2024-10-01

An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors

Ömer Söner *Yuzuncu Yil University*

Gizem Kayisoglu *Istanbul Technical University*

Pelin Bolat *Istanbul Technical University*

Kimberly Tam *School of Engineering, Computing and Mathematics*

Recommended Citation

Söner, Ö., Kayisoglu, G., Bolat, P., & Tam, K. (2024) 'An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors', *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, . Available at: https://doi.org/10.1177/1748006X241283093

DEMATEL-based Incident Analysis for Ransomware Cyber Attacks

Omer Soner*[1], Gizem Kayisoglu[2], Pelin Bolat[3], Kimberly Tam[4]

[1]Department of Maritime Transportation Management Engineering in Maritime Faculty, Van Yuzuncu Yıl University, Van, Türkiye, 65080, soneromer023@gmail.com

[2]Department of Maritime Transportation Management Engineering in Maritime Faculty, Istanbul Technical University, Istanbul, Türkiye, 34940, yukselg@itu.edu.tr

[3]Department of Basic Sciences in Maritime Faculty, Istanbul Technical University, Istanbul, Türkiye, 34940, yilmazp@itu.edu.tr

[4]School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth, UK, PL4 8AA, kimerly.tam@plymouth.ac.uk

Abstract

Ransomware is a subset of malicious cyberattacks that aims to hold an organization's data or critical infrastructure at ransom, compromising or blocking access. If the attack is public, or made public after the initial attack, it can also severely jeopardize an organization's reputation. Recently, ransomware has consistently been ranked as one of the main cybersecurity threats across a number of industries, and both public and private organizations are often unwilling to publicly report or discuss their ransomware incidents. Given the direct and immediate impact ransomware attacks can have, and the lack of in-depth sharing, additional research is needed to analyze ransomware incidents in order to understand the underlying causes of incidents in addition to the detection and prevention methods. In this paper, 22 public ransomware incidents within the marine industry have been investigated to determine their causal factors and commonalities. The fuzzy set and DEMATEL (Decision Making Trial and Evaluation Laboratory) method are used to evaluate causal factors in order to enable an organization to better adhere to operational requirements and cyber risk management strategy to increase cyber resilience against ransomware incidents. The study's findings highlight the fact that network layer cyber security mitigations, strategies for securely utilizing RDP (Remote Desktop Protocol) protocols, and investments in Operating Systems (OS) and software security are essential components of preventing future ransomware incidents. This study concludes by suggesting several suitable control and preventative measures to improve cyber security resilience against ransomware incidents in the maritime sector. .

Key words: cyber-attacks; ransomware; cyber resilience; DEMATEL; incidents analysis.

*Corresponding Author

1. Introduction

Ransomware is sophisticated and enhanced malware that is that often use Locker or Crypto functions to limit access to key computer systems and their data. While crypto ransomware encrypts the valuable files on a computer to make them unusable, the locker ransomware locks the device completely (Aziz, 2016). The vast majority of these threats aim to directly or indirectly monetize victims by demanding ransom in exchange for decryption keys (Maigida et al., 2019). Several well-known instances of ransomware that have targeted the multiple industries are NotPetya, Ryuk, GoldenEye, Maze and Wannacry. These affected business, governments, academia, healthcare, manufacturing, and technology organizations (HYPR, 2022; TREND MICRO, 2022).

