Enhancing OT Cybersecurity Using Honeypots

Paul Michael Oates
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

Context: Honeypots are an IT security tool which are used to imitate systems and 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 (TTP) that hackers utilise to gain access to systems, while also providing further insight into the intentions of hackers after the system is breached. Operational Technology (OT) is used to control Critical National Infrastructure (CNI) as well as other environments where availability to real time information is paramount. By using honeypots to identify what threat actors are targeting in OT environments, the security of these sites can be massively improved.

Aim: Honeypots will be used to improve Operational Technology (OT) cybersecurity. They will be deployed to attract threat actors, which will allow for critical analysis of their methodology and their intent. The information gained will be shared with the wider OT community to deepen our understanding of the vulnerabilities discovered by the Honeypot and how they affect real Industrial Control Systems (ICS). This information will provide practical advice on how to mitigate against these attacks.

Method: Various OT honeypots will be deployed on servers across the world to simulate vulnerable OT equipment. The characteristics of the honeypots will be critical to the success of the project therefore different types of honeypots will be used to gather detailed information and provide a clear picture of possible threats against OT equipment. The appropriate obfuscation techniques will be utilised to provide scenarios which produce realistic data. All interactions with the honeypots will be logged and critically analysed.

Results: The project will identify the TTP's real threat actors are using to target OT environments which in turn will identify the vulnerabilities in OT equipment. This will be shared via LinkedIn to the OT community.

Conclusion: The data collected during this project will highlight and inform the wider OT community of the vulnerabilities that exist within Operational Technology. This contextualised information can then be acted upon to mitigate against these particular vulnerabilities.

Keywords

Operational Technology (OT), Honeypots, Industrial Control Systems (ICS), Tactics, Techniques and Procedures (TTP), Critical National Infrastructure (CNI) and Threat Actors

1. INTRODUCTION

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., transmission grid goes out. Over recent years 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 1 GhostSec targets (Forescout, 2022)

Figure 1 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. This therefore provides sufficient justification to undertake a project in this area as it demonstrates a clear need for the enhancement of OT cybersecurity and a need to understand threat actors TTP's. 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 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) 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. The interaction the attacker has with the honeypot is recorded and critically analysed to identify threat actors' TTPs. This vital information can then be disclosed and utilised by businesses and governments alike to mitigate risk. Research honeypots will be the focus of this proposal.

Another issue that cannot be ignored for OT is 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.

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. Within an OT industry 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.

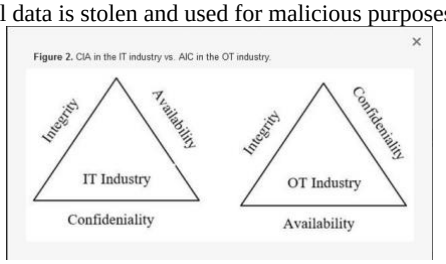

Figure-2 The AIC Triangle (Mesbah M, 2023)

Figure 2 identifies the CIA/AIC triangle highlighting the key difference between OT and IT environments. As these two environments collide in our modern world the differences in approach must be considered whilst undertaking this project.

2. BACKGROUND

Despite OT networks being obscured and isolated they are prime targets for threat actors. The negative impact of threat actors actions cannot be overstated. Malware such as "CrashOverride" or "Sandworm" specifically targeted the Ukrainian electrical transmission OT network. 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 TTP's that threat actors use is paramount to keeping nations safe.

Research undertook by Mesbah.M at Nile University, Cairo (Mesbah M, 2023) investigates using OT honeypots to collect and analyse data about the TTPs threat actors deploy. An open-source tool called 'Conpot' was used as the Honeypot. "Conpot" enables the end user to virtualise various pieces of OT hardware such as the widely used "Siemens S7" Programmable Logic Controller. The project deployed the honeypot for one month, during this time it logged what ports and protocols threat actors were using to gain access and documented their IP addresses. The results suggest that OT technology is attractive to threat actors regardless of their nationality with both NATO/BIRCS nations trying to exploit the honeypot. However, the reliability of IP addresses as locations is questionable as VPN's can mask locations. Outdated protocols such as Modbus, S7comm, and HTTP which are unencrypted were of particular interest to threat actors for their ease of exploitation. The paper recommended adhering to international standards on OT protocols to mitigate these risks.

Aalborg University, Denmark (Shreyas Srinivasa, 2022) 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 TTP's.

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-3 Various Honeypots utilised (Shreyas Srinivasa, 2022)

The figure above identifies various honeypots and the timeframe in which they were studied. From the study (Shreyas Srinivasa, 2022) the "RIoTPOT" honeypot collected 49 malware samples in 39 days, this further highlights the attractiveness of OT technology and the need for more research into OT honeypots.

