Abertay University

Enhancing OT Cybersecurity Using Honeypots

Paul Michael Oates

CMP400

Supervised by David McLuskie

Introduction

Operational Technology (OT) enables the controlling and monitoring of industrial equipment used in fields such as manufacturing, power generation, ATMs, and traffic lights. Due to our dependency on OT, it can prove attractive to threat actors aiming to disrupt this Critical National Infrastructure. (CNI)

Honeypots are systems that pretend to 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 actors are utilising.

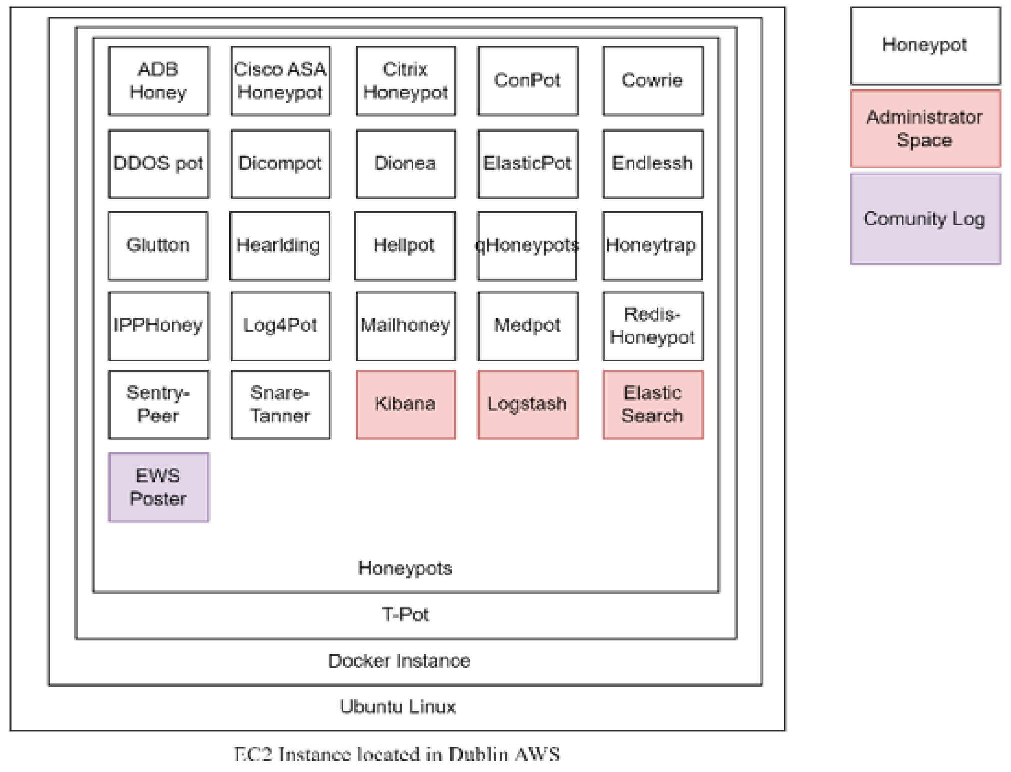
Aim

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.

Methodology

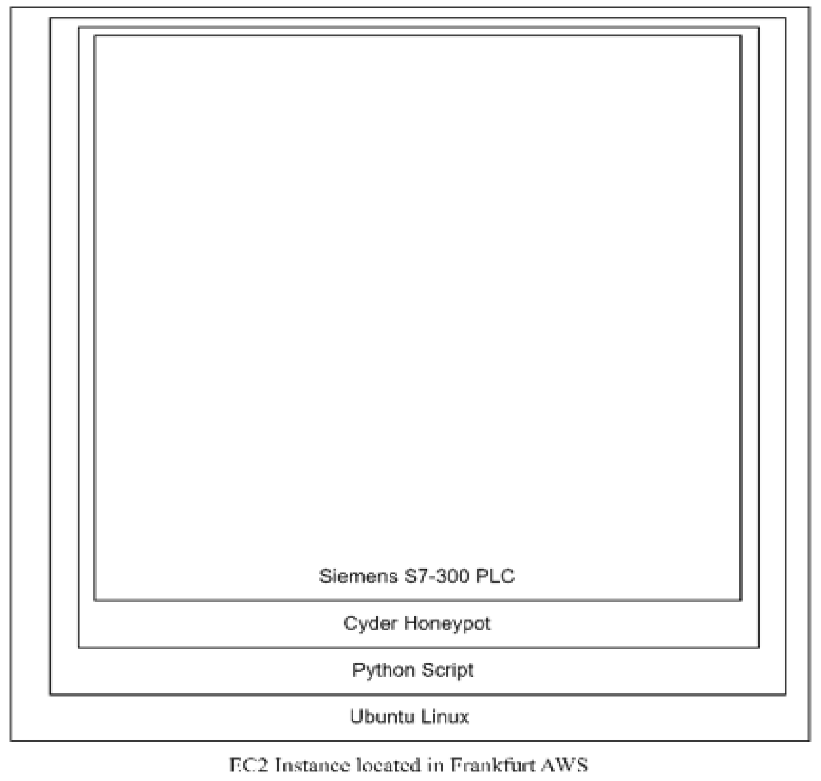
Two experiments were conducted within an AWS Cloud environment. The Honeypots were deployed for a month and both structures are displayed below

