ComproAlert: Next-Gen Threat Detection for Comprehensive Network Security

1. Introduction

1.1 Hackathon Background

Smart India Hackathon 2023 brought together engineering students from across India to tackle real-world issues in Smart Automation and Blockchain & Cybersecurity. They collaborated, ideated, and developed groundbreaking solutions, fostering innovation and entrepreneurship. The event celebrated student excellence while shaping India's tech future through collaboration and ingenuity.

1.2 Project Overview

ComproAlert is an advanced solution that revolutionizes the early detection of compromises on computing devices by leveraging AI/ML models for anomaly detection and behavioral analysis, surpassing traditional IoC-based methods. With features such as real-time email notifications, organized task management, and compatibility across platforms, ComproAlert ensures efficient and streamlined operations. It addresses the challenge of detecting compromises when IoCs are unknown, employing innovative AI/ML models for non-IoC-based detection on diverse devices. The system's evaluation focuses on ruggedness, adaptability, ease of deployment, and the ability to minimize false alarms, offering a reliable and secure approach to cybersecurity for safeguarding critical information infrastructure.

1.3 Objectives and Scope

The objective of our project is centered on revolutionizing compromise detection on computing devices, steering away from traditional IoC-dependent methods. Our primary goals include the development of an innovative approach using advanced AI/ML models, specifically emphasizing anomaly detection and behavioral analysis for real-time efficacy. We aimed for an effortless deployment, ensuring compatibility across diverse platforms, systems, and devices, prioritizing a unified user experience. The project scope encompasses creating a Centralized Analysis Alarm System, integrating features such as timely email, organized task management, and top-tier security delivery through instant notifications. Beyond immediate goals, the project addresses the broader challenge of compromise detection in scenarios where IoCs are unknown.

2. Team Information

FUTURE FITS

- Sai Shashank Bedampeta
- Aavishkar Kolte

- Rishita Gagrani
- Vaibhav Pawar
- Suvarsha Chennareddy
- John Tony

3. Problem Statement

3.1 Description of the Problem Statement

Early detection of a compromise of any compute device is critical for security of critical information infrastructure. While most of infections on ICT are detected using IoCs (Indicators of Compromises), the objective of this problem is to explore techniques for detection of compromise on devices using AI / ML models when the IoC of the compromise is not known. The developer should employ innovative models for non-IoCs based detection of compromise on devices. The evaluation of the solution will be based on the following: (a) Innovation and ruggedness of the method of detection of compromise. (b) Utility of the method developed over various types of devices including system / firewall / router / network. (c) Ease of deployment and method of reporting of detected compromise. (d) Ability to minimize false alarms of compromise.

3.2 Target Audience

Our project is tailored for IT security teams within medium to large enterprises, particularly those managing critical information infrastructure. Primary users include cybersecurity analysts, incident responders, and IT administrators responsible for safeguarding systems, firewalls, routers, and networks. The system's innovative compromise detection using advanced AI/ML models targets professionals seeking to enhance their security posture beyond conventional IoC-based approaches. The solution's ease of deployment and compatibility across diverse platforms caters to IT professionals looking for seamless integration into existing infrastructure. Specifically, the project aims to benefit organizations in finance, healthcare, and government sectors where the stakes for cybersecurity are high. Overall, the project is aimed at proactive security teams and organizations seeking an advanced and user-friendly solution for early compromise detection and improved cybersecurity resilience.

3.3 Key Challenges Addressed

Throughout the development of our cybersecurity project, we encountered and successfully addressed significant challenges. The need to detect compromises in the absence of traditional Indicators of Compromises (IoCs) was met with strategic Tactics, Techniques, and Procedures (TTPs), emphasizing the deployment of advanced AI/ML models for non-IoC-based detection. Innovating compromise detection methodologies was achieved through TTPs that prioritize dynamic behavioral analysis and anomaly detection, staying ahead of evolving cyber threats. Ensuring compatibility across diverse devices was addressed with TTPs focusing on a unified experience and adaptable strategies for streamlined deployment. Rigorous evaluation criteria, a TTP in itself, were employed to mitigate false alarms, ensuring the reliability and accuracy of compromise detection. The challenge of adapting to diverse environments was met with TTPs

emphasizing adaptability, catering to unique requirements across various industries. Additionally, comprehensive TTPs were implemented to counter adversaries exploiting vulnerabilities across platforms, extending defense mechanisms to systems, firewalls, routers, and networks. These strategic TTPs collectively fortified the project, reducing the dwell time between compromise and detection, and enhancing resilience against sophisticated cyber threats.

