

KR Maritime Cyber Safety News & Report



Vol. 059
Sept. 2023



CONTENTS

KR Cyber Security Activities

- K Shipbuilding granted approval for cyber resilient ship design
- KR awards AIP to SHI for ship cyber resilience implementation technology
- KR, Maritime Cyber Safety Expert Forum Announces

Maritime Cyber Safety News

- NHL Stenden University launches Maritime Cyber Attack Database

Maritime Cyber Security Expert Column

- Latest trends in ransomware attacks and responses
- Maritime Cybersecurity Risk Paradigm and Ransomware

Advertisement

- KR Cyber Security Training Tool & E-LEARNING

K Shipbuilding granted approval for cyber resilient ship design

Source : The KOREA MARITIME NEWS, Shipbuilding Industry Team
 Editor : AHN Jongwoo, Korean Register



< From left, Mr. KOH, Tae-Hyun (Chief Technology Officer, Division Director), Mr. KIM Daeheon (Executive Vice President of KR) and Mr. KIM, Sang-Yong (President & CEO of ForceTEC) >

Korean Register (KR, Chairman Lee Hyung-cheol) announced on June 26 that it awarded the concept approval (AIP) for the 'Methodology for the Design and Implementation of IACS UR E26' developed by K Shipbuilding (President & CEO Jang Yoon Keun).

IACS UR E26 is a common rule on cyber resilience of ships established by the (International Association of Classification Societies (IACS) in April 2022, and is mandatory for ships contracted for construction after 1 January 2024. Cyber resilience refers to the function of reducing cyber incidents and mitigating the impact of operational technologies (OT) used for safe operation of ships when they are interrupted or damaged by cyber incidents.

With this certification, K Shipbuilding met international certification standards that emphasize protection from cyber attacks and data threats when operating ships. The technology was developed in collaboration with ForceTEC.

Cyber Resilience of Ship (IACS UR E26) was established in 2022 by the IACS to protect ships' assets from hacking. It will be mandatory for all ships contracted for construction after 1 January 1, 2024, which might be delayed.

Ships to be built recently require strong cyber security technology due to the application of information and communication technology (ICT), automation, and satellite communication technology, and the International Maritime Organization (IMO) and the Ministry of Oceans and Fisheries are also designating this as recommendations. In particular, ship cyber resilience technology is a key technology for autonomous ships.

In order to protect international needs and customers' assets, research and development to reduce and restore cyber incidents by analyzing vulnerabilities of major operating technologies such as propulsion, steering, navigation, and electricity generation in ships was conducted with ForceTEC, which provides data centers, system management, and network services to K Shipbuilding's affiliates.

A maritime cyber resilience system has been established to meet international standards by preparing measures to respond to risks caused by the Internet, which is used as office work and welfare for sailors. Based on this, the validity, safety, and suitability of the concept design of ship cyber resilience were verified and the concept was certified based on KR's ship cyber risk evaluation technology.

KOH Tae-Hyun, a Chief Technology Officer and Division Director, said, "We have recognized the cyber risks that may occur during ship operation, and made continuous efforts to prevent and respond to them," adding, "We have developed a comprehensive security solution to protect networks and systems in the ship by utilizing the latest security technology and the knowledge of experts in each field, and based on this, we will provide greater trust to customers."

KR awards AIP to SHI for ship cyber resilience implementation technology

Editor : AHN Jongwoo, Korean Register



< From left, Mr. KIM Dongjoo (Head of Shipbuilding Sales Engineering Team of SHI), Mr. SONG Kanghyun (Senior Vice President of KR Decarbonization-Ship R&D Center), Mr. JANG Haeki, Executive Vice President(CTO) of SHI Engineering Operations, Mr. KIM Yeontae (Executive Vice President of KR's Technical Division), Mr. YEON Kyujin (Senior Vice President of KR Plan Approval Center), Mr. KWON Jinho (Senior Surveyor of KR) >

Korean Register (KR, Chairman Lee Hyung-cheol) has awarded an Approval in Principle (AIP) to Samsung Heavy Industries (SHI) for 'design and test procedures for implementing cyber resilience of ship and onboard systems based on IACS UR E26 and E27'. The AIP was presented at Gastech 2023 in Singapore on September 6.

