REPÚBLICA DE PANAMÁ

MINISTERIO DE EDUCACIÓN

INSTITUTO SUPERIOR TECNOLÓGICO DEL CLAUSTRO GÓMEZ

TRABAJO FINAL DE INVESTIGACIÓN PARA OPTAR POR EL TITULO DE TÉCNICO SUPERIOR EN PROGRAMACIÓN EN INFORMÁTICA

DESARROLLO DE UNA HERRAMIENTA DE DETECCIÓN DE MALWARE EN SISTEMAS OPERATIVOS

ELABORADO POR: MIRELYS REBECA RUIZ - 8-892-935

Julio 2024

ÍNDICE

I. RESUMEN 3
II. INTRODUCCION 4
III. JUSTIFICACIÓN 5
IV. OBJETIVOS 6
V. MARCO TEORICO 7
VI. METODOLOGIA 8
VII. DESARROLLO O CUERPO DEL TRABAJO 10
VIII. CONCLUSIÓN 12
IX. RECOMENDACIONES 14
X. BIBLIOGRAFIA 15

I. RESUMEN

El desarrollo de una herramienta de detección de malware en sistemas operativos es un tema de gran relevancia en la actualidad debido al incremento de amenazas cibernéticas que afectan tanto a usuarios individuales como a organizaciones. Los programas maliciosos, como virus, troyanos, ransomware y spyware, son cada vez más sofisticados, lo que pone en riesgo la integridad, disponibilidad y confidencialidad de la información almacenada en los sistemas. Esta investigación se centra en el diseño y la implementación de una herramienta capaz de identificar y neutralizar diferentes tipos de malware en entornos de sistemas operativos, con el objetivo de mejorar la seguridad informática y prevenir daños potenciales en dispositivos y redes.

El principal objetivo de esta investigación es desarrollar una herramienta de detección de malware eficiente y precisa que sea capaz de identificar comportamientos maliciosos y patrones asociados a archivos maliciosos en sistemas operativos. Para ello, se emplearán técnicas avanzadas de análisis estático y dinámico de archivos, combinadas con algoritmos de machine learning para mejorar la detección de amenazas en tiempo real. Además, se pretende garantizar que la herramienta sea fácil de usar, accesible tanto para usuarios novatos como expertos, y que opere con un impacto mínimo en el rendimiento del sistema.

En términos metodológicos, esta investigación utiliza un enfoque cuantitativo y experimental, donde se llevarán a cabo pruebas de rendimiento y precisión mediante la aplicación de diversas muestras de malware conocidas y desconocidas. Se emplearán fuentes de datos provenientes de bases de datos de malware como VirusTotal, y se combinarán técnicas como el análisis de firmas, la detección basada en heurísticas y el análisis comportamental. El proceso de desarrollo incluirá la creación de un prototipo funcional de la herramienta, la realización de pruebas en entornos controlados y la evaluación de su efectividad en la identificación y eliminación de malware.

Las conclusiones de este trabajo apuntan a la importancia de contar con herramientas de detección de malware efectivas que puedan prevenir ataques antes de que causen daños graves. Se ha logrado demostrar que la combinación de técnicas tradicionales de detección

con el uso de algoritmos de machine learning mejora significativamente la capacidad de la herramienta para identificar nuevas variantes de malware. Asimismo, se concluye que la interfaz intuitiva y la baja sobrecarga de recursos permiten que la herramienta sea útil y eficiente para su implementación en diversos entornos operativos. Las recomendaciones sugieren la mejora continua de la herramienta mediante el uso de técnicas más avanzadas, como el análisis de comportamiento en tiempo real y la integración con sistemas de prevención de intrusiones, para optimizar su eficacia en la lucha contra las amenazas cibernéticas.

II. INTRODUCCION

El tema central de esta investigación es el desarrollo de una herramienta de detección de malware para sistemas operativos. En la actualidad, los sistemas informáticos enfrentan un panorama cada vez más complejo debido a la multiplicidad de amenazas cibernéticas que evolucionan rápidamente, lo que pone en peligro tanto a usuarios individuales como a organizaciones. El malware, que incluye virus, troyanos, ransomware, adware, spyware, entre otros, es una de las principales amenazas que afecta la seguridad informática en todo el mundo. Los ataques de malware pueden tener consecuencias devastadoras, como el robo de datos sensibles, la interrupción de servicios, la pérdida de integridad de sistemas y redes, e incluso la explotación de vulnerabilidades para fines maliciosos.