With the maritime industry's enormous economic reach and the ever-increasing advances in the industry's use of technology there are many potential targets. This includes maritime ports, shipping companies, and vessels as some of the most targeted areas for ransomware attacks by profit-motivated threat actors (NJCCIC, 2022). Especially in 2021, threat actors have used ransomware to target systems that include operational technology that the maritime industry is concerned about, as they may cause the failure of physical and sometimes security-critical equipment (Chubb, 2022). Existing extensive vulnerabilities within the maritime sector, including the physical environment, Operational (OT) /Information (IT) Technology environment, Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) and Programmable Logic Controllers (PLC) also allows cyber-attacks to occur. Goodell & Corbet (2023) stated that hackers, who were reportedly linked with Russia, performed a ransomware attack causing the system breakage on the Colonial Pipeline, which is a major oil infrastructure system stretching between New York and Houston and carries around 45% of all fuel consumed on the East Coast of the United States. The company paid the ransom of $4.4 million in Bitcoin to the hackers to reinstate operational control. There are critical parallels in this case to the maritime industry. Ransomware threat actors can also threaten supply chain organizations via hazarding and blackmailing their customers. An example of this is a critical attack in 2021, which included Kaseya and SolarWinds. These two are common vendors of software for the ship owners and other maritime supply chain organizations (Lazarovitz, 2021).

As of the end of 2022, CMA CGM and COSCO, which are the world's biggest logistics and shipping companies sourced from France and China, ports in Germany, Belgium, and the Netherlands, and the biggest ferry service to Martha’s Vineyard island in the US have suffered from ransomware attacks, prevented and/or removed the availability of critical services and operations. (Lawrence, 2022).

Generally speaking, threat actors for ransomware can be organized crime gangs and activists who spot a vulnerability, sophisticated state-sponsored teams, or individual opportunists having financial motivation by selling the extracted data or blackmailing their victims. The NotPetya, which has greatly affected A.P. Moller-Maersk, a shipping line that carries around one-fifth of the freight in the world, and is the most publicized and known instance of a maritime ransomware attack. It negatively affected the company's technological infrastructure with the financial loss between $200 to $300 million range and for only resetting the software of 4,000 servers, and 45,000 PCs. (Lawrence, 2022).

Ransomware as an attack has been growing in popularity as it holds minimal risk to the attacker and can yield considerably grand rewards, even when considering other forms of cyber-attacks and other security threat activities in the maritime such as smuggling drugs or stealing cargo. Moreover, according to the TechTarget report (2022), ransomware attacks has risen 105% in 2021. While 68% of organizations were infected by ransomware in 2021, the organizations impacted from ransomware campaigns are categorized as 47% telecom, 31% transportation and shipping, 7% media and communications, 6% business services, and 5% government in the threat report of Trellix Advanced Research Center (Trellix, 2022). It can be clearly seen that transportation and shipping is one of the most targeted sectors for ransomware attacks.

By examining the cyber incident reports in maritime, it is seen that most ransomware attacks go unreported in maritime sector, and companies prefer to pay the money. However, this leaves no guarantee that attackers will release their data or resist a future attack urge. Such that in addition to the financial gain of a paid ransom, criminals can sell data they steal on the black market. For instance, the data from a shipping company as in Figure 1 is available for sale on the dark web (Pen Test Partners, 2022). These data provide to the hackers the base of other cyber-attacks such as AIS and GPS spoofing, DoS attacks against ships system, or man-in-the-middle attack for carrying out them easily.

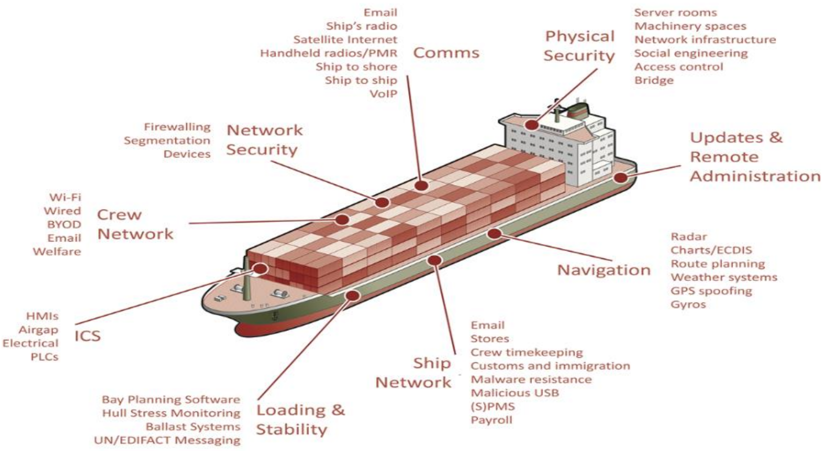

Figure 1. Data of the shipping company offered for sale on the dark web (Pen Test Partners, 2022)

