**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMATICA**
**PROCESO DE TITULACIÓN**

**ABRIL 2024 - AGOSTO 2024**

**EXÁMEN COMPLEXIVO DE GRADO DE FIN DE CARRERA**

**PRUEBA PRACTICA**

**PREVIO A LA OBTENCION DEL TITULO DE :**
**INGENIERO EN SISTEMAS DE LA INFORMACIÓN**

**TEMA :**

# ANÁLISIS DE LOS ATAQUES DE MALWARE EN SISTEMAS OPERATIVOS ANDROID Y SUS MEDIDAS DE PREVENCIÓN.

**ESTUDIANTE :**
SÁNCHEZ MORENO MELISSA MARILÚ

**TUTOR :**
ING. RUIZ PARRALES IVAN RUBEN

**AÑO 2024**

## RESUMEN

El presente estudio de casos tiene como finalidad presentar "Análisis de los ataques Malware en dispositivos Android y sus medidas de prevención", la expansión de la tecnología en la actualidad es innegable. Android siendo un sistema operativo muy completo revoluciona a la par de la vanguardia tecnológica que avanza a pasos agigantados, sin embargo debido a su gran aceptación en el mercado y la gran cantidad de información disponible sobre sus usuarios, se ha convertido en el objetivo clave de muchos desarrolladores de malware, siendo estos ciberdelincuentes cuyo deseo es cometer fraudes y aprovecharse de las personas de diversas maneras, robando su identidad, adueñándose de sus cuentas bancarias y haciendo uso malintencionado de ellas.

Se utilizó un enfoque de investigación que permitió llevar a cabo una revisión bibliográfica exhaustiva a través de fuentes, artículos académicos y científicos, y demás trabajos de investigación centrados en la seguridad informática, que es un tema de mucha relevancia hoy en día, todo aquello con el fin de establecer el comportamiento y propagación del malware, y proponer estrategias de prevención efectivas contra ataques maliciosos en las redes.


**Palabras claves:** Android, malware, tecnología, seguridad informática, usuarios.

## ABSTRACT

The purpose of this case study is to present “Analysis of malware attacks on Android devices and their prevention measures”

The expansion of technology today is undeniable. Android, being a very complete operating system, revolutionizes at the same time as the technological vanguard that advances by leaps and bounds, however, due to its great acceptance in the market and the large amount of information available about its users, it has become the key objective of many malware developers, these being cybercriminals whose desire is to commit fraud and take advantage of people in various ways, stealing their identity, taking over their bank accounts and making malicious use of them.

A research approach was used that allowed us to carry out an exhaustive bibliographic review through sources, academic and scientific articles, and other research works focused on computer security, which is a very relevant topic today, everything with in order to establish the behavior and spread of malware, and propose effective prevention strategies against malicious attacks on networks.


**Keywords:** Android, malware, technology, computer security, users.

## INDICE

## PLANTEAMIENTO DEL PROBLEMA

Para muchas personas hoy en día la palabra Android es sinónimo de avance tecnológico en dispositivos inteligentes también conocidos como smartphone, lo cual conlleva una numerosa compra de dispositivos Android de su versión actualizada. Al ser una organización con una muy buena aceptación en el entorno es objeto de ataques por parte de ciberdelincuentes considerados como hackers quienes han cumplido sus intentos de difundir los malware en dispositivos Android.

En la actualidad estos dispositivos y las nuevas capacidades que ofrecen hacen que, en general, los dispositivos móviles sean la puerta de entrada a Internet para muchos usuarios, por lo que su seguridad es muy importante. Si bien la gente es cada vez más consciente de la seguridad informática, muchos usuarios de dispositivos móviles no tienen instalado un software antivirus y sus sistemas operativos no están actualizados con las últimas actualizaciones de seguridad, lo cual es un gran problema.

A esto hay que añadirle que cada vez hay más casos de malware que se distribuye por canales de confianza como podría ser Google Play Store abusando de la confianza de los usuarios en dichos sitios., La sociedad comunitaria depende en gran medida de los dispositivos y el software, lo que la hace vulnerable al ciberterrorismo y al ciberfraude, además, que es fácil ingresar a Internet, cualquier persona guardando su anonimato puede realizar acciones difíciles de asociar.

Android puede ser considerado por muchos una plataforma segura porque su sistema operativo es gratuito para los desarrolladores, quienes a menudo intentan personalizarlo y separarlo de la seguridad. En la plataforma Android, el malware se puede instalar fácilmente a través de tiendas en línea o sitios web simplemente haciendo clic en los anuncios.

La seguridad integrada de Android cuyo objetivo es hacer de esta plataforma de software las más segura del mundo, invierte en tecnologías y servicios que mejoren la

protección de los dispositivos, servicios y aplicaciones. La avanzada inteligencia y el aprendizaje automático permiten proteger de manera proactiva contra las amenazas diarias que se puedan presentar al sistema, ayudando a defender datos personales de app malintencionadas.

La falta de sabiduría sobre la sospecha de malware es una de las razones por las que los usuarios se infectan con el malware, como resultados de estos ataques las preocupaciones sobre el malware en los dispositivos móviles y el sistema operativo Android me han llevado a analizar el asunto para encontrar maneras de detectar y prevenir la divulgación de este malware.

No hay duda de que los dispositivos móviles o comúnmente denominados teléfonos inteligentes almacenan todo tipo de información confidencial de sus usuarios, quienes a lo largo de sus jornadas laborales o actividades diarias dependen mucho de la información ubicada en sus teléfonos inteligentes.

Aunque los usuarios deben proteger sus dispositivos de posibles peligros, los desarrolladores de Android mejoran constantemente la seguridad. Es crucial reducir el riesgo de infección del software manteniéndose al día con las actualizaciones, teniendo en cuenta las precauciones de seguridad y descargando sólo de fuentes acreditadas. A la inversa, es fundamental que las personas y las instituciones comprendan los riesgos digitales y sepan cómo protegerse de ellos.

## JUSTIFICACIÓN

Actualmente, el entorno tecnológico es visible en todo el mundo y ha provocado cambios sin precedentes debido a la enorme demanda de acceso a nuevos dispositivos al mercado, como lo son los dispositivos Android, dejando una tarea difícil para los desarrolladores de software y hardware que trabajan todos los días para crear sistemas confiables y dignos de credibilidad, en conjunto con herramientas de gran rendimiento y seguridad.

Debido a su aceptación en el mercado tecnológico y la cantidad de información que se obtiene de los usuarios, el sistema Android se ha convertido en el objetivo de muchos desarrolladores de malware (conocidos como ciberdelincuentes) que desean tramar y cometer fraudes. Como Hacking, robo de identidad, suplantación de identidad, robo de cuentas bancarias y compra de datos.

El único objetivo es robar información, que suele resultar confusa para el uso de telefonía móvil. Por lo que los desarrolladores de software móvil como lo es Android son conscientes de la necesidad de desarrollar medidas de seguridad contra el malware.

Cabe señalar que el malware también puede alterar el rendimiento del dispositivo y provocar un uso excesivo de los recursos. Este estudio se centra en el sistema operativo Android y describe el impacto del malware en la plataforma móvil. Por la cual utilizaré las herramientas preventivas que se emplearán en la protección antimalware para prevenir daños y las medidas de seguridad que los usuarios pueden tomar al comprar o utilizar aplicaciones móviles.

Su sistema operativo debe estar actualizado y solo deben descargar aplicaciones de fuentes confiables, la tecnología de seguridad y el escaneo de dispositivo pueden impulsar la detección y eliminación temprana de amenazas. Por lo tanto, los usuarios deben ser conscientes de los inconvenientes y comprobar que utilizan sus dispositivos con precaución.

Esta investigación proporciona información detallada sobre el comportamiento y la propagación del malware, lo que permite el desarrollo de soluciones más sólidas y flexibles, al investigar los últimos ataques y técnicas utilizadas por los ciberdelincuentes, podemos anunciar nuevas amenazas y actualizar de forma proactiva nuestras estrategias de prevención. Otro aspecto importante es la prevención, la identificación temprana de vectores de ataque y de infección permite el desarrollo de medidas de seguridad más efectivas. Al estudiar y analizar estos aspectos, la investigación ayuda a crear políticas de seguridad y herramientas de protección que pueden prevenir infecciones antes de que ocurran. Para garantizar la integridad y privacidad de los datos en un entorno digital cada vez más amenazado, es importante adoptar herramientas y mejores prácticas de seguridad de Android.

## OBJETIVOS

Analizar los distintos tipos de ataques de Malware dirigidos a dispositivos Android y desarrollar estrategias efectivas para prevenir dichos ataques.

## OBJETIVOS ESPECÍFICOS

- Identificar los tipos de malware que afectan a dispositivos Android.
- Evaluar las técnicas y vectores de ataque más comunes utilizados para infectar dispositivos Android.
- Proponer estrategias de prevención y mitigación efectivas contra los ataques de malware en dispositivos Android.