Atkins (R. Piggin, 2016) deployed a public facing OT network honeypot with collaboration from an undisclosed industry partner, with the aim of creating a feasible honeypot network. The paper highlights that threat actors attempted to disrupt communication on the OT network, launch brute force attacks, deploy malware, and attempt to delete directories on the control PC, from worldwide IP addresses. TOR networks were also identified and most likely used to hide the source of the attack. The report details that these attacks mainly used HTTP to connect to the network however RDP was also popular. This research identified the varied and advanced ways threat actors attempted to disrupt or destroy OT equipment. Their findings when shared with the wider OT community will be invaluable in further enhancing OT cybersecurity.

***Figure-4 Increasing OT Cyberattacks* (R. Piggin, 2016)**

Figure 4 from Atkins identifies the rapid increase in cyber-attacks against ICS equipment highlighting the appetite threat actors have for OT equipment.

Finally, the Stuxnet paper by ETH Zurich (Baezner Marie, 2017) discusses both the cyber and economic impact of the Stuxnet virus. The Stuxnet virus is an advanced piece of malware targeting SCADA environments specifically the Iranian nuclear centrifuges by targeting Siemens PLC's. The malware would spin 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. This is a highly sophisticated piece of malware. Stuxnet highlights the lengths threat actors will go to exploit OT environments and highlights the need for a better understanding of how threat actors are exploiting these networks.

Target:	Centrifuges[1] used in the uranium enrichment process in Nuclear plant at Natanz in Iran.
Tool:	Stuxnet: a worm using four zero-day vulnerabilities and infecting computer networks through USB-flash drives.
Effects:	Damage to the centrifuges; modification or/and creation of cyber strategies in the world; increase in awareness of cybersecurity issues.
Timeframe	2009 - 2011

Figure -5 Summary of the Stuxnet malware (Baezner Marie, 2017)

The Figure 5 summarises the Stuxnet malware which was targeted at OT systems. From the research studied it is clear that honeypots have a vital role to play in OT cybersecurity and that continued studies are required to keep abreast of the current risks to Operational Technology in order for these risks to be mitigated.

3. METHOD

3.1 Research

Initially, the project research will focus on OT honeypots, to identify both paid and free honeypot resources, hosting methods and how to ensure honeypots are obscured on the cloud. Threat actor's information will be ethically logged and will be used for further analysis. Suitable malware analysis tools will be selected.

As S. Srinivasa (Shreyas Srinivasa, 2022) suggests the better the honeypot's interactivity the better the results, therefore research into virtualised high interactivity honeypots will be a focal point of the study. This initial research may result in some minor changes and adaptations to the methodology.

After research into OT honeypots has been concluded and the ethics committee have approved the project, various honeypots will be deployed on servers across the world. The IP addresses given to the honeypots will be analysed to check if they have any previous history, and if any issues are found their IP addresses obfuscated. If no suitable obfuscation method is found the honeypot will not be deployed, as the data collected will likely be unusable. After a week an initial analysis of the honeypots will be undertaken to ensure they have been successful and further obfuscation methods used i.e., by moving protocols to different ports will be applied. After a month the honeypots will be shut down and all results will be copied to a central machine.

3.2 Analysis

Critical analysis of the ports and protocols will be undertaken to understand the actions of the threat actors when interacting with the honeypots. IPs that are discovered will be geolocated to a country of origin to identify trends. No further analysis of IP addresses will be carried out. The results will then be analysed to identify TTP's of threat actors. The next step will be to analyse any malware deployed on the honeypots and this will be undertaken to determine the threat actor intent. An analysis of the obfuscation techniques will also be undertaken. The information gained through this exercise will be collated and shared with the wider OT community through the relevant LinkedIn group. This will be undertaken to provide actionable intelligence to the security community.

3.3 Evaluation

The findings of this project will be evaluated to determine the success of the project and to identify key areas for future work. Three key areas have been identified as indicators of success for the project: How realistic, discoverable, and interactive the deployed honeypots will be. The extent of the information captured and its usefulness. Disclosure of the information on LinkedIn to reach the OT cybersecurity community.

4. SUMMARY

As by their very nature OT systems are part of the critical infrastructure of a country, keeping them secure from cyber-attacks is vitally important. It is essential that we constantly monitor OT systems so we can identify threats and quickly mitigate against them. Honeypots may not achieve the complete security of an OT network, but they do however enhance OT cybersecurity by shining a light on the situation at present and allow for appropriate action to be taken by businesses and governments alike to improve the security of OT systems.

5. REFERENCES

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

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 October 2023].

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 October 2023].

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

R. Piggin, I. B., 2016. *Active defence using an operational technology honeypot.* [Online]
Available at:
https://www.atkinsrealis.com/~/media/Files/S/SNC-Lavalin/download-centre/en/brochure/active-defence-with-an-ot-honeypot-snc-v1.pdf
[Accessed 10 2023].

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].

Sanders, C., 2020. Intrusion Detection Honeypots. 1st ed. Oakwood(Georgia): Applied Network Defense. ISBN: 9781735188300 URL: https://books.google.co.uk/books?id=suubzQEACAAJ

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].