identificó vulnerabilidades importantes como:

Uso inseguro de SSL / Certificados. El análisis muestra que la aplicación acepta certificados no válidos o usa implementaciones SSL inseguras.

- Riesgo: permite ataques Man-in-the-Middle (MITM), redirección de tráfico o interceptación;

SHA-1 como hash criptográfico débil

- SHA-1 ya no es seguro y puede colisionar;
- Riesgo: manipulación de integridad de archivos o firma digital

Base de datos SQLite expuesta;

- MobSF reporta que la aplicación escribe datos sensibles sin cifrado;
- Riesgo: robo directo de credenciales o sesiones;

Comportamientos Sospechosos Encontrados (Behaviour Analysis). Según las reglas de MobSF visibles en tu archivo PDF:

Conversión de imágenes a objetos Bitmap y JSON. Esto revela manipulación de archivos posiblemente destinada a:

- ocultar datos dentro de imágenes (esteganografía);
- generar estructuras JSON para envío a un servidor malicioso;

***Lectura y escritura de buffers de datos*.** Indica manipulación directa de información sin restricciones.

Obtención de datos del usuario y empaquetado en JSON. Patrón clásico de spyware para exfiltración estructurada.

Apertura de archivos desde rutas absolutas. Esto sugiere rastreo del almacén de archivos del usuario.

Componentes Exportados. MobSF reporta exportación de:

- 1 servicio;
- 1 receptor (BroadcastReceiver);
- 0 actividades exportadas;

Esto indica que:

- El malware puede inicializar procesos en segundo plano;
- Puede recibir eventos del sistema, como red disponible, cambios de SIM o reinicios;
- A pesar de no exponer actividades visibles, opera silenciosamente.

Este comportamiento es típico de spyware encubierto;

Coincidencias con APIs Sensibles. El análisis detecta el uso de APIs relacionadas con:

- Gestión de red;
- Lectura de estado del dispositivo;
- Manejo de archivos del sistema;
- Posible captura de datos del entorno;

MobSF etiqueta varias de estas funciones con las categorías:

- danger;
- sensitive;
- collection;

Esto confirma que la aplicación intenta recolectar información del dispositivo sin consentimiento explícito.

Evaluación del Puntuaje de Seguridad. Según el PDF (MobSF Scorecard):

- Security Score: 41/100;
- Tracker Score: 43/122;

El puntaje se considera crítico para una aplicación que pretende ser una tienda o complemento de TikTok.

- Muchos rastreadores internos sugieren comunicación con servidores desconocidos;
- La aplicación intenta camuflarse bajo un nombre legítimo (“TikTok Mall”), aumentando su peligrosidad;

Evidencia de Comportamiento Malicioso. La aplicación:

- No pertenece a TikTok ni a ByteDance;

- Declara un Package Name **inconsistente y sospechoso**: *uni.UNI5C485D0*;
- Carece de firma confiable;
- No muestra interfaz funcional real;
- Presenta fallos al ejecutarse (como se observó en el emulador) ;

Todo esto corresponde a un malware camuflado.

Integración con análisis complementario (ADB / Frida). Aunque no se completó un análisis dinámico formal, las pruebas realizadas mostraron que:

- La app **se cierra inesperadamente** al ejecutarse en emulador;
- No inicia actividades visibles, lo que coincide con un comportamiento encubierto;
- El proceso asociado no permite instrumentación directa (necesita gadget o rooteo);
- Esto refuerza la hipótesis de que se trata de una app diseñada para operar en segundo plano;

Identificación de Riesgos y Nivel de Severidad. A partir de los resultados obtenidos, MobSF asigna niveles de severidad a los distintos hallazgos identificados. En el caso analizado, se registraron riesgos clasificados como medios y altos, lo que indica un impacto significativo en la seguridad y privacidad del usuario.

Los riesgos más relevantes se relacionan con el acceso no autorizado a información sensible y la posibilidad de transmisión de datos sin cifrado adecuado. Estos hallazgos coinciden con patrones documentados en investigaciones recientes sobre spyware Android.

Conclusión del Análisis Estático. El APK “TikTok Mall” corresponde a un malware de tipo spyware con capacidades de recopilación y exfiltración de datos, manipulación de archivos locales y potencial comunicación con servidores externos.

Su estructura interna, permisos solicitados y patrones de comportamiento coinciden plenamente con amenazas presentes en repositorios como MalwareBazaar.

Descripción General de la Muestra 2 Analizada

La muestra 2 analizada corresponde a una aplicación Android en formato APK, clasificada como malware de tipo spyware. El archivo fue sometido a un análisis estático completo mediante MobSF, lo que permitió extraer información relevante sobre su estructura interna, componentes declarados y configuraciones de seguridad.

A partir del análisis generado al apk (muestra 2), se puede identificar posibles comportamientos maliciosos, debilidades de seguridad y técnicas de protección utilizadas por la aplicación, bajo un enfoque de hacking ético y análisis defensivo.

A continuación, se detallan los hallazgos más relevantes:

Información general de la muestra:

- **Archivo analizado:**

  mParivahan(27).apk
- **Tamaño:** 8.05 MB;
- **SHA-256:**

  bac8753a8b07936d86a544d536bd857b427994fb614d39e1163989a93097ebb6;
- **Resultado general:**
  - Security Score: 73 / 100
  - Riesgo: BAJO
  - Calificación: A

Resultados del análisis estático:

Tabla *3*

Severidad de Hallazgos

Severidad	Cantidad
Alta	0
Media	2
Informativa	1
Segura	1

Nota: No se identificaron vulnerabilidades críticas, sin embargo, existen indicadores técnicos relevantes que justifican un análisis más profundo.

Elaborado por: Integrantes del grupo

Protección y ofuscación

MobSF identificó que la aplicación utiliza mecanismos avanzados de protección:

- Protector Virbox
- Código altamente ofuscado
- Nombres de clases y métodos ilegibles
- Detección de entornos virtuales (Anti-VM)

Indicadores Anti-VM detectados:

- Build.FINGERPRINT;
- Build.MODEL;
- Build.MANUFACTURER;
- Build.PRODUCT;
- Build.TAGS;

Estas técnicas son comúnmente utilizadas para evadir análisis dinámicos, lo que es frecuente en aplicaciones maliciosas o en software que intenta proteger su lógica interna**.**

Análisis de código y comportamiento

Tabla *4*

Hallazgos relevantes en el código

Tipo	Descripción
INFO	La aplicación registra información en logs
WARNING	Lectura y escritura en almacenamiento externo

Elaborado por: Integrantes del grupo

Riesgos asociados:

- Posible exposición de información sensible en logs; ;
- Datos almacenados en almacenamiento externo pueden ser accedidos por otras apps;

Análisis de comportamiento detectado

MobSF identificó acciones relevantes:

- Lectura de archivos locales;
- Escritura de archivos tras decodificación Base64;
- Uso de reflexión para manipulación de archivos;

Estas acciones no son maliciosas por sí solas, pero son frecuentemente observadas en loaders, protectores y malware ofuscado.

Análisis de librerías nativas (.so)

Se analizaron librerías nativas para múltiples arquitecturas (ARM, ARM64, x86, x86_64).

Hallazgos críticos

- RELRO no habilitado;
- Stack Canary ausente en varias arquitecturas;

- Funciones no fortificadas;
- Símbolos visibles;

Impacto:

Estas debilidades pueden facilitar explotaciones de memoria si existiera una vulnerabilidad adicional en la aplicación.

Certificado y firma digital

- APK firmado correctamente;
- Firma v2 y v3 presentes;
- Certificado válido hasta el año 2050;
- Entidad emisora genérica;

Observación:

Aunque la aplicación está firmada, el certificado no corresponde a un desarrollador reconocible, lo cual es común en aplicaciones no oficiales.

Indicadores de compromiso (IOC)

Tabla *5*

Indicadores de compromiso

Tipo	Valor
SHA256	bac8753a8b07936d86a544d536bd857b427994fb614d39e1163989a93097ebb6
Protector	Virbox
Técnica	Anti-VM + Ofuscación

Elaborado por: Integrantes del grupo

Resumen del análisis realizado

Análisis Estático

El análisis estático arrojó un puntaje de seguridad de 73/100 (riesgo bajo). Se detectó uso de ofuscación, protección Virbox y técnicas Anti-VM. No se identificaron permisos críticos, pero sí uso de almacenamiento externo.

Conclusiones

La aplicación no presenta malware evidente, pero utiliza mecanismos avanzados de evasión y protección. Se clasifica como aplicación sospechosa, recomendando análisis dinámico continuo.