## LÍNEA DE INVESTIGACIÓN

- Sistemas de información y comunicación, emprendimiento e innovación.

## SUBLINEA DE INVESTIGACIÓN

- Redes y tecnologías inteligentes de software y hardware

El presente estudio de caso se relaciona con la línea y Sublínea de investigación ya que se necesita la protección de datos y la comunicación que se realiza a través de los dispositivos Android día a día, por lo cual nuestra línea de investigación está enfocada

en desarrollar sistemas de información y comunicación que sean seguros y confiables.

Además, la sublínea de ´´Redes y tecnologías inteligentes de software y hardware´´ es necesaria para abordar el problema de malware en los dispositivos Android, por ejemplo las redes inteligentes tienen en sí la capacidad para monitorear el tráfico de datos en tiempo real lo que va a permitir que detectemos sospechas que significaran que hay presencia de Malware.

## MARCO CONCEPTUAL

### Android

Android es un sistema operativo de código abierto, basado principalmente en Linux, lo que significa que puede ser utilizado y modificado por cualquier persona según sus preferencias. Inicialmente, se creó para su uso en teléfonos móviles y tablets principalmente. Sin embargo, posteriormente se ha extendido a otros dispositivos como relojes inteligentes con Wear OS, automóviles mediante Android Auto o Android Automotive y televisores gracias a Android TV (Naranjo, 2022).

Rich Miner, Nick Sears, Chris White y Andy Rubin dieron a luz Android en el año 2003. El objetivo era alcanzar teléfonos móviles con mayor interactividad, mejor posición en el mercado y más opciones para los usuarios. Si no hubiera sido por la generosa contribución de un préstamo otorgado por Steve Perlman, amigo íntimo de Andy Rubin, el desarrollo de Android se habría detenido debido a la falta de fondos económicos. En 2005, Google adquirió Android y lo incorporó como una de sus subsidiarias con Rubin, Miner y White a carga del sistema operativo, pero bajo su supervisión.

Se anunció oficialmente Android en el año 2007 durante la presentación del consorcio tecnológico Open Handset Alliance, donde estaban presentes marcas como Samsung, Qualcomm, HTC y Google. El primer terminal con este sistema operativo en su interior hizo su aparición en el año 2008. El HTC Dream es el portador de ese honor. Desde entonces, numerosos dispositivos móviles comenzaron a adoptar el sistema operativo Android, lo que ha llevado a la situación actual donde se estima que

más del 90% de los smartphones en circulación cuentan con este software.

## Tipos de Análisis

### Análisis Estático

Hay varios tipos diferentes de análisis estático, pero los dos más importantes se dividen en:

**Análisis estático basado en patrones:** Consiste en buscar coincidencias de código que incumplan las reglas de codificación establecidas. Además de asegurarse de que el código cumple con las expectativas establecidas en términos de cumplimiento normativo o iniciativas internas, también es útil para los equipos al prevenir errores como fugas de recursos, problemas relacionados con el rendimiento y la seguridad, fallas lógicas y mal uso de la API (Camacho, 2023).

**Análisis Dinámicos**

También llamado detección de errores, es donde las distinciones entre varias pruebas comienzan a desdibujarse. Una de la característica importante es que se dedica a examinar el funcionamiento y la estructura de una aplicación. La ejecución del código se realiza mediante una prueba denominada caja blanca, as pruebas analíticas dinámicas detectan errores internos y los reportan cuando ocurren (Camacho, 2023).

Esto facilita que los evaluadores relacionen con precisión estos errores con las actividades de prueba para informar incidentes. Las pruebas dinámicas de seguridad de aplicaciones (DAST) amplían el comportamiento externo de una aplicación para centrado en la seguridad y son una prueba analítica que prueba un elemento de prueba en lugar de verificarlo. Sin embargo, se debe ejecutar el código bajo prueba.

DAST también mejora las pruebas empíricas en todos los niveles, desde las pruebas unitarias hasta las pruebas de aceptación. Esto se logra mediante la capacidad de detectar errores internos que indican errores externos indetectables que han ocurrido después de completar la prueba.

**Herramientas de análisis estático y dinámico**

**JADX**

Esto es muy importante para los investigadores de seguridad, analistas de malware y desarrolladores que trabajan con aplicaciones de Android, ya que permite realizar un análisis estático eficaz. Es una herramienta de línea de comandos con una interfaz gráfica. Le permite descompilar su aplicación APK y obtener recursos como el archivo AndroidManifest.xml. También cuenta con una herramienta de descifrado, lo que facilita el trabajo a los analistas de malware. (Cristal, 2020).

Se utiliza principalmente en el análisis estático de aplicaciones Android para:

**Pruebas de seguridad**: Detecta vulnerabilidades y comportamientos potencialmente maliciosos en el código de la aplicación.

**Ingeniería inversa:** Comprender cómo funciona una aplicación, especialmente cuando el código fuente original no está disponible.

**Análisis de malware:** Investigar e identificar aplicaciones maliciosas. Si su comportamiento o método de infección es perjudicial.

**APKTool**

Es una herramienta de ingeniería inversa de aplicaciones de Android. Los recursos se pueden decodificar de forma casi nativa y volver a ensamblar después de algunas modificaciones, lo que permite depurar el código Smali paso a paso. También ayuda a que sea más fácil trabajar con la aplicación al tener una estructura de archivos similar a un proyecto y automatizar algunas tareas repetitivas como la generación de apk, etc. Se puede utilizar para localización, agregar algunas funciones o admitir plataformas personalizadas y otras multas (Paz, 2021).

Características principales de Apktool:

- Separe los recursos de forma casi nativa (incluidos Resources.arsc, Class.dex, 9.png. y XML).
- Restaurar contenido decodificado a APK/JAR binario.
- Organizar y gestionar archivos APK en función de los recursos de Framework.
- Depuración de Smali (eliminada en la versión 2.1.0 para ser reemplazada por IdeaSmali).
- Le ayuda a realizar tareas repetitivas utilizando componentes de automatización.

Las aplicaciones de Android utilizan recursos y códigos en el propio sistema operativo, estos se denominan recursos de Framework y Apktool los usa para decodificar y generar el archivo APK correcto. Cada versión incluye la última versión de AOSP, esto te permite decodificar y ensamblar variedad de archivos apk sin tener ningún problema. Los fabricantes añaden sus propios archivos Framework además de los archivos AOSP habituales. Para usar Apktool contra estos creadores de aplicaciones, primero debe instalar los archivos de la plataforma del fabricante.

**Cuckoo Sandbox**

Este es un marco de código abierto que le permite realizar pruebas automáticas de malware en máquinas virtuales, así como sacar conclusiones sobre su comportamiento en forma de informes. Muchos programas o plataformas antivirus, como Virus Total, realizan pruebas automáticas de entorno de pruebas, pero la ventaja de Cuckoo es que

permite a los investigadores crear sus propios entornos de pruebas para escanear archivos.(Cilleruelo, 2024).

**Malware**

El malware es un programa informático diseñado para dañar, alterar y perjudicar un sistema informático. Existen diferentes tipos de malware y cada gallo de malware infecta y daña diferentes dispositivos de los usuarios, todos los tipos de malware están diseñados para promover la privacidad y seguridad de los sistemas informáticos. Algunos de los tipos de malware más dañinos roban confesiones financieras y otras confesiones confidenciales, que luego se utilizan para fraude, chantaje y robo de identidad (Belcic, 2023).

El malware en la vida es sólo una indicación para las PC con Windows: las computadoras Mac y los dispositivos móviles, además de la música, son vulnerables al malware. El malware es el final conceptual de cualquier tipo de "programa malicioso" diseñado para ingresar a su máquina sin sus instrucciones y causar daños e interrupciones en su sistema y saquear sus datos.

**Tipos de malware**

Para una comprensión clara, resumiremos a continuación los tipos de malware (Fernández, 2023).

Virus informáticos: este tipo de malware tiene como objetivo interrumpir el funcionamiento normal de su dispositivo. El virus debe ser iniciado por un usuario que crea que se trata de una aplicación legítima. Cuando esto sucede, su computadora puede replicarse e infectarse. Van desde simples bromas destinadas a molestar a otros hasta bromas que pueden dañar gravemente su computadora al eliminar o cambiar archivos que afectan directamente su funcionamiento.

**Gusano Informático:** Este malware no requiere que el usuario altere ni modifique archivos existentes, puede copiar y enviar copias a otras computadoras conectadas en su lista de contactos. A menudo se utilizan para crear botnets, redes de ordenadores zombies que pueden funcionar simultáneamente mientras el operador ordena spam masivo, propaga malware o lleva a cabo diversos tipos de ataques informáticos.

**Troyano:** Es un malware que reside dentro o se hace pasar por un programa legítimo e ingresa a su computadora. Aunque los virus suelen ser de naturaleza destructiva, los troyanos intentan pasar desapercibidos mientras obtienen acceso al dispositivo para que otro malware acceda o robe información y no se propagan por sí solos.

