**TRABAJO RELACIONADOS**

El artículo de Akhtar y Feng [8] investiga el uso de algoritmos de aprendizaje automático, tales como Decision Trees (DT), Convolutional Neural Networks (CNN) y Support Vector Machines (SVM), para la detección de malware. Los resultados demuestran que tanto DT como CNN alcanzaron precisiones superiores al 98%, destacando su superioridad frente a las técnicas tradicionales de detección. En una línea similar, la investigación de Gyamfi y Čenys [9] ofrece una revisión de las técnicas de detección de malware a nivel de sistema mediante aprendizaje automático.

Por otro lado, Gorment y Selamat [12] presentan una revisión y clasificación de los algoritmos de aprendizaje automático aplicados a la detección de malware. Este artículo evalúa la efectividad de varios métodos, discute los desafíos actuales y propone direcciones futuras para la investigación en este campo.

Selamat y Ali [13] se centran en comparar diferentes técnicas de detección de malware mediante algoritmos de aprendizaje automático, incluyendo Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees y Naive Bayes. El estudio evalúa el rendimiento de estas técnicas en términos de precisión, tasa de falsos positivos y tiempo de procesamiento, además de discutir los desafíos y limitaciones de cada una.

Djenna y Marou [10] explora un enfoque dinámico basado en inteligencia artificial para abordar la creciente amenaza del malware similar al Vinayakumar y Alazab [14]. Los autores presentan un modelo híbrido que combina métodos de aprendizaje profundo y heurísticos para la detección y clasificación de malware, abarcando tipos como adware, Radware, rootkits, malware de SMS y ransomware. Ellos investigan el uso de técnicas avanzadas de aprendizaje profundo para la detección de malware. Los estudios detallan cómo las redes neuronales profundas, incluidas las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN), pueden identificar y clasificar malware con mayor eficacia que los métodos tradicionales, destacando su capacidad para aprender características complejas y adaptarse a nuevas variantes y amenazas.

Gandotra y Sofat [11] realizan un análisis profundo de las técnicas de análisis y clasificación de malware, subrayando cómo el malware puede modificar su código para evadir las técnicas tradicionales basadas en firmas. Este artículo revisa tanto técnicas de análisis estático como dinámico y destaca la importancia de los patrones de comportamiento en la clasificación del malware mediante aprendizaje automático, mostrando una mejora significativa en comparación con los métodos tradicionales.

**TRABAJO PROPUESTO**

El trabajo propuesto sigue las reglas de Kitchedjam y comienza con la formulación de preguntas de investigación. Estas preguntas guían el estudio y mantienen el enfoque en los objetivos. Así, el estudio avanza de forma clara y ordenada, cumpliendo las metas establecidas.

1. ¿Cómo han evolucionado las técnicas de detección de malware en los últimos cinco años?
2. ¿Qué desafíos enfrentan los desarrolladores al implementar software de seguridad inteligente?
3. ¿Existen diferencias significativas en la efectividad de este software entre diferentes sistemas operativos?
4. ¿Qué papel juegan las actualizaciones de software en la mejora de la detección y prevención de malware?
5. ¿Cómo se comparan los métodos de detección basados en firmas con los métodos basados en comportamiento en términos de precisión y eficiencia?
6. ¿Qué impacto tienen las técnicas de aprendizaje automático en la detección de malware?

**JUSTIFICACIÓN**

En la actualidad, el malware representa una de las amenazas más significativas en el ámbito digital. Este software malicioso tiene la capacidad de infiltrarse en sistemas informáticos y redes, provocando una amplia gama de problemas para individuos, empresas y gobiernos. Dado que los ataques de malware se están volviendo cada vez más sofisticados y diversos, es fundamental llevar a cabo un estudio exhaustivo sobre este fenómeno. Este proyecto tiene como objetivo comprender con mayor profundidad cómo el malware explota las vulnerabilidades de los sistemas y evaluar la eficacia de las diversas técnicas de detección disponibles [22], [23].

Este trabajo es importante porque:

* **El malware sigue creciendo constantemente:** Los ciberataques son cada vez más frecuentes, y el malware se mantiene como una de las principales amenazas. Los hackers continuamente desarrollan nuevas técnicas de ataque, lo que subraya la necesidad de mantenerse a la vanguardia en la protección y detección de malware [49], [51].
* **Las consecuencias de un ataque de malware son graves:** Un ataque de malware puede provocar pérdidas financieras significativas, la filtración de datos personales y la interrupción de servicios críticos. Estos impactos no solo afectan a grandes corporaciones, sino que también pueden repercutir en la vida cotidiana de individuos y empresas [55], [56].
* **Las técnicas tradicionales de detección están quedando obsoletas:** Anteriormente, la detección de malware se basaba en la búsqueda de firmas conocidas. Sin embargo, debido a la aparición de amenazas nuevas y desconocidas, es esencial adoptar métodos más avanzados que puedan identificar estas nuevas formas de ataque [48], [50].
* **El objetivo es aportar una guía útil y actualizada:** Este proyecto tiene como meta desarrollar una guía que refleje las vulnerabilidades más comunes y las mejores prácticas para la detección de malware. La intención es que esta guía sea valiosa tanto para académicos en ciberseguridad como para profesionales en el campo.

**¿Qué beneficios esperamos?**

1. Entender mejor dónde están los huecos: Si identificamos las vulnerabilidades que el malware suele aprovechar, los expertos en seguridad podrán crear mejores defensas.
2. Ver qué métodos de detección funcionan mejor: Vamos a analizar las diferentes técnicas que se usan para detectar malware y ver cómo se pueden combinar para hacerlas más efectivas.
3. Proponer nuevas formas de protegernos: Basándonos en lo que descubramos, queremos sugerir estrategias para que las organizaciones puedan defenderse mejor de los ataques.
4. Mejorar la seguridad en general: Si las empresas y organizaciones aplican lo que aprendamos en este proyecto, esperamos que puedan fortalecer sus defensas contra futuros ataques.