Inteligencia Artificial Aplicada al Análisis de Malware: Desarrollo de Modelos Avanzados para la Detección y Mitigación de Amenazas Cibernéticas

Daniel Bustamante Lagart
Universidad Instituto Artek, Ciudad de México, México
Carrera en Ingeniería en Ciberseguridad y Auditoría informática

Nota del autor

Daniel Bustamante Lagart, área de Ciberseguridad y auditoría informática con matrícula ACM30299.

Como autor de esta investigación, mi compromiso radica en explorar las fronteras de la ciberseguridad mediante el desarrollo de sistemas de Inteligencia Artificial especializados en el análisis de malware. Esta investigación representa un esfuerzo por avanzar en la protección de entornos digitales, ofreciendo soluciones innovadoras y contribuyendo al fortalecimiento de la seguridad informática en la era de las amenazas cibernéticas.

Cualquier mensaje con respecto a este artículo debes ser enviado al correo: daniel.bustamante@artek.edu.mx

Índice

Introducción....3
Planteamiento del problema....4
Marco Teórico....5
1.ANÁLISIS DE MALWARE....5
1.1.DEFINICIÓN, TIPOS Y EVOLUCIÓN DEL MALWARE....5
1.2.TÉCNICAS DE DETECCIÓN DE MALWARE....6
1.3.TÉCNICAS AVANZADAS DE OCULTAMIENTO QUE USA EL MALWARE....6
1.4.ANÁLISIS ESTÁTICO....7
1.5.ANÁLISIS DINÁMICO....7
1.6.INGENIERÍA INVERSA....7
2.INTELIGENCIA ARTIFICIAL PARA EL ANÁLISIS DE MALWARE (MACHINE LEARNING)....8
2.1.ALGORITMOS DE INTELIGENCIA ARTIFICIAL PARA EL ANÁLISIS DE MALWARE:....8
2.2.DATOS PARA LA EVALUACIÓN DE CADA ALGORITMO.....10
2.3.EVALUACIÓN DE ALGORITMOS....11
Hipótesis....12
Objetivos....13
Experimentación y recopilación de datos....14
1.Extracto de encabezados PE para el análisis de malware con Inteligencia Artificial....14
2.Entrenamiento de la Inteligencia Artificial y evaluación de efectividad....15
3.1.Inicio de la herramienta para hacer el análisis de los archivos binarios.....16
3.2.Ir a la web de la herramienta que tiene nuestra Inteligencia Artificial.....16
3.3.Subir el malware Lagarcry.exe llamado D2L-Desktop.exe para tratar de engañar al analizador.....17
3.4 Resultados del Lagarcry.exe (Detecto que efectivamente es malware).....17
3.5 Subir ZoomInstaller.exe con el objetivo de apreciar si se equivoca la IA.....18
3.4 Los resultados están correctos porque ZoomInstaller.exe no es un malware....18
Análisis....19
Conclusiones....20
Bibliografía....21

Introducción

En la actual era digital, el imparable crecimiento de las amenazas cibernéticas plantea un desafío constante para la seguridad de la información. Entre estas amenazas, el malware ha evolucionado de manera significativa, adoptando tácticas cada vez más sofisticadas para eludir las medidas tradicionales de detección y mitigación. La Inteligencia Artificial (IA) emerge como una herramienta esencial en la defensa contra estas amenazas, proporcionando soluciones avanzadas para el análisis de malware.

Imaginemos una situación concreta: una empresa especializada en eliminar malware recibe una llamada de una empresa de software que ha sufrido un hackeo. La información personal de la empresa está siendo robada, y nuestro equipo comienza una investigación exhaustiva. Revisamos los registros de los sistemas afectados, escaneamos en busca de vulnerabilidades, reparamos brechas de seguridad y utilizamos software especializado para detectar y eliminar malware. En un golpe de suerte, identificamos un Spyware llamado Lagartcry.exe y lo eliminamos de los sistemas. Además, implementamos firmas para que los antimalware realicen una limpieza automática en toda la red de la empresa. Todo parece resuelto, pero dos días después, la empresa nos vuelve a llamar. A pesar de nuestras acciones, siguen detectando actividad maliciosa.

La situación nos desconcierta, ya que hemos seguido las prácticas estándar para eliminar malware. Sin embargo, recordamos que la Inteligencia Artificial puede proporcionar una capa adicional de análisis. El análisis de malware, que tradicionalmente se ha realizado de manera estática y dinámica, ahora se beneficia enormemente de la implementación de técnicas de IA.

El análisis estático se centra en desensamblar los componentes del malware sin ejecutarlo, mientras que el análisis dinámico observa el comportamiento del malware en tiempo real para obtener información valiosa. A pesar de sus ventajas, estas técnicas enfrentan desafíos significativos, como el error humano y la creciente sofisticación de las amenazas cibernéticas.

La introducción de la IA en el análisis de malware ha sido un avance crucial en la industria de la ciberseguridad. Herramientas que emplean machine learning han demostrado reducir los fallos en la detección y mejorar la comprensión del funcionamiento de los malwares. En este estudio, exploramos cómo la convergencia entre la Inteligencia Artificial y el análisis de malware no solo fortalece las defensas digitales, sino que también proporciona respuestas más rápidas y efectivas ante amenazas persistentes y evolutivas en la sociedad digital.