**Spyware:** El también malware se instala en su computadora o interactúa con una segunda aplicación que la ejecuta sin su conocimiento y, a menudo, opera en secreto, tratando de pasar desapercibido, para recopilar información sobre usted o la organización propietaria. computadora ilegalmente.

**Adware:** Es una aplicación similar al malware en el sentido de que no siempre daña tu computadora. Su único propósito es probarse en su computadora y comenzar a mostrar anuncios mientras navega por Internet, en una ventana emergente aleatoria o cuando se ejecuta un programa. Para ello se instala en tu ordenador de la forma habitual mediante la instalación de otras aplicaciones, casi como un troyano pero que no te daña.

**Ransomware:** Es un malware que roba datos de su computadora, pueden bloquearla por completo y para recuperar esos datos exigen un rescate financiero a cambio. Este tipo de programas pueden acceder a las computadoras a través de gusanos u otro malware. Por eso es importante nunca pagar rescates para evitar su uso y porque no garantiza la liberación de datos en su computadora.

**Los 3 tipos de malware más peligrosos para Android**

Se menciona los 3 tipos de malware más peligroso, pero no son los únicos (Stefanko, 2022):

**Ransomware para Android**: Es un tipo de código malicioso que puede bloquear su dispositivo y, en muchas ocasiones, cifra los archivos que contiene. Los atacantes piden a las víctimas que inicien sesión en el sitio web para recuperar los archivos. Existen algunos de estos ransomware para Android en los últimos años que se han analizados, como el software oculto detrás de un aplicativo falso de rastreo de contactos COVID-19 dirigida a usuarios en Canadá.

**Bancario Troyano:** Este tipo de malware se centra en robar credenciales de plataformas bancarias en línea, incluso puede eludir los sistemas de autenticación de dos factores. Una vez instalada y aceptada la aplicación, comienza a realizar una serie de acciones en el dispositivo y activa su funcionalidad, lo que le permite robar credenciales bancarias, así como la frase inicial o la clave de recuperación de la billetera de criptomonedas.

**RAT (troyano de acceso remoto):** Tiene como objetivo espiar el dispositivo de la víctima ejecutando de forma remota comandos enviados por el atacante. Este tipo de malware puede realizar diversas acciones en el ordenador infectado como: Como registrar pulsaciones de teclas o pulsaciones de teclas para buscar credenciales de inicio de sesión y otros datos confidenciales, interceptar mensajes y alertas en cualquier aplicación de redes sociales, grabar llamadas, tomar fotografías y robar referencias de aplicaciones bancarias.

**Vectores de Ataque**

En ciberseguridad, es el medio por el cual un ciberdelincuente puede entregar malware a una víctima, existen diferentes métodos y por tanto diferentes vectores. Para

entender qué son los vectores de ataque, veremos cuáles son los principales medios utilizados para este fin (Davila, 2021).

Estos vectores de amenazas determinan cómo los atacantes obtienen acceso a su sistema o red. Los vectores de ataque más comunes incluyen ataques de ingeniería social, robo de credenciales, explotación de vulnerabilidades y protección inadecuada contra amenazas internas. Por tanto, es importante bloquear los vectores de ataque siempre que sea posible para aumentar la seguridad de toda la información almacenada.

**Tipos de Vectores de ataque**

Recuerde que los vectores de ataque pueden cambiar a medida que avanza la tecnología y los ciberdelincuentes pueden utilizar Múltiples vectores en cada ataque, los vectores más comunes hoy en día son los siguientes (Vivancos, 2022):

**1: Correo electrónico y mensajería instantánea:** Los correos electrónicos y mensajes de texto de phishing se hacen pasar por organizaciones conocidas por el destinatario, como bancos, empresas de paquetería, autoridades fiscales, proveedores y sus clientes o equipos de soporte, para engañarlo con muchos trucos diferentes como haciendo clic en enlaces a sitios web falsos donde se le pedirán credenciales o descargará archivos adjuntos maliciosos que instalan malware.

**2: Navegación web:** Por no actualizar el navegador o por instalar complementos maliciosos o por visitar sitios web falsos. Cuando se enfrenta a navegadores obsoletos, los ciberdelincuentes pueden aprovechar las vulnerabilidades de seguridad utilizando los siguientes métodos:

- Drive-by download, que solo con ver un correo html o visitar una página web permite la descarga de malware.

- browser in the browser, que simulando una ventana de autenticación, donde nos pedirán ingresar las credenciales.

**3: Endpoints:** La configuración por defecto del fabricante no es muy segura en muchos casos. Por ejemplo, si utilizan contraseñas débiles para las conexiones o permiten el uso de unidades USB o unidades extraíbles, podrían transmitir malware. En otros casos, representan configuraciones de red incompletas o incompletas a las que pertenecen estos dispositivos y que permiten acceder a ellos y manipularlos.

**4: Aplicaciones web, portales empresariales, intranets y redes sociales:** Si están mal configurados o desactualizados, pueden ser un punto de acceso o una forma de proporcionar a los ciberdelincuentes información para llevar a cabo más ataques.

**5: Software de red y sistema incorrectamente configurado, desactualizado o sin parches:** Esto significa que no se siguieron los procedimientos adecuados para configurar ese software y las actualizaciones no son aplicables o no existen porque el software ha caducado. Un ejemplo de ciberdelincuentes que utilizan esta ruta de intrusión son los ataques a enrutadores como el secuestro de DNS, ataques DoS o ataques de denegación de servicio, que es lo que le sucedió a esta empresa en esta historia real.

**6: Las credenciales de los usuarios comprometidas:** Ya sea porque se filtran y se reutilizan en otros sistemas o porque se obtienen mediante fuerza bruta o ataques de ingeniería social. En otros casos, se obtiene a través de software o hardware de registro de teclas, registradores de pulsaciones de teclas o software espía en redes Wi-Fi abiertas.

**7: Contraseñas y contraseñas predeterminadas:** Esto se da cuando no se ha cambiado las contraseñas de manera habitual o permanecen por defecto que pone el fabricante y que son más detectables ya que se las pueden encontrar en sitios web.

**8. Insiders:** Personas que tienen acceso y pueden obtener información, podrían tratarse de empleados descontentos, ex empleados que conservaron sus datos de inicio de sesión debido a un error de procedimiento o aquellos que han sido sobornados por ciberdelincuentes.

**9: Desventajas del cifrado:** Debido a su debilidad, uso de claves simples y fácilmente deducibles o protocolos obsoletos o aplicación incorrecta de políticas de cifrado, por ejemplo, dispositivo móvil u olvidó cifrar documentos en la nube este vector puede provocar una fuga de información.

**10: Debilidades de la cadena de suministro:** Si su sistema falla, nuestros datos pueden verse confirmados. Por este motivo, debemos revisar las disposiciones de confidencialidad contenidas en el acuerdo de nivel de servicio. Los proveedores de servicios en la nube son un caso especial.

## Herramientas de Análisis de red y Tráfico

### Wireshark

Los problemas que este software puede resolver incluyen pérdida de paquetes, problemas de latencia e incluso actividad maliciosa de la red, como a través de solicitudes HTTP. Nos permite analizar la red como si estuviéramos mirando un portaobjetos de microscopio en un laboratorio, por así decirlo, y proporciona

herramientas y comandos para filtrar y analizar el tráfico de la red con mayor detalle, acercándonos a la causa raíz del problema (Hernández, 2024).

Los administradores de redes y sistemas lo utilizan para identificar y detectar dispositivos defectuosos que causan la pérdida de paquetes, problemas causados en cualquier parte del mundo por máquinas defectuosas que enrutan el tráfico de red, así como robo de datos e incluso intentos de ataques de malware o piratería contra la organización.

Este es una herramienta poderosa para analizar redes que requiere un conocimiento profundo, para las empresas modernas, esto significa comprender los protocolos HTTP, sus servicios y analizar los encabezados de los paquetes entrantes que contienen metadatos ricos, a veces complejos, así como su enrutamiento y conectividad, reenvío de puertos. y DHCP.

**Características de Wireshark**

Podríamos limitarnos a escribir un artículo presentando las principales características y todas sus capacidades, así como el abanico de posibilidades que nos ofrecen, pero arriba sólo las comentaremos brevemente (Altube, 2021).

- Nos permite monitorear paquetes en un flujo TCP, podemos ver todo lo relacionado con un paquete específico antes y después, potencialmente aplicándoles filtros personalizados sin perder el flujo.

- Puede decodificar paquetes, exportarlos a formatos específicos y guardar estos objetos.

- Le permite ver estadísticas sobre paquetes capturados, incluidos, entre otros, resúmenes, jerarquías de protocolos, conversaciones, puntos finales y gráficos de flujo.

- Análisis sencillo y detallado por resolución de nombres para Mac individuales, redes y más.

