Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTOR/ES:

Christian Roberto Rodríguez Reyes

Danny Leonidas Sandoval Sevilla

Hennry Pavel Tipanquiza Duque

TUTOR/ES:

Iván Reyes Chacón

Alejandro Cortés López

Análisis Forense del Ransomware LockBit 3.0 y evaluación de su impacto en la continuidad del Negocio

Quito - Ecuador

Junio - 2025

REINVENTEMOS EL FUTURO

RESUMEN

El presente trabajo de investigación se basa en el análisis forense del Ransomware LockBit 3.0, una de las variantes existentes de dicho ransomware, mediante un enfoque practico técnico, que conjuga varias metodologías de investigación, funcionamiento interno, factores de infección, tácticas de intrusión, métodos de detección y mecanismos de cifrado, mismos que permitirán determinar el impacto potencial sobre la continuidad del negocio.

Para el desarrollo de la investigación se ha planteado tres fases: recopilación y análisis de muestras adquiridas, análisis dinámico y estático en un entorno controlado virtualizado, y evaluación de resultados obtenidos.

Como fase preliminar se obtienen muestras reales de LockBit 3.0 tratando de conseguir el primer lanzamiento del ransomware sin modificaciones.

Se crea un laboratorio simulado controlado de un ataque, mismo que nos permitirá observar de manera detallada el comportamiento del malware, con lo que se implementaran técnicas de análisis dinámico y estático para la extracción de datos que posterior permitirán comprender de manera adecuada su funcionamiento.

Se propone una evaluación de impacto sobre la continuidad del negocio, considerando que tipo de conflictos genera en la operatividad de una organización. Este estudio propone una mejor comprensión y preparación ante amenazas cibernéticas. Para de esta manera crear entornos digitales más seguros.

Como parte final en necesario el planteamiento de una serie de recomendaciones y buenas prácticas enfocadas en organizaciones y responsables de seguridad digital. Concientizando de mejor manera la creación de políticas proactivas de ciberseguridad, mismas que incluyen mejoras en el tratamiento de la información manejada.

Palabras Claves: LockBit 3.0, Ransomware, análisis forense, recolección de datos, sistemas de análisis, continuidad del negocio

ABSTRACT

This research work is based on the forensic analysis of LockBit 3.0 Ransomware, one of the existing variants of this ransomware, through a practical technical approach, which combines several research methodologies, internal operation, infection factors, intrusion tactics, detection methods and encryption mechanisms, which will allow determining the potential impact on business continuity.

For the development of the research, three phases have been proposed: collection and analysis of acquired samples, dynamic and static analysis in a virtualized controlled environment, and evaluation of the results obtained.

As a preliminary phase, real samples of LockBit 3.0 are obtained trying to achieve the first launch of the ransomware without modifications.

A controlled simulated laboratory of an attack is created, which will allow us to observe in detail the behavior of the malware, with which dynamic and static analysis techniques will be implemented for the extraction of data that will allow us to properly understand its operation.

An evaluation of the impact on business continuity is proposed, considering what kind of conflicts it generates in the operability of an organization. This study proposes a better understanding and preparation for cyber threats. In order to create more secure digital environments.

As a final part, it is necessary to propose a series of recommendations and good practices focused on organizations and those responsible for digital security. Raising awareness in a better way the creation of proactive cybersecurity policies, which include improvements in the treatment of the information handled.

Keywords: LockBit 3.0, Ransomware, forensic analysis, data collection, analysis systems, business continuity.