Planteamiento del problema

La ciberseguridad se ha posicionado como una prioridad crítica en la era digital, donde el aumento exponencial de las amenazas cibernéticas desafía constantemente la integridad y confidencialidad de la información. En este contexto, el malware, con su evolución constante en tácticas avanzadas como Inteligencia Artificial, ofuscamiento, empaquetadores y lenguajes de programación no convencionales se vuelve difícil de contrarrestar, emerge como una amenaza persistente capaz de eludir las medidas tradicionales de detección y mitigación. A pesar de los esfuerzos iniciales para erradicar malware específico, como en el caso de Lagartcry.exe, la recurrencia de ataques similares subraya la necesidad de un enfoque más avanzado y adaptativo.

Esta situación se agrava al observar el aumento significativo de ataques con malware dirigidos a instituciones de gobierno, empresas y personas individuales, generando alarma en la comunidad de ciberseguridad. Con más de 77 millones de ataques a empresas a nivel mundial, representando un aumento del 37% respecto al año pasado, y notables incrementos del 170% en Asia y del 164% en LATAM, la necesidad de abordar la ciberseguridad de manera innovadora y efectiva se vuelve apremiante.

El ransomware, como principal ciberataque empresarial, ha afectado a millones de organizaciones con su modalidad de secuestro de información y la exigencia de un rescate económico. En particular, México ha experimentado 80,000 millones de intentos de ciberataques en 2023, generando pérdidas económicas significativas. El Barómetro de Riesgo de Allianz proyecta que en 2024, el costo promedio por robo de datos a empresas superará los 5 millones de dólares.

A pesar de la creciente amenaza, las herramientas actuales para detectar, analizar y combatir el malware se han mostrado ineficaces y poco adaptables a las nuevas tecnologías, principalmente debido a la mala calidad de sus análisis de malware. En este contexto crítico, mi investigación va a explorar cómo la Inteligencia Artificial Aplicada al Análisis de Malware puede proporcionar respuestas más efectivas y adaptativas, superando las limitaciones de los enfoques convencionales y garantizando una mayor seguridad en la infraestructura digital en constante evolución.

Marco Teórico

1.ANÁLISIS DE MALWARE

Para comprender a fondo el contexto de esta investigación, es esencial comenzar con conceptos básicos que faciliten la comprensión de las complejidades del análisis de malware.

1.1.DEFINICIÓN, TIPOS Y EVOLUCIÓN DEL MALWARE

Definición: La palabra “malware” es una contracción de “software malicioso”. El malware es un software intruso que está diseñado deliberadamente para provocar daños en equipos y sistemas informáticos.

Tipos.

Ransomware: Es un tipo específico de malware que se encarga de evitar que el usuario tenga acceso a su propia información (documentos, videos, imágenes, archivos) a través de la encriptación de dichos archivos.

Spyware: El atacante o hacker utiliza este tipo de malware para monitorear la actividad de los usuarios en internet. A través de un spyware es posible recolectar información sensible

Gusanos: Los gusanos informáticos tienen el objetivo de replicarse. Es decir, al infectar un dispositivo buscan pasar al siguiente, ya sea para dañar los sistemas informáticos o para robar información de los usuarios.

Troyanos: Este software malicioso le debe su nombre al famoso relato del caballo de Troya, ya que se trata de un virus que se esconde en un software que aparenta ser confiable.

Adware: El adware tiene la tarea de bombardear nuestro dispositivo con anuncios publicitarios no deseados.

Botnets: También llamados redes de robots, equipos o de códigos, los botnets son aquellos que se encargan de ejecutar un malware de forma simultánea utilizando varias computadoras.

Rootkits:Los Rootkits son utilizados para suplantar los permisos y controles de administrador con la finalidad de tomar el control de un sistema operativo por completo sin levantar ningún tipo de alerta del antivirus o software antimalware.

1.2.TÉCNICAS DE DETECCIÓN DE MALWARE

Detección de firmas: Es el enfoque clásico en el que se basaron los productos antivirus cuando surgieron. Funciona comparando los archivos almacenados o descargados en el equipo contra una lista de códigos maliciosos conocidos.

Detección de patrones / cadenas: Es una técnica utilizada en ciberseguridad para identificar software malicioso (malware) basándose en la identificación de patrones específicos en el código o el comportamiento del programa.

Análisis heurístico: El análisis heurístico es un método de detección de virus mediante el cual se examina el código en busca de propiedades sospechosas. Se diseñó para detectar virus nuevos desconocidos y versiones modificadas de las amenazas existentes (Usa algoritmos de IA para detectar anomalías).

1.3.TÉCNICAS AVANZADAS DE OCULTAMIENTO QUE USA EL MALWARE

Extensiones VBE: Es un formato de archivo que permite incrustar scripts de Visual Basic for Applications (VBA) en documentos de Microsoft Office. Al utilizar esta técnica, el malware puede ocultar su código malicioso dentro de documentos legítimos y aprovechar la ejecución de scripts permitida por las aplicaciones de Office.

PowerShell: PowerShell es una interfaz de línea de comandos y un lenguaje de scripting desarrollado por Microsoft. Los atacantes a menudo utilizan scripts de PowerShell para ejecutar comandos maliciosos en sistemas comprometidos debido a su versatilidad y capacidad para evadir las soluciones de seguridad tradicionales.