The application of ICT technology to ships, e.g. smart ship solutions, etc., is expanding. Cyber threats such as hacking and ransomware are an increasing risk as the integration and digitalization of operational technology and information technology systems accelerates.

To address this, the International Association of Classification Societies (IACS) introduced UR E26 and E27 last year. These are unified requirements for enhancing cyber resilience of ships and onboard systems. These requirements are set to become mandatory for ships contracted for construction on or after January 1, 2024. Cyber resilience goes beyond safeguarding ships against cyber threats and includes minimizing the impact of such incidents to ensure operational safety.

Since October last year, KR has been collaboratively developing design and verification methods for implementing cyber resilience based on UR E26 and E27 with SHI. This partnership was formed to proactively meet IACS's mandatory guidelines. This AIP award recognizes the successful collaboration of joint development between KR and SHI. KR provided SHI with technical advice on ship cyber resilience application technology, including security functions and network design for ship operational systems, and contributed to securing the base technology for applying cyber resilience to ships built by SHI.

KIM Yeontae, Executive Vice President of KR's Technical Division, said:

"This AIP award to Samsung Heavy Industries serves as an opportunity to internationally publicize the excellence of KR's ship cyber resilience technology. KR will continue to strengthen our technology and certification capability for ship cyber resilience with the goal of providing a higher level of service to our customers."

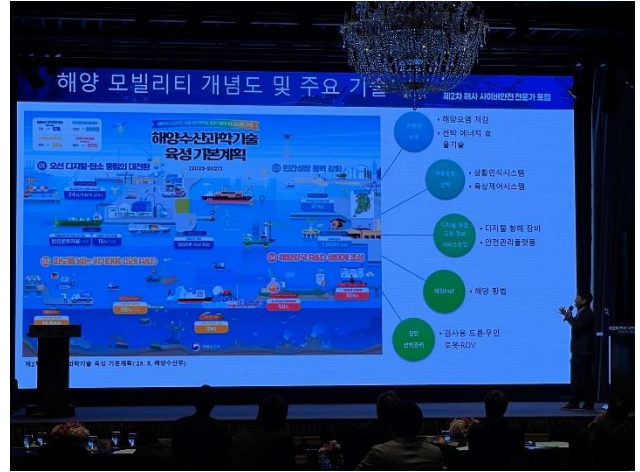
JANG Haeki, Executive Vice President(CTO) of SHI Engineering Operations, said:

"It is expected that the security of ships built by Samsung Heavy Industries will be further enhanced through this certification, which includes security application technology for cyber resilience of essential systems in ships as well as ships registered by KR, leading marine digital technology in shipbuilding."

Since 2018, KR has been providing company and ship certification services, type approval, and technical services for maritime cybersecurity, as well as online and offline training programs to strengthen cybersecurity capabilities for employees in the maritime industry.

KR, Maritime Cyber Safety Expert Forum Announces

Editor : AHN Jongwoo, Korean Register



Korean Register (KR, Chairman Lee Hyung-chul) participated in the 2nd Maritime Cyber Safety Expert Forum held at Lotte Hotel in Busan on September 6 and presented the theme of 'Cyber Safety Education for the Age of Marine Mobility.'

The Maritime Cyber Safety Expert Forum is a forum for the Ministry of Oceans and Fisheries Korea and the Korea National Intelligence Service to discuss the dangers of cyberattacks targeting ships that can cause massive human and property damage with experts from industry, academia, and related organizations.

Under the theme of 'the advanced marine mobility era, on how to secure future cyber safety', the presentation and discussion on the current status and direction of maritime cyber safety policies, technology development to expand cyber safety in the advanced maritime industry, and the direction of fostering maritime cyber safety experts and establishing a system were conducted. Mr. PARK Kaemyoung, General Manager of KR Cyber Certification Team, presented 'Cyber Safety Education for the Ocean Mobility Era' at the third session, the directional of training maritime cyber safety experts and establishing a system. In this announcement, Mr. Park explained the current status of maritime cyber safety technology and related cyber safety infrastructure to respond to cyber attacks in the maritime sector and presented a maritime cyber safety curriculum as a basic activity to secure maritime cyber safety.