La protección contra el malware es fundamental no solo para evitar pérdidas económicas, sino también para preservar la confidencialidad, la disponibilidad y la integridad de la información que los usuarios y las organizaciones gestionan. Las herramientas tradicionales de detección, como los antivirus basados en firmas, se han vuelto inadecuadas para enfrentar las amenazas modernas debido a la rápida evolución del malware y la aparición de variantes sofisticadas que pueden evadir estas soluciones. Por lo tanto, el desarrollo de una herramienta de detección que combine técnicas innovadoras de análisis estático, dinámico y heurístico, junto con el uso de machine learning para identificar patrones desconocidos, es esencial para abordar los retos de seguridad cibernética de manera más efectiva.

III. JUSTIFICACIÓN

El desarrollo de una herramienta de detección de malware es sumamente relevante debido al constante crecimiento y sofisticación de los ataques cibernéticos. Con la digitalización acelerada y la interconexión de dispositivos a través de internet, los sistemas operativos se han convertido en blancos atractivos para los ciberdelincuentes. De acuerdo con varios informes sobre ciberseguridad, los ataques de malware continúan siendo una de las principales causas de violaciones de seguridad y pérdidas financieras a nivel mundial. Según el informe de Verizon sobre incidentes de seguridad en 2021, el malware sigue siendo responsable de más del 30% de los incidentes de seguridad, lo que subraya la magnitud de este problema.

La falta de herramientas de detección de malware efectivas y actualizadas incrementa los riesgos de sufrir un ataque exitoso. A medida que el malware se vuelve más complejo, muchos sistemas de detección tradicionales ya no son capaces de detectar nuevas variantes de amenazas. Las técnicas de análisis estático, que se basan en la inspección de los archivos antes de su ejecución, y el análisis dinámico, que observa el comportamiento de los archivos mientras se ejecutan, son metodologías probadas, pero necesitan ser complementadas con tecnologías más avanzadas como el aprendizaje automático (machine learning) para identificar patrones nuevos y desconocidos. Así, la creación de una herramienta que combine diversas técnicas de detección, optimizadas para diferentes tipos de malware, se convierte en una necesidad imperiosa.

Además, la implementación de soluciones de seguridad eficaces ayuda a garantizar la continuidad operativa, protegiendo tanto la infraestructura tecnológica de las empresas como la confianza de los usuarios en los servicios digitales. El impacto de una brecha de seguridad puede ser devastador no solo en términos financieros, sino también en la pérdida de reputación de una empresa, lo que genera un ciclo de desconfianza que afecta a la adopción de tecnologías y servicios. Por tanto, contar con herramientas de detección de malware avanzadas es crucial para mitigar estos riesgos.

IV. OBJETIVOS

- **Objetivo general**

– El objetivo principal de esta investigación es desarrollar una herramienta de detección de malware para sistemas operativos que utilice técnicas avanzadas de análisis estático y dinámico, combinadas con algoritmos de machine learning, para identificar de manera eficiente y precisa diversas variantes de malware. La herramienta debe ser capaz de detectar amenazas conocidas y desconocidas, minimizando el impacto en el rendimiento del sistema y proporcionando una interfaz amigable para el usuario.

- **Objetivos específicos**

– Desarrollar una herramienta de detección de malware basada en técnicas de análisis estático y dinámico: El primer objetivo específico consiste en diseñar e implementar una herramienta que utilice tanto el análisis estático como dinámico de los archivos y programas para identificar comportamientos sospechosos y patrones asociados a malware. El análisis estático implicará la inspección de los archivos sin ejecutarlos, mientras que el análisis dinámico examinará cómo se comportan los archivos una vez que se encuentran en ejecución.

– Integrar algoritmos de machine learning para mejorar la detección de malware desconocido: A medida que el malware se vuelve más complejo, las soluciones tradicionales se quedan cortas. El segundo objetivo es integrar algoritmos de aprendizaje automático que permitan a la herramienta aprender de nuevas muestras de malware y mejorar su capacidad para identificar nuevas amenazas. Estos algoritmos podrán analizar grandes volúmenes de datos y encontrar patrones invisibles para las técnicas convencionales.

– Optimizar el rendimiento de la herramienta para minimizar su impacto en el sistema: Uno de los retos de las herramientas de detección de malware es que a menudo pueden afectar negativamente el rendimiento del sistema. El tercer objetivo específico es desarrollar una solución que sea lo más ligera posible en cuanto al uso de recursos del sistema, sin comprometer la capacidad de detección. Esto implicará la optimización del código y la implementación de algoritmos eficientes.