Redes Tor/I2p: Tor (The Onion Router) e I2p (Invisible Internet Project) son redes diseñadas para proporcionar anonimato y privacidad en línea. Algunos malware utilizan estas redes para ocultar la comunicación entre el sistema infectado y los servidores de comando y control.

Técnicas mixtas (twitter, facebook, github): Algunos malware utilizan plataformas de redes sociales como Twitter, Facebook o GitHub para alojar o recibir comandos maliciosos. Estos comandos pueden ser encriptados o camuflados en el tráfico normal de estas plataformas.

404: Algunos malware utilizan respuestas HTTP 404 (páginas no encontradas) para ocultar la comunicación con servidores de comando y control. En lugar de enviar solicitudes directas, el malware puede utilizar técnicas que parezcan solicitudes de error 404 para comunicarse.

Análisis del entorno: Algunos malware realizan análisis del entorno antes de ejecutar sus cargas útiles. Esto implica verificar variables del sistema, configuraciones y entorno de ejecución para adaptarse y evitar la detección.

WMI: WMI es una infraestructura de gestión de Windows que permite a los administradores realizar tareas de administración en sistemas locales y remotos. Los atacantes pueden utilizar WMI para ejecutar comandos maliciosos de forma remota, lo que dificulta la detección.

1.4.ANÁLISIS ESTÁTICO

El análisis estático de malwares es un conjunto de técnicas que permiten estudiar, prever y observar el funcionamiento de este tipo de softwares sin necesidad de ejecutarlos. El análisis se hace por medio de la revisión del código fuente del archivo y la identificación de elementos maliciosos en el mismo. De este modo, un analista puede hacerse una idea de las tareas que ejecuta el malware en un sistema sin correr el riesgo de infectar el ordenador con este.

1.5.ANÁLISIS DINÁMICO

Los análisis dinámicos son realizados en máquinas virtuales preparadas para ejecutar malwares dañinos y demostrar su funcionamiento en tiempo real. Se diferencian del análisis estático de malwares en que en los análisis dinámicos se ejecuta el software malicioso y se le permite que ejecute tareas dañinas en un entorno virtual controlado.

1.6.INGENIERÍA INVERSA

La ingeniería inversa es un proceso por medio del cual los analistas de malware ejecutan el software con su código fuente ensamblado, para poder ver el paso a paso de cada una de sus tareas. Este método combina las dos fases anteriores y ofrece un análisis detallado acerca del funcionamiento del virus.

Sin embargo, la ingeniería inversa es diferente al análisis estático de malwares en cuanto a que se ejecuta el programa a la vez que se estudia su código fuente. Es decir, se observan las miles de peticiones que hace el software de manera detenida y, por lo tanto, son análisis que pueden tomar varias semanas o meses. La principal desventaja de esta fase es su duración, que podría ser más larga de lo necesario para reparar las acciones de un virus.

2.INTELIGENCIA ARTIFICIAL PARA EL ANÁLISIS DE MALWARE (MACHINE LEARNING)

2.1.ALGORITMOS DE INTELIGENCIA ARTIFICIAL PARA EL ANÁLISIS DE MALWARE:

- Funcionamiento: Es un algoritmo de clasificación que predice la probabilidad de que una instancia pertenezca a una categoría específica. Utiliza la función logística para realizar esta clasificación binaria.
- Aplicación en Análisis de Malware: Puede emplearse para predecir la probabilidad de que un archivo sea malicioso o no. Se puede entrenar con conjuntos de datos etiquetados para aprender patrones y características asociadas al malware.

Máquinas de Vectores de Soporte (SVM):

- Funcionamiento: SVM busca un hiperplano que mejor separe las instancias de diferentes clases en un espacio multidimensional. Puede manejar datos no lineales mediante el uso de "kernels".
- Aplicación en Análisis de Malware: SVM puede utilizarse para clasificar archivos en benignos y maliciosos. Su capacidad para manejar datos no lineales lo hace útil para identificar patrones complejos asociados al malware.

K-Vecinos Más Cercanos (KNN):

- Funcionamiento: Clasifica una instancia según la mayoría de las clases de sus k vecinos más cercanos en el espacio de características.
- Aplicación en Análisis de Malware: Puede usarse para clasificar archivos según la similitud de sus características con archivos previamente etiquetados. Funciona bien en situaciones donde los archivos maliciosos tienden a tener características similares.

Naive Bayes:

- Funcionamiento: Basado en el teorema de Bayes, asume independencia entre las características. Es particularmente eficaz y rápido.
- Aplicación en Análisis de Malware: Puede aplicarse para calcular la probabilidad de que un archivo sea malicioso dados sus atributos. Es útil cuando se necesita una solución rápida y efectiva.

Árboles de Decisión:

- Funcionamiento: Divide iterativamente los datos en función de las características para llegar a una decisión. Puede manejar relaciones no lineales.
- Aplicación en Análisis de Malware: Se puede utilizar para construir un modelo que clasifique archivos en benignos o maliciosos basándose en características específicas.

Bosques Aleatorios:

- Funcionamiento: Es un conjunto de árboles de decisión que trabajan juntos. Cada árbol vota por la clase, y la clase con más votos se elige.
- Aplicación en Análisis de Malware: Su capacidad para manejar múltiples características y evitar el sobreajuste puede ser valiosa para clasificar archivos de manera precisa.

