Chapter 13
Proactive Solutions to Mitigate Cryptojacking

E. Helen Parimala
https://orcid.org/0009-0006-0892-1375
GITAM University (Deemed), India

ABSTRACT

Cryptojacking refers to the unauthorized utilization of computing resources to mine cryptocurrencies, threatening individuals, organizations, and, most importantly, critical infrastructures in cloud and on-premises systems. This research addresses the escalating cryptojacking threat by developing proactive solutions to effectively detect and mitigate these attacks. Leveraging security tools and technologies like machine learning, network traffic analysis, and behavioral analysis, propose a comprehensive "StyxShield" application capable of identifying and responding to cryptojacking incidents in real time. Through testing and evaluation using real-world datasets and simulated attack scenarios, we demonstrate the effectiveness of the proposed solutions in mitigating cryptojacking threats across diverse environments.This research contributes to the advancement of cybersecurity by empowering individuals and organizations to proactively defend against cryptojacking and safeguard their valuable resources from exploitation by malicious actors.

I INTRODUCTION

This research aims to investigate and propose proactive strategies to combat cryptojacking across different environments, focusing on cloud infrastructure and on-premises systems. The research seeks to develop a comprehensive "StyxShield" application capable of detecting, preventing, and responding to cryptojacking inci-

DOI: 10.4018/979-8-3693-6150-4.ch013

dents in real time by leveraging advanced technologies such as machine learning, network traffic analysis, and behavioral analysis.

Scope of the research

The scope of this research encompasses developing and evaluating proactive solutions to mitigate the threat of cryptojacking across various environments, with a primary focus on cloud infrastructure and on-premises systems. The research will explore detection and prevention techniques, including machine-learning analysis of telemetry data, network traffic analysis, signature-based detection, anomaly detection, and behavioral analysis. The proposed solutions will be designed to be applicable to a wide range of environments, including cloud infrastructure, on-premises systems, and hybrid environments. The research will evaluate the effectiveness of the solutions across different deployment scenarios and assess their scalability and compatibility. Real-world datasets and simulated attack scenarios will be used to assess the performance and efficacy of the proposed techniques in identifying and responding to cryptojacking threats. The research will consider the integration of the proposed solutions with existing security measures and technologies commonly deployed in enterprise environments, such as Security Information and Event Management (SIEM), and Endpoint Detection and Response (EDR) systems with an aim to complement and enhance existing security controls. Finally, the research will acknowledge any limitations or constraints encountered during the development and evaluation of the proposed solutions, and potential future research directions and areas for improvement will be identified to guide further exploration and advancement in the field of cryptojacking mitigation.

Objectives

The objectives of this research are:

Develop a comprehensive understanding of the threat landscape surrounding cryptojacking, including the techniques, tools, and tactics employed by malicious actors to exploit computing resources for cryptocurrency mining.
Investigate and evaluate existing detection and prevention techniques for

cryptojacking, with a focus on their applicability to cloud infrastructure and on-premises systems.

Design and implement proactive solutions to mitigate the risk of