Chapter 12

Enhancing Crypto Ransomware Detection Through Network Analysis and Machine Learning

S. Metilda Florence
SRM Institute of Science and Technology, India

Shreya Sinha
SRM Institute of Science and Technology, India

Akshay Raghava
SRM Institute of Science and Technology, India

Kavya Pasagada
SRM Institute of Science and Technology, India

M. J. Yadhu Krishna
SRM Institute of Science and Technology, India

Tanuja Kharol
SRM Institute of Science and Technology, India

ABSTRACT

Crypto ransomware presents an ever-growing menace as it encrypts victim data and demands a ransom for decryption. The increasing frequency of ransomware attacks underscores the need for advanced detection techniques. A machine learning classification model is proposed to identify ransomware families. These models utilize specific network traffic features, with a particular emphasis on analyzing the user datagram protocol (UDP) and internet control message protocol (ICMP). Importantly, this approach incorporates feature selection to enhance efficiency without compromising accuracy, resulting in reduced memory usage and faster processing times. The proposed experiment utilizes various machine learning algorithms, including decision trees and random forest, to create highly accurate models for classifying ransomware families. Furthermore, the experiment combined network traffic analysis with other sophisticated methods such as behavioral analysis and honeypot deployment to effectively scale crypto ransomware detection.

DOI: 10.4018/979-8-3693-1642-9.ch012

1. INTRODUCTION

Crypto ransomware is a malware software encrypting files, demanding payment in cryptocurrency for decryption. It spreads through phishing, exploiting vulnerabilities. Attackers prefer crypto for anonymity. Prevention involves updates, cybersecurity measures, backups, and user education. Incident response plans aid recovery from these increasingly sophisticated cyber threats.

Crypto ransomware typically relies on traditional communication protocols such as HTTP or HTTPS(Krzysztof Cabaj, Marcin Gregorczyk, and Wojciech Mazurczyk, 2018) for command and control (C2) communication, rather than UDP or ICMP. However, cyber threats evolve, and attackers may experiment with different protocols. A study conducted by (May Almousa, Janet Osawere, and Mohd Anwar, 2021) leveraged analysis of TCP packets to detect Crypto ransomware. TCP serves as a fundamental protocol in network communication; however, its application in the context of Crypto ransomware detection comes with inherent limitations. One significant challenge lies in the prevalence of encrypted traffic, a common tactic employed by modern ransomware variants. Encryption serves to secure communications, rendering the inspection of packet content a formidable task for detection mechanisms. As a result, identifying malicious behavior within encrypted TCP packets becomes increasingly challenging.

Moreover, ransomware developers often exploit the dynamic nature of TCP communication. Techniques like port-hopping, wherein the ransomware rapidly switches between different network ports, hence posing difficulties for TCP-based detection systems. The ability of these mechanisms to adapt to rapidly changing communication patterns and port numbers becomes a critical consideration in countering the evasion tactics of sophisticated ransomware variants.

Employing strong network security, monitoring, and regular updates helps mitigate risks associated with potential variations in ransomware tactics. Attackers might leverage UDP for specific purposes such as command and control communications or data exfiltration, but it’s not as prevalent as TCP.

Attackers might misuse ICMP for certain functionalities due to its presence in many networks and the possibility of bypassing some firewall rules.

1.1 Contributions to This Work

This chapter is organized into several sections to provide a comprehensive understanding of the proposed architecture for enhancing crypto ransomware detection through the integration of unconventional network protocols and machine learning algorithms. The structured approach ensures clarity and facilitates a step-by-step exploration of the research methodology and findings.

The first section of the paper delineates the foundational stages of the proposed architecture. This involves the meticulous collection of crypto ransomware network traffic data, an essential step in building a robust dataset for analysis. The chosen network protocols, UDP and ICMP, serve as the focal point for feature extraction and selection, aiming to capture distinctive patterns indicative of malicious activity. By isolating relevant packet fields, the research establishes a framework for effective data processing and subsequent utilization in machine learning algorithms.

The subsequent section delves into the intricacies of feature extraction and selection, elucidating the rationale behind choosing specific fields from UDP and ICMP packets. This process is fundamental in distilling pertinent information from the vast array of network traffic data, facilitating the identification of unique characteristics associated with crypto ransomware. The rationale behind the selection of features is expounded upon, providing insight into the considerations that guided this critical aspect of the research.