

**UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO**

FACULTAD DE CIENCIAS DE LA INGENIERÍA

SOFTWARE (REDISEÑO)

**Malware Informático:**

**Análisis de Vulnerabilidades y**

**Técnicas de Detección**

**PROYECTO DE INVESTIGACIÓN**

**Redacción Técnica**

**3ro semestre**

**AUTORES:**

FREDDY VLADIMIR FARINANGO GUANDINANGO

ELIZABETH ANAHIS BURGOS CHILAN

ANDY EMANUEL MENDOZA MOREIRA

**QUEVEDO LOS RÍOS**



JULIO, 2024

**TABLA DE CONTENIDO**

**RESUMEN:**

**INTRODUCCIÓN**

En la era digital, el malware sigue siendo una amenaza persistente y en evolución para la seguridad de la información. El malware, o software malicioso, abarca varios programas dañinos diseñados para infiltrarse, dañar o deshabilitar computadoras y redes. La sofisticación y variedad de los ataques de malware han aumentado, haciendo de este un área crítica de estudio para profesionales e investigadores en ciberseguridad. Esta introducción tiene como objetivo proporcionar una visión general de las vulnerabilidades explotadas por el malware y las técnicas empleadas para detectar y mitigar estas amenazas, basándose en la investigación científica más reciente en el campo.

Analizar las vulnerabilidades dirigidas por el malware y evaluar la efectividad de varias técnicas de detección de malware.

Los ataques de malware pueden llevar a pérdidas financieras significativas, violaciones de datos y interrupciones en los servicios, afectando a individuos, organizaciones y gobiernos. La necesidad de este estudio radica en su potencial para mejorar la comprensión de los comportamientos del malware y mejorar los mecanismos de detección para desarrollar defensas proactivas y minimizar el impacto de los ataques de malware.

Investigaciones previas han cubierto extensamente diferentes aspectos de la detección de malware y el análisis de vulnerabilidades. Una revisión sistemática de la literatura sobre técnicas de detección de malware en Windows destaca la evolución de los métodos de detección desde los basados en firmas hasta los basados en comportamiento y enfoques de aprendizaje automático [1]. Otros estudios se centran en identificar y clasificar el comportamiento del malware para mejorar la precisión de la detección [2]. El análisis de malware basado en la web proporciona información sobre los métodos utilizados para defenderse contra estos tipos específicos de amenazas [3]. La caracterización de las vulnerabilidades del hipervisor arroja luz sobre los riesgos asociados con los entornos virtualizados y la necesidad de defensas específicas [4]. El análisis estadístico y la inteligencia artificial también han sido explorados como métodos prometedores para la detección de malware, ofreciendo una mejor precisión y adaptabilidad [5], [6], [7].

EL estudio plantea la hipótesis de que la integración de múltiples técnicas de detección puede mejorar significativamente la precisión y eficiencia de la detección de malware. Las variables investigadas incluyen los tipos de malware, las vulnerabilidades que explotan y los métodos de detección empleados. La metodología de investigación implica una revisión exhaustiva y síntesis de la literatura existente, estudios de casos de ataques de malware y análisis de técnicas de detección utilizando métodos estadísticos y de aprendizaje automático.

. Los enfoques basados en comportamiento y aprendizaje automático han mostrado promesas en la identificación de malware previamente desconocido al analizar patrones de comportamiento y aprovechar grandes conjuntos de datos para entrenar modelos de detección [1], [5], [6]. Se ha sugerido que la integración de estos métodos con sistemas de monitoreo y respuesta en tiempo real puede mejorar la postura general de seguridad [3].

Los principales hallazgos de la literatura revisada indican que ningún método de detección es infalible. Sin embargo, un enfoque multifacético que combine técnicas basadas en firmas, comportamiento y aprendizaje automático puede proporcionar una defensa más robusta contra el malware [2], [5]. Además, entender las vulnerabilidades específicas explotadas por diferentes tipos de malware es esencial para desarrollar defensas y estrategias de mitigación específicas [4].

Aunque se han logrado avances significativos en la detección de malware, es necesario continuar con la investigación y el desarrollo para mantenerse a la vanguardia de las amenazas en evolución. La integración de tecnologías avanzadas como el aprendizaje automático y la inteligencia artificial en los sistemas de detección ofrece vías prometedoras para mejorar las medidas de seguridad [6].

**CAPITULO I**

* **TRABAJO RELACIONADOS**
* **TRABAJO PROPUESTO**
* **MATERIALES Y METODOS**
* **RESULTADOS Y DISCUCIÓN**
* **CONCLUCIONES Y RECOMENDACIONES**
* **REFERENCIAS**

Referencias

1. P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, “A systematic literature review on Windows malware detection: Techniques, research issues, and future directions,” *Journal of Systems and Software*, vol. 209, Mar. 2024, doi: 10.1016/j.jss.2023.111921.
2. T. Zhang and Institute of Electrical and Electronics Engineers, *2011 3rd International Conference on Computer Research and Development : ICCRD 2011 : March 11-15, 2011, Shanghai, China*.
3. J. Chang, K. K. Venkatasubramanian, A. G. West, and I. Lee, “Analyzing and defending against web-based malware,” *ACM Comput Surv*, vol. 45, no. 4, Aug. 2013, doi:

10.1145/2501654.2501663.

1. Xingming. Sun, A. Association for Computing Machinery. Special Interest Group on Security, Hangzhou shi fan da xue, Shanghai jiao tong da xue, Zhejiang da xue, and

Nanjing da xue, *Cloud Computing ’13 : proceedings of the 2013 International Workshop on Security in Cloud Computing : May 8, 2013, Hangzhou, China*.

1. Hsinchun. Chen and Association for Computing Machinery. Special Interest Group on Knowledge Discovery & Data Mining., *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics (CSI-KDD) : June 28, 2009, Paris, France, held in conjunction with SIGKDD’09*. Association for Computing Machinery, 2009.
2. F. Lalonde Lévesque, S. Chiasson, A. Somayaji, and J. M. Fernandez, “Technological and human factors of malware attacks: A computer security clinical trial approach,” *ACM Transactions on Privacy and Security*, vol. 21, no. 4, Jul. 2018, doi: 10.1145/3210311.
3. M. G. Gaber, M. Ahmed, and H. Janicke, “Malware Detection with Artificial Intelligence: A Systematic Literature Review,” *ACM Comput Surv*, vol. 56, no. 6, Jan. 2024, doi:

10.1145/3638552.

* **ANEXOS (MANUAL DE USUARIO, MANUAL TÉCNICO ADICIONAL A LA METODOLOGÍA, FOTOGRAFÍAS, IMÁGENES, Y DOCUMENTO CON LOS ENLACES A VIDEOS, DOCUMENTOS, ETC., ENTRE OTROS)**