NHL Stenden University launches Maritime Cyber Attack Database

Source : Safety4sea



Source: NHL Stenden

Researchers at NHL Stenden University of Applied Sciences have launched the Maritime Cyber Attack Database (MCAD), a database of incidents involving the worldwide maritime sector.

The database contains over 160 incidents, including the location spoofing of NATO ships visiting Ukraine in the Black Sea in 2021. The incidents in the database demonstrate the relevance of cyber security across the board of today's maritime industry and the vulnerabilities that exist.

“The scope of what is possible today is surprising, so we need to educate governments and companies about these kind of cyber-attacks and help them understand not only how to react to them, but how to be prepared for them.”

said Stephen McCombie, professor of Maritime IT Security at NHL Stenden University of Applied Sciences and leader of the Maritime Cyber Attack Database (MCAD) team.

Drawing from open source information, the NHL Stenden's Maritime IT Security research

group collected information on over 160 cyber incidents in the maritime industry for the MCAD. The database not only covers incidents impacting vessels, but also ports and other maritime facilities worldwide.

Now available publicly online, the research group expects the database will help improve cyber security awareness in the sector and provide data for further research and more accurate simulations in this critical area.

In recent years, cyber security has been a key challenge for shipping. Growing connectivity networks and digitalization efforts modernise shipping, but they also pose a severe danger to its integrity when attacked maliciously.

Latest trends in ransomware attacks and responses

Source : Prof. KIM Jongsung, Department of Information Security, Cryptology, and Mathematics, Kookmin Univ.

Editor : AHN Jongwoo, Korean Register

● Introduction

Ransomware is a combination of Ransom, which means ransom, and software, which means malicious software that locks a user's system or encrypts data, and then demands money in exchange for data access rights. Spear phishing and various vulnerabilities performed on specific targets to infiltrate victims' PCs. Then, after collecting the victim's information, data encryption is performed and money is requested.