Modelos de Redes Neuronales:

- Funcionamiento: Basados en el funcionamiento del cerebro humano, estos modelos aprenden a partir de datos mediante capas de nodos interconectados.
- Aplicación en Análisis de Malware: Pueden ser eficaces para capturar patrones complejos y no lineales en grandes conjuntos de datos de análisis de malware, pero pueden requerir entrenamiento extenso y datos significativos.

2.2.DATOS PARA LA EVALUACIÓN DE CADA ALGORITMO.

Para realizar una evaluación de cada algoritmo debemos tener en dataset que contenga malware y software benigno, el dataset es importante para entrenar los modelos, a continuación les dejaré un link donde pueden descargar los que se usaron en esta investigación (https://www.kaggle.com/datasets/amauricio/pe-files-malwares) contiene más de 19,611 archivos combinados entre malware y software benigno

VirusShare_a878ba26000edaac5c98eff4432723b3	23117	144	3	0	4
VirusShare_ef9130570fddc174b312b2047f5f4cf0	23117	144	3	0	4
VirusShare_ef84cdeba22be72a69b198213dada81a	23117	144	3	0	4
VirusShare_6bf3608e60ebc16cbcff6ed5467d469e	23117	144	3	0	4
VirusShare_2cc94d952b2efb13c7d6bbe0dd59d3fb	23117	144	3	0	4
VirusShare_eff7676f69be2b519f3424def92d3590	23117	80	2	0	4

Imagen 1. Tabla de como se ve el Dataset

2.3.EVALUACIÓN DE ALGORITMOS

Ya que entrenamos los modelos tenemos los resultados, previamente ya los juntamos para hacer una representación más sencilla de entender.

Modelo	Exactitud	Precisión	Sensibilidad	Medida-F1	Media CV	Tiempo de entrenamiento (s)
Regresión logística	0.9992	0.9991	0.9994	0.9992	0.9992	0.6570
KNN con K=1	**0.9999**	**1.0000**	**0.9999**	**0.9999**	0.9998	0.0140
KNN con K=3	0.9998	0.9999	0.9997	0.9998	0.9997	0.0140
KNN con K=5	0.9998	0.9999	0.9996	0.9998	0.9996	0.0140
KNN con K=7	0.9997	0.9999	0.9994	0.9997	0.9996	0.0140
KNN con K=9	0.9996	0.9999	0.9993	0.9996	0.9996	0.0150
Árbol de decisión	0.9998	0.9998	0.9998	0.9998	0.9999	0.2680
Bosques aleatorios	**0.9999**	**1.0000**	**0.9999**	**0.9999**	**1.0000**	5.7740
Naive Bayes	0.9969	0.9954	0.9985	0.9969	0.9968	0.0490
SVM	0.9996	0.9995	0.9997	0.9996	0.9996	6.6873
MLP	0.9999	0.9999	0.9998	0.9999	0.9998	7.5092

Imagen2. Tabla de como se desempeñan los algoritmos

En la tabla podemos observar que los mejores resultados (exactitud y precisión) lo obtuvieron los Bosques Aleatorios y KNN con K-1 por su forma de clasificación, uno de los peores evaluados fueron las redes bayesianas (Naive bayes), falta un proceso más de análisis para tener conclusiones finales.

Modelo	VP	FP	VN	FN
Regresión logística	17450	16	17348	11
KNN con K=1	17457	0	17364	4
KNN con K=3	17456	1	17363	5
KNN con K=5	17454	1	17363	7
KNN con K=7	17451	1	17363	10
KNN con K=9	17449	1	17363	12
Árbol de decisión	17458	3	17361	3
Bosques aleatorios	17459	0	17364	2
Naive Bayes	17435	81	17283	26
SVM	17456	8	17356	5
MLP	17459	0	17364	2

Imagen3. Tabla de verdaderos positivos y falsos positivos

VP(Verdaderos positivos, FP(Falsos positivos) por lo que la conclusión final es que efectivamente los mejores resultados para el análisis de malware son de Bosques Aleatorios y KNN con K-1 por lo que en está investigación probaremos si en verdad funciona alguno de ellos.

Hipótesis

Mi hipótesis se basa específicamente en que utilizando el algoritmo de Bosques Aleatorios, ofrecerá una mejora significativa en la detección y clasificación de amenazas cibernéticas. Se espera que los Bosques Aleatorios, al aprovechar la diversidad de múltiples árboles de decisión, puedan capturar patrones complejos y adaptarse eficazmente a la evolución constante de las tácticas de malware. La capacidad inherente de los Bosques Aleatorios para manejar conjuntos de datos complejos y evitar el sobreajuste podría resultar en un enfoque robusto y preciso para enfrentar las crecientes amenazas cibernéticas, proporcionando así una defensa avanzada en el ámbito de la ciberseguridad.

También se espera que los Bosques Aleatorios sean capaz de detectar un malware con técnicas avanzadas, en está investigación usaremos un malware creado por el Ingeniero Daniel Bustamante Lagart llamado lagarcry.exe que espía sistemas, el cual no lo detectan los anti malware convencionales. Otra cosa que usaremos es el instalador de zoom ya que lagarcry está basado en ingeniería inversa de esa software. Debe ser capaz la IA de detectar si es maligno uno y el otro no.

Objetivos

Lo que deseo lograr en está investigación es:

- Demostrar la efectividad de la Inteligencia Artificial para encontrar malware avanzado.
- Determinar el porcentaje de verdaderos positivos de los Bosques Aleatorios.
- Encontrar un correcto extractor de encabezados PE para el análisis de malware con Inteligencia Artificial.