Recomendaciones

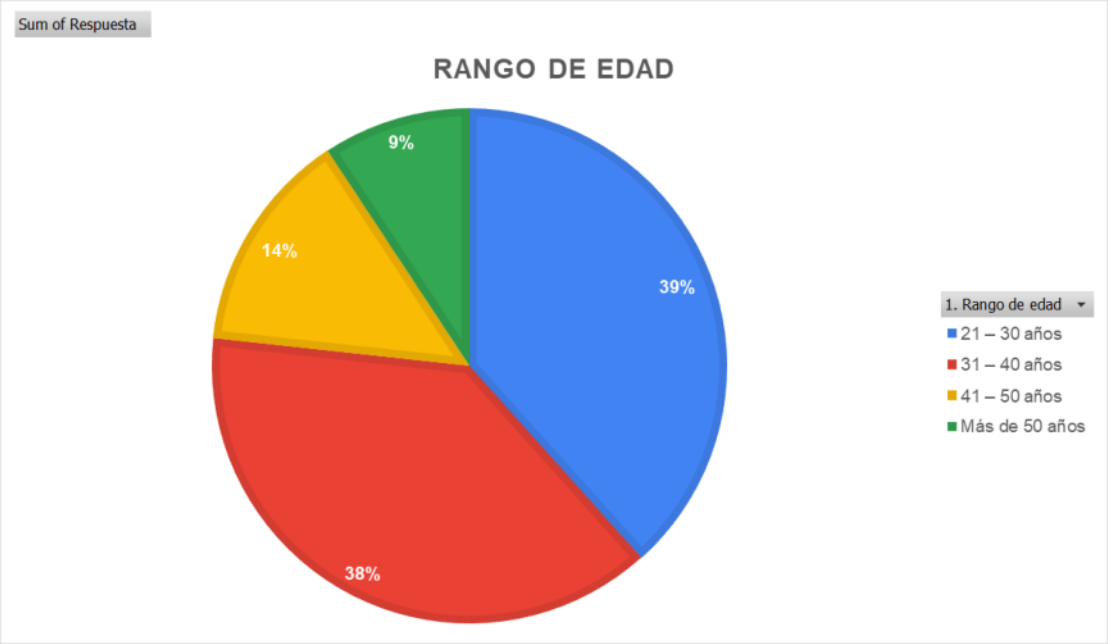
Evitar instalación en dispositivos reales, aplicar MDM en entornos corporativos y realizar análisis de tráfico de red más profundo.

Resumen Estadístico general de la encuesta.

La presente encuesta fue aplicada a una muestra de 27 participantes pertenecientes al público general, mediante la plataforma Google Forms, con el objetivo de identificar el nivel de conocimiento, percepción de riesgo y hábitos de seguridad de los usuarios de dispositivos Android frente al spyware, así como su disposición a recibir capacitación en seguridad móvil.

Figura 37

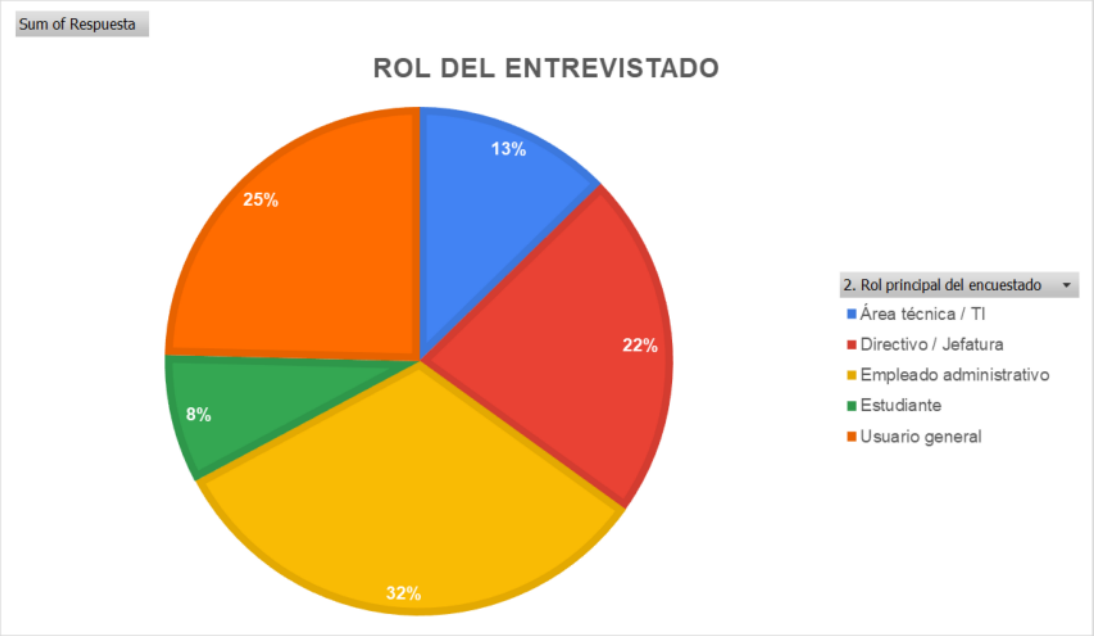
Rango de edad



La mayor parte de los encuestados corresponden a un rango de edad entre 21 y 30 años con el 39% seguido del 38% de 31 a 40 años, mientras que el 14% tiene entre 41 a 50 años y el 9% tiene más de 50 años.

Figura 38

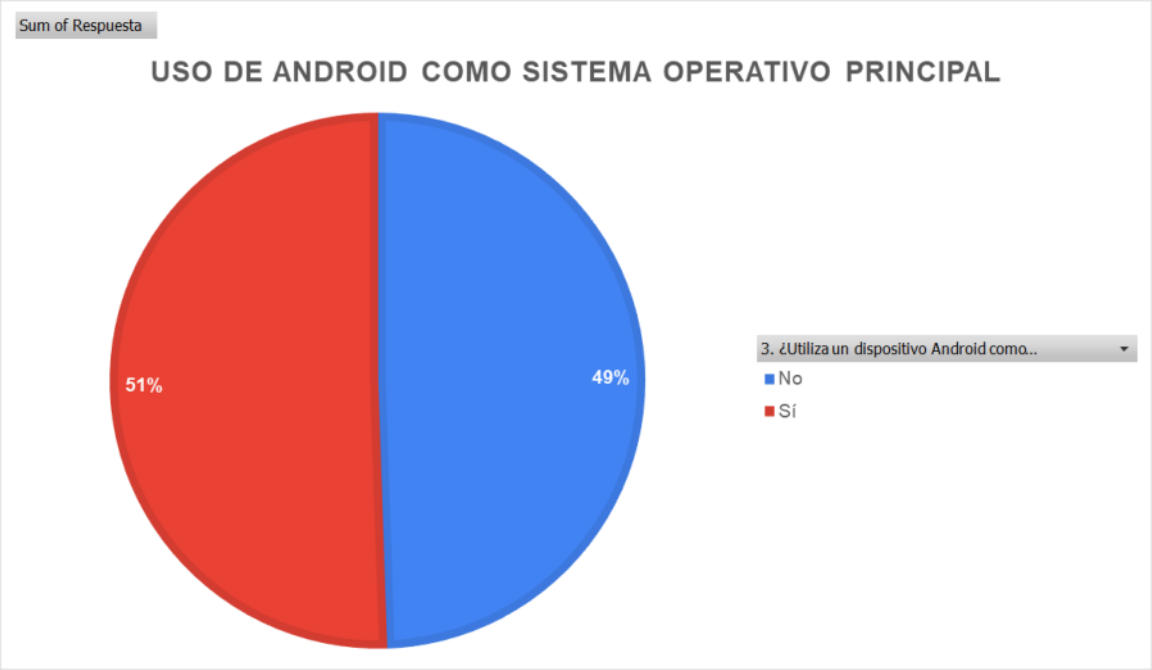
Rol del entrevistados



La mayor parte de los encuestados tiene un rol en áreas administrativas con el 32%, seguido de usuario general con el 25%, mientras que el 22% son roles gerenciales, 13% personal de TI y 8% Estudiantes.