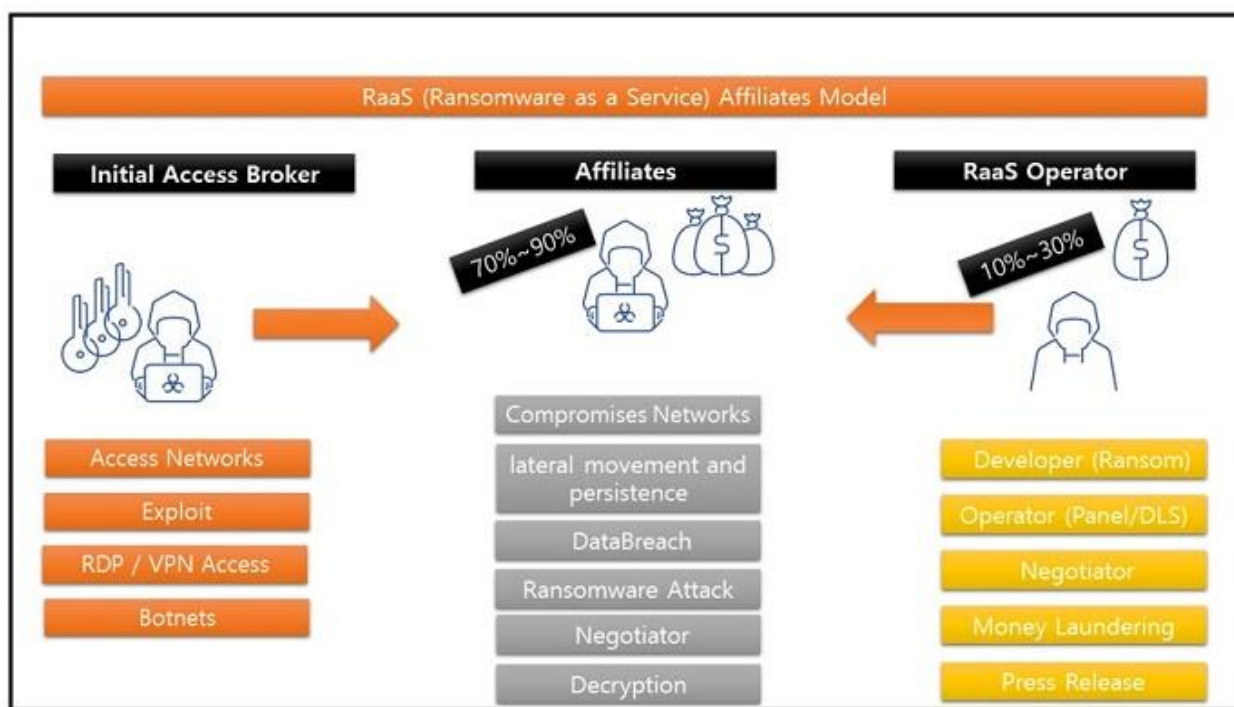
< Process of Ransomware attack [1] >

The annual amount of ransomware damage in Korea, compiled by RanCERT (Ransomware Computer Emergency Response Team Coordination Center), has increased every year since 2015 when ransomware first appeared in Korea. The total amount of damage over the seven years by 2021 is expected to reach KRW 6.86 trillion [2]. Ransomware is increasing the scale of damage by targeting key infrastructure facilities and companies in the country, including hospitals, schools, transportation facilities, and pipeline facilities, from the existing method of encrypting files to a large number of unspecified users and demanding virtual currency. In May 2021, Colonial Pipeline, a U.S. pipeline system provider, had all systems down due to a Darkside ransomware infection [3]. As a result, fuel supply problems in some parts of the United States

occurred, resulting in changes in flight schedules, fuel shortages at gas stations, and fuel prices renewed their highest prices since 2014. Colonial Pipeline paid \$4.4 million (about ₩5 billion) for data recovery.

● Ransomware Group Changes

Recently, ransomware groups are operating a Ransomware as a Service (RaaS) platform [6]. RaaS is a service model for developing and distributing ransomware and induces criminal activities by providing the tools and infrastructure necessary for development. This allows anyone to carry out ransomware attacks without expertise in development.



< RaaS Organizational Chart >

RaaS was initially run by a single developer or group. However, it gradually developed into a professional and advanced subscription model, and it became a method of paying part of the profits to ransomware developers.

● Ransomware Response in the worldwide

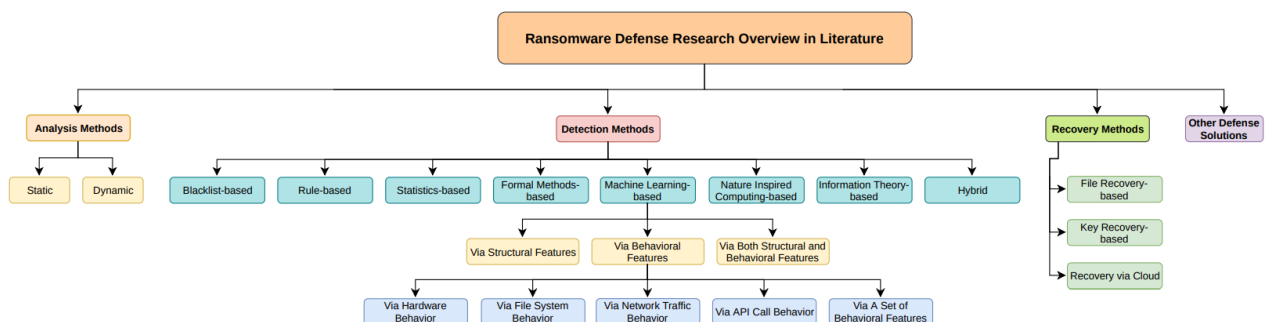
The international community is seeking ways to respond to ransomware through cooperation. In 2021, the U.S. opened the 'StopRansomware' site, a site that provides and shares

ransomware information, allowing rapid sharing of information related to ransomware collected by various organizations [7]. In Korea, a Korean-style "StopRansomware" site is also opened to provide a variety of recovery tools and provide quick response by allowing detailed reports of ransomware damage [8]. Government representatives from 35 countries, including South Korea, the United Kingdom, France and Germany, and the European Union Commission attended the second international conference on ransomware held for two days from October 31, 2022 [9]. The meeting was held focusing on ransomware infrastructure and actor response, strengthening resilience against attacks, responding to virtual currency for money laundering of criminal proceeds, and international cooperation. As such, various actions are underway to respond to ransomware and reduce damage internationally.