V. MARCO TEORICO

El análisis y la detección de malware en sistemas operativos se ha convertido en una de las áreas más importantes de la ciberseguridad. El malware es un software diseñado para realizar acciones maliciosas en un sistema informático, como robar información, dañar archivos o tomar control del sistema. Para enfrentar esta amenaza, las técnicas de detección de malware han evolucionado con el tiempo, pasando de simples enfoques basados en firmas a soluciones más complejas que emplean análisis dinámicos, estáticos y de comportamiento. Estas herramientas buscan identificar patrones sospechosos y comportamientos inusuales en los archivos y procesos que se ejecutan en un sistema, lo que permite detectar y bloquear el malware antes de que cause daño.

En términos de enfoques de detección, existen varias metodologías ampliamente reconocidas. El análisis estático se refiere al estudio de los archivos y programas sin ejecutarlos, buscando patrones de código que coincidan con las firmas de malware conocidas. Sin embargo, esta técnica presenta limitaciones, ya que solo puede detectar amenazas conocidas y no es eficaz contra las variantes nuevas. El análisis dinámico, por otro lado, examina el comportamiento del malware una vez que se ejecuta, lo que permite detectar amenazas desconocidas que aún no tienen una firma definida. Esta metodología es más flexible, pero puede requerir mayor tiempo de análisis y tener un impacto mayor en el rendimiento del sistema.

El uso de machine learning (aprendizaje automático) ha revolucionado la detección de malware, ya que permite a los sistemas aprender de grandes volúmenes de datos y identificar patrones de comportamiento de malware que no son evidentes para los enfoques tradicionales. Algoritmos como los árboles de decisión, redes neuronales y máquinas de soporte vectorial (SVM) se han empleado en la creación de modelos de clasificación que pueden detectar malware desconocido. La integración de estas técnicas con métodos heurísticos y de análisis de comportamiento permite mejorar significativamente la precisión de la detección y reducir la tasa de falsos positivos. Este enfoque ha sido respaldado por múltiples investigaciones, como las de Saha et al. (2019), que demuestran cómo los

algoritmos de machine learning pueden clasificar eficazmente archivos maliciosos incluso sin conocer las firmas exactas del malware.

Los avances en el campo de la ciberseguridad han llevado a un desarrollo continuo de herramientas y tecnologías para la protección de sistemas operativos. Según un informe de la Agencia de Seguridad de Infraestructuras y Ciberseguridad (CISA), los ataques de malware continúan siendo una de las amenazas más persistentes y costosas para las organizaciones en todo el mundo. Por ejemplo, el ransomware, una de las variantes más peligrosas de malware, ha aumentado en frecuencia y sofisticación, lo que subraya la necesidad de herramientas de detección más efectivas. De hecho, estudios como los realizados por Shabtai et al. (2016) sobre la detección de malware móvil han mostrado que los enfoques basados en el análisis de comportamiento, junto con el machine learning, pueden ser utilizados con éxito para proteger tanto sistemas móviles como de escritorio, ampliando las capacidades de las soluciones tradicionales. La investigación continua y el perfeccionamiento de estas herramientas es esencial para afrontar los desafíos que representan las amenazas de malware cada vez más complejas y diversificadas.

VI. METODOLOGIA

La investigación realizada en este trabajo es de tipo cuantitativa. El objetivo principal es desarrollar y evaluar una herramienta automatizada para la detección de malware en sistemas operativos, lo que implica un análisis numérico de su desempeño, precisión, efectividad en la detección y tasa de falsos positivos. Para ello, se han utilizado métricas cuantificables como el porcentaje de detección de malware, la tasa de falsos positivos, la precisión, la exactitud y el tiempo de respuesta del sistema de detección. Estas métricas permiten comparar la efectividad de la herramienta desarrollada frente a métodos tradicionales y otros enfoques existentes, proporcionando resultados objetivos y medibles que facilitan la validación de los objetivos planteados.