All in all, within this context, it is an highly probable that the maritime sector, including ports, vessels, and shipping companies across the globe, are attractive target for a range of cyberattacks designed to disrupt daily operations, cause loss of business, loss of productivity, and potentially the permanent loss of data, steal sensitive data, incite distrust and promote violence toward the community and customers, and encrypt critical operational data (Tam, et al., 2022). Because of this, for the stakeholders in maritime sector, it is crucially significant to recognize how the operations should be protected from both targeted attacks and from threats coming from the otherwise unsuspected external digital environment. Being conscious of what makes the sector uniquely vulnerable is crucial to come through the minor imperfections in security protocol that can induce spectacular losses. It is critical to understand the potential impacts of a cyberattack on the maritime sector or associated industrial control systems, such as damaged equipment. These cyberattacks could result in environmental and public exposure to harmful pollutants, global economic consequences (Tam, Chang, Hopcraft, & Jones, 2023), and even death or serious injury.

The aim of this study is to carry out an incident analysis on ransomware attacks in maritime in order to determine the factors that cause ransomware attacks targeting the maritime sector. For enhancing safety of a system and attenuating risks derived from mis practice, defining the etiologies of actual or perceived negatory ransomware cyber cases and undesirable consequences is an essential stage. For this purpose, the 22 ransomware incidents are analyzed by collecting data about the incident, analyzing them, marking results from the data, and advancing future resilience in this study. This process is implemented to identify root causes, which led to ransomware incidents in maritime. The method provides the understand fundamental issues on the available process or system in the business that if they were not exist, the event would not have become. Appropriate corrective actions for this threat are updating training content and frequency, updating polices, reconfiguration equipment, or rising security measures can be determined for ransomware cyber-attacks especially for targeting maritime industry. After analyzing ransomware cyber incidents in maritime, the general stages of a ransomware attack are also examined to determine the comprehensive possible factors that can cause the ransomware cyber-attacks in maritime. The Decision Making Trial Evaluation Laboratory (DEMATEL) method is used in this study for understanding the significant specific causal factors involved in ransomware cyber cases in maritime and mapping the impact relationship of these factors with each other.

In the literature, there are several studies about ransomware focusing on more detection and recovery system (Brewer, 2016; Maigida et al., 2019; Malecki, 2019; Scaife et al., 2016; Sittig & Singh, 2016) and a few other topics such as economic perspective about ransomware (August et al., 2019), behavior of specific ransomware including Notpetya, Wannacry or Windows based ransomware attacks (Berrueta et al., 2022; Kara & Aydos, 2022; McIntosh et al., 2018; Mohurle & Patil, 2017; Zimba et al., 2018). Brewer, (2016) suggested utilizing threat intelligence sources in the availability of anomalies related to ransomware in the network traffic in order to stop them or to give a warning signal and he highlighted well verified backups for recovery step against ransomware. Scaife et al., (2016) developed an early-warning system for detection of ransomware, which is called as CryptoDrop that is based on Windows platform. The work process of this system is to spectate changes on the user data instead of identifying ransomware via controlling its contents or execution unlike exist detection systems. Sittig & Singh, (2016) offered some kinds of preventing, mitigating and recovering activities including that providing more effective defense system by carrying out user-oriented strategies, involving simulation and complete use of computers and network applications, ensuring enough system protection by decent setting up and configuring computers and the networks, addressing security problems and providing training on detecting and dealing with before they cause harm, and continuous monitoring of computers and applications to detect suspicious activities. The other used techniques to detect ransomware attacks in the literature are relating to installing an enhanced early detection system for ransomware via utilizing Enhance Frequency Centric Model (EFCM) & TF-IDF Data-Centric Detection (Al-rimy et al., 2018), SDN technology approach to examine HTTP messages, contents, and size sequence for detection of ransomware (Cabaj et al., 2015), ILP system ALEPH learning algorithm for recognizing ransomware behaviors by analyzing of HTTP and DNS log data (Bhardwaj et al., 2016), and EldeRan, a machine learning classifier for detection of ransomware attack (Sgandurra et al., 2015).

