KR SERVICE

KR Maritime Cyber Safety News & Report

Vol. 064

Dec. 2024

Korean Register
www.krs.co.kr

CONTENTS

Marlink: Most common cyber security threats in shipping

Source : Safety4sea

Marlink has released the latest global maritime cyber security threat report produced by its Security Operations Centre (SOC).

The report, based on data gathered during the first half of 2024 demonstrates the changing tactics of cyber criminals, who are increasingly attempting to bypass previously effective security controls using new tools. In the first half (H1) of 2024, the Threat Intelligence team within Marlink's Security Operations Centre has observed the following activities carried out by malicious actors:

Phishing

Malicious actors send fraudulent e-mails or messages to trick individuals into revealing sensitive information like passwords or financial details. Phishing attack trends include HTM/HTML documents with embedded links and QR codes to credential harvesting login landing pages hosted on difficult-to-block infrastructure (e.g., Microsoft), as well as typosquatted and BEC(Business email compromise) senders. Phishing tactics include the use of open redirects and reverse proxies.

Commodity Malware

Widely available malware is typically sold or distributed for common use by cybercriminals and is often used in large-scale, automated attacks. For example, Agent Tesla is a phishing payload used for information theft.

DDoS

Attacks involve multiple systems overwhelming a target server or network with excessive traffic, causing it to become unavailable to users, especially affecting port infrastructure and maritime transportation companies.

Typosquat Domains and DMARC

Domains mimic legitimate websites by using slight misspellings, aimed at tricking users into visiting them to steal information or distribute malware. Maritime organizations have been spoofed by different domains.

Password Spraying

A type of brute-force attack where attackers try a few commonly used passwords across many accounts to avoid detection and gain unauthorized access. VPN gateway user accounts have been widely exploited by trying common passwords.

Scanning and Probes

Systematic examinations of systems or networks for vulnerabilities or open ports to exploit by attackers include application server protection violation attempts, SSH failed authorization attempts, SQL scanning, vulnerability scanning, and firewall probing.

Key strategies for strengthening your cyber security defences

- **Vigilance and proactive measures are essential**

Regular training, strong e-mail security, and advanced detection systems play a vital role in reducing the risk of phishing, spam, and other malicious activities.

- **Timely incident response is crucial**

SOC teams must remain vigilant and respond to alerts in real time to minimize potential damage. Automated response mechanisms can be implemented to reduce manual intervention and speed up threat containment.

- **Continuous improvement of security posture**

As threat actors evolve, so must security defences. Continuous monitoring, updating blacklists, improving detection systems, and refining incident response processes are essential in staying ahead of the threat landscape.

Marlink: Reverse phishing is an emerging cyber threat

Source : Safety4sea

In its Global Maritime Cyber Threat Report published earlier this month, Marlink explores cyber threats within the maritime industry, highlighting the increase in sophisticated attack methods such as reverse proxy phishing.

According to Marlink, during the first half of 2024 (H1 2024), a significant portion of the threats neutralized continued to follow the most common attack vector seen since 2022: phishing. However, there has been a notable increase in a more advanced form known as “reverse proxy phishing.”

“The evolution of the threat landscape in the first six months of 2024 has continued to surprise. It is clear that even vessel operators who have previously acted against cyber threats must consider this a continuous process.” said Nicolas Furgé, President Digital, Marlink in an article published on their website.

Phishing is a classic cyberattack method where attackers impersonate legitimate entities (like banks or service providers) to trick users into providing sensitive information, such as login credentials or financial data. Traditional phishing often relies on fake websites or fraudulent emails to capture user data.

As explained by MJ Casado de Amezua, Threat Intelligence Analyst, Marlink, “Reverse proxy phishing,” on the other hand, is a more sophisticated version. Instead of simply creating a fake website, the attacker sets up a “proxy” that sits between the legitimate website and the victim.

This proxy captures the user’s credentials and, in real-time, forwards them to the actual site, making the victim feel like everything is normal. The danger of this method lies in its ability to bypass multi-factor authentication (MFA), which is commonly used to protect sensitive systems.

