**MÁSTER EN INVESTIGACIÓN EN CIBERSEGURIDAD**

Trabajo de Fin de Máster

Análisis de malware troyano en Android

Autor: Raúl Núñez García

Tutor: Ángel Manuel Guerrero Higueras

Julio 2024

|  |  |  |
| --- | --- | --- |
| **UNIVERSIDAD DE LEÓN**  **Escuela de Ingenierías Industrial, Informática y Aeroespacial**  **MÁSTER EN INVESTIGACIÓN EN CIBERSEGURIDAD**  **Trabajo de Fin de Máster** | | |
| **ALUMNO:** Raúl Núñez García | | |
| **TUTOR:** Ángel Manuel Guerrero Higueras | | |
| **TÍTULO:** Análisis de malware troyano en Android | | |
| **CONVOCATORIA: j**ulio 2024 | | |
| **RESUMEN:**  En este Trabajo de Fin de Máster (TFM) se | | |
| **Palabras clave:** | | |
| **Firma del alumno:** | **VºBº Tutor:** | **VºBº Cotutor:** |

**Abstract**

In this Master Thesis Project

**Índice de contenidos**

[Índice de figuras 4](#_Toc167743348)

[Índice de tablas 5](#_Toc167743349)

[Glosario de términos 6](#_Toc167743350)

[Introducción 9](#_Toc167743351)

[Capítulo 1: Estudio del problema 11](#_Toc167743352)

[1.1 EL CONTEXTO DEL PROBLEMA 11](#_Toc167743353)

[1.2 EL ESTADO DEL ARTE 12](#_Toc167743354)

[1.2.5 Conclusión 13](#_Toc167743355)

[1.3 DEFINICIÓN DEL PROBLEMA 13](#_Toc167743356)

[1.4 MALWARE ELEGIDO 13](#_Toc167743357)

[1.4.2 Tecnologías requeridas 13](#_Toc167743358)

[Capítulo 2: Gestión del proyecto 14](#_Toc167743359)

[2.1 ALCANCE DEL PROYECTO 14](#_Toc167743360)

[2.2 PLAN DE TRABAJO 14](#_Toc167743361)

[2.2.1 Identificación de tareas 14](#_Toc167743362)

[2.2.2 Estimación de tareas 15](#_Toc167743363)

[2.2.3 Planificación de tareas 15](#_Toc167743364)

[2.3 GESTIÓN DE RECURSOS 16](#_Toc167743365)

[2.3.1 Especificación de recursos 16](#_Toc167743366)

[2.3.2 Presupuesto 16](#_Toc167743367)

[2.4 GESTIÓN DE RIESGOS 16](#_Toc167743368)

[2.4.1 Identificación de riesgos 16](#_Toc167743369)

[2.4.2 Análisis de riesgos 16](#_Toc167743370)

[2.5 LEGISLACIÓN Y NORMATIVA 17](#_Toc167743371)

[Capítulo 3: Solución 18](#_Toc167743372)

[3.1 DESCRIPCIÓN DE LA SOLUCIÓN 18](#_Toc167743373)

[3.2 EL PROCESO DE DESARROLLO 18](#_Toc167743374)

[3.2.1 Análisis estático 18](#_Toc167743375)

[3.2.1.1 Especificación de requisitos 18](#_Toc167743376)

[3.2.1.2 Consideraciones adicionales 18](#_Toc167743377)

[3.2.2 Análisis dinámico 18](#_Toc167743378)

[3.2.2.1 Especificación de requisitos 18](#_Toc167743379)

[3.2.2.2 Consideraciones adicionales 18](#_Toc167743380)

[3.3 RESULTADOS DEL DESARROLLO 18](#_Toc167743381)

[Capítulo 4: Evaluación 19](#_Toc167743382)

[Capítulo 5: Conclusión 19](#_Toc167743383)

[5.1 APORTACIONES REALIZADAS 19](#_Toc167743384)

[5.2 AMPLIACIONES FUTURAS 19](#_Toc167743385)

[5.3 PROBLEMAS ENCONTRADOS 19](#_Toc167743386)

[5.4 OPINIONES PERSONALES 19](#_Toc167743387)

[Bibliografía 20](#_Toc167743388)