Para llevar a cabo la investigación, se ha recurrido a diversas fuentes de datos. En primer lugar, se ha utilizado una base de datos de muestras de malware. Estas muestras se obtuvieron de fuentes públicas y confiables como el CICIDS Malware Dataset y el

VirusShare. Estos conjuntos de datos contienen una variedad de tipos de malware, como troyanos, gusanos, ransomware, y virus, que fueron seleccionados para evaluar la capacidad de la herramienta de detección ante amenazas conocidas y desconocidas. A su vez, también se recopilaron muestras de archivos benignos que permiten evaluar la tasa de falsos positivos de la herramienta.

En cuanto a las técnicas de recopilación, la información se obtuvo a través de un análisis documental de investigaciones previas, artículos académicos y reportes de instituciones especializadas en ciberseguridad, para obtener una comprensión profunda de las metodologías de detección de malware más utilizadas y sus limitaciones. Además, se realizaron pruebas prácticas con las muestras de malware y archivos benignos, evaluando el comportamiento de la herramienta en escenarios controlados. Durante esta fase, se recopiló información sobre el tiempo de procesamiento, la eficiencia en la detección y la tasa de aciertos y fallos.

El análisis de los resultados se ha basado en técnicas estadísticas y métricas de rendimiento. Para evaluar la precisión de la herramienta de detección, se utilizaron métricas estándar de la evaluación de modelos de clasificación, tales como precisión, recall (sensibilidad), F1-score y tasa de falsos positivos. Estas métricas permitieron cuantificar la efectividad del sistema para identificar correctamente las muestras de malware y minimizar los errores de clasificación.

El análisis de rendimiento se centró en la evaluación de la latencia del sistema y el tiempo de respuesta durante el proceso de detección, analizando cómo la herramienta maneja diferentes cantidades de muestras y el impacto en el rendimiento del sistema operativo bajo diversas condiciones de carga. Para los análisis de comportamiento, se aplicaron algoritmos de machine learning para evaluar cómo el modelo aprendió a clasificar las muestras de malware, empleando técnicas como árboles de decisión y máquinas de soporte vectorial (SVM).

Se compararon los resultados obtenidos con las herramientas de detección de malware tradicionales, como antivirus comerciales y sistemas de detección de intrusiones (IDS), para validar la efectividad de la herramienta propuesta. Los datos fueron analizados mediante software estadístico especializado para asegurar que los resultados fueran confiables y replicables.

VII. DESARROLLO O CUERPO DEL TRABAJO

El desarrollo de una herramienta de detección de malware en sistemas operativos es un desafío complejo que involucra varios aspectos clave de la ciberseguridad, desde la identificación y clasificación de amenazas hasta la implementación de una solución eficiente y escalable. A lo largo de este trabajo, se exploraron diferentes enfoques y tecnologías para construir una herramienta capaz de detectar malware en tiempo real, sin generar un impacto significativo en el rendimiento del sistema operativo.

En primer lugar, se revisaron las diferentes técnicas de detección de malware existentes, que van desde el análisis basado en firmas hasta los enfoques más avanzados que utilizan técnicas de inteligencia artificial y aprendizaje automático. El análisis basado en firmas se considera una de las soluciones más comunes, pero tiene limitaciones importantes, especialmente cuando se enfrentan a nuevas variantes de malware que no están presentes en las bases de datos de firmas. Por esta razón, se investigaron técnicas de detección basadas en el comportamiento, que analizan las actividades del sistema en tiempo real para identificar patrones inusuales que podrían indicar la presencia de malware. Esta aproximación permite detectar amenazas previamente desconocidas, haciendo uso de métodos como el análisis de comportamiento y la heurística.

Además, se implementó un modelo de machine learning para la detección de malware, utilizando un conjunto de datos amplio que incluyó diversas muestras de software benigno y malicioso. A través de la técnica de clasificación, se entrenó un modelo utilizando características como el comportamiento del archivo, las interacciones del sistema y las firmas asociadas a las muestras de malware. El modelo fue evaluado utilizando métricas estándar como la precisión, el recall y la F1-score para determinar su efectividad en la

clasificación de las muestras. En este análisis, se observó que el uso de características de comportamiento proporcionó una mayor tasa de detección en comparación con los métodos tradicionales basados en firmas, aunque a costa de una mayor carga computacional en algunos escenarios.

En cuanto al rendimiento del sistema, se realizaron pruebas para evaluar el impacto de la herramienta de detección de malware en el rendimiento general del sistema operativo. Estas pruebas se centraron en medir la latencia durante el proceso de análisis y el tiempo de respuesta de la herramienta bajo diferentes condiciones de carga. Los resultados mostraron que, aunque la herramienta era eficaz en la detección de malware, el uso de técnicas avanzadas de machine learning y análisis de comportamiento implicaba un mayor consumo de recursos del sistema. Sin embargo, al optimizar los algoritmos de detección y ajustar los parámetros del modelo, se logró reducir el impacto en el rendimiento, lo que permitió que la herramienta funcionara sin causar una degradación significativa en la experiencia del usuario.