4. Solution Overview

4.1 Project Name

ComproAlert- Advanced AI/ML Compromise Detection System

ComproAlert is an innovative project dedicated to the development of an advanced AI/ML tool designed specifically for detecting compromises in systems, firewalls, routers, and networks. Departing from traditional methods heavily reliant on Indicators of Compromises (IoCs), ComproAlert employs cutting-edge techniques that go beyond IoC detection. This project aims to revolutionize the landscape of cybersecurity by introducing a sophisticated approach to compromise detection that ensures a proactive defense against evolving threats. The integration of AI/ML models enables ComproAlert to analyze anomalies and behavioral patterns, providing a comprehensive and dynamic solution for identifying potential compromises in real-time.

4.2 Key Features

- **Dynamic DNS Activity Montioring:** Real-time tracking and analysis of DNS behaviors, emphasizing dynamic patterns instead of relying solely on static Indicators of Compromises (IoCs).
- **IP Geolocation Filtering:** Robust filtering based on IP addresses using HDBSCAN clustering algorithm, focusing on detecting anomalies or outliers, enhancing precision and adaptability.
- **Behavioral Process Analysis:** Continuous eBPF monitoring of Linux system calls enables proactive threat detection by analyzing real-time behavior patterns, ensuring heightened resilience against evolving cybersecurity threats.
- **Adaptive Network Flow Anomaly Detection:** Aggregation of port-level network traffic flow using autoencoder-based approach, focusing on dynamic anomalies rather than static IoCs, ensuring resilience against sophisticated threats.
- **Ransomware Detection Canary (Non-Signature Based):** Deployment of ransomware detection canaries that operate without relying solely on signatures or predetermined IoCs, offering a dynamic and adaptive defense mechanism.
- **Endpoint Security for Windows (Chainsaw) and Linux (Non IoC Based):** Versatile endpoint deployment on Windows (Chainsaw) and Linux systems, ensuring security without solely depending on traditional Indicators of Compromises (IoCs).

4.3 Technologies Used

- **Berkeley Packet Filter (eBPF):** The project leverages BPF technology, specifically BCC (BPF Compiler Collection) and BPF SOCKET_FILTER, for capturing and analyzing network packets efficiently. BPF programs are attached to raw sockets, allowing packet filtering at the socket level.
- **TensorFlow and scikit-learn:** Machine learning plays a crucial role in anomaly detection. TensorFlow, an open-source machine learning framework, is utilized to create autoencoder neural networks for detecting anomalies in system call behavior. Additionally, scikit-learn is employed for implementing the HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise) algorithm, contributing to geolocation-based threat monitoring.
- **HTTP Requests (requests library):** The requests library is integrated into the project for facilitating real-time alerts. Upon detecting anomalies, the system triggers HTTP POST requests to a specified endpoint, providing timely alerts for potential security threats.
- **BPF_HASH Data Structure:** To store and retrieve IP addresses along with packet counts efficiently, the project utilizes the BPF_HASH data structure. This in-kernel hash table, named ip_hash, enhances the performance of IP address data management.
- **Linux kernel Header Files:** The project incorporates Linux kernel header files to access packet structures and constants, enabling seamless integration with BPF programs for packet parsing and analysis.
- **BCC (BPF Compiler Collection):** BCC serves as a set of tools and libraries for creating, compiling, and loading BPF programs. It acts as a bridge between BPF and Python, enabling efficient packet filtering and monitoring in the Linux kernel.
- **NumPy and Pandas:** NumPy and pandas are employed for efficient data manipulation and analysis, facilitating the processing of large datasets generated during network monitoring.
- **Time Module:** The time module is utilized to introduce delays between iterations, ensuring controlled and continuous monitoring of network activity.
- **Frontend:** React, Next.js, and Tailwind CSS power the frontend, delivering a dynamic, responsive interface. Tailwind CSS contributes to a polished design, and the stack includes correlation logic for identifying and responding to threat correlations.
- **Backend:** The backend employs Node.js, Express, MongoDB, and a RESTful API. Node.js and Express ensure scalability and responsiveness, while MongoDB manages data efficiently. The RESTful API architecture facilitates seamless communication between frontend and backend components.