[Anexo A: Control de versiones 21](#_Toc167743389)

[Anexo B: Seguimiento del proyecto 22](#_Toc167743390)

[B.1 FORMA DE SEGUIMIENTO 22](#_Toc167743391)

[B.2 PLANIFICACIÓN INICIAL 22](#_Toc167743392)

[B.3 PLANIFICACIÓN FINAL 22](#_Toc167743393)

**Índice de figuras**

1 4

**Índice de tablas**

**Glosario de términos**

Android

Troyano

Infostealer

Dalvik

APT

FRIDA

Ghidra

MEDUSA

AndroidStudio

Chameleon

JADX

**Introducción**

**PLANTEAMIENTO DEL PROBLEMA**

**OBJETIVOS**

El objetivo principal de este trabajo es el análisis en profundidad de una muestra de malware de tipo troyano desarrollado para plataformas Android. Los objetivos que se esperan cumplir mediante la realización del proyecto son los siguientes:

O1

O2

**METODOLOGÍA**

El trabajo y la gestión del proyecto se llevarán a cabo siguiendo la metodología en cascada (conocida más comúnmente como waterfall). Esto es debido a que existe una clara demarcación entre algunas de las fases debido a su diferente naturaleza. Sin embargo, pese a ser fases individuales claramente definidas, no se trata de unidades aisladas. Los datos obtenidos en cada una de las etapas serán de gran ayuda en otras fases, permitiendo ampliar de manera continua el conocimiento acerca del funcionamiento del malware.

Las etapas del proyecto serán por lo tanto las siguientes:

1. Diseño de los análisis
2. Realización de los análisis y pruebas
3. Documentación de los resultados obtenidos

**ESTRUCTURA DEL TRABAJO**

Esta memoria tiene una estructura dividida en capítulos y anexos. A continuación, se muestra un listado de cada uno de ellos, así como una descripción detallada de los contenidos que componen cada ítem:

* **Introducción. Planteamiento del problema a resolver, resumen de objetivos, metodología de trabajo, estructura de la memoria…**
* **Capítulo 1**. Investigación previa, selección de malware a analizar…
* **Capítulo 2**. Planificación temporal, presupuestos, gestión de riesgos, materia de legislación…
* **Capítulo 3. Análisis estático de la muestra de malware elegida**, pruebas realizadas, método de trabajo detallado
* **Capítulo 4**. Análisis dinámico, resultados obtenidos…
* **Capítulo 5.** Resultados generales obtenidos, problemas encontrados, posibles futuras mejoras o ampliaciones…
* **Anexo A.** Documentación del progreso realizado y materiales generados, control de versiones…
* **Anexo B. Seguimiento del proyecto, cambios respecto al inicio…**

**Capítulo 1: Estudio del problema**

## 1.1 EL CONTEXTO DEL PROBLEMA

En este proyecto se ha llevado a cabo un análisis de muestra de malware Android de tipo troyano. Se han empleado aproximadamente 3 meses en llevar a cabo la tarea incluyendo las investigaciones iniciales, ya que, a pesar de ser un tema cercano a las temáticas del máster, no se cuentan con conocimientos extensos del análisis, especialmente para plataformas móviles como Android. No obstante, algunas asignaturas del título han servido para sentar las bases y permitir avanzar más rápidamente, así como para familiarizarse con algunas de las herramientas a utilizar.

Para llevar a cabo un análisis en profundidad que identifique los vectores de ataque del malware, así como sus procedimientos y objetivos, se han de realizar los siguientes pasos:

* Investigación de la literatura existente respecto al malware y familias relacionadas
* Análisis estático de la muestra obtenida, que permita entender el funcionamiento interno del malware y las tareas que puede realizar.
* Análisis dinámico del malware en un entorno controlado, que posibilite visualizar y obtener datos acerca del funcionamiento del troyano en un dispositivo Android, que en este caso será una versión virtualizada del sistema.
* Análisis de los resultados obtenidos en las fases anteriores, determinando

## 1.2 EL ESTADO DEL ARTE

Malware en Android

Troyanos en Android

Métodos de distribución

Abuso de permisos de accesibilidad

### 1.2.5 Conclusión

## 1.3 DEFINICIÓN DEL PROBLEMA

## 1.4 MALWARE ELEGIDO

¿Qué familia de malware se ha elegido?, por qué? Cómo se han obtenido las muestras y cómo se distribuye a los usuarios

### 1.4.2 Tecnologías requeridas

A mencionar en estado del arte también

# Capítulo 2: Gestión del proyecto

En este apartado se especifica cómo se ha realizado la gestión del proyecto, incluyendo la planificación temporal del mismo, los presupuestos de su realización, la gestión de riesgos existentes, así como el empleo de la legislación aplicable correspondiente.

