Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de

AUTOR/ES:

Jorge Eduardo Burgos Simbaña

Devvin Wellington Mena Tinoco

Erika Mariela Pupiales Cuenca

Iván Rafael Román López

TUTOR:

Alejandro Cortés

INGENIERÍA INVERSA DEL RANSOMWARE CLOP: ANÁLISIS DE FUNCIONAMIENTO Y ESTRATEGIAS DE DEFENSA EMPRESARIAL

Quito - Ecuador

Junio – 2025

REINVENTEMOS EL FUTURO

Resumen

Este estudio analiza el ransomware Clop desde una perspectiva técnica y de ciberseguridad empresarial. Se examinan su origen, evolución, campañas conocidas y técnicas utilizadas, mapeadas al framework MITRE ATT&CK. Mediante ingeniería inversa, se realiza un análisis estático y dinámico de muestras reales en entornos controlados, utilizando herramientas open source. A partir de los hallazgos, se proponen medidas de detección y mitigación accesibles para entornos corporativos. El objetivo es aportar un enfoque práctico y replicable para fortalecer la defensa ante amenazas de ransomware.

Palabras Claves: Ransomware, Clop, Ciberseguridad, Ingeniería inversa, MITRE ATT&CK, Análisis de malware.

Abstract

This study analyzes Clop ransomware from a technical and enterprise cybersecurity perspective. It examines its origin, evolution, known campaigns, and techniques used, mapped to the MITRE ATT&CK framework. Through reverse engineering, a static and dynamic analysis of real samples in controlled environments is performed using open-source tools. Based on the findings, accessible detection and mitigation measures for corporate environments are proposed. The goal is to provide a practical and replicable approach to strengthening defenses against ransomware threats.

Keywords: Ransomware, Clop, Cybersecurity, Reverse Engineering, MITRE ATT&CK, Malware Analysis