Marco historico:

Local:

En la actualidad, la historia del malware es muy conocida por todos los daños que pueden causar, son pocos usadas y conocidas las técnicas que se tiene para la detección de malware. En Ocaña y en la región, para la detección de malware se utiliza antivirus y software que ayudan al reconocimiento y la limpieza, muchos de estos softwares cuentan con licencias que son pagas, sin contar con que se tenga una versión pirata. Tener conocimiento sobre las técnicas, como lo son el análisis dinámico o estático puede ser útil, saber qué tipo de amenaza está afectando el ordenador, y tener la posibilidad de saber cómo encontrar una solución a este problema, como el saber reconocer la serie de patrones que utilizan cada uno de estos softwares maliciosos para comprender dónde está el problema y arrancarlo de raíz, sin la necesidad de un antivirus o del formateo del dispositivo.

En Ocaña y la Región actualmente no se ha realizado ningún trabajo relacionado con el análisis de malware ya sea dinámico o estático, pues estas prácticas son muy poco conocidas e utilizadas, en la universidad se enfoca más en el desarrollo de software, que en la seguridad informática que es otra de las múltiples ramas con las que cuenta la ingeniera de sistemas, este tipo de análisis nos permite tener seguridad en nuestros dispositivos; tener conocimiento sobre utilizar un análisis dinámico entendiendo el comportamiento de una amenaza en un ambiente controlado, considerando sobre como ejecutar la amenaza para saber cómo es su comportamiento y siguiendo una metodología para esta detección, o por el contrario si se tiene conocimiento sobre el análisis estático se puede permitir revisar el comportamiento de malware sin ejecutarlo, puesto que esta es bastante rápida y efectiva a su vez, para este también se utiliza una metodología diferente y efectiva para la recolección de información.

Por último, teniendo conocimiento de esto se es fácil decidir por cuál de los dos tipos de análisis se quiere efectuar, dependiendo del gusto o de la facilidad que se tenga, siguiendo una serie de metodologías definidas, esto nos permitiría obtener soluciones para mantener la seguridad en todos nuestros archivos y documentos.

**Nacional:**

En Colombia hay un amplio conocimiento sobre la seguridad informática y existen ciertos trabajos e investigaciones que ayudan a ampliar y fundamentar más este proyecto, puesto que hace algunos años que se está trabajando en el área de la seguridad informática, mejorándose los conocimientos y las bases teóricos planteadas en sus orígenes.

Las técnicas de detención y análisis de malware existentes en Colombia se han estudiado e investigado en la ciudad de Medellín como trabajo de grado de la universidad de San Buenaventura por un grupo de tres de estudiantes de la facultad de ingenierías.

Determinar que las herramientas SysInspector de ESET y GetSusp de McAfee pueden servir para detectar archivos infectados, ambos programas trabajan basados en reputación de los archivos y valores hash conocidos, así cuando detectan archivos del sistema modificados, archivos ejecutables con hash desconocidos informan en sus resultados estos hallazgos con el objetivo de realizar un análisis diferente. Estos archivos reportados pueden ser subidos a VirusTotal para que sea revisado automáticamente por aproximadamente 57 motores de antivirus diferentes. (Zapata Pareja, Cubides Corrales, & Murcia Guzman, 2015)

Con ello se hace referencia a la extensa forma de la utilización del análisis de malware dinámico ya que en esta se hacen uso de herramientas de software y análisis online como lo son GetSusp y Sysinspector para comprender y analizar su funcionamiento, estas herramientas sirven para detectar los archivos modificados y los hash conocidos los cuales informan sobre las posibilidades de archivos infectados en el software, mientras que los hash desconocidos son reportados y pueden ser subidos a VirusTotal para su análisis.

En el país actualmente se han obtenido nuevas técnicas que por ahora están en estado de prueba como lo es el análisis de malware basado en machine learning o el uso de la inteligencia artificial, fundamentándose en técnicas como el análisis dinámico y el estático que en un futuro será una excelente practica más efectiva y con mejores técnicas, donde se evalúan algoritmos y se utilizan una serie de clasificadores que permiten analizar si el malware es malicioso como lo estipula (Urcuqui & Navarro, 2016, p.3 ), ya que mediante ellos se pueden obtener datos de una aplicación específica, donde el reto es abstraer información para así poder clasificarla como maliciosa o benigna.

