A Ship Honeynet Project to Collect Data on Cyber Threats to the Maritime Sector

Stephen James McCombie
Maritime IT Security Research Group
NHL Stenden University of Applied Sciences
Leeuwarden Netherlands
Email: stephen.mccombie@nhlstenden.com

Jeroen Pijpker
Maritime IT Security Research Group
NHL Stenden University of Applied Sciences
Emmen Netherlands
Email: jeroen.pijpker@nhlstenden.com

***Abstract*— This paper discusses the development of a ship Honeynet. The criticality and fragility of the Global Maritime Transportation System (GMTS) has been clearly demonstrated during the COVID-19 Pandemic. At the same time, fleets are aging and their technology is aging with them and thus they are more vulnerable to cyber-attacks. This paper will describe a project aiming to gather information on current cyber-attacks on vessels using a Honeynet to gather data. Honeypots are Internet systems deployed for the sole purpose of being compromised to observe adversaries. Networks of Honeypots are termed Honeynets and, like network telescopes, are typically deployed on an otherwise unused address space. While Honeypot/Honeynets are not new, simulating all the different systems of a ship to research cyber attackers targeting them is a new concept. A ship in real life consists of multiple digital systems including for navigation, communication, safety, propulsion, cargo management and numerous other purposes. This paper will explain the concept of Honeynets and a ship Honeynet in particular, as well as their design considerations and benefits. This paper will also discuss the challenge of making the Honeynet digitally realistic and attractive for cyber attackers to interact with and drop targeted malware and other interesting artefacts.**

Keywords – Cybersecurity; Maritime Security; Cyber-Physical Security; Vessel; Honeynet; Honeypot; Cyber Deception.

I. INTRODUCTION

This paper will discuss the concept, development and use of a ship Honeynet to gather information on current cyber-attacks on vessels. This will be achieved by luring cyber attackers to interact with the ship Honeynet and capturing that interaction for later analysis. The criticality and fragility of our supply chains have been demonstrated during the COVID-19 Pandemic. This is particularly evident within the GMTS. The GMTS is a system of systems and includes not just vessels but also waterways, ports, and land-side connections, moving people and goods to and from the water. The role of GMTS in the global economy is significant with over 80% of the world's cargo transported by ship [2] and representing 70% of global trade by value [3]. At the same time, fleets are aging, and their technology is aging with them and thus they are more vulnerable to cyber-attacks. 38% of oil tankers and 59% of general cargo ships are more than twenty years old [4]. Supply chains themselves are increasingly vulnerable to cyber-attacks. This is particularly stark in recent years, "…European sources estimated a 400% growth in supply chain cyberattacks in 2021 compared to 2020" [5]. GMTS is clearly a key part of global supply chains and will be increasingly targeted by cyber threat actors. Since 2018, state sponsored threat actors from China (amongst others) have specifically targeted the maritime industry [6].

Honeypots are Internet systems deployed for the sole purpose of being compromised in order to observe adversaries. Networks of Honeypots are termed Honeynets and, like network telescopes, are typically deployed on an otherwise unused address space [1]. While Honeypot/Honeynets are not new, simulating all the different systems of a ship to research cyber attackers targeting them is a new concept. A ship in real life consists of multiple digital systems including for navigation, communication, safety, propulsion, cargo management and numerous other purposes. The Honeynet needs to simulate this.

Part of the process is to make the Honeynet to appear realistic to potential attackers and the paper identifies a number of features that would make the Honeynet more realistic and thus more likely to attract and engage attackers. The ship Honeynet is going to use a technique proposed by Luo et al. [7] called intelligent interaction. The paper also discusses methods to capture all interactions with those attackers including connection details, commands executed, files dropped, and other relevant activity.

The Honeynet data and any discovered attacker Tactics, Techniques and Practices (TTPs), will be used for a number of important purposes. To build industry awareness of this rising threat. To create research reports/publications. To report any identified vulnerabilities to vendors. Lastly to create realistic maritime cyber incident simulations for industry education and research into human factors.

The structure of this paper is firstly a description of the background of Honeynets, etc., followed by a description of the cyber threats to the maritime sector, then the project plan and design considerations for a ship Honeynet and, finally, the conclusions and future research.

