//UCIENCIA/23
CONVENCIÓN CIENTÍFICA INTERNACIONAL

Temática: III Taller Internacional de Ciberseguridad

Malware Detection using Machine Learning Algorithms for Windows Platform

Detección de malware mediante algoritmos de aprendizaje automático para la plataforma Windows

Vladimir Milián Núñez [1*]

[1] Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños km 2 ½, . vmilian@uci.cu

[*] Autor para correspondencia: vmilian@uci.cu

Resumen
Windows es un sistema operativo popular basado en interfaz gráfica de usuario que brinda servicios como almacenamiento, ejecución de software de terceros, reproducción de videos, conexión de red, etc. El malware es una de las principales preocupaciones de seguridad para la plataforma Windows. Malware es cualquier tipo de software informático que perturba la disponibilidad de los servicios informáticos. Los sistemas de detección tradicionales, como sistema de detección/prevención de intrusos, software antivirus, etc., no pueden detectar malware oculto debido al uso de métodos basados en firmas. Por lo tanto, existe la necesidad de detectar con precisión este tipo de malware en el

entorno de Windows. En este trabajo, se presenta un sistema de detección de malware basado en Machine Learning (ML) que extrae características del encabezado de los archivo Portable Executable para detectar si el ejecutable es malicioso o no. Después de preprocesar los datos, se aplican varios modelos ML para hacer detectar el malware. Además, se lleva a cabo un análisis comparativo entre los modelos de ML para seleccionar el apropiado para el problema objetivo. Los resultados experimentales muestran que Random Forest superó a los demás con un nivel de precisión del 99,44% para la detección de malware. Esto se puede usar para desarrollar una aplicación de escritorio para escanear el malware para la plataforma Windows con la capacidad adicional de personalizar el proceso de escaneo.

Palabras clave: *Aprendizaje Automático, Ejecutable Portable, malware*