- Existe una herramienta de línea de comandos similar a una Terminal Linux que realiza funciones llamada TShark.

**Qué es un firewall y qué funciones tiene en Android**

Firewall para Android es una aplicación que reacciona como intermediario entre otras aplicaciones ya instaladas y la conexión a Internet. Es decir, es una herramienta que permite bloquear el intercambio de varios paquetes de comunicación, una aplicación puede conectarse a Internet con intenciones maliciosas y un firewall la bloqueará y luego esta comunicación funcionará entre ellas protegiendo así la seguridad de su teléfono móvil. Una característica interesante sobre el Firewall de Android es que puede limitar la conexión a Internet de las aplicaciones que consumen más energía (Alcántara, 2022).

Si cree que una aplicación está usando demasiados datos en su plan de datos, puede usar un firewall para controlar el tráfico de paquetes y guardar los datos móviles que necesitará más adelante. En definitiva, un firewall se encarga de controlar las comunicaciones entre los teléfonos móviles e Internet, permitiendo o bloqueando la transmisión de mensajes para proteger el dispositivo final. Echemos un vistazo a los mejores firewalls que puedes descargar para tu Android ahora mismo.

**NetGuard**

Una solución es utilizar una aplicación como NetGuard, la forma más pura de firewall de Android que viene con sistemas operativos como Windows, macOS y Linux. Su propósito es monitorear las aplicaciones instaladas y determinar si pueden conectarse, qué conexiones usar, etc. Gracias a NetGuard, puede reducir cuidadosamente su consumo de datos, tener una mayor duración de la batería y también proteger su privacidad al decidir si puede conectarse o no, ofrecemos versiones simples y avanzadas para satisfacer a nuestros usuarios (López, 2020).

Para controlar la seguridad esta es una de las mejores aplicaciones ya que es un firewall gratuito que no requiere rootear tu teléfono. Una de las funciones más importantes que tiene esta aplicación es que permite bloquear el acceso a Internet ya sea a través de datos móviles o WiFi. También puede recibir notificaciones cuando una aplicación quiera conectarse a Internet y recibir registros de acceso para todas las conexiones a Internet.

De esta manera se mejora la privacidad y la calidad, protege sus datos y amplía la duración de la batería. Esta es una aplicación solo para Android que no requiere privilegios de administrador o root para ejecutarse, instalarse o ejecutarse.

## MARCO METODOLÓGICO

El marco metodológico de este estudio se utilizara el metodo Bibliográfico basado en dar a conocer el malware en dispositivos Android y desarrollar estrategias eficaces para su prevención y mitigación. Para ello, se llevó a cabo una revisión Bibliográfica donde se consultó una amplia gama de fuentes, incluidos artículos académicos, informes de seguridad y estudios de casos de organizaciones centradas en la seguridad informática.

## Revisión de la literatura

La tabla presenta un resumen de la búsqueda literaria relacionada sobre la utilización de VirusTotal y AV-TEST destacando Artículos académicos, informes de seguridad.

*Tabla 1. Virus total y AV- TEST*

| Autor/es | Título | Año | Publicación | Enfoque | Hallazgos Clave | VirusTotal/AV-TEST |
|---|---|---|---|---|---|---|
| Smith, J. et al. | Evaluación de la eficacia de VirusTotal en la detección de ransomware | 2023 | Journal of Cybersecurity | Comparativa de motores antivirus | Alta tasa de detección, limitaciones en variantes nuevas. | VirusTotal |
| Equipo de Investigación de VirusTotal | Tendencias en malware móvil | 2022 | Informe de Seguridad | Análisis de malware móvil | Aumento de troyanos bancarios, nuevas técnicas de evasión. | VirusTotal |
| AV-TEST Institute | Evaluación comparativa de soluciones EDR | 2023 | Informe de Seguridad | Pruebas de productos de seguridad para empresas | Superioridad de soluciones nativas en detección de ataques dirigidos. | AV-TEST |
| Lee, K. | Falsos positivos en VirusTotal: Un análisis en profundidad | 2021 | Conferencia Internacional de Seguridad Informática | Evaluación de la precisión de VirusTotal | Alta tasa de falsos positivos en archivos legítimos. | VirusTotal |
| Equipo de Investigación de AV-TEST | Pruebas de detección de phishing | 2022 | Informe de Seguridad | Evaluación de productos antivirus | Dificultad de detectar sitios de phishing altamente sofisticados. | AV-TEST |

**Elaborado por:** Melissa Sanchez

Los estudios revisados indican que, aunque herramientas como VirusTotal y AV-TEST ofrecen una alta tasa de detección de diversas amenazas cibernéticas, existen áreas de mejora significativa, especialmente en la detección de variantes nuevas y en la reducción de falsos positivos. Además, las tendencias actuales en malware móvil y phishing señalan la falta de innovaciones continuas para contrarrestar las técnicas de evasión creciente de los ataques.

## 1. Identificación y Clasificación de Tipos de Malware en Android

Se realizo una revisión exhaustiva de la literatura con lo cual se pudo identificar las herramientas de análisis estático y dinámico por la cual a continuación se procedió a la elaboración de la tabla.

*Tabla 2**. Identificacion y clasificacion de malwares en android***

| **Herramienta** | **Tipo de Análisis** | **Fortalezas** | **Debilidades** | **Escenarios de Uso** |
|---|---|---|---|---|
| JADX | Estático | Descompilación de Código bytecode a código fuente de alto nivel (Java).<br><br>Fácil de usar y con una interfaz gráfica intuitiva.<br><br>Ideal para análisis de código fuente. | Limitado a aplicaciones Android. Puede generar código desensamblado difícil de leer. | Análisis de aplicaciones Android, ingeniería inversa, identificación de vulnerabilidades. |
| APKTool | Estático | Descompilación de archivos APK a recursos y código fuente (smali). Permite modificar y recompilar aplicaciones. Ampliamente utilizado en la comunidad de desarrollo Android. | Requiere conocimientos básicos de smali y el ecosistema Android. No realiza un análisis dinámico del comportamiento. | Modificación de aplicaciones, creación de parches, análisis de malware. |
| Cuckoo Sandbox | Dinámico | Análisis automatizado de archivos sospechosos en un entorno aislado. Genera informes detallados sobre el comportamiento del malware.<br><br>Soporta múltiples plataformas y tipos de archivos. | Puede ser complejo de configurar y mantener. Requiere recursos computacionales significativos. | Detección de malware, análisis de comportamiento, investigación de incidentes. |

**Elaborado por:** Melissa Sanchez

Las aplicaciones de Android, el análisis de malware y las herramientas de ingeniería inversa tienen sus fortalezas y debilidades. JADX descompila el código de bytes de Java mediante una interfaz gratuita que es ideal para realizar ingeniería inversa y detectar vulnerabilidades de seguridad en aplicaciones de Android, aunque puede producir código difícil de leer. APKTool descompila y recompila archivos APK de pequeño formato, lo cual es útil para modificar aplicaciones y analizar malware, pero requiere conocimientos básicos de formato pequeño y no proporciona análisis dinámico. Cuckoo Sandbox realiza análisis de malware automatizados en un entorno aislado adecuado para la detección de malware y análisis de comportamiento, aunque es difícil de configurar y requiere importantes recursos.

Para identificar los tipos de malware dirigidos a dispositivos Android, realizamos una revisión exhaustiva de la literatura y preparamos una tabla.

*Tabla 3**. Tipos de malware y efectos en dispositivos android***

| Tipo de Malware | Descripción | Características | Ejemplo Notable | Técnicas de Infección Comunes |
|---|---|---|---|---|
| **Troyanos** | Programas maliciosos que se disfrazan de aplicaciones legítimas. | Roban información personal, envían mensajes SMS premium, descargan otros tipos de malware. | Anubis | Ingeniería social, aplicaciones de terceros. |
| **Spyware** | Monitorea actividades del usuario y recopila información sensible sin consentimiento. | Registra mensajes de texto, llamadas, ubicaciones GPS y otra información personal. | SpyNote | Ingeniería social, vulnerabilidades en el sistema. |

| | | | | |
|---|---|---|---|---|
| **Adware** | Muestra anuncios no deseados en el dispositivo del usuario. | Redirige el navegador a sitios web maliciosos, instala otras aplicaciones sin permiso. | Hiddad | Aplicaciones de terceros, ingeniería social. |
| **Ransomware** | Bloquea el acceso al dispositivo o cifra los datos del usuario, exigiendo un rescate. | Utiliza ingeniería social para engañar a los usuarios y hacer que descarguen el malware. | SLocker | Ingeniería social, vulnerabilidades en el sistema. |
| **Rootkits** | Permiten a los atacantes obtener privilegios de administrador en el dispositivo infectado. | Difíciles de detectar y eliminar, pueden ocultar la presencia de otros tipos de malware. | DroidDream | Vulnerabilidades en el sistema, actualizaciones y parches no aplicados. |
| **Worms** | Programas autónomos que se replican y se propagan a otros dispositivos sin intervención del usuario. | Consumen recursos del sistema y causan degradación del rendimiento. | Android/Plankton | Aplicaciones de terceros, vulnerabilidades en el sistema. |

**Elaborado por:** Melissa Sanchez

La tabla presentada destaca la diversidad y sofisticación de los tipos de malware que afectan a dispositivos Android, cada uno con características únicas y técnicas de infección variadas, los troyanos se disfrazan de aplicaciones legítimas para robar información y realizar acciones maliciosas, subrayando la importancia de la cautela al descargar aplicaciones, el spyware monitorea y registra actividades del usuario sin su consentimiento, lo que requiere herramientas de detección robustas, el adware muestra anuncios no deseados e instala aplicaciones sin permiso, resaltando la importancia de verificar la fuente de las aplicaciones.