II. BACKGROUND OF DECEPTION, HONEYPOTS AND HONEYNETS

Honeypots and the use of deception against cyber attackers date back to the 1980s. Astronomer Clifford Stoll in his seminal hacking tale, The Cuckoo's Egg, described when working as a part time system administrator at Lawrence Berkeley National Lab in the USA his efforts to uncover hackers who had penetrated his system [8]. This

 ISBN: 978-1-61208-996-6

early Honeypot was born of his scientific approach to observe his attackers and get them to reveal more of themselves, "Do research...OK, I'll watch the guy and call it science" [9]. In 1999, the Honeynet Project was formed with 30 members from the, at that stage, small cyber security community. Amongst that group of 30 was Lance Spitzner and he described a Honeypot as:

"A … security resource whose value lies in being probed, attacked, or compromised… It does not matter what the resource is (a router, scripts running emulated services, a jail, an actual production system). What does matter is that the resource's value lies in its being attacked" [10].

Common deployment strategies for Honeypots were described by Scottberg et al. [11]. They include: "Sacrificial Lamb", an isolated system that has no entry point to production systems; a "Hacker Zoo", an entire subnet of Honeypots with varied platforms, services, vulnerabilities, and configurations, which are isolated from production systems; a "Minefield", a number of Honeypots placed in forefront to serve as first attack targets; a "Proximity Decoy", a Honeypots deployed in close proximity to production systems; a "Redirection Shield External", that appear on production systems through port redirection and, lastly, a "Deception Port", simulating services (e.g., SMTP, DNS, FTP) on production systems.

III. CRITICAL CYBER THREAT TO MARITIME

As stated in the introduction the criticality and fragility of our supply chains is particularly evident within the Global Maritime Transportation System (GMTS).

In a 2019 report 'Shen attack: Cyber risk in Asia Pacific ports' – produced by the University of Cambridge Centre for Risk Studies, researchers described a hypothetical cyber-attack across the Asia Pacific against 15 ports using malware that jumped from ships to ports. They projected the loss could go as high as USD$110 Billion with the vast majority of that amount not being covered by any insurance [12]. Such a cyber-attack on this scale has not as yet been seen in the maritime sector, but we have seen numerous ports and ships impacted by attacks using ransomware, destructive malware, and the even hacking of Operational Technology (OT). These attacks have been initiated by both criminal groups and nation-state hackers. The well-known case of Maersk which lost over USD$200 million in 2017 in the NotPetya malware attack is a significant example [13].

In a non-cyber case in March 2020, the MV Evergiven blocked the Suez Canal and caused major disruption to the GMTS. While the incident was caused by human error rather than a cyber-attack it demonstrates the fragility of the GMTS costing some USD$9 Billion per day [14]. Such an incident could easily be deliberately caused by a cyber-attack. The threat actor could achieve this by compromising the navigation or propulsion systems of a ship or in a number of other ways. The aim of such an attack might be a part of a great power conflict (i.e., USA/China), a regional conflict (i.e., Israel/Iran), or by cybercriminals demanding ransom or shorting the stock market.

IV. PROJECT PLAN AND DESIGN CONSIDERATIONS FOR SHIP HONEYNET

A. *Project Plan*

The initial phase of the project to develop the ship Honey ship is as follows:

- Design of the ship Honeynet.
- Initial deployment in a test environment.
- Internal testing of the ship Honeynet.
- Penetration test by EC Council Certified Ethical Hacking (CEH) students.
- Initial deployment on the Internet.
- Examination of result of initial deployment and data gathered on cyber attacker activity.
- Analysis of cyber attacker information and artefacts gathered.
- Subsequent deployments with improvements.

B. *Architecture*

Ships are a complex network with a wide range of information and communication technologies onboard. Ships also have networked Operational Technology (OT) often directly connected to their IT networks.

Due to this significant complexity for the first version of the maritime Honeynet it was decided to just simulate the Integrated Bridge System (IBS) of a ship. This was to simplify the task for this initial version and also because of the critical nature of the IBS. The IBS acts as the main command and control of a vessel as it interconnects various digital devices used for navigation in open seas and is also connected to other on-board systems of a vessel, e.g., navigation and control, propulsion and machinery management system, cargo management system and safety management system, core infra structure systems, administrative and crew welfare systems, etc. [15]. Additionally, it also provides a gateway to the Internet.