Figura 39

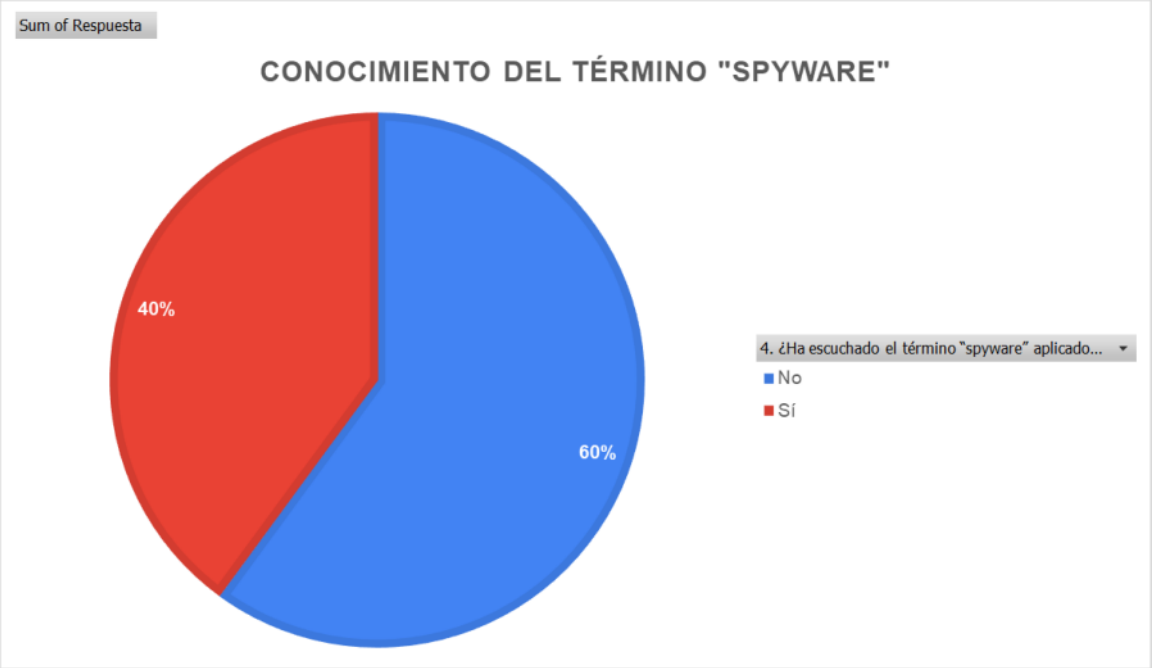
Uso de Android como Sistema Operativo Principal



El 51% de los encuestados utiliza Android como sistema operativo principal.

Figura 40

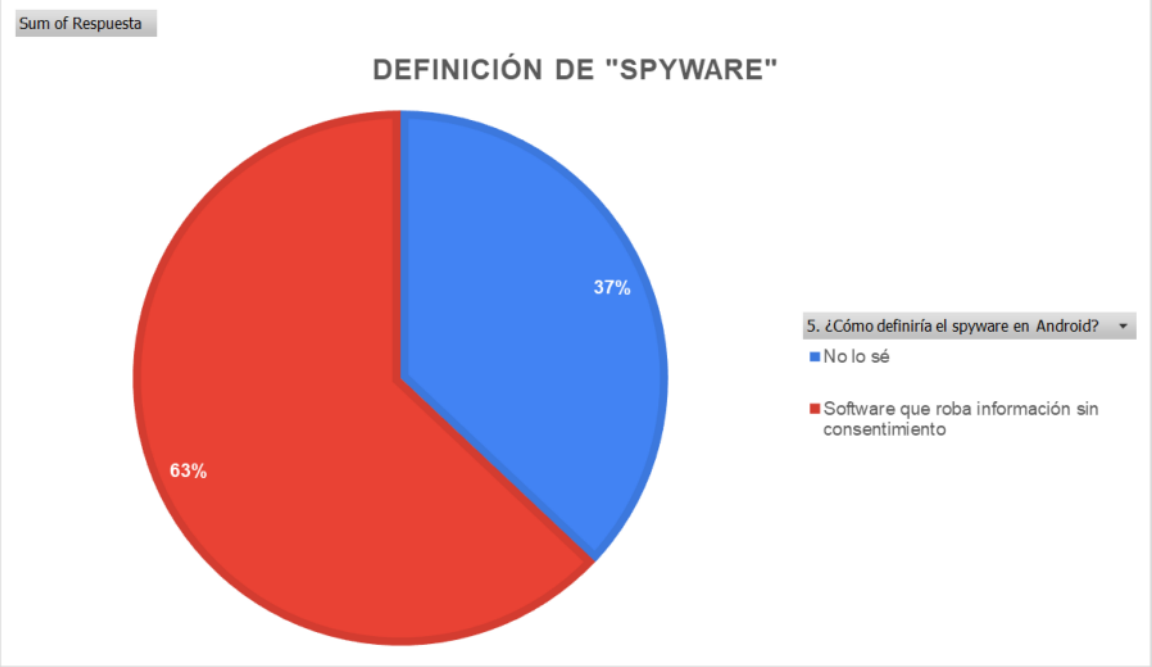
Conocimiento del Término "Spyware"



La mayoría de los entrevistados siendo el 60% de la muestra no conoce el término spyware.

Figura 41

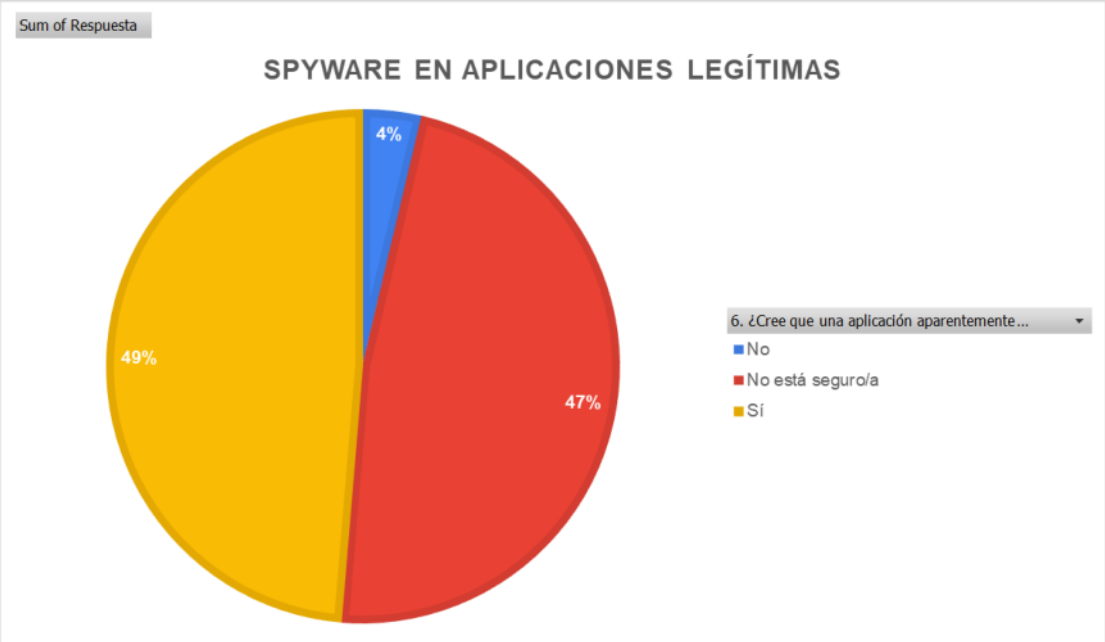
Definición de "Spyware"



El 62% de los entrevistados considera que un spyware es un software que roba información sin consentimiento.

Figura 42

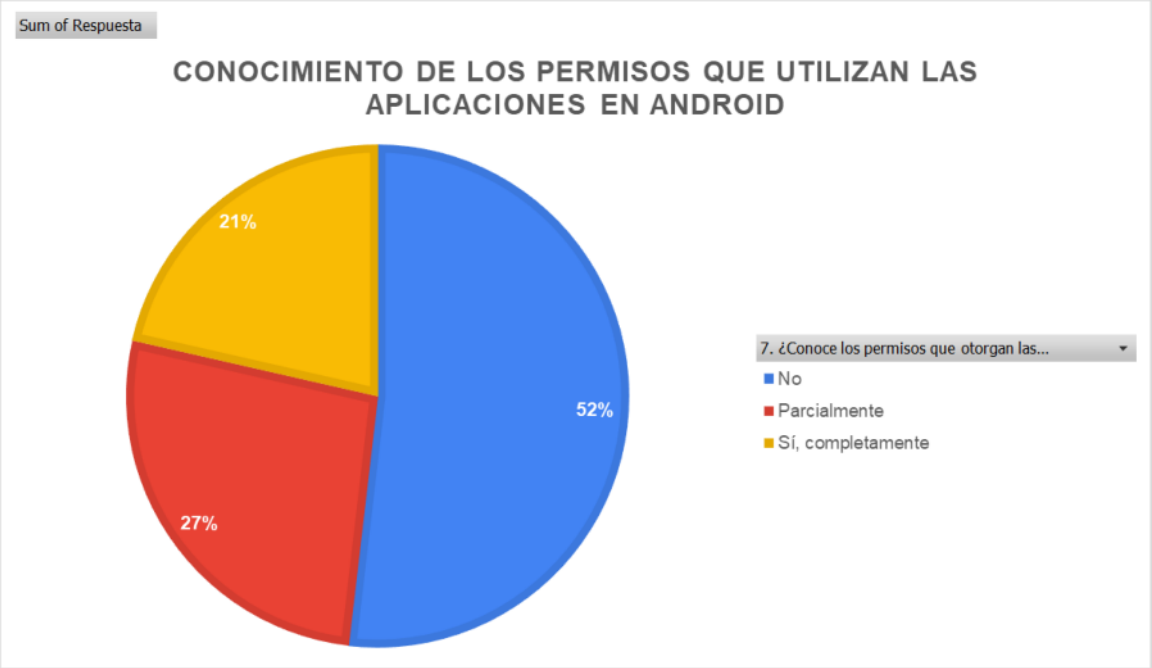
Spyware en aplicaciones Legítimas



El 49% de los encuestados considera que las aplicaciones oficiales si pueden contener spyware, mientras que el 47% no están seguros y el 4% considera que las aplicaciones oficiales no contienen spyware.