El ransomware bloquea el acceso al dispositivo o cifra datos, exigiendo un rescate, lo que enfatiza la necesidad de copias de seguridad regulares y educación sobre tácticas

de ingeniería social, los rootkits permiten a los atacantes obtener privilegios de administrador, siendo difíciles de detectar y eliminar, destacando la importancia de mantener el sistema actualizado y aplicar parches de seguridad y los worms se replican y propagan a otros dispositivos sin intervención del usuario, consumiendo recursos del sistema, lo que pone de manifiesto la necesidad de prácticas de seguridad rigurosas al instalar aplicaciones y gestionar actualizaciones.

### 2. Evaluación de Técnicas y Vectores de Ataque

**Simulación de Ataques:** En esta tabla se muestra el uso de emuladores de Android, dispositivos físicos.

*Tabla 4**. Uso de emuladores en Android*

| Entorno de Prueba | Descripción | Ventajas | Desventajas | Escenarios de Uso |
|---|---|---|---|---|
| **Emuladores de Android** | Programas que replican el sistema operativo Android en un entorno de escritorio. | Facilidad de configuración<br>Costo efectivo<br>Flexibilidad en la creación de entornos<br>Acceso a herramientas de depuración y análisis | Limitaciones en el comportamiento real<br>Rendimiento más lento que los dispositivos físicos | Pruebas de aplicaciones<br>Ingeniería inversa<br>Desarrollo y depuración |
| **Dispositivos Físicos** | Dispositivos Android reales utilizados para pruebas de seguridad. | Comportamiento realista<br>Mejor rendimiento<br>Interacción directa con el hardware y sensores | Mayor costo debido a la compra de hardware<br>Menos flexibilidad para crear múltiples entornos | Pruebas de seguridad en condiciones reales<br>Análisis de comportamiento de malware<br>Evaluación de rendimiento de aplicaciones |

**Elaborado por:** Melissa Sanchez

Esta tabla ofrece una comparación visual de la simulación de ataques en un entorno de pruebas controlado utilizando un dispositivo físico y un emulador de Android, los emuladores de Android son herramientas adaptables y de precio razonable que dan acceso a funciones de depuración y análisis y permiten configurar fácilmente distintos entornos de prueba. No obstante, su capacidad para replicar el comportamiento

auténtico del hardware es limitada y su velocidad puede ser inferior a la de los dispositivos físicos.

Aunque permiten la conexión directa con el hardware y los sensores y ofrecen un comportamiento más realista y un mayor rendimiento en las pruebas en profundidad, los dispositivos físicos conllevan mayores costes de hardware y menos flexibilidad a la hora de configurar distintos entornos de prueba.

Esta tabla proporciona una visión general de las herramientas Wireshark y Burp Suite, destacando sus funcionalidades, ventajas, desventajas y escenarios de uso más comunes.

*Tabla 5. Ventajas y desventajas de Wireshark y Burp Suite*

| Herramienta | Descripción | Funcionalidades Principales | Ventajas | Desventajas | Escenarios de Uso |
|---|---|---|---|---|---|
| **Wireshark** | Analizador de tráfico de red de código abierto que captura y examina paquetes de datos en tiempo real. | Captura y análisis detallado de paquetes<br>Filtros avanzados para examinar tráfico específico<br>Decodificación de protocolos<br>Visualización de flujos de red | Amplia compatibilidad con protocolos<br>Interfaz gráfica intuitiva<br>Capacidad para trabajar en diferentes plataformas | Puede generar grandes volúmenes de datos, dificultando el análisis<br>Requiere conocimientos técnicos para interpretar datos complejos | Diagnóstico de problemas de red<br>Análisis de tráfico malicioso<br>Evaluación de seguridad de redes |
| **Burp Suite** | Plataforma de prueba de seguridad web que incluye herramientas para interceptar y analizar tráfico HTTP/HTTPS entre el navegador y el servidor. | Interceptor de tráfico web<br>Escáner de vulnerabilidades<br>Herramientas de análisis de solicitudes y respuestas<br>Funcionalidades de automatización de pruebas | Potente para pruebas de seguridad de aplicaciones web<br>Herramientas integradas para análisis de vulnerabilidades<br>Interfaz adaptada a pruebas de seguridad web | Focalizado en tráfico web, no en redes generales<br>La versión completa es de pago | Pruebas de seguridad de aplicaciones web<br>Identificación de vulnerabilidades en tráfico HTTP/HTTPS<br>Evaluación de configuraciones de seguridad web |

**Elaborado por:** Melissa Sanchez

La tabla compara Wireshark y Burp Suite, dos herramientas esenciales para el análisis de redes y tráfico, Wireshark es robusta para capturar y examinar paquetes de datos, ofreciendo una visión detallada y compatible con diversos protocolos, ideal para diagnósticos y análisis de seguridad de red y Burp Suite se enfoca en la seguridad de aplicaciones web, interceptando y analizando tráfico HTTP/HTTPS con herramientas avanzadas para identificar vulnerabilidades y automatizar pruebas. Su principal limitación es su enfoque específico en tráfico web y el costo de la versión completa.

## 3. Desarrollo de Estrategias de Prevención y Mitigación

La tabla resume las principales directrices de seguridad del OWASP Mobile Security Project y NIST, proporcionando una visión general de las prácticas recomendadas para proteger aplicaciones móviles y sistemas de información.

*Tabla 6**. Directrices de seguridad del OWASP, project y NIST***

| Estándar | Directrices Clave | Descripción |
|---|---|---|
| **OWASP Mobile Security Project** | **Seguridad del Código** | Asegurar el código fuente mediante técnicas como la ofuscación y prácticas de codificación segura. |
| | **Autenticación y Autorización** | Implementar mecanismos de autenticación robustos y gestionar permisos de usuario de manera efectiva. |
| | **Protección de Datos** | Cifrar datos sensibles en reposo y en tránsito para proteger la información del usuario. |
| | **Seguridad en la Comunicación** | Utilizar protocolos seguros (como TLS) para proteger la comunicación entre la aplicación y los servidores. |
| | **Pruebas de Seguridad** | Realizar pruebas regulares para identificar vulnerabilidades y corregir problemas de seguridad. |

| | | |
|---|---|---|
| **NIST** | **Marco de Ciberseguridad (NIST CSF)** | Ofrecer un enfoque estructurado para gestionar el riesgo de ciberseguridad a través de la identificación, protección, detección, respuesta y recuperación. |
| | **Control de Acceso (NIST SP 800-53)** | Establecer controles para gestionar el acceso a sistemas y datos, asegurando que solo usuarios autorizados puedan acceder a la información. |
| | **Gestión de Incidentes (NIST SP 800-61)** | Proporcionar directrices para la gestión y respuesta a incidentes de seguridad, incluyendo identificación, contención y remediación de incidentes. |
| | **Protección de Datos (NIST SP 800-122)** | Ofrecer directrices sobre la protección de información sensible, incluyendo la clasificación de datos y el cifrado. |

**Elaborado por**: Melissa Sanchez

La tabla muestra las directrices clave de seguridad según OWASP Mobile Security Project y NIST, ambas ofrecen enfoques detallados para proteger aplicaciones móviles y sistemas de información, abarcando seguridad del código, autenticación, protección de datos y gestión de incidentes, OWASP se enfoca en aplicaciones móviles, destacando la protección del código, autenticación robusta, cifrado de datos y seguridad en la comunicación, además de la necesidad de pruebas regulares y NIST ofrece un marco más amplio para la ciberseguridad, incluyendo gestión de riesgos, protección de datos, control de accesos y gestión de incidentes.

**Implementación de Herramientas de Seguridad:**

Esta tabla resume las principales herramientas de seguridad y sus características, destacando sus funcionalidades, ventajas, desventajas y los escenarios en los que son más efectivas.