Para predecir si una aplicación es maligna se basan en una serie de estudios donde dicen que “no todos los algoritmos funcionan de manera eficiente para el mismo problema, es por ello que se consideró necesario hacer un estudio de los más adecuados, además estas herramientas requieren de un conjunto de datos para aprendizaje y pruebas” (Urcuqui & Navarro, 2016, p.2) esto para Colombia es un gran avance en seguridad informática, ya que este tipo de investigaciones nos dejan una gran visión y reto para ir construyendo un futuro inteligente y seguro.

**Internacional:**

Los primeros virus o malware eran demostraciones tecnológicas de los investigadores, en 1971 Robert Thomas crea Creeper el cual se encargaba de infectar ordenadores conectados a la red Arpanet en el que se desplegaba un mensaje, seguidamente en 1982 un estudiante del instituto Rich Skrenta crea el primer virus fuera del laboratorio, este se trataba de un código culto que infectaba ordenadores Apple II a través de diskettes, los anteriores virus no afectaban directamente el sistema operativo, mientras que en 1983 en Pensilvania (EEUU) se acuña directamente el término de virus informático, el cual constaba de un código que infectaba las maquinas específicamente con sistema operativo Unix, este se daba mediante un código oculto este se instalaba a sí mismo , replicándose en pocos minutos infectando a otras máquinas conectadas, de forma similar a un virus biológico. (BBVA OpenMind , 2017)

A finales de los 80 comenzaron a proliferar los códigos que borraban datos o inutilizaban sistemas, el llamado malwarecomenzó a diversificarse en familias diferentes: los **gusanos** son programas que se mueven de un ordenador a otro sin ocultarse en otra aplicación, mientras que los **troyanos** son programas nocivos con apariencia inocente. En 1995 aparecía WM/Concept, que infectaba documentos de Word. “Abrió la puerta para una plaga de malware**basado en documentos** que dominó el panorama de las amenazas durante varios años”, dice Harley. (BBVA OpenMind , 2017)

Los procesos donde intervienen las tecnologías de la información ha tenido un rápido desarrollo, el malware se ha ido complicando, evolucionando y mejorando; los primeros virus encontrados fueron los gusanos y los troyanos, actualmente se están dando a conocer más los virus rootkits y backdoors, han evolucionado tanto que sus características son compartidas entre varios tipos de virus razón, por la cual su taxonomía y clasificación no ha sido fácil. (Rivera Guevara, 2018, p.8)

(Zapata, Cubides, & Murcia, 2015) dicen que el malware es un programa que se inserta de forma encubierta en otro programa con la intención de destruir los datos, ejecutar programas destructivos o intrusivos, o de otra manera comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones, o el sistema operativo de la víctima citando a (NIST, 2013). (p.9)

En los últimos años malware ha tenido un gran auge convirtiéndose en la amenaza que lidera los rankings en los índices de infecciones más comunes en el host, a nivel organizacional se ha tenido que controlar y mitigar ya que sigilosamente ingresando en el ordenador hasta lograr su objetivo.

El análisis de malware está mejor documentado y estudiado actualmente, pues existen gran variedad de investigaciones, trabajos y artículos científicos de habla hispana como en otros idiomas que se han encargado de desarrollar a lo largo de los años técnicas que brinden seguridad a los ordenadores con el fin de evitar amenazas como lo dicho anteriormente.

Actualmente el análisis de malware tanto estático como dinámico son de las técnicas más utilizadas por los analistas de malware de todo el mundo, por lo cual cada quien tiene su propia metodología y su forma para analizar y estudiar los malware.

Es de destacar que el análisis estático es bastante rápido y a su vez bastante efectivo, si bien es cierto que el análisis dinámico es mucho más efectivo solo que este requiere de más tiempo, (Rivera Guevara, 2018) en su trabajo explica que “El análisis estático frecuentemente se realiza antes del análisis dinámico, ya que este último demanda más recursos, y los resultados del análisis estático pueden servir de entrada para el análisis dinámico.” (p.18), esto hace referencia al avance en tanto a las técnicas y recursos de la máquina que se invertiría para realizarlo, en ella se propone una mejor manera de mitigar estos riesgos realizando primero un análisis estático y luego el dinámico.