## 2.1 ALCANCE DEL PROYECTO

## 2.2 PLAN DE TRABAJO

Para llevar a cabo la planificación de este proyecto se han estimado una serie de tareas a realizar y una duración aproximada del tiempo que se podría tardar en ejecutarlas. Más adelante en el [Anexo B](#_B.1__) se mostrará la duración real que han tenido finalmente dichas tareas.

### 2.2.1 Identificación de tareas

Las tareas principales que se han definido para conseguir llegar a la solución propuesta son las siguientes:

* **Tarea 1: realizar un análisis estático de las muestras del malware, con la finalidad de entender el código que lo compone y las tareas que realiza.**
* **Tarea 2: realizar un análisis dinámico de las muestras, recabando los IoCs y observando el comportamiento del troyano (tanto malicioso como no malicioso).**

### 2.2.2 Estimación de tareas

Para la elaboración de este proyecto se estima una duración total de unas 250 horas repartidas a lo largo de 3 meses, lo que equivaldría a unas 2,7 horas de trabajo diario.

### 2.2.3 Planificación de tareas

## 2.3 GESTIÓN DE RECURSOS

### 2.3.1 Especificación de recursos

* **Recursos materiales**
* **Recursos humanos**

### 2.3.2 Presupuesto

**Coste de recursos materiales**

**Coste de recursos humanos**

**Beneficio industrial**

**Coste total**

## 2.4 GESTIÓN DE RIESGOS

### 2.4.1 Identificación de riesgos

### 2.4.2 Análisis de riesgos

## 2.5 LEGISLACIÓN Y NORMATIVA

**Capítulo 3: Solución**

## 3.1 DESCRIPCIÓN DE LA SOLUCIÓN

## 3.2 EL PROCESO DE DESARROLLO

### 3.2.1 Análisis estático

### 3.2.1.1 Especificación de requisitos

### 3.2.1.2 Consideraciones adicionales

### 3.2.2 Análisis dinámico

### 3.2.2.1 Especificación de requisitos

### 3.2.2.2 Consideraciones adicionales

## 3.3 RESULTADOS DEL DESARROLLO

**Capítulo 4: Evaluación**

**Pendiente de valoración sobre qué tipo de contenido o si incluir parcialmente en otros capítulos.**

**Capítulo 5: Conclusión**

En este apartado se comentan los resultados obtenidos en el proyecto, las aportaciones que se han realizado, se mencionan posibles ampliaciones que se podrían realizar en el futuro, se mencionan los problemas encontrados durante la realización de la tesis y, por último, se encuentra una sección de opiniones en la que se emitirán algunas valoraciones a título personal tras la realización del proyecto.

## 5.1 APORTACIONES REALIZADAS

## 5.2 AMPLIACIONES FUTURAS

## 5.3 PROBLEMAS ENCONTRADOS

## 5.4 OPINIONES PERSONALES

**Bibliografía**

|  |  |
| --- | --- |
| [1] |  |

**Anexo A: Control de versiones**

Se ha creado un [repositorio público en GitHub](https://github.com/raulng9/TFM_MalwareAnalysis) con los materiales utilizados en la realización del proyecto, incluyendo documentos con recursos utilizados, resultados derivados de los análisis, muestras de malware utilizadas y notas acerca del proceso.

**Anexo B: Seguimiento del proyecto**

## B.1 FORMA DE SEGUIMIENTO

A lo largo de todo el proceso se han realizado reuniones periódicas con el tutor para monitorizar el progreso llevado a cabo, así como dar recomendaciones y correcciones al alumno, además de tratar las próximas etapas a realizar.

## B.2 PLANIFICACIÓN INICIAL

## B.3 PLANIFICACIÓN FINAL