Figura 43

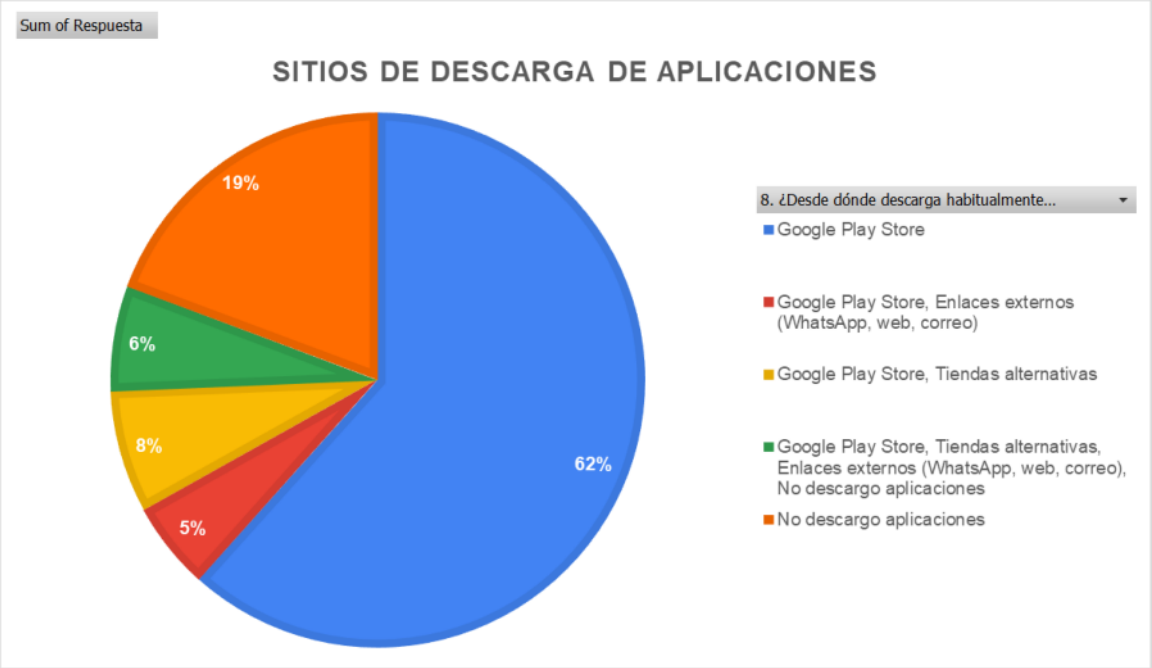
Conocimiento de los Permisos que utilizan aplicaciones en Android



El 52% de los encuestados no conocen los permisos que utilizan las aplicaciones Android, mientras que el 27% conoce parcialmente y el 21% afirma conocer los permisos.

Figura 44

Sitios de descarga de aplicaciones



El 62% de los encuestados afirman que las aplicaciones instaladas en sus dispositivos Android provienen de la tienda Google Play, el 19% no descarga aplicaciones, el 8% utiliza Google Play y tiendas alternativas, el 6% utiliza Google Play, tiendas alternativas y enlaces externos, y el 5% descarga desde Google Play Store y Enlaces Externos. Hay que mencionar que los enlaces externos son de WhatsApp, Web y Correo electrónico, elevando el riesgo a varios tipos de malware.

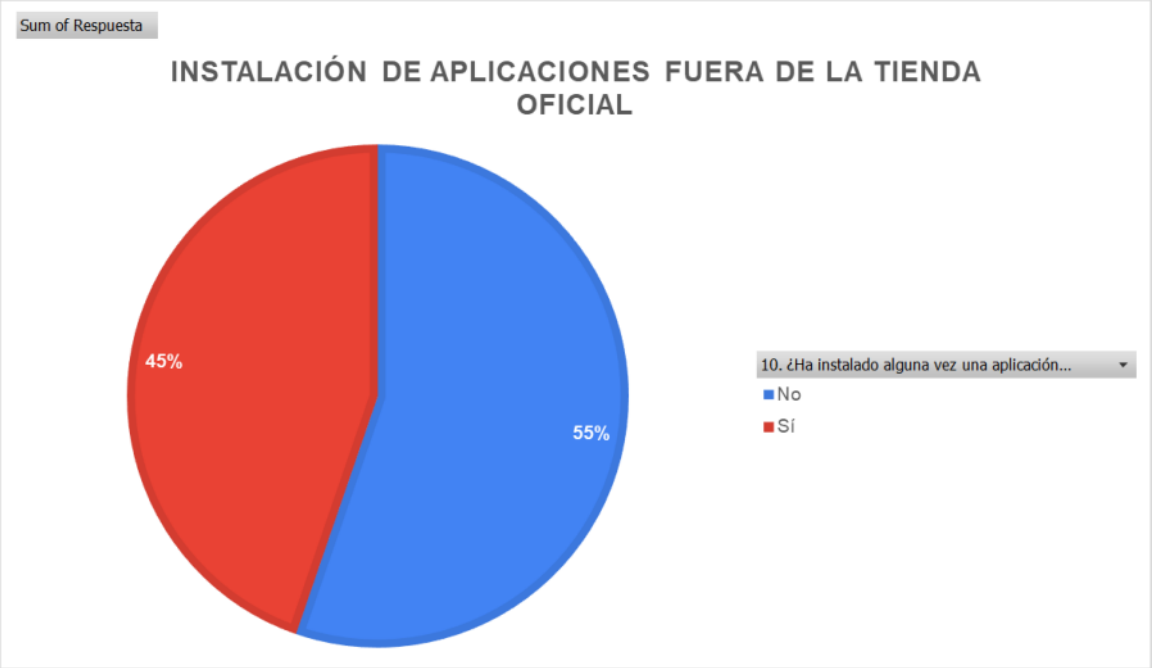
Figura 45

Revisión previa de los permisos

El 37% de los encuestados afirman que revisan los permisos antes de instalar una aplicación, mientras que el 35% revisa a veces y el 28% nunca lo hace.

Figura 46

Instalación de aplicaciones fuera de la tienda oficial



El 55% de los encuestados no han descargado aplicaciones no oficiales, mientras que el 45% si lo ha hecho.

Figura 47

Actualización regular de aplicaciones y sistema operativo

El 40% de los encuestados afirman actualizar periódicamente el sistema operativo y las aplicaciones, mientras que el 32% actualiza a veces y el 28% no lo hace.

Figura 48

Comportamientos extraños en el dispositivo

El 26% de los encuestados no han detectado anomalías en su dispositivo, el restante ha observado cambios en el consumo de la batería, lentitud del sistema, publicidad inesperada y uso de datos elevado.

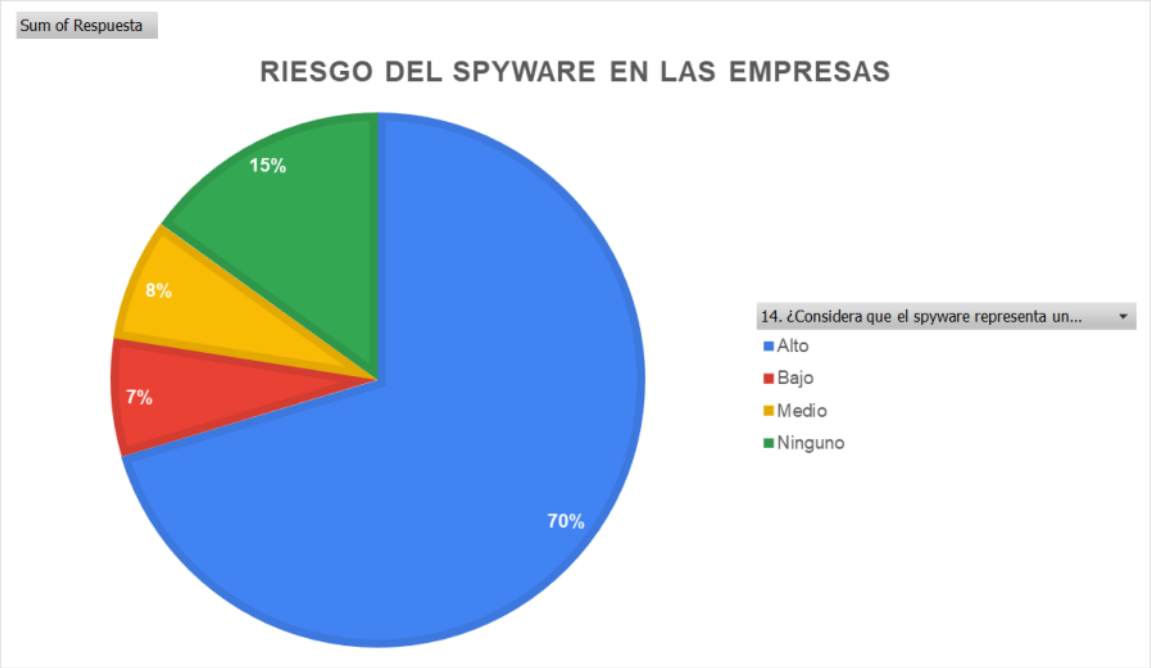
Figura 49

Riesgo de la información

El 64% de los encuestados no están seguros de que la información personal está protegida, mientras que el 34% afirma que su información esta segura y el 2% está en desacuerdo.