Reverse proxy phishing opens the door to serious cybersecurity threats such as Command and Control (C&C) systems, botnets, and Remote Access Trojans (RATs). Once attackers gain access to a network, they can deploy C&C infrastructure to remotely control compromised systems, potentially creating botnets—large networks of infected devices used for malicious activities like Distributed Denial of Service (DDoS) attacks.

Additionally, attackers may install RATs(Remote Access Trojan), granting them full control over the victim's machine, allowing them to monitor activity, steal more data, or execute commands covertly.

In the maritime sector, these attacks can significantly impact operations, disrupting shipping logistics and manipulating sensitive communication systems. Delays, loss of reputation, and costly recoveries are just a few of the possible outcomes. To combat these threats, it is critical that maritime companies adopt advanced security technologies. Security Operations Centres (SOCs) must enhance their monitoring capabilities with real-time threat detection, AI-driven behavioral analysis, threat intelligence, and stronger MFA(Multi-Factor Authentication) solutions.

"Focusing on the combination of people, procedures and precautions, these companies can better protect themselves and their stakeholders, ensuring safer and more resilient operations." explained Nicolas Furgé.

By doing so, organizations can better protect themselves from this evolving cybersecurity threat, ensuring safer and more resilient operations.

Strength in numbers – why maritime cyber security is a team sport

Source : Wärtsilä

A ship-to-shore data connection seems to have been compromised. Do you pull the plug right away or wait for more details to better assess the risks? What decisions need to be made and who needs to be informed? These are just some of the questions you might face if you participate in a cyber incident exercise. How would you manage and what would you learn?

As the maritime industry becomes ever more connected and data driven, there are enormous new opportunities, but also intensifying threats. Cyber criminals are constantly finding new and clever ways to hack systems and steal data. Until recently, however, there was very little in terms of mandatory cyber security requirements on maritime equipment.

In the summer of 2022, the International Association of Classification Societies adopted two new Unified Requirements on maritime cyber security. If you contract a newbuild vessel on or after July 1, 2024, it will need to comply with these requirements. Some of the responsibility lies with the owner, some with the shipyards and some with the equipment vendors who supply the equipment for the vessel.

With new standards and equipment, the maritime industry should be a lot better prepared to face cyberattacks. But as with any safety equipment or procedures, they need to be tested regularly so that you know how to respond effectively if things ever go wrong.

Incident exercises – the fire drills of cyber resilience

Just like an office fire drill, the aim of a cyber incident exercise is to prepare you for the real thing – to give your people the experience and skills they need to make the right decisions when it really matters.

Wärtsilä regularly conducts these cyber incident exercises. In a recent exercise, participants from the Wärtsilä Marine management team were told that there had been a potential hack of the Wärtsilä connection for sending and receiving data between shoreside operations and cruise vessels.

The connection is working properly but somebody might have taken over the system with unknown consequences. Do we pull the plug immediately, causing service disruptions and costing everyone involved significant amounts of money, or do we wait for more details to assess risks more accurately? Is this even a real attack?

The aim of the exercise was not to find technical solutions but to enhance decision making, cooperation and communication skills. Participants focused on risk assessment, mitigation planning and crisis management, while the exercise evolved in real time as more information became available and new issues were thrown into the mix.

“The exercise was very realistic and pretty stressful – and that was before things took an unexpected twist. Suddenly a call came into the situation room from Leigh Carr, Vice President, Maritime Cybersafety at Carnival Corporation. This was not an actor but a genuine customer, and she wanted to know what was happening. Suddenly things became even more realistic,” explains participant Andrea Morgante, Vice President Performance Services, Marine at Wärtsilä.

A united front is the best defence

At first the participants felt uncomfortable, but it soon became clear that transparency, open communication and a united front against the common threat was the best line of defence.

Because knowledge is power, the more information that is available – and the faster it is shared within the team – the more each party can bring their own experiences and expertise to the table. And this is not just in terms of finding technical solutions to the problem, but also aspects such as communicating to employees, stakeholders and, in this case, passengers.

The winning team is the one that plays together

The best teams don’t win by just turning up to the game and doing their best. They win because their skills and the way the players interact have been perfected over countless hours of practice. Cyber resilience is no different. The more you practice, the better you play together and the harder it is for the opposition to divide and conquer you.