En el 8vo (Congreso Internacional México-Colombia CICOM, 2018) se expuso un artículo relacionado con el análisis de malware basado en agenten inteligentes lo que para mucho es el futuro del análisis de malware y de lo cual se puede decir que se necesita de un buen laboratorio para tener un ambiente controlado y a su vez poder realizar las pruebas adecuadas.

Su capacidad de ataque cada día avanza cautelosamente y con objetivos específicos para cumplir la finalidad de convertirse en una ciberamenaza, y en la actualidad el ciberespionaje (gobierno, entidades públicas, financieras, privadas entre otras.), con ánimos de lucro. Las siguientes son las áreas más significativas de la evolución del malware:

• Métodos de infección y vectores

• Persistencia

• Mecanismos de protección

• Directiva

• Interacción con el atacante

Esta evolución se convirtió en Amenazas persistentes avanzadas (APT). La característica de estas amenazas es su fragmentación, descomposición en módulos y el ensamble de piezas. (Zapata, Cubides, & Murcia, 2015, p.14)

|  |  |
| --- | --- |
| **Year** | **Number of new mallware specimen (count in millins)** |
| 2007 | 0,13 |
| 2008 | 0.89 |
| 2009 | 1,58 |
| 2010 | 2,09 |
| 2011 | 2,57 |
| 2012 | 2,64 |
| 2013 | 3,38 |
| 2014 | 5,99 |
| 2015 | 5,14 |
| 2016 | 6,83 |
| 2017 | 9,78 |

**Tabla 1.**   
Especímenes de malware por año.

**Nota.** El crecimiento de especímenes de malware desde el 2007 hasta el 2017 ha sido de las cifras más escandalosas, datos obtenidos de (Gorugantu, 2018, p.15) para ser usados como fuente de historia del malware.

Finalmente, es muy claro que cada día se avanza más cuando se habla de tecnología, a su vez el aumento de malware es notable pues según (Gorugantu, 2018) en su trabajo ,desde el año 2007 se contaban con apenas 0.13 millones de especímenes nuevos de malware hasta ese año, según (esET, 2015, p. 3) en sus laboratorios al día de todo el mundo les llegaban aproximadamente 200 mil nuevos códigos maliciosos por día, lo que da una idea de la afectación que podrían padecer los ordenadores de los usuarios y las empresas. Para el año 2017 (Gorugantu, 2018) ya se tenían aproximadamente 9.78 millones de especímenes nuevos de malware lo que es una cifra escandalosa para 10 años en los cuales se nónuplo de forma exagerada, esto nos deja ver que el conocer un poco de análisis de malware es vital y esencial para la protección de nuestros datos, el conocer por lo menos el análisis estático nos ayudara en un futuro a salvar nuestra información.

**Marco contextual:**

El contexto en el que se desarrollará este proyecto será en la zona del Catatumbo y el nororiente colombiano, en donde se encuentra ubicada la Universidad Francisco de Paula Santander seccional Ocaña, el cual cuenta dentro de sus facultades académicas con el plan educativo de ingeniera de sistemas modalidad presencial, donde se enfocan en formar profesionales analíticos en el área de las tecnologías basados en principios éticos e innovadores.

El análisis de malware es una herramienta que brinda seguridad principalmente a los archivos o documentos que se descarguen y almacenen en sus memorias, equipos de cómputo tanto personales como los de las salas con los que cuentan las instalaciones de la universidad en el programa de ingeniería de sistemas.

Es por ello que el presente proyecto se enfoca en la obtención de mecanismos de análisis de malware como lo son el análisis dinámico y el análisis estático, donde el personal académico podrá decidir con cual tipo de análisis realizar para la protección de sus archivos, por lo cual se orientará para realizarse en las salas de computo del programa académico

Marco conceptual

Los conceptos por los cuales se rige la elaboración de este proyecto son los siguientes:

El análisis según la (Real Academia Española, 2014) es la “Distinción y separación de las partes de algo para conocer su composición” de esta manera se realiza un estudio de forma detallada con el fin de identificar los componentes que en su medida afectan al ordenador. Para la identificación de estos componentes se hace necesario tener claro los conceptos y las técnicas, por las cuales se realiza el análisis en un ordenador.