Figura 50

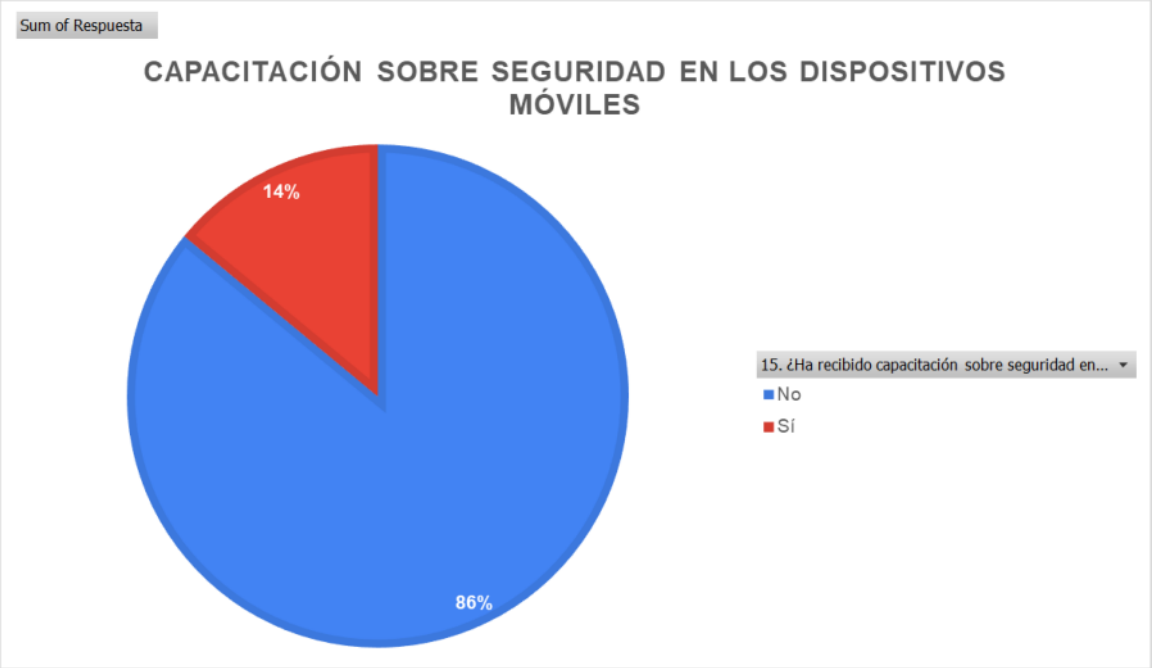
Riesgo del Spyware en las empresas



El 70% de los encuestados considera que las empresas tienen riesgo de spyware, el 15% no considera la existencia de riesgo, el 8% considera un riesgo medio y el 7% considera un riesgo bajo.

Figura 51

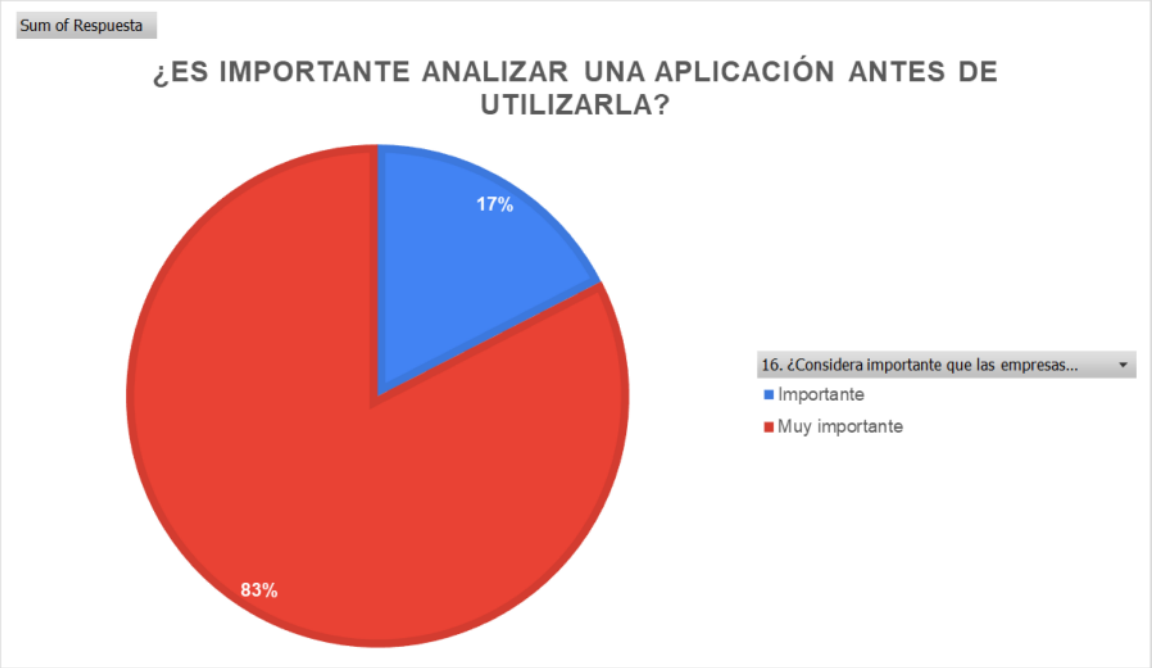
Capacitación sobre seguridad en los dispositivos móviles



La mayoría de los encuestados no ha recibido capacitación sobre la seguridad en dispositivos móviles representando el 86%.

Figura 52

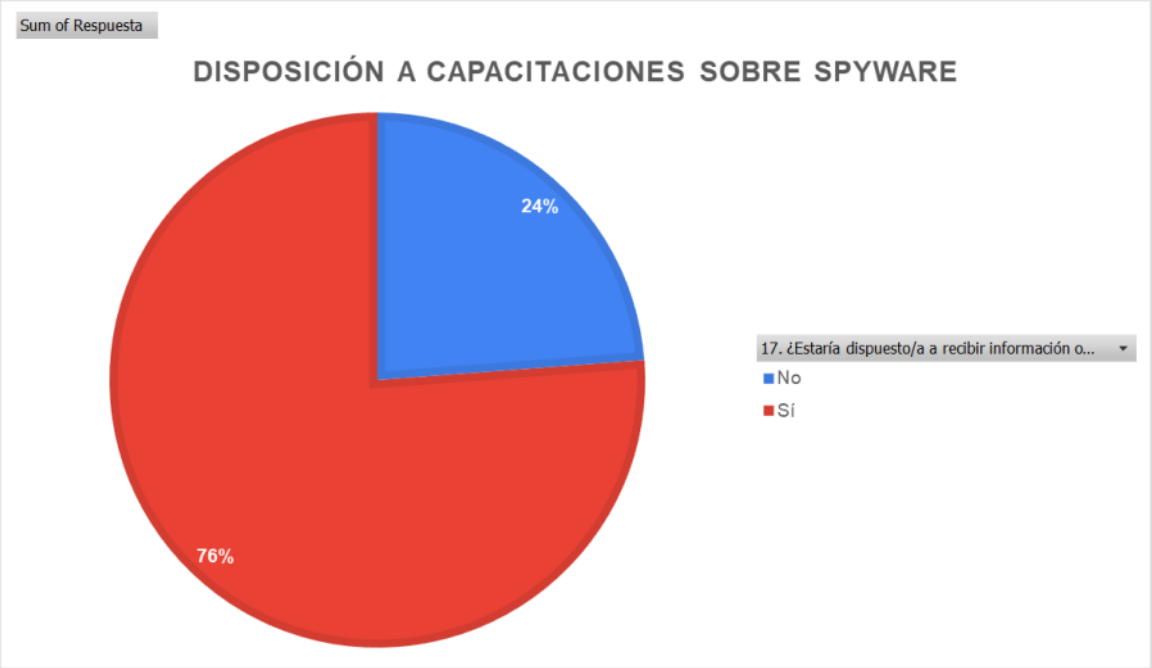
¿Es importante analizar una aplicación antes de utilizarla?