For the participants from the Wärtsilä Marine management team, the exercise with a participant from Carnival was a great opportunity to share and develop best practices as well as to test plans and procedures. Exercises like this mean that if there ever is a real situation, the affected parties will have a big head start when it comes to neutralising the threat because the basics will be second nature. Joint preparedness raises collective resilience.

“Wherever you are in the maritime value chain – a ship owner or operator, a yard, a port or a supplier – the value of joint cyber incident exercises cannot be overstated. If you have a cyber security team and see cyber resilience as a key focus area, let’s learn and develop together,” says Morgante.

Cybersecurity and Maritime in the EU: Navigating the Digital Seas

Source : gtg

The maritime industry, a vital pillar of global trade, is now at a crossroads, facing an alarming and rapidly escalating threat from cyber attacks. As digital technologies become an inseparable part of naval operations, the need for robust cybersecurity measures has reached a critical and immediate point.

Cybersecurity is a global challenge that transcends national borders. The interconnected nature of maritime operations means that a single cyber incident, regardless of origin, can have profound and far-reaching consequences. Integrating Information Technology (IT) and Operational Technology (OT) in the maritime sector presents unique cybersecurity challenges. OT systems, which control physical processes such as navigation, engine management, and cargo handling, are increasingly connected to IT networks, exposing them to cyber threats. As critical nodes in the maritime supply chain, ports are particularly vulnerable to cyberattacks.

Several high-profile cyber incidents have highlighted the vulnerabilities within the maritime sector, including the following :

- Maersk NotPetya Attack (2017): The attack led to significant financial losses, estimated at around $300 million, highlighting the critical need for robust cybersecurity measures in the maritime industry.
- Port of San Diego Ransomware Attack (2018): This incident underscored the vulnerability of port infrastructure to cyber threats and the importance of securing both IT and OT systems.
- COSCO Shipping Lines Cyber Attack (2018): The attack disrupted communication and booking systems, demonstrating the far-reaching impact of cyber incidents on global shipping operations.
- Mediterranean Shipping Company (MSC) Cyber Incident (2020): MSC experienced a cyber incident, highlighting cybersecurity's importance in maintaining the continuity of maritime operations.

This sector is governed by a plethora of international conventions and regulations, including the Convention on the High Seas (1958), the International Regulations for Preventing Collisions at Sea (1972), the International Convention for the Safety of Life at Sea (SOLAS, 1974), and the United Nations Convention on the Law of the Sea (UNCLOS, 1982). These conventions primarily focus on physical safety and navigation, with little to no provisions for cybersecurity.

In 2016, the International Maritime Organization (IMO) recognised the importance of cybersecurity, issuing temporary risk management guidelines, later superseded by formal guidelines. In 2017, the IMO adopted Resolution MSC.428(98), mandating that shipping companies incorporate cybersecurity risk management into their Safety Management Systems by January 2021. IMO has been at the forefront of addressing these cybersecurity issues. However, the maritime industry also relies heavily on the principles outlined in the NIST CSF to bolster its cybersecurity measures.

This framework, updated to version 2.0, is designed to enhance cybersecurity risk management across various sectors, including maritime operations. It introduces a sixth core function, 'Govern,' which emphasises integrating cybersecurity practices with overall organisational governance to ensure that cyber risk management aligns with broader business objectives.

Whilst the maritime industry has made strides in aligning with NIST CSF, there remain significant gaps, particularly in cybersecurity supply chain risk management. Aside from the latter, the available principles and guidelines provide high-level principles without detailed implementation strategies, leaving a significant gap in cybersecurity preparedness. Given cyber threats' evolving and increasingly sophisticated nature, there is a growing consensus that existing regulations are insufficient. The current conventions were established long before the digital age, and their provisions do not adequately address the complexities and urgency of cybersecurity.

The EU's updated Network and Information Systems Directive (NIS2) and the Critical Entities Directive (CED) are set to impact the maritime sector significantly. NIS2 expands the scope of the original NIS Directive, imposing stricter cybersecurity requirements on a broader range of entities, including those in the marine industry.

