**MÁSTER EN INVESTIGACIÓN EN CIBERSEGURIDAD**

Trabajo de Fin de Máster

Análisis de troyano Chameleon 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 troyano Chameleon en Android | | |
| **CONVOCATORIA: j**ulio 2024 | | |
| **RESUMEN:**  En este Trabajo de Fin de Máster (TFM) se | | |
| **Palabras clave: malware, Android, troyano, infostealer, Chameleon** | | |
| **Firma del alumno:** | **VºBº Tutor:** | **VºBº Cotutor:** |

**Abstract**

In this Master Thesis Project

**Índice de contenidos**

[Índice de figuras 4](#_Toc168521717)

[Índice de tablas 5](#_Toc168521718)

[Glosario de términos 6](#_Toc168521719)

[Introducción 9](#_Toc168521720)

[Capítulo 1: Estudio del problema 12](#_Toc168521721)

[1.1 EL CONTEXTO DEL PROBLEMA 12](#_Toc168521722)

[1.2 EL ESTADO DEL ARTE 14](#_Toc168521723)

[1.2.5 Conclusión 15](#_Toc168521724)

[1.3 DEFINICIÓN DEL PROBLEMA 15](#_Toc168521725)

[1.4 MALWARE ELEGIDO 15](#_Toc168521726)

[1.4.2 Tecnologías requeridas 15](#_Toc168521727)

[Capítulo 2: Gestión del proyecto 17](#_Toc168521728)

[2.1 ALCANCE DEL PROYECTO 17](#_Toc168521729)

[2.2 PLAN DE TRABAJO 17](#_Toc168521730)

[2.2.1 Identificación de tareas 17](#_Toc168521731)

[2.2.2 Estimación de tareas 18](#_Toc168521732)

[2.2.3 Planificación de tareas 18](#_Toc168521733)

[2.3 GESTIÓN DE RECURSOS 19](#_Toc168521734)

[2.3.1 Especificación de recursos 19](#_Toc168521735)

[2.3.2 Presupuesto 19](#_Toc168521736)

[2.4 GESTIÓN DE RIESGOS 19](#_Toc168521737)

[2.4.1 Identificación de riesgos 19](#_Toc168521738)

[2.4.2 Análisis de riesgos 19](#_Toc168521739)

[2.5 LEGISLACIÓN Y NORMATIVA 20](#_Toc168521740)

[Capítulo 3: Solución 21](#_Toc168521741)

[3.1 DESCRIPCIÓN DE LA SOLUCIÓN 21](#_Toc168521742)

[3.2 EL PROCESO DE DESARROLLO 21](#_Toc168521743)

[3.2.1 Análisis estático 21](#_Toc168521744)

[3.2.1.1 Especificación de requisitos 21](#_Toc168521745)

[3.2.1.2 Consideraciones adicionales 21](#_Toc168521746)

[3.2.2 Análisis dinámico 21](#_Toc168521747)

[3.2.2.1 Especificación de requisitos 21](#_Toc168521748)

[3.2.2.2 Consideraciones adicionales 21](#_Toc168521749)

[3.3 RESULTADOS DEL DESARROLLO 21](#_Toc168521750)

[Capítulo 4: Evaluación 22](#_Toc168521751)

[Capítulo 5: Conclusión 22](#_Toc168521752)

[5.1 APORTACIONES REALIZADAS 22](#_Toc168521753)

[5.2 AMPLIACIONES FUTURAS 22](#_Toc168521754)

[5.3 PROBLEMAS ENCONTRADOS 22](#_Toc168521755)

[5.4 OPINIONES PERSONALES 22](#_Toc168521756)

[Bibliografía 23](#_Toc168521757)

[Anexo A: Control de versiones 24](#_Toc168521758)

[Anexo B: Seguimiento del proyecto 25](#_Toc168521759)

[B.1 FORMA DE SEGUIMIENTO 25](#_Toc168521760)

[B.2 PLANIFICACIÓN INICIAL 25](#_Toc168521761)

[B.3 PLANIFICACIÓN FINAL 25](#_Toc168521762)

**Índice de figuras**

1 4

**Índice de tablas**

**Glosario de términos**

Troyano: tipo de malware que en la mayoría de los casos se hace pasar por legítimo pero realmente permite a los atacantes tomar el control del dispositivo infectado.

Infostealer: tipo de malware diseñado con el objetivo de realizar una exfiltración de datos del dispositivo infectado para obtener información que pueda resultar de interés a los atacantes.

Ofuscación: técnica de modificación del código fuente de un sistema que busca aumentar la dificultad de su comprensión mediante el empleo de estrategias como la reordenación del código o el empleo de cifrado. Este sistema puede ser utilizado por atacantes para tratar de hacer más difícil la labor de análisis del malware.