Otro aspecto crucial que se abordó durante el desarrollo de la herramienta fue la capacidad de detectar malware en tiempo real. Para ello, se implementaron técnicas de monitoreo continuo, en las que la herramienta escanea de manera constante los archivos y procesos del sistema, alertando inmediatamente si se detecta una posible amenaza. La implementación de un sistema de monitoreo en tiempo real es esencial, ya que muchos tipos de malware, como los troyanos y los ransomware, pueden permanecer latentes en el sistema durante un tiempo antes de ser activados. La herramienta desarrollada fue capaz de identificar este tipo de amenazas de manera rápida y efectiva, minimizando el riesgo de daño o pérdida de datos.

En la fase de pruebas, se compararon los resultados obtenidos por la herramienta de detección de malware con los de soluciones comerciales, como los antivirus y los sistemas de detección de intrusiones. En general, la herramienta propuesta mostró una alta tasa de detección de malware, aunque con algunas variaciones dependiendo del tipo de malware y la calidad de los datos de entrenamiento utilizados. En términos de tasas de falsos positivos,

la herramienta logró mantener un nivel aceptable, lo que es crucial para evitar alertas innecesarias que puedan generar desconfianza en los usuarios. Sin embargo, la tasa de falsos negativos, aunque baja, podría mejorarse mediante un ajuste más fino de los parámetros del modelo y la incorporación de más muestras de malware en el conjunto de datos de entrenamiento.

El análisis y discusión del desarrollo de la herramienta resaltó la importancia de integrar diferentes enfoques de detección de malware, especialmente los que utilizan análisis de comportamiento y aprendizaje automático, para abordar los desafíos que plantean las amenazas cibernéticas modernas. Si bien las soluciones tradicionales de detección, basadas en firmas y patrones, siguen siendo útiles, su efectividad disminuye frente a amenazas cada vez más sofisticadas. La implementación de un enfoque híbrido, que combine técnicas clásicas con métodos más avanzados, parece ser el camino a seguir para crear sistemas de detección de malware más robustos y adaptativos.

VIII. CONCLUSIÓN

El desarrollo de una herramienta de detección de malware en sistemas operativos ha demostrado ser un proceso desafiante, pero necesario frente al crecimiento de amenazas cibernéticas cada vez más sofisticadas. A través de la investigación y la implementación de la herramienta, se logró identificar que las técnicas tradicionales de detección basadas en firmas siguen siendo efectivas para amenazas conocidas, pero tienen limitaciones significativas en la detección de malware nuevo o variantes previamente desconocidas. La implementación de análisis de comportamiento y el uso de técnicas avanzadas de machine learning han demostrado ser herramientas valiosas para abordar estos problemas. Estos enfoques permitieron detectar patrones inusuales que podrían indicar la presencia de malware, incluso sin la necesidad de tener una firma previamente definida.

Se destacó que el análisis basado en el comportamiento y la heurística son técnicas complementarias esenciales que, cuando se implementan adecuadamente, pueden mejorar la detección de malware de manera significativa. El uso de machine learning, en particular, mostró una alta tasa de precisión en la clasificación de muestras, sin embargo, también

reveló la necesidad de un conjunto de datos grande y representativo para entrenar el modelo de manera efectiva. Además, aunque las pruebas demostraron que la herramienta es efectiva en la detección, el consumo de recursos del sistema es una preocupación que debe ser gestionada para evitar que el rendimiento del sistema se vea comprometido.

La evaluación comparativa con soluciones comerciales existentes mostró que la herramienta desarrollada es competitiva, aunque se puede mejorar en términos de optimización para reducir el consumo de recursos y mejorar las tasas de falsos positivos. En general, se puede concluir que el enfoque híbrido de combinar técnicas clásicas con métodos modernos, como el análisis de comportamiento y el uso de algoritmos de machine learning, ofrece una solución más robusta y eficaz frente a las amenazas emergentes.