Maritime companies must invest more in cybersecurity and ensure compliance with these new regulations. Member States play a crucial role in developing and enforcing cybersecurity standards within the EU. For instance, the EU's General Data Protection Regulation (GDPR) and the NIS Directive (1 and 2) have significant implications for the maritime industry, requiring companies to implement robust cybersecurity measures and report incidents promptly. They also aim to enhance cybersecurity across member states by promoting cooperation and harmonising national cybersecurity capabilities by introducing the first European cyber crisis liaison organisation network (EU-CyCLONe), a cooperation network for Member States' national authorities in charge of cyber crisis management.

The Critical Entities Directive (CED) complements NIS2 by focusing on the resilience of critical infrastructure, including ports and maritime transport facilities. CED requires member states to identify essential entities and implement robust security measures to protect against physical and cyber threats.

The EU's Artificial Intelligence Act (AI Act) also has significant implications for the maritime sector, particularly regarding the use of AI in operational technology and ports. The AI Act ensures that AI systems are safe and transparent and respect fundamental rights. For the maritime industry, AI systems used in navigation, cargo handling, and other critical operations must meet stringent requirements for robustness and cybersecurity.

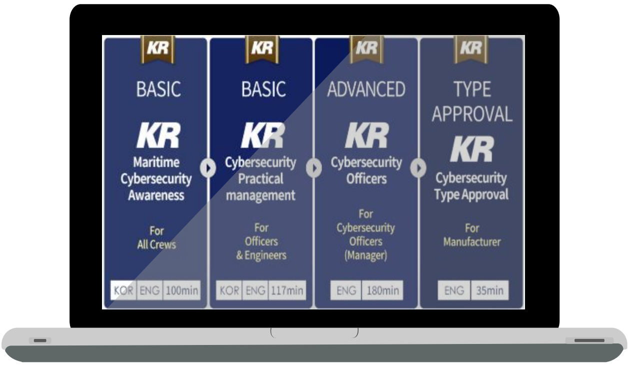
The industry is at a critical juncture, facing increasing cyber threats that require a coordinated and comprehensive response. Updating existing regulations and harmonising everything into a coherent framework is essential to enhancing maritime cybersecurity. However, this is not enough. International cooperation, robust standards, and proactive measures by naval companies are equally crucial. The global marine community can collectively strengthen its cybersecurity defences by sharing information, best practices, and resources. This will ensure the maritime industry can navigate the digital seas safely and securely.

Online Training

KR Maritime Cybersecurity e-Learning Center training course

Korean Register's
Maritime Cyber Security
e-Learning Course

MCS e-Learning system open!



BASIC
KR
Maritime Cybersecurity Awareness
For All Crews
KOR | ENG | 100min

BASIC
KR
Cybersecurity Practical management
For Officers & Engineers
KOR | ENG | 117min

ADVANCED
KR
Cybersecurity Officers
For Cybersecurity Officers (Manager)
ENG | 180min

TYPE APPROVAL
KR
Cybersecurity Type Approval
For Manufacturer
ENG | 35min

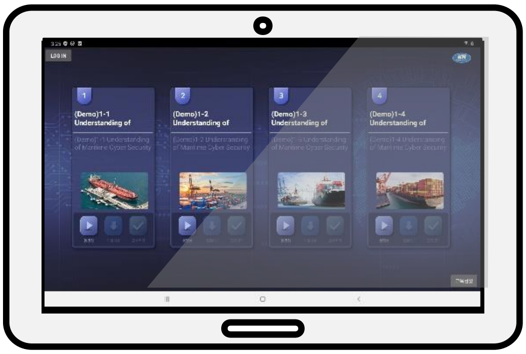
Q&A : https://edu.orangecq.com/

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

KR CS++

KR Cybersecurity training tool


LOG IN
1
(Demo)1-1
Understanding of
(Demo)1-1 Understanding of Maritime Cyber Security
2
(Demo)1-2
Understanding of
(Demo)1-2 Understanding of Maritime Cyber Security
3
(Demo)1-3
Understanding of
(Demo)1-3 Understanding of Maritime Cyber Security
4
(Demo)1-4
Understanding of
(Demo)1-4 Understanding of Maritime Cyber Security

No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.

KOREAN REGISTER

Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr

Copyright @ 2023 ALL RIGHTS RESERVED BY KOREAN REGISTER