APK: tipo de archivo empaquetado utilizado tanto por el sistema Android como las aplicaciones que se distribuyen en el ecosistema. Contiene todos los materiales necesarios para la instalación de una aplicación, incluyendo su código, recursos y certificados. Se construye a partir de código fuente en Java o Kotlin.

ART: Android Runtime es la máquina virtual que utilizan los dispositivos Android. Es el sistema sucesor de Dalvik y hace las veces de máquina virtual Java, pero cuenta con su propio sistema de bytecode. Realiza la traducción entre el bytecode generado y las instrucciones nativas del dispositivo.

DEX: iniciales de Dalvik Executable, formato de bytecode que utiliza la máquina virtual de Dalvik de las aplicaciones Android. El compilador DEX es el encargado de traducir el código fuente Java o Kotlin en DEX.

APT: acrónimo en inglés de Advanced Persistent Thread. Hace referencia a grupos de atacantes informáticos de gran sofisticación y cantidad de recursos. Suelen ser grupos con financiación y apoyo de grandes organizaciones, a menudo algunas de ellas estados.

IoC: indicadores de compromiso en español, son conjunto de datos y evidencias generados por una actividad realizada que indican las características de una amenaza. Pueden englobar ficheros creados, procesos ejecutados, dominios o IPs contactadas entre otros.

MD5: algoritmo de reducción que genera un valor de 128 bits a partir de una entrada de valor arbitrario. Se utiliza a entre otros a modo de checksum para verificar la integridad de los datos.

DDoS: ataque distribuido de denegación de servicio, consistente en la sobrecarga de una infraestructura informática como puede ser un sitio web o un servidor y provocando problemas de disponibilidad en este. En gran parte de los casos, estos ataques utilizan redes de dispositivos infectados y controlados remotamente, conocidos como botnets, para llevar a cabo las ofensivas.

Cryptojacking: tipo de delito informático en el que los dispositivos infectados son utilizados por los atacantes para el minado de criptomonedas sin el conocimiento de la víctima que posee el dispositivo y con el fin de obtener un beneficio económico.

DNS: sistema de nombres de dominio jerárquico y distribuido que establece un sistema de nombres y direcciones para dispositivos que forman parte de Internet. Delega la responsabilidad de gestionar nombres y relaciones para cada dominio a sus servidores DNS autoritativos correspondientes.

C&C: del inglés Command & Control, también conocido como C2, alude a la infraestructura utilizada por los atacantes para controlar los equipos infectados de manera remota a través de una comunicación entre los servidores del C2 y los dispositivos.

**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 – Enmarcar este malware y la familia de la que procede dentro del ecosistema actual de troyanos de plataformas Android.

O2 - Realizar un análisis de los vectores de ataque y mecanismos de distribución del malware.

O3 - Llevar a cabo un análisis estático del malware para tratar de comprender sus capacidades y modus operandi.

O3 – Realizar un análisis dinámico del malware en un entorno controlado, que permita observar cómo se comporta una vez instalado y ejecutado en un dispositivo infectado.

O4 – Obtener una serie de indicadores de compromiso y procedimientos que permitan identificar el malware en el caso de encontrarse este presente en un dispositivo.

**METODOLOGÍA**

El trabajo y la gestión del proyecto se llevarán a cabo siguiendo de manera aproximada la metodología ágil (también conocida como agile), ya que, pese a que existe una clara demarcación entre algunas de las fases debido a su diferente naturaleza, no se trata de unidades aisladas. Los datos obtenidos en cada una de las etapas serán de ayuda en otras fases, permitiendo ampliar de manera continua el conocimiento acerca del funcionamiento del malware. El análisis estático y dinámico se complementarán entre sí, aportando información que permitirá progresar globalmente. No obstante, es importante que no se ha seguido completamente la modalidad con sprints claramente definidos y entregables al final de cada uno como está definido en algunas variantes de agile como puede ser Scrum. Las razones de esto son por un lado la dificultad de concretar plazos para ciertas tareas al tratarse de un proyecto que cuenta con un componente importante de investigación, y por lo tanto de varias incógnitas que impiden estimar tiempos con una precisión alta, y por otro lado a la complejidad de compatibilizar el trabajo en el proyecto de manera totalmente definida con el horario laboral del alumno. Sin embargo, se ha tratado en la medida de lo posible de seguir el modelo y su filosofía de cambios e iteración frecuente.