*Tabla 7***:** *Principales herramientas de seguridad*

| Tipo de Herramienta | Descripción | Funcionalidades Principales | Ventajas | Desventajas | Escenarios de Uso |
|---|---|---|---|---|---|
| **Aplicaciones Antivirus** | Programas diseñados para detectar, prevenir y eliminar software malicioso en los dispositivos. | Escaneo de archivos y aplicaciones<br>Eliminación de malware<br>Protección en tiempo real<br>Actualizaciones de definiciones de virus | Protección contra una amplia gama de malware<br>Interfaz generalmente amigable<br>Actualizaciones frecuentes de definiciones | Puede consumir recursos del sistema<br>No siempre detecta amenazas nuevas o sofisticadas | Protección de dispositivos contra virus y malware<br>Escaneo regular de archivos y aplicaciones |
| **Firewalls** | Dispositivos o software que controlan el tráfico de red entrante y saliente basado en reglas de seguridad. | Filtrado de tráfico de red<br>Control de acceso a aplicaciones<br>Monitoreo de conexiones entrantes y salientes<br>Prevención de intrusiones | Protección contra accesos no autorizados<br>Capacidad para bloquear tráfico sospechoso<br>Configuración personalizada según necesidades | Configuración y gestión pueden ser complejas<br>Puede requerir ajustes frecuentes para adaptarse a nuevas amenazas | Protección de redes contra intrusiones y accesos no autorizados<br>Gestión de tráfico de red y acceso a aplicaciones |
| **Herramientas de Monitoreo** | Software que supervisa el sistema y la red en tiempo real para detectar y responder a incidentes de seguridad. | Monitoreo continuo del tráfico de red y actividades del sistema<br>Detección de anomalías y patrones sospechosos<br>Generación de alertas y reportes<br>Análisis forense | Visibilidad en tiempo real de la actividad de red y sistema<br>Capacidad para detectar y responder a incidentes rápidamente<br>Informes detallados para análisis de seguridad | Puede generar grandes volúmenes de datos que requieren análisis<br>Costos asociados con herramientas avanzadas y su implementación | Detección temprana de amenazas y anomalías<br>Respuesta rápida a incidentes de seguridad<br>Análisis forense y auditorías de seguridad |

**Elaborado por:** Melissa Sanchez

La tabla destaca tres herramientas de seguridad clave: aplicaciones antivirus, firewalls y herramientas de monitoreo, las aplicaciones antivirus protegen contra malware mediante escaneo y eliminación de amenazas, aunque pueden consumir muchos recursos, los firewalls filtran el tráfico de red y controlan el acceso, proporcionando defensa robusta, pero su configuración puede ser compleja y las herramientas de monitoreo ofrecen visión en tiempo real del tráfico y actividades.

## RESULTADOS

La aplicación de las estrategias metodológicas en este estudio han aportado importantes resultados sobre la comprensión del malware en los dispositivos Android y la forma de mitigarlo. Inicialmente, la tabla de las herramientas para la ingeniería inversa y el análisis de malware revelan distintas capacidades y limitaciones, la herramienta estática JADX permite descompilar código bytecode a Java, siendo útil para el análisis de código fuente de aplicaciones Android, aunque su uso está limitado a aplicaciones Android y puede generar código desensamblado difícil de interpretar.

APKTool, también una herramienta estática, permite descompilar y modificar archivos APK, siendo ampliamente utilizada en la comunidad Android, aunque requiere conocimientos básicos y no ofrece análisis dinámicos, la tabla proporciona información detallada sobre los tipos de malware y métodos de infección comunes,

como troyanos, spyware, adware, ransomware, rootkits y gusanos. Por ejemplo, los troyanos falsifican aplicaciones legítimas y roban información personal, a menudo difundida a través de ingeniería social y aplicaciones de terceros; software espía que monitorea las actividades de los usuarios y recopila información confidencial sin el consentimiento del usuario mediante la explotación de vulnerabilidades del sistema y técnicas de ingeniería social, el adware muestra anuncios no deseados y redirige los navegadores a sitios web maliciosos, el ransomware bloquea el acceso al dispositivo o cifra los datos y exige un rescate, los rootkits permiten a los atacantes obtener privilegios administrativos, pero son difíciles de detectar y eliminar. Si se deja, el gusano se reproduce y se propaga sin la intervención del usuario, consumiendo recursos del sistema.

El análisis también aborda los entornos de prueba utilizados para el análisis de seguridad, los emuladores de Android replican el sistema operativo en un entorno de escritorio, ofreciendo facilidad de configuración y bajo costo, aunque presentan limitaciones en el comportamiento real y un rendimiento más lento que los dispositivos físicos. Los dispositivos físicos, por otro lado, proporcionan un comportamiento realista y mejor rendimiento, pero a un costo mayor y con menos flexibilidad para crear múltiples entornos.

En cuanto a las herramientas para el análisis de tráfico de red y la seguridad web, Wireshark se destaca como un analizador de tráfico de red que permite la captura y análisis detallado de paquetes en tiempo real, ofrece una amplia compatibilidad con protocolos y una interfaz gráfica intuitiva, aunque puede generar grandes volúmenes de datos, lo que dificulta su análisis. Burp Suite, una plataforma de prueba de seguridad web, incluye herramientas para interceptar y analizar tráfico HTTP/HTTPS,

siendo potente para pruebas de seguridad de aplicaciones web, aunque su versión completa es de pago.

Finalmente, la tabla destaca los estándares y directrices en ciberseguridad, como el OWASP Mobile Security Project, enfocado en la seguridad del código, autenticación, protección de datos, seguridad en la comunicación y pruebas de seguridad, también se menciona el NIST, que ofrece un marco estructurado para gestionar el riesgo de ciberseguridad y directrices para control de acceso, gestión de incidentes y protección de datos

Al analizar ataques maliciosos en dispositivos Android, se utilizan varias herramientas para recopilar información detallada sobre el comportamiento de aplicaciones sospechosas,
la herramienta JADX descompila los archivos APK de una aplicación para calcular el código fuente de la aplicación esto facilita la revisión del código Java y ayuda a identificar partes específicas de la aplicación que pueden estar involucradas en actividades maliciosas, este dispositivo puede identificar fugas de datos o códigos que procesan datos confidenciales de forma insegura, como en el almacenamiento sin cifrado. Además, le permite reconocer los manifiestos y recursos de su aplicación, esto le brinda una mejor comprensión de la funcionalidad de su aplicación, incluida la verificación de los servicios, componentes y permisos que requiere la aplicación. Examinando el archivo AndroidManifest.xml en particular para detectar cualquier permiso excesivo o sospechoso, el descompilar con APKTool le permite examinar de cerca estos componentes, la identificación de solicitudes de permiso que podrían indicar intenciones maliciosas en la solicitud fue facilitada por esta revisión. Comunicación con un servidor externo o acceso no autorizado a datos confidenciales

son ejemplos, el tráfico de red de las aplicaciones se puede capturar con Wireshark. Para asegurar un análisis transparente y evitar interrupciones en los sistemas de producción, esta recopilación se realiza en máquinas virtuales en un ambiente controlado. Wireshark permite una inspección minuciosa de los paquetes de datos después de capturar el tráfico.

Las solicitudes y respuestas HTTP/HTTPS generadas por las aplicaciones se pueden analizar, lo que nos permite identificar patrones inusuales y comportamientos sospechosos. La aplicación envió datos a servidores externos sin la autorización adecuada o estaba conectada a direcciones IP que se sabe que están asociadas con actividad maliciosa.

La herramienta NetGuard proporciona información sobre la actividad de una aplicación en la red al monitorear las direcciones IP y los puertos a los que intenta conectarse, al utilizar estos bloques, puede observar cómo responde su aplicación Academy a las restricciones de la red, lo que le ayuda a encontrar una solución alternativa y le informa sobre la dependencia de su aplicación de la conectividad de la red; Además, NetGuard ofrece la capacidad de bloquear o permitir conexiones particulares, así como de bloquear solicitudes de red que parezcan innecesarias o sospechosas.

## DISCUSION DE RESULTADOS

La discusión de resultados de este estudio revela importantes hallazgos sobre el análisis y mitigación del malware en dispositivos Android.

Primero, las herramientas de ingeniería inversa utilizadas ofrecen capacidades y limitaciones específicas, JADX permitió descompilar código bytecode a Java, facilitando el análisis de código fuente de aplicaciones Android, aunque su utilidad se limita a este entorno y el código desensamblado puede ser difícil de interpretar. APKTool facilitó la descompilación y modificación de archivos APK, siendo útil para la comunidad de desarrollo Android, aunque requiere conocimientos de smali y no ofrece análisis dinámico, Cuckoo Sandbox por su parte proporcionó un análisis automatizado detallado del comportamiento del malware en un entorno aislado, aunque

su configuración y mantenimiento son complejos y requiere muchos recursos computacionales.