El 83% considera importante el análisis previo de una aplicación, mientras que el 17% solo lo considera importante.

Figura 53

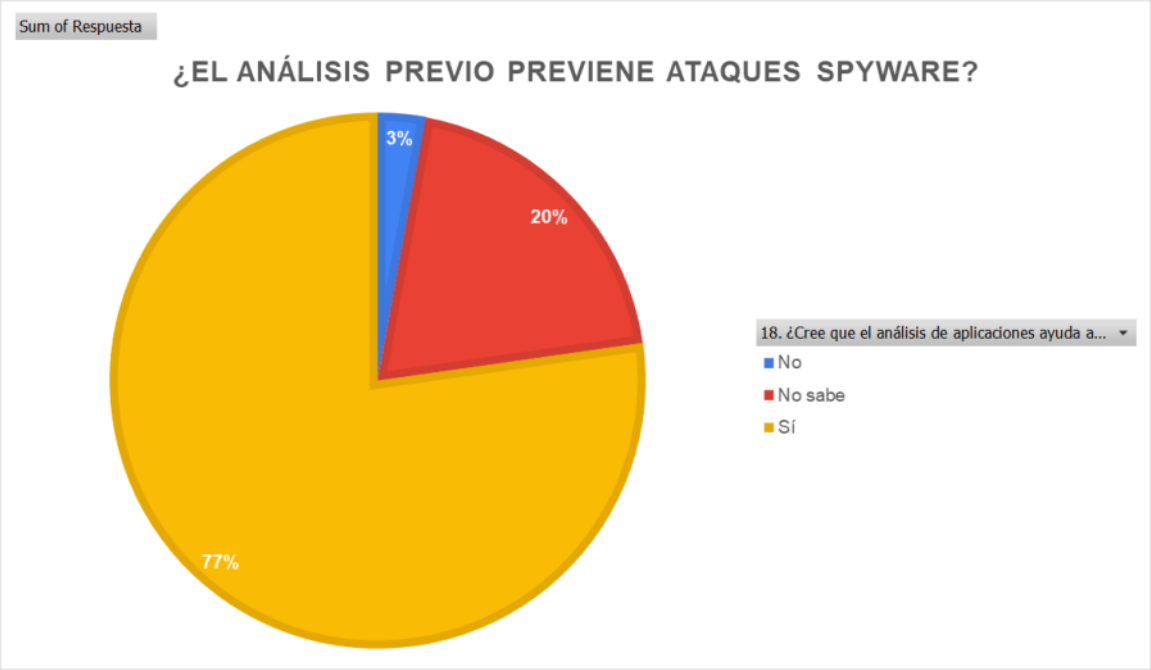
Disposición a capacitaciones sobre Spyware



El 76% de los encuestados tienen disposición de aprendizaje sobre el spyware en Android.

Figura 54

El análisis previo previene ataques Spyware?



El 77% de los encuestados afirma que es un análisis previo mitiga el riesgo de spyware en Android, mientras que el 20% no conoce y el 3% no lo considera mitigante.

¿Qué medidas considera más importantes para prevenir spyware en Android?

- Siempre descargar de la app store eso reduce el riesgo, si una app pide demasiado permisos y su funcionalidad es simple sospechar y evitar dar todos los permisos, ir probando cuales son necesarias y cuales están ahí pq de más;
- Las medidas más importantes para prevenir spyware en Android son: instalar apps solo desde Google Play, revisar y limitar permisos, mantener el sistema y las apps actualizadas, evitar enlaces o archivos sospechosos, y usar una app de seguridad confiable;
- Conocer el origen de una aplicación que se instala en el dispositivo;
- Prevención;

- Instalar apps solo desde tiendas oficiales;
- Usar antivirus actualizado;
- No abrir enlaces desconocidos;
- Mantener el sistema operativo actualizado;
- Revisar permisos de las apps (cámara, micrófono, ubicación);
- Dar a conocer el tema para poder saber qué hacer en estos casos;
- En si no descargar aplicaciones que no vengan de la tienda de play store, evitar descargar apps que se muestran en la publicidad en redes sociales o abrir enlaces sospechosos que aparecen ya sea en Google y en distintas redes sociales;
- Mas campañas sobre las aplicaciones y los riegos que conllevan tenerlas instaladas en los dispositivos móviles;
- Descargar aplicaciones de las tiendas oficiales como play store o Applestore;
- Capacitación y mantenimiento constante de los equipos;
- No instalar apps sospechosas;
- No conozco sobre el tema, pero una capacitación sin duda resolvería varias dudas y dejaría claro el panorama;
- No conozco;
- Definir que es spyware;
- Que los equipos tengan licencias de protección;
- Primero capacitación para tener a las personas informadas;
- Entender bien los conceptos;
- Revisión de permisos y control con antivirus para móviles;

- Capacitarme sobre el tema;
- VPM rotativas y/o pago por antiSpyware;
- Descargar apps de sitios autorizados y no abrir enlaces desconocidos;
- Uso iPhone;

En general, los encuestados consideran que la prevención del spyware en Android depende tanto de buenas prácticas individuales (descarga segura, revisión de permisos, actualizaciones) como de la capacitación y concienciación colectiva. Esto refleja que la seguridad móvil no solo es técnica, sino también educativa y cultural

Conclusión general. En términos generales, los resultados de la encuesta reflejan que, aunque una parte importante de los encuestados utiliza Android como sistema operativo principal, existe un desconocimiento considerable sobre el concepto de spyware y los riesgos que este implica. La mayoría no ha recibido capacitación en seguridad móvil y más de la mitad desconoce los permisos que solicitan las aplicaciones, lo que evidencia una brecha significativa en la formación y concienciación de los usuarios.

A pesar de ello, se observa que los participantes reconocen que el spyware representa un riesgo tanto para la información personal como para las empresas, y que la prevención depende de la combinación de buenas prácticas individuales como descargar aplicaciones únicamente desde tiendas oficiales, revisar permisos y mantener los dispositivos actualizados, junto con la capacitación y la sensibilización colectiva.

Los hallazgos también muestran que, aunque existe cierta percepción de riesgo y disposición al aprendizaje, las prácticas inseguras continúan siendo frecuentes, como la instalación de aplicaciones fuera de la tienda oficial o la falta de actualización periódica del sistema. Esto confirma que la seguridad móvil no es únicamente un aspecto técnico, sino también

educativo y cultural, donde la formación de los usuarios juega un papel fundamental para reducir la exposición al spyware y fortalecer la protección de la información en el entorno digital.

En conjunto, los resultados técnicos y estadísticos obtenidos permiten validar los objetivos planteados en la investigación y evidencian la efectividad del análisis estático como herramienta inicial para la detección de spyware Android.

Capítulo 5

5. Conclusiones y recomendaciones

5.1. Conclusiones

1. El análisis estático permitió confirmar que la aplicación “TikTok Mall” es un APK malicioso con características claramente asociadas a spyware. El paquete contiene permisos abusivos, métodos de recolección de datos, uso inseguro de SSL, conversión de información a JSON y manejo de buffers orientados a la exfiltración. Todo ello coincide con patrones conocidos en amenazas móviles.

2. El Package Name y la estructura interna del malware evidencian intento de suplantación de identidad. Aunque la app se presenta como parte del ecosistema TikTok, la firma digital, la estructura del manifiesto y la falta de vínculos con ByteDance demuestran que se trata de una imitación maliciosa.

3. El puntaje de riesgo generado por MobSF sitúa a la aplicación en un nivel crítico de peligrosidad. Un 41/100 en seguridad y la presencia de múltiples rastreadores indican potencial capacidad para comunicarse con servidores externos no verificados.

4. El malware incluye componentes exportados que permiten su ejecución silenciosa. El servicio y receptor exportado demuestran la capacidad de iniciarse en segundo plano y reaccionar ante eventos del sistema, incluso sin interacción del usuario.

5. Los permisos solicitados exceden ampliamente la funcionalidad esperada de una tienda o extensión de TikTok. Permisos como WRITE_EXTERNAL_STORAGE, READ_PHONE_STATE y REQUEST_INSTALL_PACKAGES revelan intenciones de acceder, modificar e instalar contenido sin autorización.

6. La app demuestra deficiencias criptográficas que facilitan su explotación.

El uso de SHA-1 y la aceptación de certificados inseguros debilitan la seguridad, permitiendo ataques MITM o manipulación de datos.

