MECANISMOS DE OBTENCIÓN Y ANALISIS DE MALWARE EN ENTORNOS UNIVERSITARIOS EN SISTEMAS OPERATIVOS WINDOWS.

Autor

BRAYAN FERNANDO BERMUDEZ CASELLES

Trabajo de Grado presentado como requisito para optar al título de Ingeniero de Sistemas

Director

Ing. LUIS ANDERSON CORONEL

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia octubre de 2019

Tabla de contenido

[**Capítulo 1. Título** 4](#_Toc41418411)

[1.1 Planteamiento del Problema. 4](#_Toc41418412)

[1.2 Formulación del problema. 5](#_Toc41418413)

[1.3 Objetivos. 5](#_Toc41418414)

[1.3.1 Objetivo general. 5](#_Toc41418415)

[1.3.2 Objetivos Específicos. 5](#_Toc41418416)

[1.4 Justificación. 5](#_Toc41418417)

[1.5 Delimitaciones. 6](#_Toc41418418)

[1.5.1 Geográfica. 6](#_Toc41418419)

[1.5.2 Temporal. 6](#_Toc41418420)

[1.5.3 Conceptual. 6](#_Toc41418421)

[1.5.4 Legal. 6](#_Toc41418422)

[**Capítulo 2. Marco Referencial** 7](#_Toc41418423)

[2.1 Marco Histórico. 7](#_Toc41418424)

[2.2 Marco Contextual. 7](#_Toc41418425)

[2.3 Marco Conceptual. 7](#_Toc41418426)

[2.4 Marco Teórico. 7](#_Toc41418427)

[2.5 Marco Legal. 7](#_Toc41418428)

[**Capítulo 3. Diseño metodológico** 7](#_Toc41418429)

[3.1 Tipo de investigación. 7](#_Toc41418430)

[3.2 Población y muestra. 7](#_Toc41418431)

[3.2.1 Población. 7](#_Toc41418432)

[3.2.2 Muestra. 7](#_Toc41418433)

[3.3 Diseño de instrumentos de recolección de la información y técnicas de análisis de datos. 7](#_Toc41418434)

[3.4 Análisis de información. 7](#_Toc41418435)

[3.5 Cronograma de actividades. 7](#_Toc41418436)

[**Capítulo 4. Administracion del proyecto.** 7](#_Toc41418437)

[4.1 Recursos humanos. 7](#_Toc41418438)

[4.1.1 Recursos humanos. 7](#_Toc41418439)

[4.1.2 Recursos institucionales. 7](#_Toc41418440)

[4.1.3 Recursos Financieros. 7](#_Toc41418441)

[**Referencias.** 7](#_Toc41418442)

[**Apéndices.** 7](#_Toc41418443)

# **Capítulo 1. Título**

MECANISMOS DE OBTENCIÓN Y ANALISIS DE MALWARE EN ENTORNOS UNIVERSITARIOS EN SISTEMAS OPERATIVOS WINDOWS.

## Planteamiento del Problema.

El análisis de malware hace referencia al arte de la detección de software malicioso, entendiendo como funcionan, como se identifican y derrotan estos virus, que a diario y durante los últimos años ha ido evolucionando transformándose en epidemias para nuestras computadoras, teléfonos inteligentes, tabletas, dispositivos o máquinas que están conectados a una red. Las infecciones por malware llegan como el caudal, cada uno con sus propios métodos de ataque que pueden ser sigilosos y solapados o en muchos de los casos sutiles; en pocas palabras el malware es un software que tiene cierto tipo de intenciones como lo son dañar dispositivos, robar datos y en general causar muchos problemas.

Sin embargo, en los últimos años se han creado diseños de ciertas técnicas y metodologías que con el pasar de los años se han ido incrementado pero no siendo todas de gran efectividad, así como en la vida real existen antibióticos o enfermeros, en la informática existen los encargados del análisis de malware , quienes en su diario vivir utilizan ciertas técnicas, metodologías que ayudan a dar solución a las problemáticas de software malicioso, como lo realiza (Rivera Guevara, 2014) en su investigación en la cual identifica las características de ciertos archivos ejecutables efectuando la técnica de análisis estático, en donde estudia las características para poder detectar si existen nuevas versiones y para ello se encarga de clasificarlos por medio de una base de datos de malware “malicia”; una de las muchas técnicas que se pueden tener en cuenta para dar una buena solución, además de eso nos permite estudiar el comportamiento de malware.

En Colombia muy poco se habla de los estudios o de investigaciones que tengan que ver con técnicas que permitan saber cómo defendernos o bien saber cómo nuestros dispositivos se encuentran infectados por un malware, pero hay excepciones un grupo de estudiantes (Zapata Pareja, Cubides Corrales, & Murcia Guzman, 2015), desarrollaron una investigación haciendo utilidad de herramientas para la detección de análisis como GetSusp, Sysinspector, Regshot para los cuales utilizan entornos virtuales para realizar las pruebas lo cual es una buena práctica y su investigación va orientada a un análisis dinámico, haciendo utilidad de dos malware bastante comunes para ello, en su investigación hacen utilidad de buenas tecnicas para la detección de archivos en el sistema donde analizan los has y las firmas digitales.

