**UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO**

**FACULTAD DE CIENCIAS DE LA INGENIERÍA**

**SOFTWARE (REDISEÑO)**

**ENSAYO DEL TEMA DEL PROYECTO**

Redacción Técnica

3ro semestre “A”

**AUTORES:**

Freddy Vladimir Farinango Guandinango

Elizabeth Anahís Burgos Chilan

Andy Emanuel Mendoza Moreira

**QUEVEDO LOS RÍOS**



Agosto, 2024

**MALWARE INFORMÁTICO:**

**ANÁLISIS DE VULNERABILIDADES**

**Y TÉCNICAS DE DETECCIÓN**

En la actualidad, el malware representa una amenaza constante para la seguridad de los sistemas informáticos en todo el mundo. Desde el robo de datos personales hasta el daño a infraestructuras críticas, los efectos del malware son amplios y preocupantes. Por esta razón, es fundamental entender tanto las vulnerabilidades que permiten estos ataques como las técnicas que se están desarrollando o que estén disponibles para detectarlos. Este ensayo se centra en estos dos aspectos, considerando enfoques que combinan métodos tradicionales con técnicas más innovadoras que buscan adaptarse a un entorno digital en constante cambio.

**Análisis de Vulnerabilidades**

El análisis de vulnerabilidades es un proceso que busca identificar las debilidades en los sistemas que podrían ser explotadas por el malware. Según el estudio de Berrere [1], es importante utilizar métodos tanto estáticos como dinámicos para obtener un panorama completo de estas debilidades. Esto significa que no basta con revisar el código fuente análisis estático, sino que también es necesario observar cómo se comporta el software durante su ejecución. Este enfoque permite detectar errores de configuración, accesos indebidos, o incluso la falta de actualizaciones de seguridad.

El análisis de vulnerabilidades no solo sirve para encontrar puntos débiles en los sistemas, sino que también es una herramienta fundamental para planificar defensas más efectivas. Por ejemplo, El estudio de Lin [2] sobre la detección de malware en dispositivos IoT menciona que una evaluación robusta de vulnerabilidades puede ayudar a crear barreras de seguridad más fuertes frente a ataques dirigidos a estos dispositivos.

**Técnicas de Detección de Malware**

Las técnicas tradicionales de detección, como el análisis de firmas y el comportamiento del software, siguen siendo útiles, pero enfrentan limitaciones frente al malware más avanzado. Por eso, se ha empezado a desarrollar métodos más innovadores para mejorar la precisión y adaptarse a nuevas amenazas.

* **Detección Basada en Inteligencia Artificial**

Una de las técnicas emergentes para la detección de malware se basa en el uso de inteligencia artificial (IA). En particular, Parsa [3] propone que el uso de redes neuronales artificiales pueden aprender a reconocer patrones de comportamiento asociados con el malware. Esta técnica imita cómo funciona el cerebro humano, utilizando modelos de aprendizaje para mejorar la precisión en la detección y reducir los errores.

Este enfoque ha demostrado ser efectivo al analizar grandes volúmenes de datos en tiempo real. De manera similar, Mirza [4] dice que los sistemas basados en la nube ofrecen una plataforma poderosa para la detección de malware, ya que permiten procesar grandes cantidades de datos rápidamente y a bajo costo.

* **Análisis Estático y Dinámico**

Las técnicas tradicionales de detección, como el análisis estático y dinámico, siguen siendo relevantes. Según Wang [5], el análisis estático, que examina el código del software sin ejecutarlo, puede ser útil para identificar amenazas comunes, pero es menos efectivo frente a técnicas de ofuscación que los atacantes utilizan para esconder el malware. Por otro lado, el análisis dinámico observa el comportamiento del software mientras se ejecuta, lo que permite detectar comportamientos anómalos que no serían evidentes con un análisis estático.

Estas técnicas pueden ser complementarias: mientras el análisis estático es rápido y eficiente para revisar grandes cantidades de código, el análisis dinámico puede identificar amenazas más sofisticadas, aunque a un costo mayor en términos de recursos computacionales.

* **Detección Basada en Visualización**

La visualización de datos es otra técnica que ha ganado popularidad en los últimos años. Brosolo [6] dice que utilizar gráficos y otras formas de visualización ayuda a los analistas a identificar patrones inusuales que podrían indicar la presencia de malware. Esta técnica es especialmente útil cuando se manejan grandes volúmenes de datos, como en los sistemas de monitoreo continuo.

**Conclusión**

En conclusión, la detección de malware y el análisis de vulnerabilidades son componentes esenciales de la ciberseguridad moderna. Como hemos visto, las técnicas tradicionales como el análisis estático y dinámico siguen siendo útiles para identificar amenazas, pero deben complementarse con enfoques más avanzados, como la inteligencia artificial y la visualización de datos. Cada método tiene sus fortalezas y limitaciones, pero su combinación puede ofrecer una defensa más sólida frente a los ataques de malware que continúan evolucionando rápidamente. Es importante que la investigación y el desarrollo en estas áreas continúen, ya que las amenazas cibernéticas se vuelven cada vez más sofisticadas y diversas. Al integrar diferentes técnicas de detección, podemos estar mejor preparados para enfrentar los desafíos que presenta el malware en un entorno digital en constante cambio.

**Referencias**

[1] M. Barrere, R. Badonnel, and O. Festor, “Vulnerability assessment in autonomic networks and services: A survey,” 2014, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/SURV.2013.082713.00154.

[2] G.-Y. Lin, P.-Y. Wang, S.-M. Cheng, and H.-M. Lee, “Improving Robustness in IoT Malware Detection through Execution Order Analysis,” *ACM Transactions on Embedded Computing Systems*, Aug. 2024, doi: 10.1145/3689427.

[3] M. Parsa, K. N. Khasawneh, and I. Alouani, “A Brain-inspired Approach for Malware Detection using Sub-semantic Hardware Features,” in *Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI*, Association for Computing Machinery, Jun. 2023, pp. 139–142. doi: 10.1145/3583781.3590293.

[4] Q. K. A. Mirza, G. Mohi-Ud-Din, and I. Awan, “A cloud-based energy efficient system for enhancing the detection and prevention of modern malware,” in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, Institute of Electrical and Electronics Engineers Inc., May 2016, pp. 754–761. doi: 10.1109/AINA.2016.133.

[5] Z. Wang, J. Cai, S. Cheng, and W. Li, *DroidDeepLearner: Identifying Android Malware Using Deep Learning*. 2016. doi: 10.1109/SARNOF.2016.7846747.

[6] M. Brosolo, V. Puthuvath, A. Ka, R. Rehiman, and M. Conti, “SoK: Visualization-based Malware Detection Techniques,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2024. doi: 10.1145/3664476.3664514.