● Ransomware Response Research Trends

Ransomware research has been conducted in various ways from two perspectives: pre-response and post-response. Pre-response is a study from the perspective of detecting and preventing ransomware before it is infected. Post-response is a study from the perspective of recovering corruption and encrypted data after ransomware infection.

In 2016, a study was proposed to detect ransomware through screen changes and file system changes using large datasets [10]. In 2021, a study was proposed to summarize ransomware prevention and detection studies to identify trends [11]. According to the paper, ransomware prevention techniques use access control, data and key backup, and hardware-based solution-based techniques. In addition, the ransomware detection technology uses a combination of dynamic analysis, static and dynamic analysis, and machine learning model-based techniques.



Magniber v2's decryption paper published in 2020 identified vulnerabilities in the process of using Magniber v2 ransomware to generate encryption keys and suggested a way to decrypt encrypted data based on this [12]. In addition, in 2022, Kookmin University and the Korea Internet & Security Agency jointly developed a decryption tool for Hive ransomware issued by the FBI as a number of cases of damage, including medical institutions. Hive ransomware used its own cryptographic algorithm and discovered vulnerabilities that existed at this time and succeeded in decrypting data for the first time in the world [13]. In addition to this, there are a number of ransomware response studies.

● Conclusion

Ransomware is becoming more sophisticated, and attacks on healthcare institutions and infrastructure providers are increasing. As a result, not only companies that have been directly damaged, but also the general public who use the company's services will suffer. In addition, ransomware makes it difficult to prevent and respond by introducing new encryption and operation methods. Therefore, in order to reduce the risk of ransomware attacks, it is important to take preventive measures such as backup, applying the latest security updates, and using ransomware detection and blocking solutions.

● References

1. Begovic, Kenan, Abdulaziz Al-Ali, and Qutaibah Malluhi. "Cryptographic ransomware encryption detection: Survey." *Computers & Security* (2023): 103349.
2. KBS, 2021-07-15, <https://news.kbs.co.kr/news/view.do?ncd=5233638>
3. The New York Times, "Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers", 2021-05-13, <https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>
4. Trend Micro, "The Near and Far Future of Ransomware Business Models", 2022-12-15, https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf
5. ITWorld Korea, 2023-05-16, <https://www.itworld.co.kr/news/290809>
6. AhnLab 2023-07-03, <https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=33688>
7. "Stop Ransomware", <https://www.cisa.gov/stopransomware>

8. "KISA Stop Ransomware", <https://boho.or.kr/ransom/main.do>
9. Yonhap News Agency 2022-10-31, <https://www.yna.co.kr/view/AKR20221031023100071>
10. Kharaz, Amin, et al. "{UNVEIL}: A {Large-Scale}, automated approach to detecting ransomware." 25th USENIX security symposium (USENIX Security 16). 2016.
11. Oz, Harun, et al. "A survey on ransomware: Evolution, taxonomy, and defense solutions." ACM Computing Surveys (CSUR) 54.11s (2022): 1-37.
12. Sehoon Lee, Myungseo Park, and Jongsung Kim. "Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator." Electronics Vol.10(1), (2020): 16.
13. Giyoon Kim, Soram Kim, Soojin Kang, Jongsung Kim, "A method for decrypting data infected with Hive ransomware", Journal of Information Security and Applications, vol. 71, Dec 2022: 103387

Maritime Cybersecurity Risk Paradigm and Ransomware

Source : Kim Mi Hee, Security & Intelligence, IGLOO Corp.

Editor : AHN Jongwoo, Korean Register

● Current Status of Cyber Attack Damage in the Maritime Sector

With the development of information and communication technology, digitalization of the entire marine ecosystem is rapidly progressing. Next-generation maritime ecosystems such as MASS and Smart Port are further highlighting the importance of cybersecurity as they expand the contact point between onshore and ships. In addition to the two-week suspension of loading and unloading operations due to a ransomware infection at the port terminal IT system of the world's largest shipping company A.P. M. øller-Maersk in 2017, direct and indirect damage caused by cyberattacks has occurred in various maritime fields such as shipping companies, ports, and container carriers such as MSC, CMA CGM, Semcorp Marine, and DNV over the past three years.