4.4 Architecture Overview

ComproAlert employs a robust, distributed architecture designed to safeguard your network and systems from a diverse range of malicious activities. Its multi-layered

approach combines dedicated agents, sophisticated analytics, and machine learning (ML) to ensure comprehensive protection.

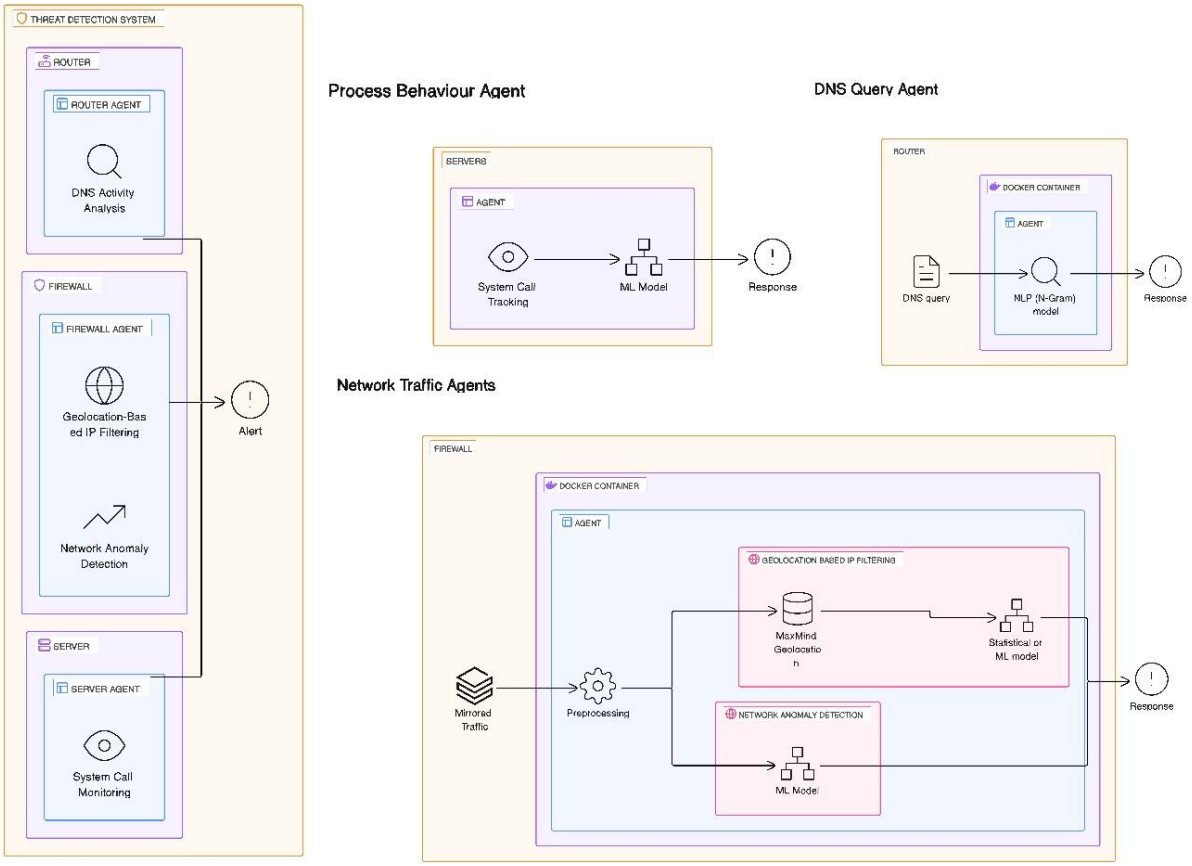
I. Components:
    1. Router Agent:
        - Monitors router-level network traffic.
        - Captures and forwards relevant data for in-depth analysis.
    2. Firewall Agent:
        - Resides within the firewall, actively scrutinizing network traffic.
        - Identifies anomalies and potential threats.
    3. System Agent:
        - Deployed on servers, tracks system calls and process behavior.
        - Flags any suspicious activity for further investigation.
    4. DNS Activity Analysis Agent:
        - Analyzes DNS queries for malicious patterns.
        - Detects phishing or malware propagation attempts.