Para terminar el análisis de malware es importante tenerlo en cuenta para todos aquellos quienes dominan dispositivos electrónicos conectados a una red, saber de él y reconocer ciertas formas de saber cuándo estamos siendo atacados o cuando uno de nuestros dispositivos se encuentra infectado, identificando ciertas cualidades que ocurren en ellos. Se ha detectado que en la UFPSO (Norte de Santander) todavía no se realiza una investigación relacionada con el análisis de malware, siendo este uno de los temas de vital importancia ya que sus jóvenes y diferente personal de la universidad hacen utilidad de diferentes dispositivos electrónicos, cabe aclarar que las técnicas que se utilizarán a lo largo de esta investigación serán dos las cuales son análisis estático de malware y análisis dinámico de malware para cada uno, con su respectiva metodología de análisis donde se utilizaran entornos virtuales que permitirán realizar pruebas a muestras activas de malware y así permitirnos dar soluciones a las hallazgos.

## Formulación del problema.

¿Comprender el funcionamiento y la comunicación del malware una vez infectado el entorno virtual, mediante las técnicas de análisis estático y dinámico de malware?

## Objetivos.

### 1.3.1 Objetivo general.

Analizar y obtener mecanismos de análisis de malware en entornos virtuales de sistemas operativos Windows.

### 1.3.2 Objetivos Específicos.

•Analizar el funcionamiento de malware mediante técnicas que permitan identificar si los archivos contienen software malicioso o indeseables.

•identificar incidentes haciendo uso de las técnicas planteadas de análisis de software que permitan hallar infecciones y comportamientos por malware.

•Generar entornos virtuales que permitan testear infraestructura analizando archivos infectados con malware haciendo uso de las técnicas y metodologías planteadas.

•Realizar un informe de los hallazgos encontrados más significativos.

## Justificación.

El análisis de malware es la mejor practica ante los problemas relacionados con ataques maliciosos o infecciones por virus, permitiéndonos determinar su origen, funcionalidad y el impacto que pueden llegar a tener las muestras activas de malware, donde pueden afectar gravemente la seguridad y la integridad de la información que se posee, es importante detectar cuándo estamos siendo atacados o cuando se encuentran hurtando la información por medio de un malware. Saber cómo reconocer que tipo de malware se encuentra afectándonos ya sea un virus, un troyanos, un keyloger, un spyware o un ransoware por mencionar los más conocidos e utilizados por los creadores de malware, es de vital importancia poder identificar qué tipo de malware es; pues cada uno de ellos cumple ciertas funciones y se comportan de maneras diferentes, atacando funciones del sistema operativo diferentes teniendo un objetivo específico ya sea encriptar la información como lo es el caso de los ransoware o capturar las pulsaciones del usuario en el sistema como lo es el caso de los keyloger.

En análisis de malware se basa principalmente en dos técnicas que son análisis estático donde se estudia la estructura de los archivos sin ejecutarlos, cabe decir que es bastante rápido y efectivo, y el análisis dinámico que comprende el comportamiento de un malware en un ambiente controlado que a su vez es algo riesgoso porque se tiene que ejecutar el archivo para saber su comportamiento, los malware se comportan de diferentes manera por lo cual para su análisis existen distintas metodologías para hacer uso de cada una de las técnicas.

Si bien a diario en la UFPSO se hace utilidad de dispositivos electrónicos es necesario tener un control total ante amenazas de malware tanto para sus estudiantes como para el personal en sí, el fin de este proyecto es plantear técnicas para determinar qué tipo de acciones se pueden ejecutar para el control y la eliminación de los malware, identificando el tipo de amenaza de malware con el que se está lidiando y definiendo que tipo de herramienta o análisis se puede efectuar haciendo uso de una metodología a la sospecha de archivos o documentos infectados.

## 1.5 Delimitaciones.

### 1.5.1 Geográfica.

Este trabajo se desarrollará en la Universidad Francisco de Paula Santander Ocaña, en el programa de Ingeniera de Sistemas.

### 1.5.2 Temporal.

Para el desarrollo de la investigación se estimó un tiempo determinado de 3 meses.

### 1.5.3 Conceptual.

Los términos que enmarcan este proyecto son los siguientes: análisis estático, análisis dinámico, malware, metodología, técnicas.

### 1.5.4 Legal.

Este proyecto de investigación está determinado por una metodología exploratoria, donde se centrará en analizar muestras activas de malware en entornos virtuales de sistemas operativos Windows por medio de técnicas de análisis estático y dinámico de malware, para realizar un informe de recomendaciones y soluciones.

# **Capítulo 2. Marco Referencial**

## 2.1 Marco Histórico.

### 2.1.1 Local:

### 2.1.2 Nacional:

### 2.1.3 Internacional:

## 2.2 Marco Contextual.

## 2.3 Marco Conceptual.

## 2.4 Marco Teórico.

## 2.5 Marco Legal.

# **Capítulo 3. Diseño metodológico**

## 3.1 Tipo de investigación.

## 3.2 Población y muestra.

### 3.2.1 Población.

### 3.2.2 Muestra.

## 3.3 Diseño de instrumentos de recolección de la información y técnicas de análisis de datos.

## 3.4 Análisis de información.

## 3.5 Cronograma de actividades.

# **Capítulo 4. Administracion del proyecto.**

## 4.1 Recursos humanos.

### 4.1.1 Recursos humanos.

### 4.1.2 Recursos institucionales.

### 4.1.3 Recursos Financieros.

# **Referencias.**

# **Apéndices.**