By analyzing literature for ransomware attacks in maritime, it is seen that ransomware attacks have not been considered separately in maritime literature in contrast of above-mentioned studies. Only, various cyber incidents and challenges in maritime including ransomware are stated in the exist studies (Androjna et al., 2020; Dadiani, 2018; Lagouvardou, 2018; Mraković & Vojinović, 2019; Svilicic et al., 2019, 2020). In these studies, general cyber security solutions are suggested in order to eliminate or minimize the cyber risk in maritime.

The authors concluded from this literature review that the technologic-based novel methods for ransomware cyber-attacks for general targeting areas are only ones offered to detect and response the threat. However, in the field of maritime, it is only underlined the importance of cyber-attacks and their increasing problem. Neither in studies relating to the general ransomware attacks nor studies relating to the maritime cyber securityis there an in-depth incident analysis and influence relationship between causal factors for ransomware attacks specifically for maritime sector. This study aims to fill this gap, as it is equally critical to understand the overall threat to the sector. In this respect, to the best of author’s knowledge, this paper is the one of the first studies that implement an incident analysis on ransomware cyber-attacks specifically for maritime. For this reason, this study has contribution to the both academic literature and sectoral area in terms of understanding etiologies of the ransomware attacks in maritime and influence loop between them.

2. Material and Methodology

2.1 Material

In this section, the common stages of ransomware attack and various ransomware incidents in maritime are examined as the part of the incident analysis and used as a material in this study in order to create comprehensive factors on ransomware in maritime.

2.1.1 Ransomware Attack Process

In general, the majority of ransomware share the initial stages for intrusion the target systems. More general steps of a ransomware attack is shown as in Figure 2 (Logan et al., 2021). At the start of a typical ransomware attack, threat actors can use numbers of methods and entry points depending on their target such as phishing emails, compromised accounts, or vulnerabilities on the system itself (e.g., unprotected network port). For instance, while it is seen that some ransomware like Ryuk, RansomEXX, and Egregor have used phishing emails for initial access, ransomware like RansomEXX and Sodinokibi have also used remote access vulnerabilities (e.g CVE-2019-19781, CVE-2019-11510, and CVE-2019-11510) for the first stage in their attacks. Other common ways for ransomware to gain initial access is Remote Desktop Protocol (RDP) brute force attacks that includes to usage of unsecured and opened RDP ports. Lastly, from a more social-engineering aspect, ransomware can often use stolen accounts, provided by other attackers via selling the accounts for data exfiltration campaigns on the dark webs.

Once the malware is on a system, an optional next step for ransomware attacks is to explore its network for lateral movement, which include to gain access to as many systems as possible by compromising domain controllers via using different penetration, hack, and open-source tools. This is not always the case, the key aspect of ransomware is to acquire "ransom" for a critical data or services, but more victims incases the potential payout. Therefore, many modern tend to have the capability to seek and infect other victims. The threat actors can make an inventory of the target's network during this process to sell the target's data in the dark webs before implementing its ransomware attack. After that, before attackers encrypt the target's files, they are in a position to steal significant information that can be used as trump against the target by exfiltration of the sensitive information and uploading the stolen information to the cloud or to remote File Transfer Protocol (FTP) locations via using different tools such as Megasync or Rclone. A sophisticated attack may also be able to disable available defenses, services and running processes to ensure to prevent the victim from preventing or recovering from ransomware on the system by using different tools such as Custom Scripts, or PsEcec and they send an encryption notification to the victims. Ransomware attacks are observed to occur days to weeks (Logan et al., 2021).

