Titulo:

Metodologías para la obtención y análisis de amenazas informáticas específicamente en un entorno de sistemas operativos Windows.

Justificación:

Análisis desde punto de vista

Enfocada en la solución del problema

Técnicas a utilizar

Objetivos:

Formular técnicas para determinar si archivos ejecutables contienen algún tipo de software malintencionado o no deseado.

Recomendar las mejores herramientas para el análisis de software que ayuden a evidenciar infecciones por malware e identificar su comportamiento.

Realizar el análisis a dos archivos infectados con malware aplicando algunas de las técnicas y herramientas escogidas.

Realizar un informe con los hallazgos encontrados más significativos

Objetivo general:

Reconocer diferentes tipos de amenazas de malware utilizando técnicas como análisis estático de malware y análisis dinámico de malware, haciendo uso de distintas metodologías para el análisis de archivos infectados que nos permitan entender y determinar sus comportamientos en entornos virtuales para la recomendación de soluciones óptimas

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.

Planteamiento del problema:

El análisis de malware hace referencia al arte de la detección de software malicioso, entendiendo como funcionan, como identificar y derrotar 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 Richard Rivera en su investigación: “ANÁLISIS DE CARACTERÍSTICAS ESTÁTICAS DE FICHEROS EJECUTABLES PARA LA CLASIFICACIÓN DE MALWARE” de la universidad politécnica de Madrid(España) donde analiza ciertos archivos ejecutables 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 de la especialidad en seguridad informática de la universidad de san buenaventura de la ciudad de Medellín, desarrollaron una investigación haciendo utilidad de herramientas para la detección y análisis como GetSusp, Sysinspector, Regshot para los cuales utilizan entornos virtuales para realizar las pruebas lo cual es una buena práctica, haciendo utilidad de dos malware bastante comunes para ello, en su investigación encuentran buenas técnicas para la detección de archivos en el sistema donde analizan los has y las firmas digitales.

El análisis de malware se basa en técnicas y metodologías son las que permiten entender el malware

Tecnicas: análisis estatico y análisis dinamico

Metodologias: paso a paso para efectuar el análisis estatico y a su vez el análisis dinamico.

Funcionamiento del malware:

El malware funciona en tres etapas que son:

Creación, infección, elimminacion.

Creacion:

1. Arquitectura del malware(lenguaje): se tiene en cuenta el lenguaje para desarrollar malware.
2. Objetivo del malware(funciones): que se quiere que haga el virus, si se quiere que el virus sea de tipo ranseware el cual va a encriptar la información o si se prefiere que sea un k eyloger para capturar las pulsaciones del usuario en el sistema.
3. Como hacerlo indetectable(FUD): en este paso se logra que el usuario cuando realice doble clic sobre ese archivo que se ha enviado no salte el antivirus y dañe las etapas que se han realizado.
4. Como mantenerlo indetectable: es una de las etapas más importantes, si bien se logra que el archivo ya se ejecute y permita el acceso al sistema, se debe tener en cuenta que los antivirus se actualizan cada cierto tiempo.
5. Arquitectura destino (sistema operativo):si bien es cierto que si un malware fue diseñado para el sistema operativo Windows no podrá servir para el sistema operativo Linux y viceversa para todos los demás sistemas operativos

Infección:

1. Conexión correcta y estable: es importante tener una conexión estable, pues si se requiere que la ultimación de un puerto debe ser exactamente por el cual se especificó.
2. Detección nula: en esta etapa se sigue en juego la indeteccion del malware durante el tiempo que vaya a estar efectuando las funciones que se le especifico en la etapa uno
3. Cumplimiento de objetivos: en esta etapa se obtiene la información durante el tiempo que se le haya especificado permitiendo obtener ya sea las credenciales del usuario que ingresa o las pulsaciones en el teclado, se determina si el malware a cumplido los objetivos o las funciones que se les ha establecido.
4. Beneficio económico: La mayor parte de estos ejemplos se puede ver cuando se realizan ataques con ransoware, donde el atacante encripta la maquita infecta la información luego pidiendo un rescate en bitcoin a la victima

Analisis estatico: estudiar la estructura de un archivo sin ejecutarlo, son bastante rapidas y bastante efectivas.

* Permite conocer el funcionamiento de un archivo y conocer como se comunica la maquina afectada y el atacante de manera que no se tenga que ejecutar el archivo utilizando una metodologia.
* Donde iniciar? Obtener la información del archivo sacarle el hashing y ejecutar el análisis
* Obtener la información del ejecutable: se hace relación a los ejecutable por ejemplo los ddl que se están utilizando
* Hacer la recolección de los strings, cadenas de texto que incluyen el archivo malisioso

Metodologia:

* Identificar la extencion correcta del archivo.
* Extraer el hash.
* Analizar el Hash con un motor automatizado.
* Identificar los DLL utilizados.
* Extraer los Strings del PE.

Base de datos virus total se utilizará

Que son los dll biblioteca de enlace dinamico encargados entre los intermediadores de un programa y el sistema operativo, el malware llega a utilizar mucho de los dll que se tienen en Windows el kernel32.dll se encargara de sobrescribir o modificar procesos en la memoria del sistema, wsock32.dll y el ws2\_32.dll si los encargados de la comunicación en la red de nuestro sistema cuando actúan probablemente se esté comunicando con el atacante de manera activa

Analisis Dinamico: comprender el comportamiento de una amenaza en un ambiente controlado, se tiene que ejecutar para saber como se comporta.

* Preparar el entorno
* Ejecutar el archivo
* Analizar comportamiento probar
* Detectar cambios
* Eliminar amanaza
* Recuperar el entorno

Metodologia:

* Identificar el estado inicial.
* Verificar cambios en el sistema.
* Detectar nuevos procesos.
* Detección de registros rutas modificadas.
* Conocer la comunicación del malware.
* Detectar archivos persistentes.