Todo esto para enseñarle al campo de la ciberseguridad que los hackers éticos debemos de generar herramientas igual de potentes para protegernos y no solo eso, también ir migrando nuestro segmento al área de Inteligencia Artificial para poder superar a los ciberdelincuentes actuales.

“a grandes problemas, grandes soluciones grandes” Hipócrates (469 a. C. -377 a.)

Experimentación y recopilación de datos

1.Extracto de encabezados PE para el análisis de malware con Inteligencia Artificial

Para realizar este paso en específico nos encontramos con un gran problema la mayoría de extractores no son compatibles con la inteligencia artificial porque generan datos diferentes con el que se entrenó la Inteligencia Artificial, por lo que se tuvo que hacer Ingeniería Inversa para poder crear la propia herramienta en python que nos ayude a completar este paso importante para la evaluación de los Bosques Aleatorios. Herramienta original: http://www.pe-explorer.com/

Resultados de la herramienta:

```
PS C:\Users\danie\OneDrive\Documentos\Proyecto Análisis de malware web> & C:/Users/danie/
Proyecto Análisis de malware web/IA/Reporte PE.py"
e_magic: 0x5a4d
e_cblp: 0x90
e_cp: 0x3
e_crlc: 0x0
e_cparhdr: 0x4
e_minalloc: 0x0
e_maxalloc: 0xffff
e_ss: 0x0
e_sp: 0xb8
e_csum: 0x0
e_ip: 0x0
e_cs: 0x0
e_lfarlc: 0x40
e_ovno: 0x0
e_oemid: 0x0
e_oeminfo: 0x0
e_lfanew: 0x100
Machine: 0x8664
```

Imagen4. Herramienta de extracción PE creada por el alumno

Los datos recopilados que obtuvimos con está herramienta son necesarios para el análisis del malware para nuestra Inteligencia Artificial de Bosques Aleatorios.

2.Entrenamiento de la Inteligencia Artificial y evaluación de efectividad

En el paso 2 nos concentramos en crear el script de la Inteligencia Artificial, el entrenamiento con datos de más de 200,000 malwares, también de la extracción de 0los porcentajes de éxito que tiene y por último exportar la IA entrenada en un archivo para usarlo con el script del PE

Resultados del entrenamiento de la IA Bosques Aleatorios.

```
Number of used features: 75
              precision    recall  f1-score   support

  Not Malware       0.99      0.96      0.98      1003
      Malware       0.99      1.00      0.99      2920

     accuracy                           0.99      3923
    macro avg       0.99      0.98      0.98      3923
 weighted avg       0.99      0.99      0.99      3923
```

Imagen5. Datos del Bosque aleatorio y su efectividad

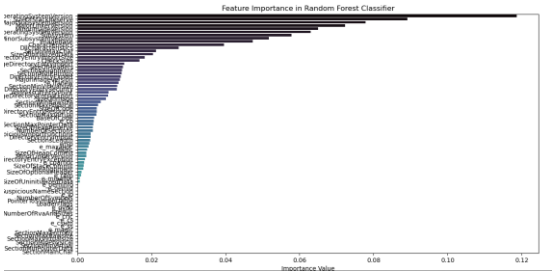

Imagen6. Características de datos para evaluar malware

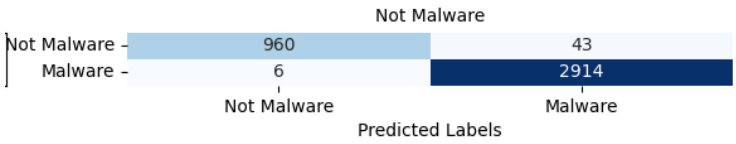

Imagen7. Predicted labs sobre el malware y softare beningno

Análisis de resultados.

Los resultados arrojaron que tuvo un 0.99 de precisión siendo el 1 el 100%, podemos ver que en la gráfica extrae características que le hacer sospechar a la IA que Binario es un malware, con esto sabemos que nuestro entrenamiento si es efectivo porque detecta con casi nulo error el malware.

3.Pruebas con malware avanzado y binarios benignos

Para el paso 3 nos concentramos en mejorar la interfaz de nuestra IA y la herramienta de extracción de encabezados PE, es la prueba definitiva para averiguar si la IA puede detectar el malware lagarcry,exe y el instalador de zoom, los resultados que se esperan son que a lagarcry le ponga malware y al otro no.

Necesitamos el malware lagarcry.exe(D2L-Desktop.exe) y al ZoomInstaller.exe.

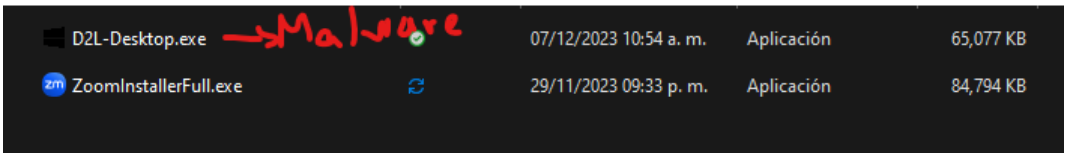

Imagen8. Los 2 archivos con los que haremos la prueba

3.1.Inicio de la herramienta para hacer el análisis de los archivos binarios.