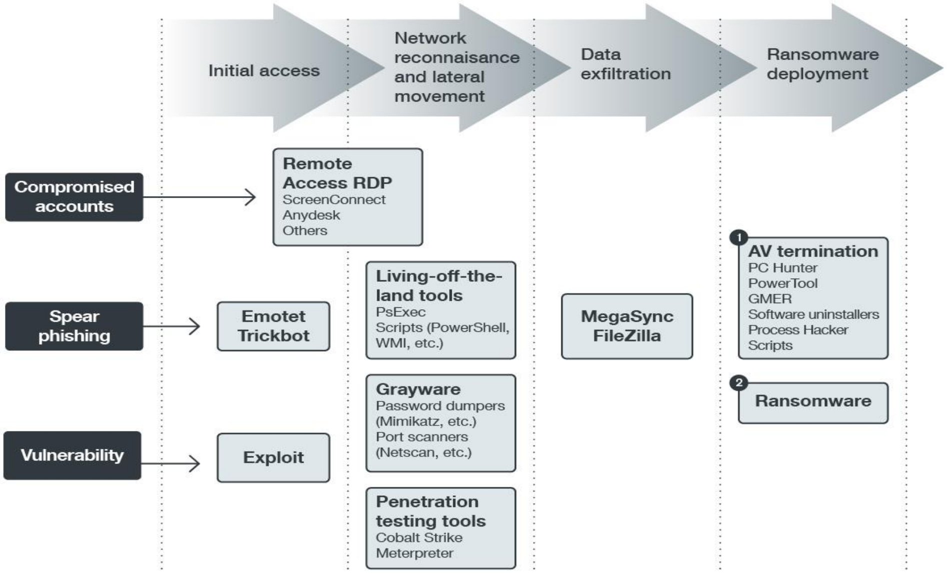

Figure 2. General steps of a ransomware attack (Logan et al., 2021)

2.1.2 The Ransomware Incidents in Maritime

Meland et al. (2021) presented 46 cyber incidents that targeted the maritime field in their study. They have provided a top-10 list of maritime cyber threats. The groups have been identified according to resembling characteristics between the cases. They have identified targets and typical attack vectors for each category such as the category of exposed carrier or shipping company IT-systems, the category of exposed communication systems, or the category of economic fraud.

This source is used as a material in this study by re-examining in different perspective to put forward the importance of the ransomware attacks in maritime and their possible causes under the incident analysis. Of the 46 cyber incidents, 14 have been against the sea side of maritime industry such as ships, offshore platforms, or drilling rig. The remain parts have been against the shore side of maritime industry such as shipping companies, port systems, ship-building groups, custom authorizations, or maritime service providers. While the some of the incidents have included various kind of malware attacks, AIS and GPS spoofing, Icefog, phishing e-mails, spoofing e-mail and man in the middle attack, 22 of them have been specifically ransomware attacks. A cyberattack has the potential to inflict substantial disruption to port and vessel operations and, due to the sheer volume of business conducted in ports worldwide, could result in significant monetary losses.

The examined ransomware incidents in maritime sector are shown in Table 1. Although, detail reasons and information about the incidents are not present in these reports due to the worries of the companies in terms of confidentiality of information sharing for cyber security, in the most of ransomware incidents, it is clearly stated that the attack has started via opening malicious link or an attachment by operator in the victim company (I1, I4, I5, I8, I10, I12). Only in one incident (I11), it has started via using malicious USB by the operator on the system and in one incident (I20), it has started via using the vulnerabilities of RDP by the attacker. It is seen that the specific types of ransomwares in maritime have been Notpeyta, Ryuk, Hermes 2.1, Egregor, Ragnar Locker, DoppelPaymer and Sodinokibi.