En cuanto a los tipos de malware, se observó que los troyanos se disfrazan de aplicaciones legítimas para robar información, el spyware monitorea actividades del usuario sin consentimiento, el adware muestra anuncios no deseados y redirige a sitios maliciosos, el ransomware cifra datos o bloquea el acceso al dispositivo exigiendo un rescate, los rootkits permiten privilegios de administrador y son difíciles de eliminar, y los worms se replican y propagan sin intervención del usuario, consumiendo recursos del sistema.

El estudio también abordó los entornos de prueba, destacando que los emuladores de Android ofrecen facilidad y bajo costo pero presentan limitaciones en comportamiento real y rendimientoy los dispositivos físicos ofrecen un comportamiento más realista pero a un costo mayor y menos flexibilidad.

En el análisis de tráfico de red y seguridad web, Wireshark permitió una captura y análisis detallado de paquetes en tiempo real, mostrando una amplia compatibilidad con protocolos, aunque con grandes volúmenes de datos difíciles de manejar, Burp Suite se centró en la seguridad de aplicaciones web, siendo potente para pruebas de seguridad, pero con un costo asociado en su versión completa.

Finalmente, el estudio reflejó la aplicación de directrices de seguridad de OWASP Mobile Security Project y NIST, abordando aspectos como la protección del código, autenticación, y protección de datos, las herramientas utilizadas permitieron una comprensión detallada del comportamiento de las aplicaciones sospechosas, desde la descompilación de código y análisis de permisos hasta la captura y análisis de tráfico

de red, estas prácticas ayudaron a identificar comportamientos maliciosos, detectar vulnerabilidades, y establecer medidas de mitigación adecuadas, reflejando la importancia de una estrategia integral y bien estructurada en la ciberseguridad.

## CONCLUSIONES

La investigación realizada proporcionó una observacion importante sobre el malware en dispositivos Android, resaltando la diversidad y dificultad de las amenazas actuales, a través de una revisión bibliográfica exhaustiva y el uso de herramientas avanzadas de análisis, se logró identificar y clasificar los tipos de malware más dominantes, considerando su comportamiento, objetivos y técnicas de infección. Esta clasificación es fundamental para comprender mejor las amenazas y desarrollar contramedidas efectivas.

Asimismo, la simulación de ataques en entornos controlados permitió un estudio profundo de los vectores de ataque y el comportamiento del malware en situaciones reales, el uso de la herramientas Wireshark facilitó la identificación de patrones de

tráfico de red y técnicas de interacción maliciosa, proporcionando información valiosa sobre los métodos de ataque utilizados por los ciberdelincuentes.

Finalmente, el desarrollo del planteamiento de prevención y mitigación basadas en estándares de la industria y buenas prácticas mostró ser esencial para fortalecer la seguridad de las aplicaciones Android, la implementación de políticas de seguridad, junto con herramientas de protección como firewalls, demostró ser efictivo para reducir la vulnerabilidad de los dispositivos. Las pruebas de penetración y auditorías de seguridad realizadas permitieron ajustar y mejorar continuamente estas estrategias, asegurando un planteamineto profesional y adaptativo frente a las amenazas emergentes.

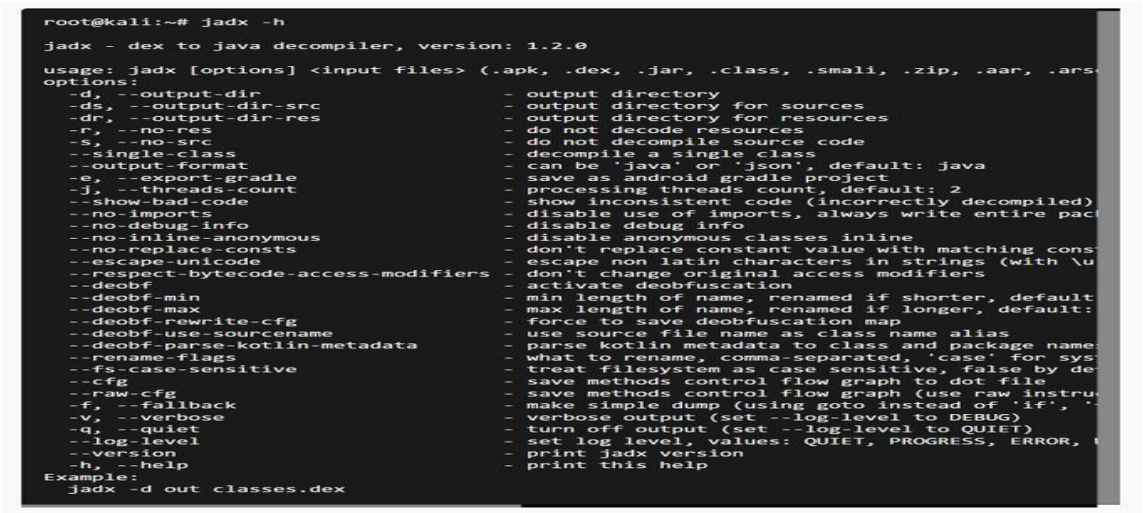
## RECOMENDACIONES

Es recomendable actualizar continuamente las herramientas de detección de malware como VirusTotal y AV-TEST para mejorar su capacidad de detectar nuevas variantes y reducir los falsos positivos, la implementación de sistemas de aprendizaje automático puede mejorar la inteligencia para identificar nuevas amenazas y técnicas de evasión avanzada.

Es recomendable utilizar herramientas de análisis adicionales, aprovechando al máximo el análisis de malware y las herramientas de ingeniería inversa como JADX y APKTool, aprovechando cada una de sus fortalezas específicas al combinar el análisis estático y dinámico para comprender mejor el comportamiento del malware y las vulnerabilidades de aplicaciones.

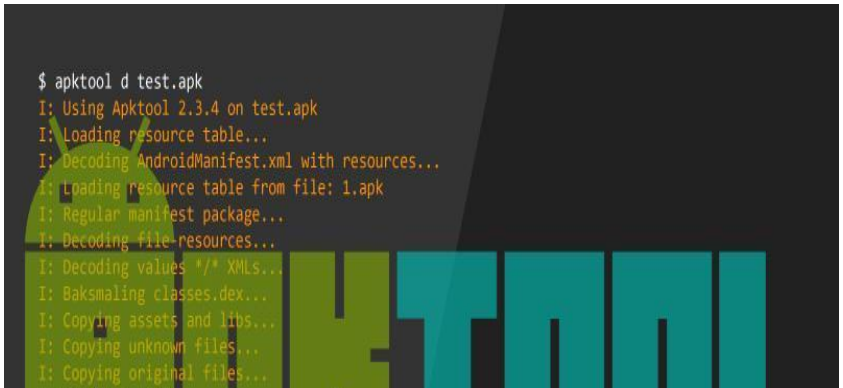
A medida que mejore sus estrategias de seguridad es recomendable desarrollar y mantener políticas de seguridad actualizadas basadas en el Proyecto de seguridad móvil OWASP y los modelos NIST, implementar herramientas de seguridad como firewalls y en general realizar pruebas de penetración y auditorías de seguridad con regularidad para ayudar a mejorar la prevención y estrategias para combatir las amenazas emergentes y mejorar la seguridad de las aplicaciones de Android, mantener informados continuamente a los usuarios y desarrolladores sobre las mejores prácticas de seguridad es esencial para mantener un entorno sin ataques ciberneticos.