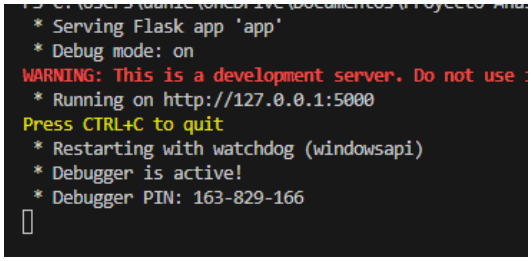

Imagen9. Iniciar el servicio de flask para usar la herramienta

3.2.Ir a la web de la herramienta que tiene nuestra Inteligencia Artificial.

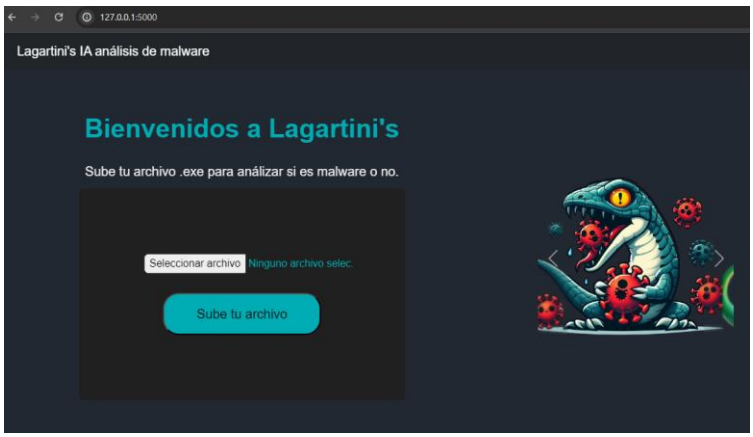

Imagen10. Herramienta funcionando

3.3.Subir el malware Lagarcry.exe llamado D2L-Desktop.exe para tratar de engañar al analizador.