By examining these specific ransomware functions, for instance, it is seen that Notpetya ransomware can occur because of the having the victims the vulnerabilities of OS against ransom malwares such as a vulnerability in Windows' Server Message Block (SMB) protocol and Eternalblue, lack of patches for supported versions of OS, lack of awareness of operators (For instance, while these malwares encrpt the files after they infected the system, "fictitious chkdsk" appears on the screen. At that time, if an infected computer is shut down immediately, the encryption process may be possible stopped), lack of creating read-only files, lack of backup strategy (Fayi, 2018). The other intrusion way to victims' system is to use RDP. The port 3389 is utilized by RDP as its default listening port. This information is known by the attackers and to scan for 3389 ports that have been connected to the internet a script can be run by attackers. When they found an exposed port, they need to capture the login credentials. This can be realized via using fundamental techniques of achieving credentials including brute force attacks or social engineering.

After they are inside, backdoors can be left for spreading ransomware or future access. (Wang et al., 2018). Ragnar Locker is kind of a ransomware, which leaks to system by compromising RDPs for the companies' network. Once the attackers achieve their victim's network, they upgrade their privileges by running arbitrary code via using the vulnerability of CVE-2017-0213 found in Windows COM Aggregate Marshaler. Ragnar Locker ransomware utilizes enhanced defense-evasion techniques to bypass anti-malware solutions, therefore, it is a huge risk for institutions. (Kang et al., 2021). Finally, different from others, DoppelPaymer is a beneficiary of BitPaymer ransomware and comes from Dridex malware family. It spreads by using phishing email attacks. Once victims open the malicious documents attached in the e-mail and download the VBScript or JavaScript code, which embedded in the document, on the machine, the toolkit of PowerShell Empire is used by attackers in order to practice a brute-force attack on Active Directory. For clearing passwords from the system memory, The Mimikatz module is utilized. For initializing, DoppelPaymer foist its code into explorer.exe by using the DLL hijacking technique. After victim credentials are achieved, the ransomware seperate into the network and encryption process for the confidential data starts. Recently, it is known that DoppelPaymer exploits the vulnerability of the CVE-2019-19781 (Wagner, 2021).

Table 1 Ransomware Incidents in Maritime (Meland et al., 2021)

Incident	Definition	Category	Cyber Attack
I1	The Danish Maritime Authority came under a cyber-attack, which started with infected PDF attachment in the e-mail that caused to steal information and documents in network.	Maritime Authority	phishing e-mail and ransomware
I2	Clarksons, British ship broker, came under a cyber-attack that caused to steal confidential information and to reduce the stock value by around 5%. The point of entry was a lone user account, which the company said it disabled as soon as it discovered its role in the hack.	Broker firm	ransomware
I3	The NotPetya ransomware, which has been targeted A.P. Moller-Maersk that carries around one-fifth of the freight in the world, carried out. It is based on EternalBlue and uses vulnerabilities in Microsoft Windows. It led to crashing the company's technological infrastructure with the financial loss between $200 to $300 million range and resetting 2500 applications, software, 4,000 servers, and 45,000 PCs.	Shipping company	ransomware (Notpetya)
I4	The Ryuk ransomware cyber-attack, which initiated by phishing email for the employees in the facility and influence only IT systems rather that ship traffic via achieving important network files of the institution, encrypting them, and blocking access of facility to sensitive files, is reported by Port of Barcelona.	Port system	ransamware (Ryuk)
I5	After 5 days of the mentioned incident in I4, another Ryuk ransomware cyber-attack, which resulted in for restricting the local functions at the port, is reported by Port of San Diego.	Port system	ransamware (Ryuk)
I6	Austol, which is from the Australian shipbuilder and makes naval vessels for the US and Australia, reported a ransomware attack that ship designs and information is stolen and provided for sale on the dark web.	Shipbuilding company	ransomware
I7	A ransomware cyber-attack, which resulted in communication by network telephone and e-mail is blocked for 5 days, carried out against COSCO Shipping Lines.	Shipping company	ransomware
I8	Ryuk ransomware, which initiated by phishing email and resulted in to make non-functional access control systems, CCTV cameras, and critical process monitoring, infected a disguised American port.	Port system	ransomware (Ryuk)
I9	James Fisher and Sons, British marine services provider, came under a ransomware cyber-attack that caused to crash digital systems and to reduce the stock value by around 7%.	Marine services provider	ransomware
I10	A ransomware, highly possible Ryuk, which initiated by phishing email and resulted in to stop operations by affecting IT and OT systems for two days, infected a natural gas compression facility at disguised American pipeline operator.	A natural gas compression facility	ransomware (Ryuk)

