Defensive Honeypots for IP IoT Devices: Quantitative Comparison between Vanilla and Sandboxed Honeypots

Franek Kruczynski

September 2025

Contents

Chapter 1

Introduction

1.1 Background

Abstract of the project goes here

The Internet of Things (IoT) is vastly expanding, driving a brand new and complex wave of device inter-connectivity worldwide, with an approximate 27-billion devices by the end of 2025*(Jinesh, 2025)*.

1.2 Aims & Objectives

1.2.1 Aim

To evaluate the effectiveness of containment and sandboxing mechanisms, in preventing malware propagation (specifically its spread into external systems) within a IoT IP device Honeypot framework. Such will be achieved through quantitatively comparing the same malware programs on two separate Honeypots, contained high-interaction against vanilla low-interaction.

1.2.2 Objectives

The objectives are as follows:

- Design, develop and deploy a secure Honeynet framework within Virtual Machines,
- To deploy two separate Honeypots:
    1. **Vanilla Honeypot:** Low-interaction with no advanced security,
    2. **Sandboxed Honeypot:** High-interaction within a secured container.

- To create and design a virtual network, providing both logical addressing to all IoT IP devices, Virtual Machines and, providing security through sub-netting. In essence mimicking a small office network.
- To collect and store the following malware properties for quantitative comparison and analysis:

  1. Network traffic,

  2. Payloads,

  3. Malware type

  4. Activity data

  5. Propagation attempts outside the container.
- Quantitatively compare the data of all malware, and conclude whether attack behaviors differ based on environment.

1.3 Product Review

1.3.1 Scope

The project involves the design and deployment of a secure IoT Honeynet environment for a range of IP IoT devices simulated within a small office network. Two separate and distinct honeypots will be implemented, a high-interaction sandboxed Honeypot and, a low-interaction vanilla Honeypot operating within a secure, isolated Docker container. The Honeypots will operate within a singular Virtual Machine sequentially.

Each malware sample will be executed within the Honeypots, with all relevant data including its type, payloads and various activity logs securely collected. A dedicated Virtual Machine (separate to the Honeynet) will store and process the data using tools such as ElasticSearch, guaranteeing all data remains isolated from the external network.

In essence, the project will simulate realistic attacking behaviours and sequences of events that occur during malware spread within smaller networks. Findings will lead to a better understanding of the importance of segmentation within networks and Honeypots, to aid in strengthening IoT security by identifying attacker patterns *(Kocaogullar, 2023)*. Furthermore, it'll help expand on pre-existing research and highlight the importance of practical implementation methods for secure environments.

1.3.2 Audience

The primary audience for this project involves cyber security researchers, network analysists and academic institutions which study digital forensics, analyse malware behaviour and the administrators that deal with IoT security. Such groups will benefit from the projects structured and quantitative evaluation of containment-based Honeypots and networks, as it provides improved threat detection and response; enhanced threat intelligence through dynamic analysis and prevention; and the overall impact of a secure Honeypot environment.

Furthermore, Cybersecurity lecturers and students will benefit through providing a practical framework for a safe and secure virtual environment for malware deployment, for experimentation and research. The projects architecture may server as a teaching tool for demonstrating both the dangers of types of malware, and analysis practices for security.

Lastly, IoT administrators and developers in smaller organisations may gauge a better understanding of malware behaviour within contained and non-contained environments. Understanding malware patterns with supporting data may help in more advanced intrusion detection systems (IDS), through ensuring comprehensive flaws within IoT devices are identified *(Fortinet, 2025)*.

Chapter 2

Background Review

2.1 Existing Approaches

Add on to 1.1, provide overview of similar products and why they aren't sufficient

2.2 Related Literature

Self explanatory

- Look through thesis provided by supervisor

Chapter 3

Methodology & Techniques

3.1 Approach

- Link back to objectives?
    - Two separate VMs
    - Lab VM = honeypots
    Analysis VM = protected

3.2 Technologies

3.3 Version Control & Management

Introduce GitHub & Supervisor Google Drive

Chapter 4

Project Management

4.1 Activities

4.2 Schedule and Time Management

- Calendar - Allocating times during week

4.3 Data Management

- How is this data going to be stored? (Analysis VM using pcaps) - CSV files for extracting

4.4 Deliverables

Chapter 5

References

Bibliography

Fortinet (2025). *What Is An Intrusion Detection System (IDS)?* URL: https://www.fortinet.com/uk/resources/cyberglossary/intrusion-detection-system.

Jinesh (2025). *How Many IoT Devices Are There in 2025?* URL: https://autobitslabs.com/how-many-iot-devices-are-there/.

Kocaogullar, Y et al. (2023). *Hunting High or Low: Evaluating the Effectiveness of High-Interaction and Low-Interaction Honeypot*. URL: https://kar.kent.ac.uk/102122/1/STAST2022.pdf.