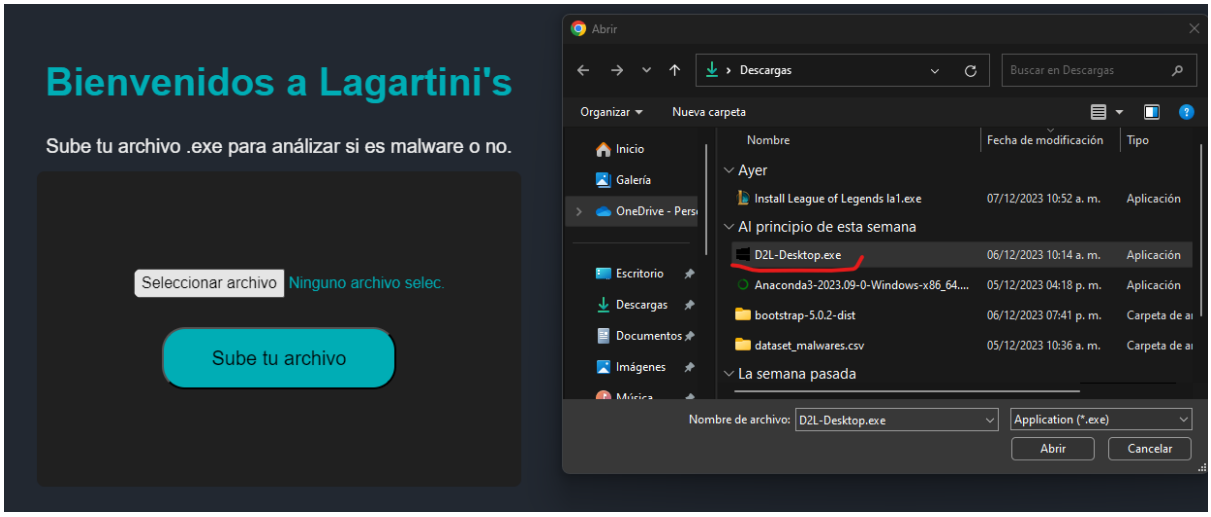

Imagen11. Seleccionar el lagart.cry

3.4 Resultados del Lagarcry.exe (Detecto que efectivamente es malware).

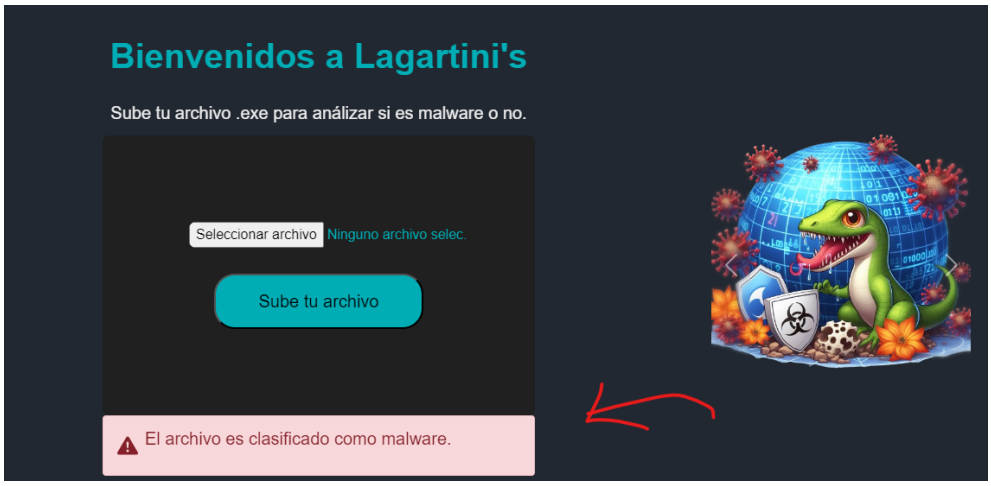

Imagen12. Resultado del análisis

3.5 Subir ZoomInstaller.exe con el objetivo de apreciar si se equivoca la IA.

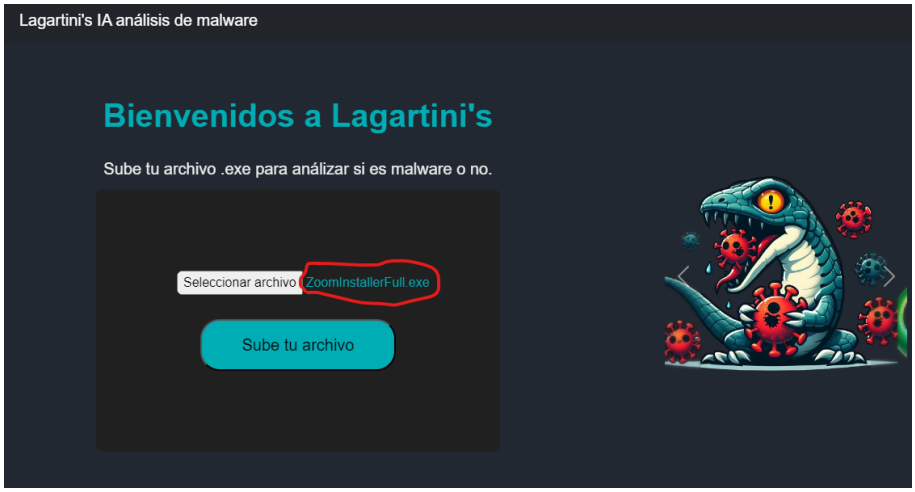

Imagen13. Selecciona el instalador de zoom

3.4 Los resultados están correctos porque ZoomInstaller.exe no es un malware

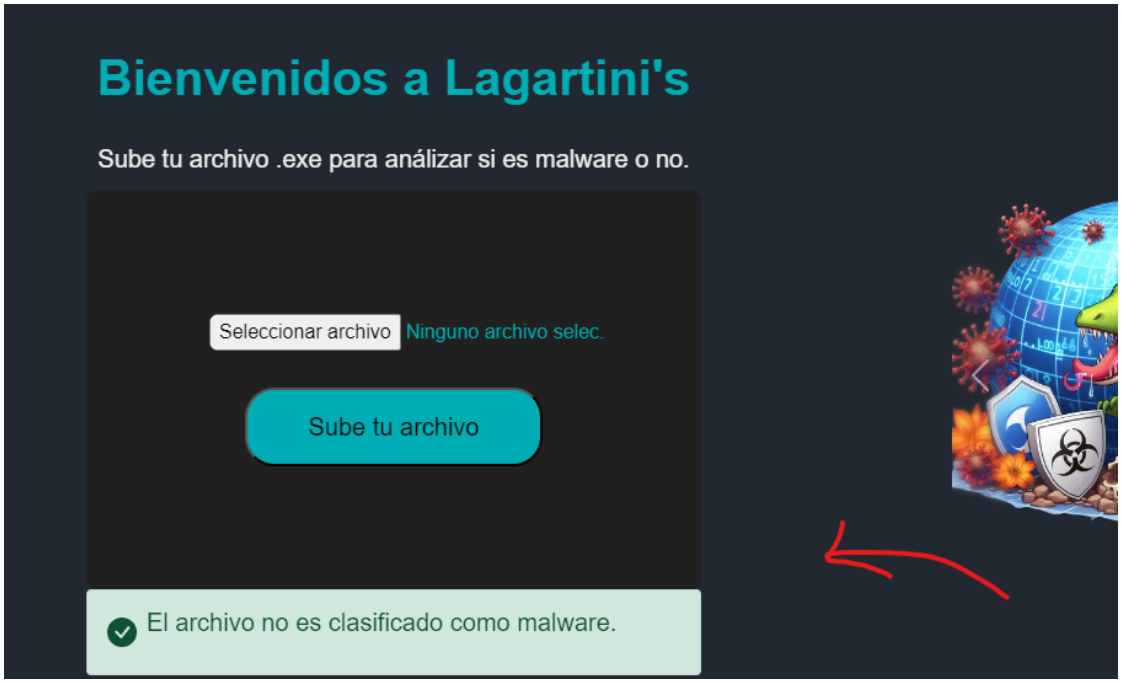

Imagen 14. Resultado del análisis

Análisis

La herramienta que acabamos de crear para comprobar el si el funcionamiento de la Inteligencia Artificial dio muy buen rendimiento y sobre todo logró detectar malware muy avanzado, supo diferenciar entre un software benigno y maligno.

Al crear un nuevo script para sacar los PE lo vuelve mucho más controlable que usar algunos que ya están obsoletos en el mercado, por lo que en general esta parte dio buenos resultados.

La inteligencia a su vez si cumplio lo prometido, su porcentaje de detección si es mayor del 99% y la recopilación de datos en está sección nos ayudó a sacar nuestras conclusiones sobre el objetivo de la investigación.