I11	A ransomware, which is thought a phishing attack, a USB device, or RDP as probable attack vectors and caused to delete backup disk, infected an administrations server of a tanker near the port of Naantali in Finland. After 4 months, the same ship came under a cyber-attack again near the same port.	Sea Side (Ship/Offshore/Drilling Rig)	ransomware
I12	The ransomware Hermes 2.1, which initiated with malicious Word attachment in the e-mail and influenced various workstations on the administrative networks, infected two vessels under the same owner	Sea Side (Ship/Offs./Dril. R.)	ransomware (Hermes 2.1)
I13	The Ryuk ransomware, which caused to encrypt and loss of all data and required a full reinstall for recovering the system, infected the server and several computer clients of a vessel anchored near Tynemouth, UK.	Sea Side (Ship/Offs./Dril. R.)	ransomware (Ryuk)
I14	The ransomware Sodinokibi, which caused to leak information ("ransomtheft") and encrypt data, infected administrative systems of three vessels with American flag.	Sea Side (Ship/Offs./Dril. R.)	ransomware (Sodinokibi)
I15	A ransomware, which caused to blocked headquarters in Geneva for five days, infected to the shipping company MSC.	Shipping company	ransomware
I16	A ransomware attack, which caused operational delay in critical level and because of the stopped shipbuilding temporary job loss occurrence, is carried out against Norwegian shipbuilder Vard.	Shipbuilding company	ransomware
I17	Two times of ransomware in two years, which caused to steal credit card details and personal information of employees and customers, are carried out against Cruise operator Carnival Corporation & plc.	Shipping company	ransomware
I18	A cyber-attack, which caused to block online systems for five days, is carried out against Transport Malta, who is the Maltese transport authority. (It starts with answering the questions, which came from a website and e-mail. Therefore, it starts a phishing mail and understood that some data was stolen. It is a ransomware)	Shipping company	phishing e-mail and ransomware
I19	The Egregor ransomware infected Diana Shipping, which is the Greek shipping company. There is no enough information about this incident.	Shipping company	ransomware (Egregor)
I20	The Ragnar Locker ransomware, which caused to block some of online services and influenced various of Chinese offices, infected to CMA CGM that is the French container carrier company.	Shipping company	ransomware (Ragnar Locker)
I21	A ransomware, which caused to become unavailable of the systems for a couple of days because of the reinstalling from offline backups, infected to the IT systems of Port of Kennewick.	Port system	ransomware
I22	A ransomware, which caused to become unavailable several main systems for a couple of days, and to steal passenger information including passport data, infected to Hurtigruten, which is Norwegian cruise operator.	Shipping company	ransomware

On the other hand, NJCCIC (2022) stated that at minimum, the maritime sector, including interconnected organizations, should implement the following for their OT/IT environments: Tamper-resistant controls on field devices, Trusted procurement procedures, Patching and updating operating systems and software, Encryption on the devices, Authentication and access control procedures, Penetration testing and internal audit, Employee training and awareness, Network segmentation, Use of different technologies: Segregation of duties and minimum privileges, Catalog and reduce system dependencies, Minimize unified closed loop, Create backups, Recovery plan, Ensure password security, Use secure networks only, Email security.

Apart from these materials, the recommendations from other authoritative sources, including the National Institute of Standards and Technology (NIST) (Barker et al., 2022; NIST, 2021) and CISA (CISA, 2016) are also utilized to identify the factors for ransomware attacks in maritime.

By presenting the stage of a typical ransomware and examining the ransomware incidents in maritime and several authoritative sources in this section, the factors, which possibly cause to the ransomware attacks in maritime, are tried to be understand and created as in Table 2.