The International Maritime Organisation (IMO) defines an IBS as combination of systems which are interconnected in order to allow centralized access to sensor information or command/control from workstations, with the aim of increasing safe and efficient ship's management by suitably qualified personnel [16].

The main components that are part of the IBS are Automatic Identification System (AIS), Electronic Chart Display Information System (ECDIS), radar, conning display, Bridge and Watch Alarm System (BNWAS) / Bridge Alert Management System (BAMS), Voyage Data Recorder (VDR), and autopilot. Sensors like compass, speed log, and echo sounder are also providing information to the system in the IBS [17]. In most cases there is Satellite terminal connected to provide the access through to the Internet.

 ISBN: 978-1-61208-996-6

The diagram in Figure 1 represents an architectural drawing of the ship Honeynet consisting of the following components ECDIS, Satcom, AIS, Long-Range Identification and Tracking (LRIT), VHF communications and VDR. These are the identified minimum components to run a realistic ship Honeynet. While not all the potential components of an IBS are represented the key systems are present.

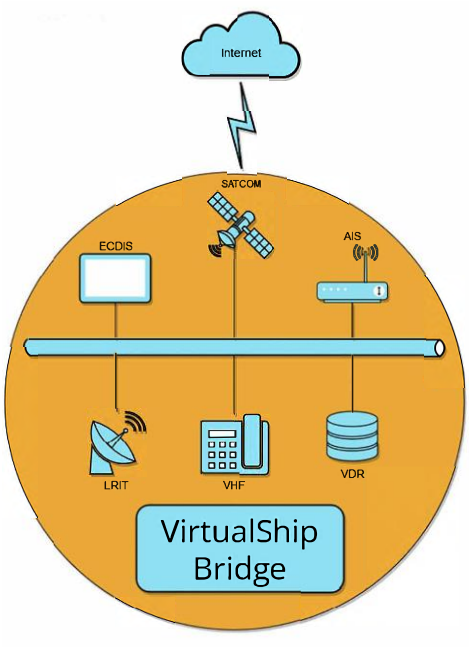

Figure 1. Minimal architectural drawing of the ship Honeynet. [18]

Figure 1 also describes the components that will each be hosted in so called docker containers. A docker container image is a lightweight, standalone, executable package of software that includes everything needed to run that application: code, runtime, system tools, system libraries and settings [19]. In practice, a container is easy to deploy and maintain. Utilising docker containers also provides security to prevent cyber attackers jumping from the ship Honeynet to the host system.

C. *Making the ship Honeynet an attractive target*

Considerations also needs to be made to make the ship Honeynet attractive and believable to potential cyber attackers.

To make the IBS attractive to cyber attackers as possible the following considerations will be taken into account [18]:

- Logical server location.
- Logical sailing route with realistic AIS data.
- Network speeds when using satellite should be slow.
- Network signs of life with traffic between systems.
- Logical entry point for cyber attackers i.e., Satcom, remote access portal etc.
- System architecture appropriate to type and size of ship.

The ship Honeynet is also going to use a technique proposed by Luo et al. [7] called intelligent interaction. The goal of intelligent-interaction is to learn the 'correct' behaviours to interact with clients from zero-knowledge about the maritime Honeynet.

D. *Entry point for ship Honeynet*

The entry point for a cyber attacker into the IBS is the satellite terminal for the first version of the ship Honeynet. Different vulnerability reports have revealed the misconfiguration of these types of remote management terminals are common. Leaving them open allows entry and also access to the network that sits behind it. So, when a cyber attacker is scanning the IBS they will find for example an open SSH port of the satellite terminal to attack and enumerate.

A specific example of a possible attack vector for the cyber attacker and a way of gaining access to the IBS can be done by emulating a Cobham SeaTel terminal. This type of terminal is being used as a gateway to the Internet. The Cobham SeaTel terminal has vulnerability regarding injection of malicious JavaScript using the devices TELNET built-in commands [20]. This way the attacker can gain access to the IBS directly from the Internet then move around the connected ship Honeynet in a realistic fashion.