Lagarcry.exe fue detectado con éxito ahora los cibernautas estarán seguros y prevenidos contra mí malware espía (Spyware) lagartcry.exe, posiblemente si probamos con más podríamos detectarlos pero no quiero comprometer mi equipo de trabajo.

En pocas palabras, la experimentación y recopilación de datos destacan la creación de la herramienta integral que combina un extractor de encabezados PE y la IA de Bosques Aleatorios. La efectividad de esta herramienta se demuestra con la detección exitosa de un malware avanzado, Lagarcry.exe, y la diferenciación precisa con un instalador de software benigno.

Conclusiones

En la incesante batalla contra las amenazas cibernéticas, esta investigación destaca la importancia de la Inteligencia Artificial (IA) en el análisis de malware. El crecimiento exponencial de ataques sofisticados exige soluciones avanzadas, y la convergencia entre IA y ciberseguridad emerge como un baluarte crucial.

El estudio abordó las limitaciones de las técnicas convencionales, como el análisis estático y dinámico, destacando la necesidad de un enfoque más adaptativo. El malware, evolucionando con tácticas como inteligencia artificial, ofuscación y lenguajes no convencionales, desafía las medidas tradicionales.

El aumento alarmante de ataques, especialmente de ransomware, evidencia la urgencia de soluciones innovadoras. Las herramientas actuales se han mostrado ineficaces, impulsando la investigación hacia la aplicación de IA al análisis de malware.

Explorando algoritmos como Bosques Aleatorios, Máquinas de Vectores de Soporte, K-Vecinos Más Cercanos, Naive Bayes, Árboles de Decisión y Modelos de Redes Neuronales, se identificó la relevancia de cada uno en el análisis de malware.

La hipótesis sobre la eficacia de los Bosques Aleatorios se respalda con resultados notables. La herramienta creada, combinando la IA entrenada con un extractor PE personalizado, demostró una precisión del 99%. Se evaluaron diversos algoritmos, destacando Bosques Aleatorios y KNN por su rendimiento superior.

El análisis específico de Lagartcry.exe y ZoomInstaller.exe validó la capacidad de la IA para diferenciar entre malware avanzado y software benigno. El sistema brindó respuestas rápidas y precisas, mejorando la seguridad cibernética.

En conclusión, esta investigación no solo subraya la importancia de la Inteligencia Artificial en la defensa contra el malware, sino que también proporciona una herramienta práctica y eficaz para la detección y análisis avanzado de amenazas cibernéticas. El camino hacia una ciberseguridad más robusta y adaptativa reside en la integración continua de la IA en nuestras defensas digitales.

Bibliografía

Staff, F. (2022, August 2). México registra 80,000 millones de intentos de ciberataques en 2022. Forbes México. https://www.forbes.com.mx/mexico-registra-80000-millones-de-intentos-de-ciberataques-en-2022/

Ehrhardt, M. (2023, January 18). Ciberataques e inflación, lo que más preocupa alas empresas. dw.com. https://www.dw.com/es/ciberataques-e-inflaci%C3%B3n-lo-que-m%C3%A1s-preocupa-a-las-empresas/a-64430159

Jiménez, M. M. (n.d.). Casos de ciberataques a empresas en 2022. https://www.piranirisk.com/es/blog/ciberataques-empresas-en-2022

7 formas en las que tus dispositivos se pueden infectar con malware. (2021, January 5). https://www.welivesecurity.com/la-es/2021/01/05/formas-comunes-dispositivos-pueden-infectarse-con-malware/

Software anti-malware frente a software antivirus: ¿Qué diferencia hay? (2023, April 19). www.kaspersky.es. https://www.kaspersky.es/resource-center/preemptive-safety/malware-remover-vs-antivirus-software

Malwarebytes. (2020, June 3). ¿Es lo mismo antimalware y protección antivirus? Malwarebytes. https://es.malwarebytes.com/antivirus/

Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa | Empresas | INCIBE. (n.d.). https://www.incibe.es/empresas/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

¿Qué es XDR? (n.d.). Trend Micro. https://www.trendmicro.com/es_mx/what-is/xdr.html

KeepCoding, R. (2022, August 23). Análisis estático de malwares | KeepCoding Bootcamps. KeepCoding Bootcamps. https://keepcoding.io/blog/analisis-estatico-de-malwares/

¿En qué consiste el análisis heurístico? (2023, August 18). www.kaspersky.es. https://www.kaspersky.es/resource-center/definitions/heuristic-analysis

Chavez, J. J. S. (2023, October 3). ¿Qué es un malware? Tipos y cómo funcionan. https://deltaprotect.com/blog/tipos-de-malware

Técnicas avanzadas de ocultamiento de malware. (2017, March 7). [Slide show]. PPT. https://es.slideshare.net/dfpluc/tecnicas-avanzadas-de-ocultamiento-de-malware

PE Explorer: EXE File Editor, DLL View Scan Tool for 32-bit Windows PE files. (n.d.). http://www.pe-explorer.com/

Karthikapadmanaban. (2023, February 15). Malware Detection using Random Forest. Kaggle. https://www.kaggle.com/code/karthikapadmanaban/malware-detection-using-random-forest/input

Samuel Mouro González (A Coruña, septiembre de 2022.). Técnicas de aprendizaje máquina para análisis de malware. https://ruc.udc.es/dspace/bitstream/handle/2183/32112/MouroGonzalez_Samuel_TFG_2022.pdf?sequence=3