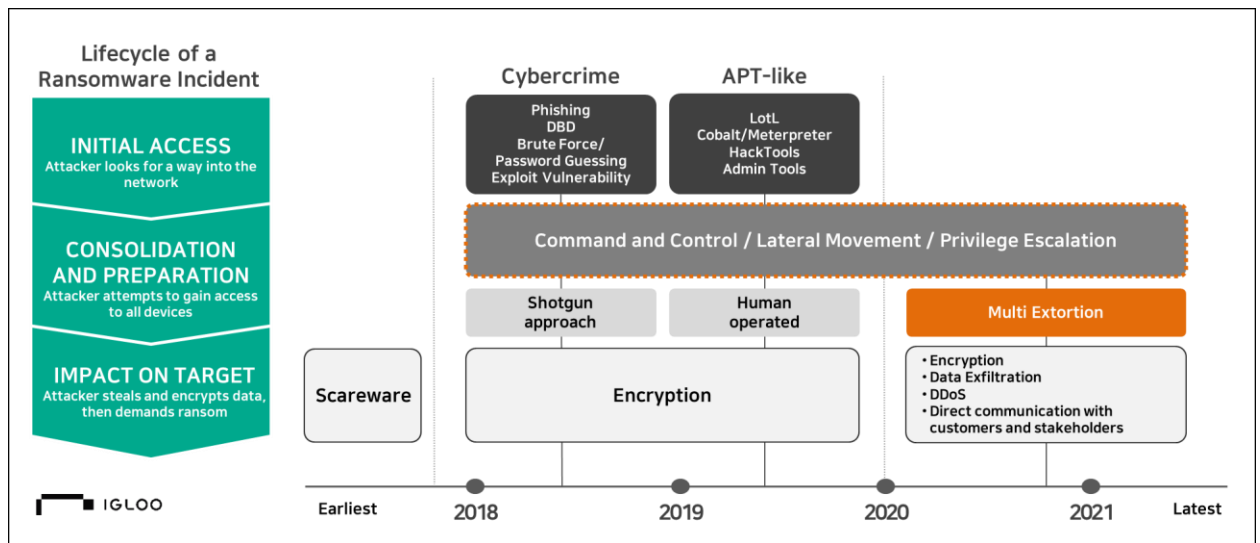
Date	Target	Method	Damage status
2017.06	A.P. Møller-Maersk	Ransomware	<ul style="list-style-type: none"> Ransomware infections in the port terminal IT system of the world's largest shipping company have halted shipping and unloading operations for two weeks, resulting in losses of \$200-300 million
2018.07	COSCO Shipping Lines	Ransomware	<ul style="list-style-type: none"> China's state-run shipping company COSCO is infected with ransomware, but some networks in the U.S. are suspended due to coastal-based system network errors
2019.03	H Shipping	Ransomware	<ul style="list-style-type: none"> Infection of ransomware on board some of the 90 ships, such as automobile carriers and bulk carriers, belonging to the fleet
2020.04	MSC	Malware	<ul style="list-style-type: none"> Malicious code infection attacks data centers at Geneva headquarters, including main website and online booking platform

2022.09	CMA CGM	Unauthorized access	<ul style="list-style-type: none"> Two-week website suspension after shipping container carrier is infected with Ragnar Locker ransomware
2022.08	Sembcorp Marine	Unauthorized access	<ul style="list-style-type: none"> Unauthorized access accidents occur in shipyard systems that build special ships and drilling ships
2022.12	Voyager Worldwide	Ransomware	<ul style="list-style-type: none"> Vessel Navigation Solution Company System Down with Ransomware
2022.12	4 EU Marine IT companies and shipping company	Ransomware	<ul style="list-style-type: none"> 2023.01 Attack Group PLAY Reveals Corporate Critical Data On Dark Web After 2022.12 Ransomware Infection
2022.12	Lisbon Port	Ransomware	<ul style="list-style-type: none"> System down and information such as port documents and cargo information is stolen by ransomware attack group LockBit
2023.01	DNV	Ransomware	<ul style="list-style-type: none"> Ship management SW server hacking of ship management SW companies, which account for 21% of the total share of the marine industry, is affected by 1,000 ships from 70 customers Immediately shut down the IT server and ShipManager connected to the ship management system to minimize damage to ransomware