E. *Broader scenario development for ship Honeynet*

The research team have gathered information on 152 maritime cyber incidents dating from 2001 to 2022. This is currently being formatted and will be published in December 2022. Analysis of those different cyber-attacks will inform scenario development for the Honeynet. For example, there was a malware attack targeting a deep draft Vessel travelling to the Port of New York in 2019 [21]. The malware in this example was transferred via USB drive. We would alter this ship cyber incident so the transfer could occur through the Internet gateway of the ship Honeynet since the introduction of malware via a USB is difficult to simulate within a ship Honeynet.

F. *Capturing the cyber attacker interaction*

An essential part of the maritime Honeynet is capturing the activity of the cyber attackers and storing it for later analysis. One basic but important element is capturing the source of the attack. The source refers to the origin of the attack and it includes the country and location. While source information such as IP addresses used by cyber attackers are often proxied to hide their origin or use anonymizing networks such as Tor they still may allow for attribution. Research on attribution has shown numerous methods of identifying the source of cyber-attacks [22]-[24]. This also includes examining the characteristics of the attack tools utilised.

 ISBN: 978-1-61208-996-6

Retaining the actual network traffic in the form of a packet captures is a preferred option for the project, but can cause storage issues if not managed carefully. Other network parameters and connection information will also be captured. Naturally all cyber attacker keystrokes and files will be captured.

G. Testing the ship Honeynet

NHL Stenden University of Applied Sciences teach the EU Council Certified Ethical Hacking program. Researchers working with students of that program will thoroughly penetration test the ship Honeynet for its functionality, realism and security. This will be an iterative process as new versions are created. Students involved will complete detailed surveys to identify weaknesses and areas for potential development in the ship Honeynet. Researchers will also evaluate the monitoring and data capture to ensure it is capturing all activity of the cyber attacker.

H. Secrecy and deception of the ship Honeynet

While it may appear an unusual approach to talk about the ship Honeynet if the aim is to trick cyber attackers it believing it is real. However, the nature of deception means that even if a cyber attacker reads this research they will not know when scanning the Internet and they find something that looks like a ship whether in fact it is a Honeynet or the real thing and may conclude that it is a Honeynet when in fact it is the real digital footprint of a ship. Research on cyber deception has shown it may significantly slow down their progress and negatively influence the decision making of a cyber attacker [25], [26].

V. CONCLUSIONS

While the design, development, and operation of a ship Honeynet is a quite complex project the benefit of intelligence that it would provide on current cyber attacker activity including modus operandi, motive and origin make it a worthwhile effort. The project itself will involve a series of ship Honeynets to build capability and to explore different aspects of the maritime sector.

A. Future Research

One area of further research is to focus is going to be on developing a more mature model that also represents both Information Technology and Operational Technology networks in ship environments.

This is a challenge because the maritime industry has a lot of standards for interconnecting components. The most relevant protocols are NMEA 2000, NMEA 0183, TCP/IPv6, and the latest one NMEA OneNet [27].

Other options include exploring simulating various types of ship environments such as container ships, cruise ships, tugboats, and executive yachts.

While a ship Honeynet in this case is used to study cyber attackers, it can also be a method to delay, frustrate and confuse them. This is an area studied under cyber deception but also an opportunity for further research in this area.

B. Benefits of the ship Honeynet

As stated, the ultimate purpose of a Honeynet is to be "probed, attacked, or compromised" by cyber attackers and by this process we learn more of the nature of those attacks, the threat they pose, the modus operandi of those attackers including their Tactics, Techniques and Practices (TTPs), their motives and other relevant features of their activity. This intelligence will be used for industry awareness, research reports/publications, reporting any identified vulnerabilities to vendors, and creating realistic maritime cyber incident simulations.

ACKNOWLEDGMENT

The authors would like to thank the contribution of the software engineering student group from Windesheim University of Applied Sciences, Rick Rijnierse, Erik Vedelaar, Stan van der Veen and Sami el Farj.

REFERENCES

[1] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, 2021, doi: 10.1109/COMST.2021.3106669.

[2] C. Bronk and P. deWitte, "Maritime cybersecurity: Meeting threats to globalization's great conveyor," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2020, vol. 2020-January. doi: 10.24251/hicss.2020.240.