T-Pot



The T-Pot structure

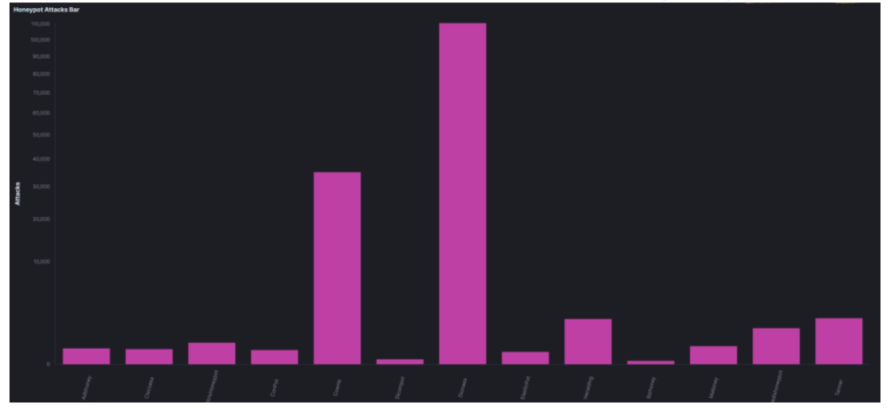
Cyder



The Cyder structure

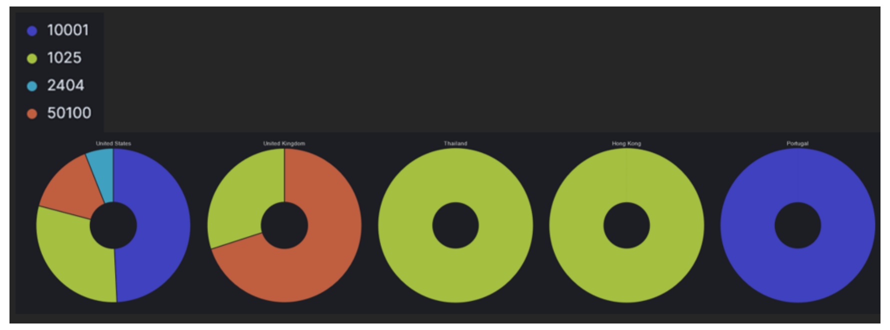
Results

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 month of deployment .



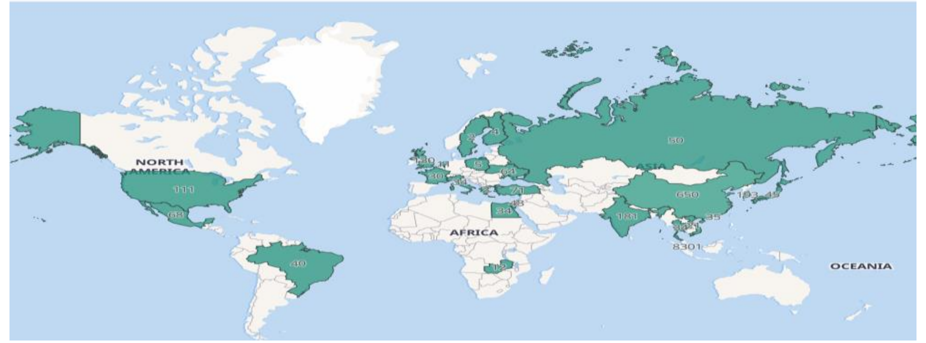
T-Pot Honeypot's popularity

Specifically, regarding 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.



ConPot port popularity by country

With regards Cyder it received over ten thousand interactions over the month.



Cyder IP origin Map

Discussion

This report found that Honeypots are a valuable tool in a cybersecurity professional's arsenal. Threat actor's interactions with the Honeypot can be analysed using frameworks such as the MITRE ATT&CK for ICS which reveals threat actors TTP's.

The T-Pot Honeypot was very popular and revealed the CVE's threat actors attempted to exploit and malware samples deployed, which were analysed and disclosed to the wider security community.

The Cyder Honeypot proved less popular however revealed the possibility of an OT specific credential dictionary being used by threat actors, due to credentials such as "Telecomadmin" being present.

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 actor's operations.

References

MITRE, 2020. MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy.

Shreyas Srinivasa, J. M. P. E. V., 2022. Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots.

Trend Micro, 2020. Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats

R. Piggin, I. B., 2016. Active defence using an operational technology Honeypot.

Richard Derbyshire, B. G. C. v. d. W. D. H., 2023. Dead Man's PLC: Towards Viable Cyber Extortion for Operational Technology.