< Current status of maritime cyber attack damage, IGLOO Corp. >

Ransomware has become the central point of cyberattacks as it is possible to acquire attack tools and technologies for cyberattacks such as credentials and leaked sensitive information as well as high-impact vulnerability transactions such as zero-day vulnerabilities through the Black Triangle. Considering that many of the cyberattacks in the maritime sector are caused by ransomware, it can be seen that the cyberattack paradigm is also reflected in the maritime ecosystem. Ransomware combines various attack technologies in order to maximize its influence, not just simple file encryption technologies.

Ransomware based on Scareware has developed into a form that advocates APT attacks (PAT-Like) in cybercrime aspects such as phishing, DBD, and Exploit Vulnerability. Accordingly, in addition to file encryption, it is taking a multi-extension strategy to gain an upper hand in negotiations with victims such as data leakage, DDoS attacks, and stakeholder attacks.



< Changing Ransomware Attack Paradigm Over Time, Partial Reorganization of Igloo Corporation >

Source : THE STATE OF RANSOMWARE 2020's Catch-22, TrendMicro, February 03, 2021 and LIFECYCLE OF RANSOMWARE INCIDENT, CERT NZ partially Reorganization

The cyber attack paradigm combines next-generation ICT technology to cause enormous damage to the entire maritime sector, where digitization is in full swing, and ultimately threatens human life as well as economic damage caused by cyber attacks, including ransomware. Accordingly, it is necessary to recognize awareness of cybersecurity in the maritime field and establish response strategies.

● Cybersecurity Risk Response Strategy in the Maritime Sector of Maritime Affairs

In order to minimize cybersecurity risks in the maritime sector, a joint response strategy between the government and the private sector that reflects management, physical, and technical factors is needed in consideration of the supply chain across the maritime ecosystem rather than strengthening security for each single object such as ships and ports. This trend is also reflected in the fact that strengthening supply chain security was adopted as a major agenda at the 2022 Marine Cyber Security Conference organized by the European Maritime Safety Agency (EMSA).

In order to strengthen the security of the maritime supply chain, it is necessary to establish international standards and support policies at the national level. To this end, IEC 63154:2021 (TC 80) carried out an international standard specifying "Maritime navigation and radio

communication equipment and systems – general requirements, methods of testing and required test results" to strengthen cybersecurity response in the maritime ship sector. In Korea, there is an active movement to establish a roadmap and strengthen related regulations to strengthen maritime cybersecurity..

In October 2021, the Ministry of Oceans and Fisheries announced that it will develop key technologies in the next-generation ship industry with the aim of commercializing fully autonomous ships by preparing a "preemptive regulatory innovation roadmap for autonomous ships" to promote the development and early commercialization of autonomous ship technology by 2031. In particular, it includes "establishing a cybersecurity system and developing cyber attack response standards" to cope with cyber risk management that may arise from autonomous ships, which can be seen as a result of recognizing and reflecting the impact of cybersecurity in the maritime sector in Korea.

In April 2023, the Ministry of Oceans and Fisheries established the Maritime Cyber Safety Management Guidelines (notification) for the first time in the transportation sector to define the role of the government and the private sector. The government establishes and implements maritime cyber safety measures, discovers and improves system vulnerable factors, and the private sector recommends the role of risk assessment, protection, detection, response, and recovery. Although there are differences in effectiveness as it is defined as a recommendation, it is meaningful in that it can serve as a standard for the establishment and operation of shipping companies' own cyber safety management system in line with the trend of strengthening international regulations such as the International Maritime Organization (IMO).

In order to strengthen maritime cybersecurity in terms of technology, you can refer to the security threats and countermeasures presented in "Managing Cyber Security Risks of the Cyber-Enabled Ship." It identifies six security threats that can occur in 14 Cyber Physical Systems (CPS) that make up the ship environment (C-ES) with ICT technology, including spoofing, tempering, denial of information exposure, denial of service, and authority increase, and applies security measures such as denial prevention, confidentiality, integrity, and availability in consideration of the impact on CPS. When applying countermeasures according to security threats, appropriate security measures should be applied within a limited resource

by reflecting the impact of attacks caused by security threats and the importance of assets.