II. Advanced Defense Mechanisms:
    1. Geolocation-Based IP Filtering:
        - Blocks or restricts traffic from known malicious IP addresses or entire geographic regions.
    2. Network Anomaly Detection:
        - Leverages statistical models and ML to identify unusual network patterns signaling potential attacks.
    3. Process Behavior Analysis:
        - Tracks system calls and process activity.
        - Detects anomalies or unauthorized behavior, thwarting insider threats and malware infections.

III. Data Flow and Threat Response:
    1. Network traffic, system calls, and DNS queries directed to specific agents for analysis.
    2. Each agent employs dedicated ML models and detection techniques to identify potential threats.
    3. Upon confirming a threat, the system triggers actions such as:
        - Blocking malicious traffic at the firewall.
        - Quarantining suspicious files or processes.
        - Sending immediate alerts to security personnel for investigation and response.

IV. Key Features:
    1. Distributed Deployment: Strategically position agents across the network for unparalleled visibility and protection.
    2. Multi-Layered Defense: Utilizes diverse detection techniques to counter a broad spectrum of threats effectively.

3. ML-Powered Detection: Incorporates cutting-edge ML models for heightened accuracy and adaptability to evolving threats.
4. Geolocation-Based Filtering: Adds an extra layer of security by proactively blocking traffic from known malicious sources.



5. Usage

5.1 User Guide

- **ComproAlert User Interface:** Explore the ComproAlert user interface, which includes Geolocation-based IP Filtering, DNS monitoring, Behavioral process analysis, network flow anomaly detection, ransomware canary detection, and correlation between them.

- **User Roles and Permissions:** ComproAlert is specifically designed for cybersecurity administrators, providing them with powerful tools to enhance their security operations. To begin using ComproAlert, users need to log in, ensuring secure and tailored access to the system's features and functionalities. By requiring authentication through login credentials, ComproAlert ensures that only authorized

personnel can access and utilize its robust cybersecurity capabilities. This login mechanism adds an essential layer of security, safeguarding sensitive data and ensuring that administrators have full control over their security operations within the ComproAlert platform.

- **Set Up Monitoring Agents:** ComproAlert captures real-time network and system behaviors, ensuring accurate and comprehensive data for threat detection. By configuring monitoring agents properly, users can rely on ComproAlert to provide real-time insights into potential threats. This timely information allows for proactive security measures to be taken, ensuring the safety of systems and networks. With ComproAlert's emphasis on accurate configuration and real-time data capture, users can confidently detect and respond to threats effectively.

- **Dashboard:** To stay informed about the overall system alerts and potential threats in ComproAlert, it is important to regularly monitor the dashboard. The dashboard provides an overview of the system's security status through key metrics, visualizations, and correlations between them. By paying attention to these indicators, users can quickly identify anomalies or suspicious activities that may require further investigation. The combination of visual representations and the ability to correlate different metrics enhances the ability to detect potential threats and take proactive measures to mitigate them. By actively monitoring the dashboard, users can maintain a high level of situational awareness and promptly respond to any security issues that may arise.

- **Investigate Alerts:** When an alert is triggered within ComproAlert, an automatic email notification is sent to the designated recipients responsible for investigating security incidents. The email includes key information such as the source IP, destination IP, timestamps, and affected systems. These details provide crucial context for the investigation, allowing the recipients to assess the severity and potential impact of the alert.

- **Seek Support and engage with the ComproAlert Community:** If you have any difficulties or questions about ComproAlert, please check the Help section for assistance.