## ANEXOS

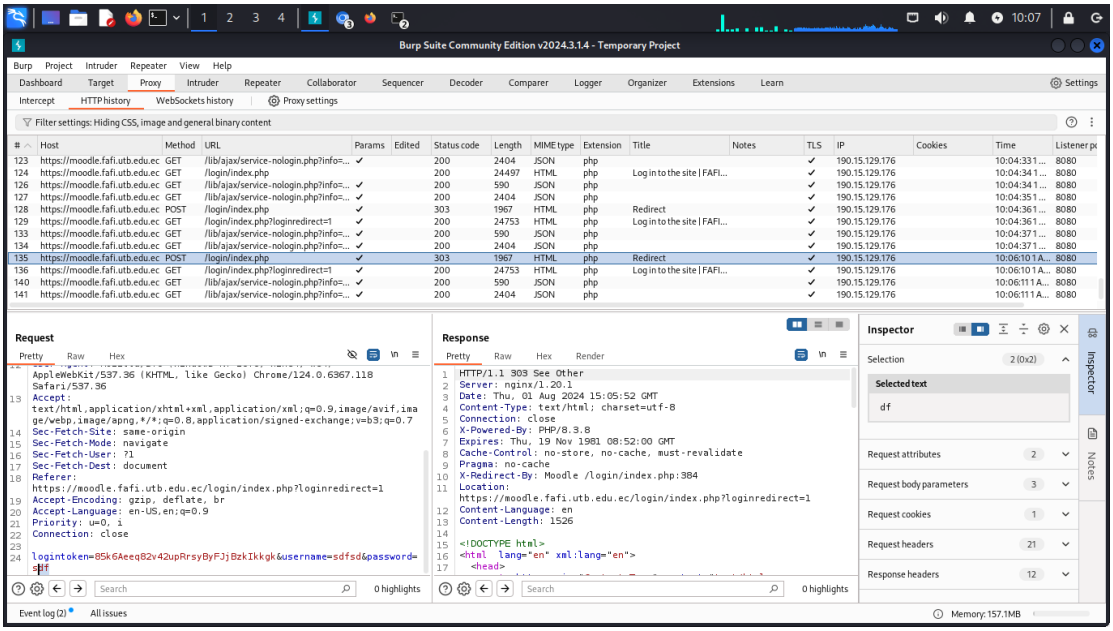



**Anexo 1.** Analisis de codigo fuente

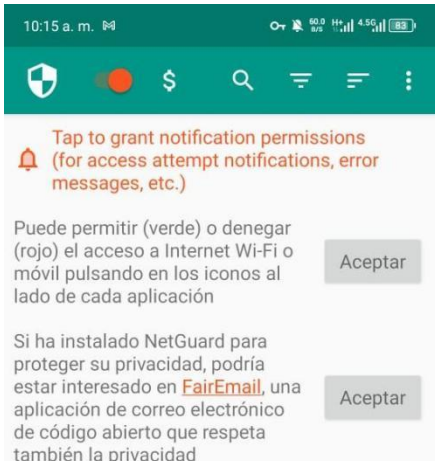
**Elaborado por:** Melissa Sánchez



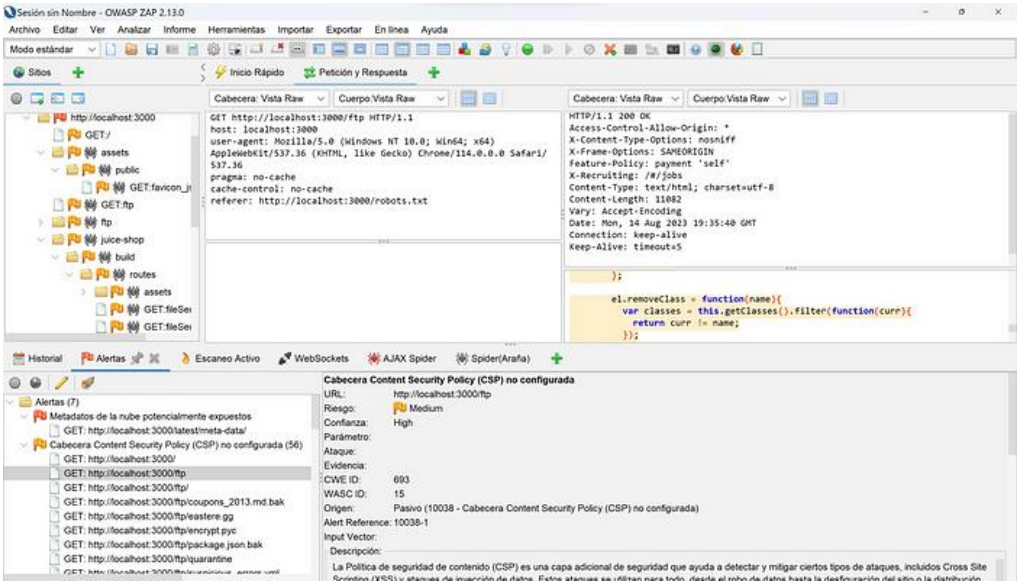
**Anexo 2**. Codigo fuente de aplicaciones maliciosas
**Elaborado por:** Melissa Sánchez



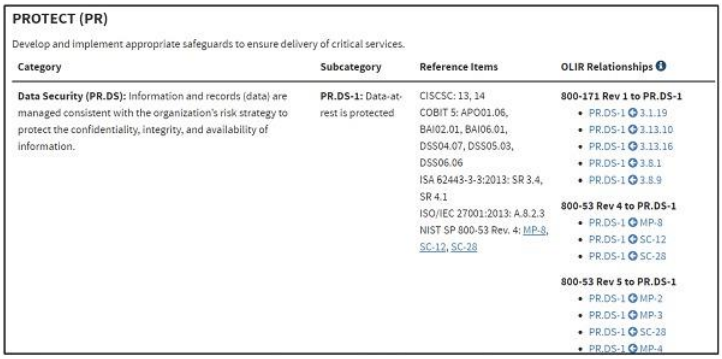

**Anexo 3:** Wireshark Trafico de red
**Elaborado por:** Melissa Sánchez



**Anexo 4.** Herramienta NetGuard
**Elaborado por:** Melissa Sánchez




**Anexo 5:** Vulneravilidades web con Owasp
**Elaborado por:** Melissa Sánchez



**PROTECT (PR)**

Develop and implement appropriate safeguards to ensure delivery of critical services.

| Category | Subcategory | Reference Items | OLIR Relationships |
|---|---|---|---|
| **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | **PR.DS-1:** Data-at-rest is protected | CISCSC: 13, 14<br>COBIT 5: APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06<br>ISA 62443-3-3:2013: SR 3.4, SR 4.1<br>ISO/IEC 27001:2013: A.8.2.3<br>NIST SP 800-53 Rev. 4: MP-8, SC-12, SC-28 | **800-171 Rev 1 to PR.DS-1**<br>• PR.DS-1 3.1.19<br>• PR.DS-1 3.13.10<br>• PR.DS-1 3.13.16<br>• PR.DS-1 3.8.1<br>• PR.DS-1 3.8.9<br>**800-53 Rev 4 to PR.DS-1**<br>• PR.DS-1 MP-8<br>• PR.DS-1 SC-12<br>• PR.DS-1 SC-28<br>**800-53 Rev 5 to PR.DS-1**<br>• PR.DS-1 MP-2<br>• PR.DS-1 MP-3<br>• PR.DS-1 SC-28<br>• PR.DS-1 MP-4 |

**Anexo 6:** Herramienta NIST Cybersecurity Framework (CSF)
**Elaborado por:** Melissa Sánchez

## Bibliografía


Adeva, R. (2024). *Qué es Android: todo sobre el sistema operativo de Google*. Obtenido de https://www.adslzone.net/reportajes/software/que-es-android/

Alcántara, B. (2022). *Los mejores firewalls para Android gratis*. Obtenido de https://www.lavanguardia.com/andro4all/aplicaciones-gratis/mejores-firewalls-android

Altube, R. (2021). *Wireshark: Qué es y ejemplos de uso*. Obtenido de https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

Belcic, I. (2023). *¿Qué es el malware y cómo protegerse de los ataques?* Obtenido de https://www.avast.com/es-es/c-malware

Camacho, R. (2023). *Análisis estático y análisis dinámico*. Obtenido de https://es.parasoft.com/blog/static-analysis-and-dynamic-analysis/

Castillo, G. (2023). *Burp Suite: Qué es y cómo se utiliza*. Obtenido de https://www.innovaciondigital360.com/cyber-security/burp-suite-que-es-como-se-utiliza/

Cilleruelo, C. (2024). *¿Qué es Cuckoo Sandbox?* Obtenido de https://keepcoding.io/blog/que-es-cuckoo-sandbox/

Cristal, J. (2020). *Android: JADX*. Obtenido de https://crhystamil.medium.com/android-jadx-c995deec910f

Davila, V. (2021). *Vectores de ataque*. Obtenido de https://www.studocu.com/es-ar/document/universidad-nacional-de-la-rioja/seguridad-informatica/vectores-de-ataque/40393938

Fernández, Y. (2023). *Malware: qué es, qué tipos hay y cómo evitarlos*. Obtenido de https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Gómez, L. (2024). *¿Qué es Burp Suite?* Obtenido de https://keepcoding.io/blog/que-es-burp-suite/

Hernández, B. (2024). *Wireshark: La herramienta indispensable para el análisis de redes*. Obtenido de https://community.listopro.com/wireshark-la-herramienta-indispensable-para-el-analisis-de-redes/

López, J. (2020). *Un sencillo cortafuegos para Android que controlará todas tus aplicaciones*. Obtenido de https://hipertextual.com/2020/11/netguard-cortafuegos-android-controlar-aplicaciones

Naranjo, M. (2022). *Android: historia, versiones, Google Play y todas sus novedades*. Obtenido de https://computerhoy.com/reportajes/tecnologia/android-historia-versiones-google-play-todas-novedades-1134319

Paz, Á. (2021). *Herramienta para la ingeniería inversa de archivos apk de Android.* Obtenido de https://gurudelainformatica.es/herramienta-para-la-ingenieria-inversa-de-archivos-apk-de-android

Stefanko, L. (2022). *Los 3 tipos de malware más peligrosos para Android*. Obtenido de https://www.welivesecurity.com/la-es/2022/05/09/tipos-malware-mas-peligrosos-android/

Vivancos, E. (2022). *Los 10 vectores de ataque más utilizados por los ciberdelincuentes*. Obtenido de https://www.incibe.es/empresas/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes