Maestría en CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTORES:

Alex Ruben Barre Gabilanes

Giovanny Patricio Chicaiza Garcia

Edison Martin Molina Soria

Carlos Andres Orozco Lara

TUTOR/ES:

Alejandro Cortés López

Iván Reyes Chacón

DETECCIÓN DE ARTEFACTOS DE RANSOMWARE EN SISTEMAS WINDOWS

Quito - Ecuador

enero – 2026

REINVENTEMOS EL FUTURO

RESUMEN

El ransomware se ha consolidado como una de las amenazas más críticas en el ámbito de la ciberseguridad debido a su capacidad para cifrar información y exigir rescates económicos, generando pérdidas significativas y afectaciones operativas en entornos corporativos y personales. Este proyecto tiene como finalidad diseñar un modelo de detección temprana de artefactos asociados al ransomware en sistemas operativos Windows, identificando señales iniciales de infección antes de que el ataque se ejecute por completo mediante el análisis de familias recientes de ransomware y la clasificación de sus artefactos característicos, como archivos generados, procesos sospechosos, modificaciones de registro y extensiones de cifrado.

La propuesta incorpora métricas de evaluación que permiten medir precisión, tasa de detección y tiempos de respuesta, acompañadas de una validación experimental dentro de un laboratorio controlado que simula escenarios reales de infección utilizando herramientas forenses y de monitoreo. Finalmente, se plantean lineamientos para integrar el modelo en entornos corporativos y domésticos mediante soluciones como EDR y sistemas SIEM, contribuyendo al fortalecimiento de estrategias de detección temprana ante la constante evolución de estas amenazas.

Palabras Claves: Ransomware; artefactos; Windows; ciberseguridad; detección temprana; IOc; análisis forense; malware.

ABSTRACT

Ransomware has emerged as one of the most critical threats in the field of cybersecurity due to its ability to encrypt information and demand financial ransom, causing significant losses and operational disruptions across corporate and personal environments. This project aims to design an early detection model for ransomware-related artefacts in Windows operating systems, identifying initial infection signals before the attack fully executes. The methodology is grounded in the analysis of recent ransomware families and the classification of their characteristic artefacts, including generated files, suspicious processes, registry modifications, and encryption extensions.

The proposed model incorporates evaluation metrics to measure detection accuracy, false rates, and response times, supported by experimental validation in a controlled laboratory environment that simulates realistic infection scenarios through forensic and monitoring tools. Additionally, guidelines are provided for integrating the model into corporate and home environments using solutions such as EDR and SIEM systems. This work contributes to strengthening early detection strategies by offering a methodology that is adaptable and capable of evolving alongside emerging threats.

Keywords: Ransomware; artifacts; Windows; cybersecurity; early detection; IoC; forensic analysis; malware.