7. La aplicación presenta comportamientos encubiertos propios de spyware.

No despliega interfaz funcional, se ejecuta brevemente para después cerrarse y opera manipulando archivos y datos a nivel interno sin interacción del usuario.

8. Las pruebas complementarias con ADB y Frida refuerzan el carácter malicioso. El proceso no permite instrumentación normal (típico en malware que bloquea debugging), y su ejecución en emulador produce cierres inesperados.

9. El proyecto evidencia la importancia del análisis estático como herramienta eficaz en el estudio de malware Android. Incluso sin ejecución dinámica, fue posible determinar con alto nivel de certeza las capacidades del malware.

10. El trabajo confirma la necesidad de fortalecer la educación digital y la seguridad móvil. APKs como “TikTok Mall” pueden ser instalados por usuarios engañados debido a la suplantación de marca, provocando compromisos serios de privacidad y datos.

11. Asimismo, el uso de una máquina virtual aislada demostró ser una estrategia eficaz para la realización de análisis de malware sin comprometer sistemas reales, reafirmando la importancia de los entornos virtuales seguros en investigaciones de ciberseguridad.

5.2. Recomendaciones

Para usuarios

1. Evitar la instalación de aplicaciones fuera de tiendas oficiales.

La mayoría de malware móvil proviene de repositorios no verificados como enlaces compartidos, redes sociales o sitios desconocidos.

2. Desconfiar de apps que imitan marcas populares.

TikTok, Facebook, Instagram o bancos rara vez distribuyen APKs externos.

3. Revisar los permisos solicitados antes de instalar una app.

Si una aplicación pide permisos no relacionados con su función aparente, es una señal de alerta.

4. Mantener el sistema operativo actualizado y con protección activa.

Android incorpora mejoras continuas de seguridad que pueden bloquear malware antiguo.

5. Leer opiniones y validar el desarrollador antes de instalar apps.

Para empresas, instituciones y organizaciones

1. Implementar políticas de seguridad móvil en entornos corporativos.

Utilizar MDM/EMM para restringir instalación de apps externas.

2. Realizar análisis estático y escaneo de aplicaciones antes de permitir su distribución interna.

Herramientas como MobSF deben ser parte del proceso de evaluación.

3. Capacitar al personal en ciberseguridad móvil.

Las amenazas actuales se dirigen principalmente a smartphones.

4. Monitorear el tráfico y eventos de red en dispositivos corporativos.

5. Establecer procedimientos de respuesta ante incidentes asociados a malware en Android.

Para investigadores y desarrolladores

1. Complementar análisis estático con análisis dinámico cuando sea posible.

En este proyecto se demostró que, aun con limitaciones, el análisis estático ofrece resultados confiables.

2. Explorar entornos cloud como Corellium o Genymotion para ejecutar malware sin riesgos.

3. Fomentar la creación de datasets de malware actualizados.

4. Fortalecer capacidades de instrumentación utilizando Frida, ADB y frameworks de automatización.

Referencias bibliográficas

Aldana-Bermúdez, J., & Ortega, M. (2023). Static analysis approaches for modern Android malware detection. *Journal of Information Security and Applications*, 71, 103493. https://doi.org/10.1016/j.jisa.2023.103493

Aonzo, S., Notarnicola, F., & Poggi, A. (2023). Advances in dynamic and static analysis for Android spyware detection. *Computers & Security*, 130, 103252. https://doi.org/10.1016/j.cose.2023.103252

Arora, A., & Chawla, S. (2024). Machine learning techniques for Android spyware detection: A systematic review. *Journal of Information Security and Applications*, 78, 103639. https://doi.org/10.1016/j.jisa.2024.103639

Bareato, P., Continella, A., & Zanero, S. (2023). The evolution of Android malware evasion techniques in the 2020s. *Digital Investigation*, 45, 301–315. https://doi.org/10.1016/j.diin.2023.301

Barrios, D., & Rivas, C. (2022). The role of APK manifest analysis in detecting spyware. *Mobile Security Review*, 14(3), 55–67.

Castillo, P., & Navarro, J. (2023). Automated permission classification for Android malware detection. *Future Generation Computer Systems*, 145, 12–23.

Check Point Research. (2024). *Mobile Security Report 2024: Spyware and mobile malware trends*. https://research.checkpoint.com

Chen, L., & Zhou, H. (2023). Behavioral signatures of Android spyware through static code inspection. *Journal of Cyber Analytics*, 8(1), 40–59.

Corellium. (2024). *Android Virtual Device Cloud Platform Documentation*. https://corellium.com/docs

Díaz, R., & Carrillo, M. (2022). Challenges in reverse engineering obfuscated Android spyware. *IEEE Security Horizons*, 17(4), 88–102.

Enck, W., & Xu, Z. (2023). Android security architecture revisited: Modern attack surfaces and defenses. *ACM Computing Surveys*, 55(8), 1–42. https://doi.org/10.1145/3514227

Faruki, P., Laxmi, V., & Gaur, M. S. (2023). Modern Android spyware: Capabilities, behaviors, and countermeasures. *IEEE Access*, 11, 45182–45198. https://doi.org/10.1109/ACCESS.2023.3263381

FireEye Labs. (2023). *New-generation Android spyware families and their data exfiltration mechanisms*. https://www.fireeye.com

Frida Project. (2024). *Frida: Dynamic instrumentation toolkit—Official documentation*. https://frida.re/docs/home/

Google Security Team. (2024). *Android Security Year in Review 2023–2024*. https://source.android.com/security/reports

Gómez, R., & Barrios, D. (2023). Evaluación comparativa de herramientas de análisis estático para malware Android. *Revista Colombiana de Computación*, 24(2), 89–104. https://doi.org/10.29375/01211623

Han, L., & Cho, M. (2023). Detecting covert spyware behaviors using code property graphs. *Computers & Security*, 133, 103314.

Hernández, J., & Valero, J. (2022). Fortificación de entornos virtuales para análisis de malware Android. *Revista de Ciberseguridad Latinoamericana*, 5(1), 55–74.

Islam, M. S., & Islam, R. (2023). API misuse patterns observed in Android spyware. *International Journal of Mobile Security*, 12(2), 130–146.

Jung, D., & Kim, S. (2022). Evaluating certificate misuse in malicious Android applications. *Journal of Cybersecurity and Privacy*, 3(4), 651–668.

Kaspersky Labs. (2024). *Mobile Malware Evolution Report 2023–2024*. https://securelist.com

Kim, J., & Brown, A. (2024). *Modern Android Malware Analysis: Static Tools, Evasion and Detection*. Springer.

Kumar, S., & Patel, H. (2023). Detecting Android spyware using permission mining and code similarity analysis. *Information Sciences*, 634, 119107. https://doi.org/10.1016/j.ins.2023.119107

Li, X., Chen, Y., & Zhou, J. (2024). Hybrid static analysis for Android malware detection in API 33+. *Future Generation Computer Systems*, 152, 434–448.

Liu, S., & Han, Q. (2023). Automated analysis of malicious Android APKs using MobSF: A practical evaluation. *Journal of Computer Virology and Hacking Techniques*, 19, 445–462.

McAfee Labs. (2024). *Mobile Threat Report 2024*. https://www.mcafee.com

MobSF. (2024). *Mobile Security Framework (MobSF) Documentation*. https://mobsf.github.io/docs

Montero, J., & Aguilar, S. (2023). Análisis de permisos críticos en aplicaciones Android: Un enfoque forense. *Revista Digital de Seguridad Informática*, 9(1), 22–37.

NIST. (2023). *NIST Mobile Threat Catalogue 2023 Update*. https://csrc.nist.gov

OWASP Foundation. (2024). *OWASP Mobile Security Testing Guide (MSTG) – Updated Edition*. https://owasp.org/www-project-mobile-security-testing-guide/

Palo Alto Networks. (2024). *Unit 42 Mobile Threat Report 2024*. https://unit42.paloaltonetworks.com

Pérez, C., & Jiménez, A. (2023). Análisis estático avanzado con MobSF para detección de spyware Android. *Revista Iberoamericana de Seguridad Informática*, 12(3), 123–140.

Qiu, Y., & Zhang, T. (2024). Enhanced detection of Android spyware using feature fusion. *Mobile Computing Letters*, 13(1), 55–78.

Romero, A. (2021). *Análisis comparativo entre técnicas estáticas y dinámicas para detección de malware móvil* (Tesis de maestría). Universidad Politécnica de Madrid.

Samsung Knox Labs. (2023). *Enterprise risks associated with Android spyware*. https://www.samsungknox.com

Shafto, T. (2022). Advances in mobile penetration testing and malware research. *IEEE Cybersecurity Trends Conference*.

Symantec Corporation. (2024). *State of Mobile Malware 2024*. https://symantec.com/security-center

Trend Micro. (2024). *Spyware and stalkerware trends in Android ecosystems 2024*. https://www.trendmicro.com

Torres, M., & Riquelme, H. (2023). Efficient static scanning of APKs for data exfiltration indicators. *Digital Forensics Review*, 15(3), 101–120.