[3] W. Loomis, V. V. Singh, G. C. Kessler, and X. Bellekens, "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity," Oct. 2021.

[4] K. Tam and K. D. Jones, "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping," *Journal of Cyber Policy*, vol. 3, no. 2, 2018, doi: 10.1080/23738871.2018.1513053.

[5] G. Kessler and S. Shepherd, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. Daytona Beach, Florida: Independently published, 2022.

[6] Mandiant, "Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries," Alexandria VA, 2018.

[7] T. Luo, Z. Xu, X. Jin, Y. Jia, and X. Ouyang, "IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices," *Black Hat 2017*, 2017.

[8] C. Stoll and J. W. D. Connolly, "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage," *Phys Today*, vol. 43, no. 8, 1990, doi: 10.1063/1.2810663.

[9] C. Stoll, "The Cuckoo's Egg: A True Story of International Computer Espionage,". 1989. Doubleday, New York. ISBN: 0-385-24946-2.

[10] L. Spitzner, *Honeypots: Tracking Hackers By Lance Spitzner*, vol. 52, no. 1. 2002.

[11] B. Scottberg, W. Yurcik, and D. Doss, "Internet honeypots: protection or entrapment?" in *IEEE 2002*

International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No.02CH37293), 2002, pp. 387–391. doi: 10.1109/ISTAS.2002.1013842.

[12] J. Daffron and S. Ruffle, "Shen Attack: Cyber Risk in Asia Pacific Ports," 2019.

[13] L. Matthews, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," *Forbes*, 2017.

[14] J. M. Lee and E. Y. Wong, "Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain," *MATEC Web of Conferences*, vol. 339, 2021, doi: 10.1051/matecconf/202133901019.

[15] M. S. Kaleem Awan and M. A. A. Ghamdi, "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)," *J Mar Sci Eng*, vol. 7, no. 10, 2019, doi: 10.3390/jmse7100350.

[16] BIMCO, "The Guidelines on Cyber Security Onboard Ships," *International Chamber of Shippinger of Shipping*, vol. 4, 2021.

[17] C. Hemminghaus, J. Bauer, and E. Padilla, "Brat: A bridge attack tool for cyber security assessments of maritime systems," *TransNav*, vol. 15, no. 1, 2021, doi: 10.12716/1001.15.01.02.

[18] R. Rijnierse, E. Vedelaar, S. van der Veen, and S. el Farj, "Ship Honeynet Student Project," Windesheim, 2022.

[19] S. Bistarelli, E. Bosimini, and F. Santini, "A report on the security of home connections with IoT and docker honeypots," in *CEUR Workshop Proceedings*, 2020, vol. 2597.

[20] The Mitre Corporation, "CVE-2018-5071," 2018.

[21] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *Network*, vol. 2, no. 1, 2022, doi: 10.3390/network2010009.

[22] S. McCombie, "Threat actor-oriented strategy: knowing your enemy to better defend, detect and respond to cyber-attacks," *Journal of the Australian Institute of Professional Intelligence Officers*, vol. 26, no. 1, pp. 24–41, 2018.

[23] T. Rid and B. Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, Jan. 2015, doi: 10.1080/01402390.2014.977382.

[24] S. Goel, "Cyberwarfare," *Commun ACM*, vol. 54, no. 8, pp. 132–140, Aug. 2011, doi: 10.1145/1978542.1978569.

[25] K. J. Ferguson-Walter *et al.*, "The Tularosa study: An experimental design and implementation to quantify the effectiveness of cyber deception," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2019, vol. 2019-January. doi: 10.24251/hicss.2019.874.

[26] K. E. Heckman, F. J. Stech, B. S. Schmoker, and R. K. Thomas, "Denial and Deception in Cyber Defense," *Computer (Long Beach Calif)*, vol. 48, no. 4, 2015, doi: 10.1109/MC.2015.104.

[27] K. Tran, S. Keene, E. Fretheim, and M. Tsikerdekis, "Marine Network Protocols and Security Risks," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 239–251, 2021, doi: 10.3390/jcp1020013.

 ISBN: 978-1-61208-996-6