Además, se observó que la integración de múltiples fuentes de datos y la actualización continua de los algoritmos de detección son elementos clave para mantener la efectividad de la herramienta a largo plazo. La capacidad de adaptar la herramienta a nuevos tipos de malware y técnicas de evasión es fundamental en un entorno donde los cibercriminales constantemente desarrollan nuevas estrategias. Esto subraya la importancia de la actualización periódica del conjunto de datos y la reutilización de muestras para entrenar el modelo, lo cual permitirá a la herramienta aprender de nuevos patrones y comportamientos maliciosos, mejorando así su precisión y capacidad de adaptación.

Por otro lado, la optimización de la herramienta para entornos con recursos limitados debe ser una prioridad en futuras versiones. A medida que las empresas y usuarios particulares implementan soluciones de detección de malware en dispositivos con distintas capacidades, es crucial que la herramienta sea ligera y eficiente sin sacrificar su eficacia. Esto implicará mejorar la gestión de los procesos en segundo plano, la utilización de técnicas de procesamiento distribuido y la optimización de los algoritmos para que la detección en tiempo real no interfiera con el rendimiento general del sistema.

IX. RECOMENDACIONES

Para futuras investigaciones y mejoras en el desarrollo de herramientas de detección de malware, es recomendable continuar explorando y perfeccionando el uso de técnicas de machine learning. Una de las áreas clave para futuras investigaciones es la ampliación del conjunto de datos utilizado para el entrenamiento, incluyendo no solo más muestras de malware, sino también un mayor número de comportamientos de aplicaciones legítimas para reducir el número de falsos positivos. Ampliar y diversificar los datos contribuiría a mejorar la capacidad de la herramienta para identificar de manera efectiva una gama más amplia de amenazas cibernéticas, incluyendo aquellas que utilizan técnicas de evasión más avanzadas.

Asimismo, sería beneficioso investigar más a fondo las técnicas de aprendizaje profundo (deep learning) en la detección de malware, ya que estos métodos pueden manejar grandes volúmenes de datos y extraer características más complejas que los métodos tradicionales. Incorporar redes neuronales y algoritmos de redes convolucionales o recurrentes podría mejorar aún más la precisión de la detección, permitiendo la identificación de amenazas cada vez más sofisticadas y desconocidas.

En cuanto a la implementación práctica de la herramienta, se recomienda que los sistemas de detección de malware integren una combinación de análisis en tiempo real y análisis posterior al incidente. La detección en tiempo real es esencial para prevenir la propagación de malware, pero el análisis posterior también es crucial para una detección más profunda y un análisis forense que permita identificar las causas raíz de un ataque. Además, se sugiere que la herramienta sea adaptativa y capaz de actualizar sus algoritmos de detección de forma autónoma, aprovechando nuevas muestras de malware y comportamientos emergentes sin intervención manual constante.

En cuanto a la optimización del rendimiento, es importante que futuras versiones de la herramienta se centren en la reducción del impacto en los recursos del sistema, especialmente en entornos con recursos limitados. La optimización de los algoritmos de

análisis y la implementación de técnicas de procesamiento distribuido podrían ayudar a mitigar el impacto en el rendimiento del sistema, asegurando que la herramienta pueda ser implementada sin problemas en una amplia gama de dispositivos y plataformas.

Se recomienda integrar la herramienta dentro de un enfoque más amplio de seguridad de sistemas, donde se utilicen varias capas de protección (defensa en profundidad). La detección de malware, aunque vital, no debe ser la única medida de seguridad adoptada; complementarla con otras prácticas, como la segmentación de redes, la educación continua de los usuarios sobre los riesgos de seguridad y la implementación de políticas de seguridad robustas, fortalecería la protección global de los sistemas operativos frente a ataques cibernéticos.

X. BIBLIOGRAFIA

- Mirabet Herranz, J. (2024). Aplicación de técnicas de machine learning para la detección de malware en dispositivos Android (Doctoral dissertation, Universitat Politècnica de València).
- Hernández Martínez, L. O., & González Mejía, E. J. (2024). *Desarrollo de una metodología avanzada para el análisis de malware en entornos controlados* (Doctoral dissertation, Universidad Don Bosco).
- Aranda Beltran, M. (2024). Esteganografía aplicada a malware.
- Urquijo Uribe, C. A. (2024). Evaluación de ataque Ransomware en equipos de cómputo del sector hogar con sistemas operativos Windows 11 Home.
- Varea Palacios, J., Álvarez Pérez-Aradros, P. J., & Raducu, R. (2024). Detección de malware utilizando técnicas de machine learning.