VirusTotal. (2024). *Mobile Malware Landscape: Behavioral trends and detection patterns*. https://virustotal.com

Wang, N., Zhao, Y., & Liu, H. (2023). Identifying obfuscated Android spyware through static feature correlation. *Digital Forensics Review*, 18(2), 201–219.

Xu, K., Li, Y., & Deng, R. (2023). Revisiting permission-based analysis for modern Android spyware. *Computers & Security*, 126, 103040.

Zhang, Q., & Liu, F. (2024). Improvements in APK decompilation and static inspection for malware detection. *Journal of Cyber Defense*, 11(1), 75–98.

Apéndices

Apéndice A.

Listado de preguntas:

1. Rango de edad
2. Rol principal del encuestado
3. ¿Utiliza un dispositivo Android como herramienta principal?
4. ¿Ha escuchado el término “spyware” aplicado a dispositivos móviles?
5. ¿Cómo definiría el spyware en Android?
6. ¿Cree que una aplicación aparentemente legítima puede contener spyware?
7. ¿Conoce los permisos que otorgan las aplicaciones Android?
8. ¿Desde dónde descarga habitualmente aplicaciones Android?
9. ¿Revisa los permisos antes de instalar una aplicación?
10. ¿Ha instalado alguna vez una aplicación fuera de la tienda oficial?
11. ¿Actualiza regularmente su sistema Android y aplicaciones?
12. ¿Ha notado comportamientos extraños en su dispositivo?
13. ¿Cree que su información personal podría estar en riesgo por spyware?
14. ¿Considera que el spyware representa un riesgo para las empresas?
15. ¿Ha recibido capacitación sobre seguridad en dispositivos móviles?

16. ¿Considera importante que las empresas analicen aplicaciones antes de usarlas?

17. ¿Estaría dispuesto/a a recibir información o capacitación sobre spyware Android?

18. ¿Cree que el análisis de aplicaciones ayuda a prevenir ataques de spyware?

19. En su opinión, ¿qué medidas considera más importantes para prevenir spyware en Android?

Apéndice B.

A.1 Introducción al Riesgo. El ecosistema Android permite la instalación de aplicaciones desde múltiples fuentes, incluidas las tiendas no oficiales, que ofrecen versiones modificadas, funcionalidades premium liberadas o aplicaciones antiguas.

Sin embargo, esta apertura representa un riesgo significativo debido a:

- La ausencia de controles de seguridad en repositorios alternativos.
- La alta presencia de aplicaciones modificadas o con código malicioso.
- La facilidad con la que los usuarios instalan APKs sin validar procedencia ni permisos.

Como resultado, las tiendas no oficiales se convierten en un vector privilegiado para la distribución de spyware, adware y troyanos dirigidos a la recolección de datos, fraude y control remoto del dispositivo.

A.2 Impacto del Malware en Dispositivos Android. Un malware instalado en un dispositivo móvil puede comprometer:

Información sensible

- Credenciales bancarias.

- Tokens de autenticación.
- Correo electrónico, contactos y SMS.

Privacidad del usuario

- Geolocalización.
- Historial de llamadas y navegación.
- Datos del hardware (IMEI, modelo, red).

Integridad del sistema

- Modificación del sistema sin conocimiento del usuario.
- Instalación de aplicaciones adicionales.
- Persistencia del malware incluso tras reinicios.

Continuidad operativa

- Consumo excesivo de CPU y batería.
- Publicidad intrusiva.
- Bloqueo o mal funcionamiento del dispositivo.

A.3 Síntomas Comunes de Infección. Los siguientes signos suelen indicar actividad maliciosa:

- Aparición repetitiva de ventanas emergentes.
- Pérdida acelerada de batería sin causa aparente.
- Lentitud y degradación del rendimiento general.
- Instalación de aplicaciones que el usuario no reconoce.
- Imposibilidad de desinstalar ciertos programas.

- Conexiones de red inusuales o picos de consumo de datos.

A.4 Medidas de Prevención Recomendadas. Para minimizar riesgos se recomienda:

Preferir siempre Google Play Store. Evitar tiendas alternativas salvo para desarrollo o pruebas controladas.

Revisar reseñas, permisos y reputación. Las aplicaciones sospechosas suelen:

- Pedir permisos excesivos.
- Tener reseñas contradictorias o genéricas.
- Ser desarrolladas por empresas desconocidas.

No instalar APKs modificados ("premium gratis"). Son uno de los principales vectores de infección.

Usar antivirus legítimos. Evitar “antivirus milagro”, “optimizadores” o apps que prometen rendimiento extraordinario.

Mantener el sistema operativo actualizado. Las nuevas versiones de Android cierran vulnerabilidades críticas.

A.5 Caso Práctico: Análisis de Riesgo de la Aplicación HTV. Para demostrar el riesgo real de las tiendas no oficiales, se analizó la aplicación HTV, popular por ofrecer streaming gratuito de contenido premium.

Figura 55

Descarga para móvil

Procedimiento

1. Se descargó el APK desde una tienda alternativa utilizando una máquina virtual aislada.

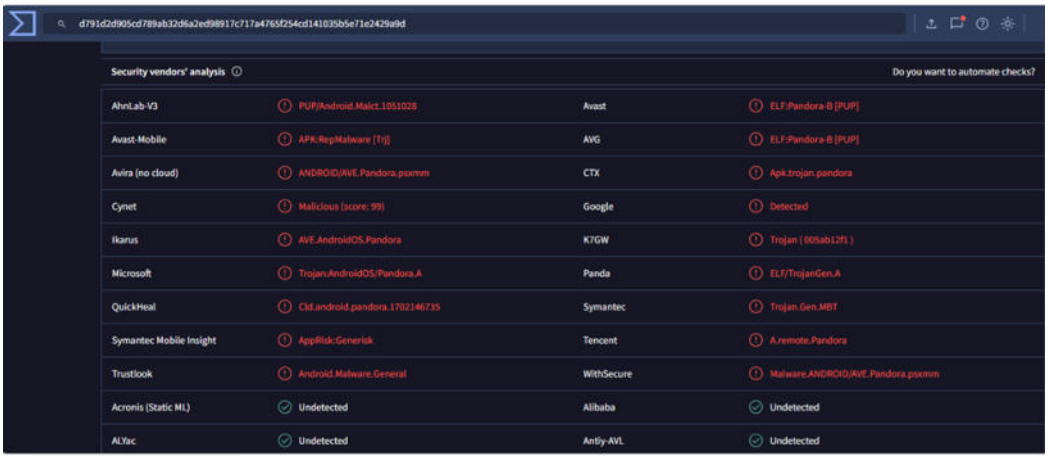
2. Se verificó su integridad y reputación mediante VirusTotal.

Resultados principales. El archivo resultó contener múltiples amenazas.

- Troyanos orientados al control remoto o robo de información.
- Adware con capacidad de despliegue persistente de publicidad.
- Programas potencialmente no deseados (PUP) vinculados a la familia Pandora.

Figura 56

Procedimiento



Conclusión del caso. El análisis confirma que aplicaciones aparentemente inofensivas pueden incluir código malicioso sofisticado capaz de comprometer datos personales y recursos del dispositivo.

A.6 Conclusión General del Apéndice. Las tiendas no oficiales representan un riesgo crítico para la seguridad en Android debido a la ausencia de mecanismos de control, verificación de firmas y protección contra aplicaciones alteradas.

El caso práctico evidencia que aplicaciones populares como HTV pueden estar contaminadas con malware altamente intrusivo, lo que confirma la necesidad de:

- Medidas de prevención.
- Educación al usuario.
- Uso responsable de repositorios de software.
- Pruebas en entornos controlados antes de ejecutar APK sospechosos.

Apéndice C.

Repositorio del entorno virtual de análisis

Con el fin de garantizar la reproducibilidad del estudio y permitir la verificación técnica de los procedimientos descritos a lo largo del presente trabajo, se ha puesto a disposición un repositorio que contiene la máquina virtual utilizada para la realización de todas las pruebas y análisis.

La máquina virtual incluye el sistema operativo Ubuntu configurado, las herramientas empleadas (Android Studio, ADB, MobSF, Docker, Frida), así como los archivos de configuración y evidencias generadas durante el análisis del malware Android tipo spyware.

El acceso al entorno virtual se proporciona exclusivamente con fines académicos y de revisión técnica, a través del siguiente enlace:

Repositorio MEGA – Máquina Virtual del Proyecto: https://mega.nz/folder/vlUHUY6Z#vEoP9C2ft4G0qk1FoW3UWw

El contenido del repositorio permite a otros investigadores reproducir el entorno de laboratorio seguro descrito en este trabajo, sin comprometer sistemas reales ni información sensible.