Tras la planificación inicial, las etapas del proyecto quedan definidas de la siguiente manera:

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 cuenta en su parte final con anexos relativos a temas generales del proyecto. 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 y presentación de la estructura de la memoria.
* Capítulo 1. Investigación previa realizada y proceso de selección del malware a analizar.
* Capítulo 2. Planificación temporal creada inicialmente, junto con presupuestos, la gestión de riesgos y la materia de legislación aplicable al proyecto.
* Capítulo 3. Organización de los análisis a realizar, siendo estos el análisis estático y el dinámico. Presentación del método de trabajo a utilizar durante la realización de las actividades.
* Capítulo 4. Presentación de los resultados obtenidos a raíz de los análisis aplicados.
* Capítulo 5. Aportaciones realizadas a través de los resultados obtenidos al igual que comentario y contextualización de estos. En otro orden de cosas, también se hará una enumeración de los problemas encontrados durante la realización del proyecto, así como posibles futuras mejoras o ampliaciones a aplicar.
* Anexo A. Documentación del progreso realizado y materiales generados, control de versiones del trabajo.
* Anexo B. Seguimiento del proyecto y cambios efectuados respecto a las planificaciones iniciales.

**Capítulo 1: Estudio del problema**

## 1.1 EL CONTEXTO DEL PROBLEMA

En este proyecto se ha llevado a cabo un análisis de una muestra de malware Android de tipo troyano perteneciente a la familia Chameleon. 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 en profundidad para la realización 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 tipo de malware elegido y las familias relacionadas, con el fin de conocer su naturaleza y los procedimientos más habituales.
* Análisis estático de la muestra obtenida, que permita entender el funcionamiento interno del malware y las tareas que puede realizar, así como código que pese a no ser ejecutado necesariamente en las pruebas dinámicas también forma parte de la amenaza, pudiendo ser ejecutado bajo ciertas condiciones especiales.
* 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 las amenazas que presenta el malware a los sistemas Android, por qué tiene éxito en sus ataques y cuáles son los signos o indicadores de su presencia en un dispositivo.

## 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

Se ha elegido una muestra de la familia de troyanos conocida como Chameleon. Esta variedad de troyano en Android apareció online a principios de 2023, y desde entonces ha pasado por diferentes iteraciones, aumentando el área de sus ataques e introduciendo nuevos mecanismos para obtener sus objetivos. Las razones detrás de esta elección son varias. En primer lugar, se trata de un malware reciente y que se encuentra actualmente en el foco debido a la gran cantidad de dispositivos infectados que se han encontrado. Asimismo, esta nueva versión es diferente a las anteriores, y también a otros troyanos para sistemas Android, en la manera en que gestiona los parámetros de accesibilidad para hacerse con el control del dispositivo y evitar la protección biométrica para su desbloqueo. Asimismo, pese a ser un malware relativamente popular en estos últimos años, no se encuentran muchos artículos especializados ni análisis respecto a este. Sin embargo, sí que existen multitud de artículos generalizados en medios de comunicación haciendo referencia a la amenaza que presenta para los usuarios. Por todas estas razones expuestas se ha decidido finalmente seleccionar esta familia de malware como temática del proyecto

### 1.4.2 Tecnologías utilizadas (a rellenar)

A continuación, se incluyen las tecnologías utilizadas a lo largo de la realización del proyecto, formando parte de ambas fasse de análisis del malware. En primer lugar, se comentan las herramientas utilizadas pare realizar el análisis estático del código.

* JADX
* Apktool
* Simplify
* Sublime Text
* Android Studio

En lo relativo a la sección de análisis dinámico del troyano, las herramientas utilizadas fueron las siguientes:

* Android Studio
* Genymotion
* FRIDA
* Burp Suite
* DB Browser

Por último, se presentan herramientas adicionales utilizadas durante el proyecto sin pertenecer a ninguna de las fases en particular, si no que han sido empleadas para tareas diversas durante todas las fases:

* Brew: gestor de paquetes utilizado en el sistema Mac para la instalación de programas y utilidades.
* HexFiend: visualización del dump de archivos en hexadecimal para tratar de averiguar el tipo de fichero dada su firma.

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 estudio de la literatura existente de malwares troyanos en Android para tener una perspectiva general del estado actual de amenazas en la plataforma.
* Tarea 2: elegir una familia concreta de malware y obtener muestras para su posterior análisis, además de estudiar sus medios de distribución habituales.
* Tarea 3: realizar un análisis estático de las muestras del malware, con la finalidad de entender el código que lo compone y las tareas que realiza en la medida de lo posible. Sin requerir el descifrado completo de su código en el caso de estar este encriptado u ofuscado, será importante comprender una cantidad suficiente como para discernir el funcionamiento general del malware y las acciones (maliciosas o no) que realiza en el dispositivo.
* Tarea 4: realizar un análisis dinámico de las muestras, recabando los IoCs que puedan registrarse y observando el comportamiento del malware, comprobando paralelamente que los resultados obtenidos en el análisis estático se corresponden con los patrones observados en el dispositivo infectado.

### 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**

**Capítulo 5: Conclusión**

En este apartado se comentan los resultados obtenidos previamente, 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