NOTA DE PRENSA

UNIR desarrolla una técnica más rápida y eficiente para detectar el malware con Inteligencia Artificial

- **Investigadores de la Universidad Internacional de La Rioja (UNIR) participan en el proyecto que ha logrado un sistema para clasificar familias de software malicioso, que mejora la defensa contra los ciberataques y supone un avance significativo en la aplicación de la IA a la ciberseguridad.**

- **Este enfoque combina técnicas de aprendizaje profundo con un análisis semántico, una intersección poco explorada en la literatura científica previa, lo que subraya la novedad de la investigación.**

Logroño/Madrid, 22 de mayo de 2025.-

Una investigación en la que ha participado la **Universidad Internacional de La Rioja** (UNIR) ha desarrollado una nueva técnica que posibilita, gracias a la Inteligencia Artificial, una detección de malware más rápida, eficiente y capaz de adaptarse a las nuevas amenazas con mayor agilidad.

Esta técnica utiliza redes neuronales convolucionales (CNN), un sistema de aprendizaje automático inspirado en el cerebro humano, para clasificar familias de malware con una precisión del 99.54%. Para ello se enfoca en el análisis de las partes funcionales -o semánticas- de los archivos ejecutables Portable Executable (PE), el formato predominante en Windows.

El estudio demuestra que, en lugar de analizar la totalidad del archivo, centrarse en partes específicas como la cabecera, el código o los datos, permite alcanzar una precisión de clasificación comparable e incluso superior a los sistemas tradicionales, con menos recursos computacionales y reduciendo significativamente los tiempos de procesamiento.

La industria de la ciberseguridad y las empresas pueden beneficiarse de esta técnica para mejorar su defensa contra el malware, optimizar sus recursos de seguridad y adaptarse a un paisaje de amenazas cibernéticas en constante evolución.

El malware (o software malicioso) es cualquier tipo de programa informático diseñado para infiltrarse en un dispositivo (ordenador, teléfono móvil, tableta, etc.) sin el consentimiento del propietario y realizar acciones dañinas, como el robo de información personal (contraseñas, datos bancarios, etc.), el cifrado de archivos para exigir un rescate (ransomware), el envío de spam o el espionaje de la actividad del usuario, entre otros.

"Al utilizar la segmentación semántica, particularmente enfocándonos en el encabezado de los archivos PE, se logró una precisión excepcional del 99.54% en la clasificación de malware. Esto resalta la eficacia de identificar patrones distintivos en los encabezados que pueden ser cruciales para diferenciar entre familias de malware", explica **Javier Bermejo Higuera**, investigador de UNIR y uno de los autores de la investigación. Los otros autores proceden del Systems Development Center de Brasilia y la Universidad Camilo José Cela.

Bermejo explica que "la cabecera contiene patrones y firmas únicas que caracterizan a las diferentes familias de malware, por lo que emplear datos extraídos de partes específicas de los archivos PE, en lugar de utilizar secuencias de bytes completas, permite una reducción en el número de parámetros entrenables en las redes neuronales, lo que puede llevar a modelos más eficientes sin sacrificar el rendimiento".

Este enfoque combina técnicas de aprendizaje profundo con un análisis semántico, una intersección poco explorada en la literatura científica previa, lo que subraya la novedad de la investigación.

"Dado que los atacantes a menudo utilizan técnicas como el polimorfismo, cifrado, empaquetado, etc. para evadir sistemas de detección, mejorar los métodos de clasificación y detección con un enfoque semántico tiene el potencial de ofrecer soluciones más robustas ante las variantes emergentes de malware", asegura el investigador de UNIR.

Principales beneficios

Esta técnica ofrece adaptabilidad a diferentes entornos y formatos de archivo (como PE y ELF), ayuda a reducir los falsos positivos, lo que permite a los equipos de seguridad enfocarse en amenazas reales, y mejora la eficiencia operativa al optimizar el uso de recursos. Así, los principales beneficios son:

-Mayor precisión y menos falsos positivos: La alta precisión alcanzada, especialmente con el análisis de la cabecera, puede reducir significativamente el número de falsas alarmas, permitiendo a los equipos de seguridad centrarse en las amenazas reales.

-Detección más rápida: Al analizar solo una porción del archivo, el tiempo necesario para clasificar un potencial malware se reduce drásticamente, lo que posibilita una respuesta más ágil ante incidentes de seguridad.

-Optimización de recursos: La capacidad de lograr una alta precisión con menos datos implica un menor consumo de recursos computacionales, lo que facilita la implementación de estos sistemas en entornos con limitaciones de hardware.

-Adaptabilidad a nuevas amenazas: La naturaleza del aprendizaje profundo permite que el modelo se adapte continuamente a las nuevas variantes de malware, mejorando su capacidad de detección a lo largo del tiempo.

Este estudio presenta un avance significativo en la aplicación de la Inteligencia Artificial a la ciberseguridad. Al demostrar el valor informativo de las partes semánticas de los archivos ejecutables, allana el camino hacia sistemas de detección de malware más inteligentes, rápidos y eficientes, que fortalezcan la defensa contra las ciberamenazas del futuro.

Referencia bibliográfica:

Martins, E., Bermejo-Higuera, J., Sant'Ana, R., Bermejo-Higuera, J.R., Sicilia-Montalvo, J. A., Piedrahita-Castillo, D. Semantic Malware Classification Using Artificial Intelligence Techniques. *Computer Modeling in Engineering & Sciences* 2025, 142(3), 3031-3067. https://doi.org/10.32604/cmes.2025.061080

SOBRE UNIR:

UNIR es una universidad que ofrece una educación superior de calidad a través de las tecnologías más innovadoras, siempre con el estudiante en el centro de su actividad. En España, imparte 55 grados, 155 másteres oficiales, 83 títulos propios y 4 programas de doctorado que tienen como objetivo acercar una educación integral y personalizada a los más de 90.000 estudiantes que trabajan en sus aulas presenciales-virtuales desde un centenar de naciones, principalmente en España e Hispanoamérica. Su método de enseñanza, adecuado a las demandas del mercado laboral, hace de UNIR una auténtica palanca social que rompe barreras y ayuda a que cada uno, esté donde esté, cumpla sus sueños de formación y de progreso personal y profesional. UNIR pertenece al grupo educativo Proeduca, que, junto a otros centros de enseñanza superior y no reglada, atiende a más de 105.000 estudiantes.

PARA MÁS INFORMACIÓN

Departamento de Comunicación UNIR comunicacion@unir.net www.unir.net
Sala de prensa: http://www.unir.net/sala-de-prensa/ Twitter: @UNIRUniversidad y @PrensaUNIR

Paloma Gamarra (La Rioja) 94 121 02 11 ext. 1285 paloma.gamarra@unir.net
Sara Puerto 648 573 733 sara.puerto@unir.net
Isabel Álvarez 639 117 638 isabel.alvarezcastro@unir.net
Diego Caldentey (LATAM) 659 641 848 diego.caldentey@unir.net
José María Fillol (LATAM) 628 902 302 josemaria.fillol@unir.net
Bosco Martín (Director) bosco.martin@unir.net