Para realizar este tipo de análisis se tienen en cuenta los archivos ejecutables, los cuales son diseñados para inicializar un programa, estos contienen instrucciones precisas para realizar un tipo de tarea específica.

El análisis estático está basado en examinar los archivos ejecutables sin la necesidad de ver las instrucciones reales.

Este análisis puede confirmar si un archivo es malicioso, proporcionar información sobre su funcionalidad, y a veces proporcionan información que le permitirá producir firmas de redes simples. Es sencillo y puede ser rápido, pero es en gran medida ineficaz contra el malware sofisticado, y se puede pasar por alto comportamientos importantes. (Zapata, Cubides, & Murcia, 2015, p.77)

Este tipo de análisis se fundamenta en dos enfoques, el primero se basa en realizar un análisis al código ensamblador del malware con el fin de conseguir una mejor comprensión y funcionamiento sin tener que ejecutar el archivo, y el segundo enfoque se orienta hacia el análisis de las características del fichero, de esta manera se consiguen las características del malware para así atacarlo. (Rivera Guevara, 2018, p.15)

Según (Rivera Guevara, 2018) esto permite “revelar lo que es capaz de hacer, cómo detenerlo y conocer sus características estáticas, es decir aquellas características que no dependen de la ejecución del fichero” (p.16), mediante el uso de uno de los enfoques se revela información importante, y de esta manera poder estudiar la estructura de un archivo sin ejecutarlo, de forma más rápida y efectiva, puesto que nos permite conocer el funcionamiento y como se comunica la maquina afectada y el atacante, de esta manera se logra que no se tenga que ejecutar el archivo.

El análisis dinámico es aquel que permite comprender el comportamiento de una amenaza en un ambiente controlado, se debe ejecutar para saber su comportamiento, para ello (Zapata, Cubides, & Murcia, 2015) dicen que antes de “ejecutar el malware de forma segura, debe configurar un entorno que le permitirá estudiar el malware ejecutándose sin riesgo de daño a su sistema o red” (p.77), con el fin de observar su actividad y los cambios que produce al momento de ejecutarse y tener control de ello.

Durante el análisis dinámico de un código malicioso (Jumbo Tene, 2017) estipula las siguientes tareas:

* Análisis de los procesos en tiempo real.
* Monitorización del registro.
* Monitorización de la creación, eliminación o modificación de archivos.
* Monitorización del tráfico de red.

El software malicioso conocido con la abreviatura de Malware según (Rivera Guevara, 2018) hace referencia a “programas de software diseñados para dañar o realizar otras acciones no deseadas en un sistema informático”(p.8) es conocido por tener gran variedad de software hostiles, molestos e intrusivos en el código de programas.

La definición de malware ha variado, actualmente se tiene como un software diseñado para infiltrarse o dañar un sistema informático sin el permiso informado al dueño del ordenador. Su evolución ha sido rápida y sus características compartidas son de varios tipos, para lo cual la clasificación del mismo no ha sido algo fácil, sus principales tipos son: virus y gusanos, troyanos, rootkit, rootkit modo usuario, rootkit modo kernel, backdoors, spyware and adware, bot, ransonware, rogueware o scareware, advanced persistent threat. (Rivera Guevara, 2018, p.8)

Los métodos son las herramientas que permiten al personal de seguridad a identificar lo que se encuentra atacando el ordenador, identificando si es un malware conocido o desconocido, indagando el tipo de riesgo al que puede estar expuesto el ordenador. (Zapata, Cubides, & Murcia, 2015, p.5).

Según la (Real Academia Española, 2014) métodos es un “Procedimiento que se sigue en las ciencias para hallar la verdad y enseñarla”, en este proyecto será usado como el procedimiento a seguir para identificar el malware que afecte la ejecución de archivos.