Threat	Risk	Requirement	Objective	Control Category
Spoofing	High	The use of ECDIS must be restricted only to authorized and well trained personnel.	Authenticity, Integrity	Device Identification and Authentication (IA-3), Port and I/O Device Access (SC-41), Time Stamps (AU-8), Plan of Action and Milestones (CA-5)
Tampering	Medium	The ECDIS must be able to control the flows of voyage-related data sent to other ships and to the SCC.	Integrity, Authenticity	Device Identification and Authentication (IA-3), Audit Review Analysis and Reporting (AU-6 (3), (6)), Plan of Action and Milestones (CA-5)
Repudiation	Medium	The ECDIS should be able to audit sent and received data to external actors.	Integrity, Non repudiation	Internal System Connections (CA-9), Time Stamps (AU-8), Physical Access Control (PE-3), Monitoring Physical Access (PE-6 (1))
Information Disclosure	High	The confidentiality and integrity of the data exchanged between internal (on board systems and external actors (SCC or other vessel) should be ensured by appropriate mechanisms depending on the actors and the type of the data in transit.	Confidentiality	Cryptographic Protection (SC-13), Port and I/O Device Access (SC-41), Device Identification and Authentication (IA-3), Protection of Information at Rest (SC-28)
Denial of Service	High	The communication between the ECDIS and the satellite system should be continuously available.	Availability	Internal System Connections (CA-9), Incident Handling (IR-4 (4)), Denial of Service Protection (SC-5)
Elevation of Privileges	Low	The use of ECDIS must be restricted only to authorized and well trained personnel	Possession and Control	Device Identification and Authentication (IA-3), Unsuccessful Logon Attempts (AC-7)

< Control selection for the Electronic Chart Display and Information System (ECDIS) >

Source : Managing Cyber Security Risks of the Cyber-Enabled Ship

● Suggestions for strengthening maritime cybersecurity

So far, we have looked at the paradigm and countermeasures of cyberattacks that can occur in the ecosystem. As cybersecurity risks in the maritime ecosystem are increasing due to digitalization and automation, it is important to establish a preemptive response strategy.

Accordingly, maritime companies should establish a cybersecurity risk assessment and management system to prevent cyberattacks and strengthen their response capabilities to minimize damage in the event of an accident. In addition, security defense mechanisms for major maritime systems should be established through secure coding and software security enhancements, and periodic security patches should be performed to enhance the security of ships and shipping systems.

Cybersecurity in maritime ecosystems is an important issue to protect industrial safety and life.

In order to maintain the technological edge of domestic ship manufacturing and lead the global market, we look forward to the development of the domestic maritime ecosystem through the development of maritime digital source technology in line with the era of the 4th industrial revolution and the establishment of an ecosystem applying cybersecurity.

● References

1. IEC 63154:2021 ED1

https://www.iec.ch/dyn/www/f?p=103:52:309604824180372::::FSP_ORG_ID,FSP_LANG_ID:1271,34

2. CENELEC LIST OF EXEMPTIONS FROM PARALLEL PROCEDURES

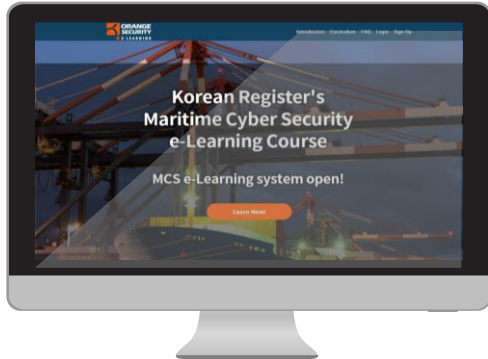
https://boss.cenelec.eu/media/BOSS%20CENELEC/ref/fa_parallel_exemptions_list.html

3. Managing Cyber Security Risks of the Cyber-Enabled Ship

<https://www.mdpi.com/2077-1312/8/10/768>

Online Training

KR Maritime Cybersecurity e-Learning Center training course



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



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.



Providing the best services, Creating a better world

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

Copyright © 2023 ALL RIGHTS RESERVED BY KOREAN REGISTER