Table 2 Factors for Ransomware Attacks

Code	**Causes**
C1	Lack of whitelisting (allow list) policy *(which includes a cybersecurity strategy that approves a list of email addresses, IP addresses, domain names, serial number of equipment (e.g. USBs) or applications, while denying all others.)(For instance, it can cover an allow-list to only allow approved IP addresses to connect to the RDP serve, to only allow approved USB drivers on the systems, to only allow approved e-mail addresses for opening.)*
C2	Opening a malicious any kind of electronic messaging
C3	Lack of running up-to-date end-point security and anti-virus software for all company's electronic messaging
C4	Lack of anti-phishing campaigns and lack of capabilities for blocking malicious websites and window pop-ups
C5	Using several USB without pre-scanned
C6	Having the vulnerabilities of OS against ransom malwares (crypto viruses) *(such as having the vulnerabilities in Windows' Server Message Block (SMB) protocol or Oracle WebLogic Server vulnerability CVE-2019-2725 for Sodinokibi ransomware)*
C7	Lack of patches for supported versions of OS
C8	Lack of updating the system and software
C9	Lack of anti-malware tool on the systems and software
C10	Lack of activating Controlled Folder Access to protect company's important local folders from unauthorized programs like ransomware or other malware.
C11	Lack of identity management and least privilege access *(It means that the access approval process is designed to grant access based on the user's role and job duties which is referred to the principle of least privilege, which states users, devices, programs, and processes which are interconnected or must access each other to communicate and take certain actions, should be granted just enough permissions to do their required functions.)*
C12	Lack of multi-factor authentication for the system and files access
C13	Lack of creating read-only files
C14	Lack of encryption and key management for the system and files. *(It means that Encryption is recommended for data at rest and data in transit to prevent disclosure of data (inadvertent or malicious). Encryption technologies include disk encryption, data file encryption typically included in data loss prevention, and data transmission using Transport Layer Service and HTTPS. Planning for file/data encryption may identify dependencies such as encryption key management to prevent file/data loss.)*
C15	Lack of training of staff for ransomware attacks
C16	Lack of awareness of staffs about how can they protect their business from the social engineering tactics such as phishing, vishing, impersonation, or web ads behind ransomware
C17	Lack of awareness of staffs to detect and response the ransomware *(For instance, while NotPetya encrypting malwares encrypt the files after they infected the system, "fictitious chkdsk" appears on the screen. At that time, if an infected computer is immediately shut down, it may be possible to stop the encryption process)*
C18	Leaving open Remote Desktop Protocol (RDP) ports used by the company to the internet
C19	Lack of using VPN, while RDP ports open to internet
C20	Lack of network segregation
C21	Lack of network firewall *(Such as lack of creating a rule in the network firewall to deny RDP from any system behind the firewall from being accessible to the Internet)*
C22	Lack of using network-level authentication to approve attempts to connect to a remote device
C23	Lack of limit failed logins attempts to the network connection or the systems and files
C24	Lack of network traffic monitoring and tracking system
C25	Lack of backup system (especially offline backup system) or strategy for all data *(The data can be files located on physical devices, virtual environments or the public cloud, Office 365 including SharePoint and OneDrive data, or SQL data)*

2.2 Methodology

The fuzzy set and DEMATEL are integrated in this study to understand which factors influence the occurrence of ransomware attacks in the maritime industry and the potential relationship between the factors in terms of the cause and effect. The fuzzy DEMATEL is a reliable and comprehensive way to analyze a complex system that takes causal relationships between contributing components into account. Therefore, it is utilized for this study since it highlights the crucial factors, distinguishing characteristics, and interrelationships of variables in ransomware attacks in maritime industry. Thus, finding the most crucial elements that influence other elements has become possible. The model has been applied in many fields, such as; cloud computing (Thavi et al., 2022), ICT (Saketh & Puppala, 2023), Industry 4.0 (Vinodh & Wankhede, 2021), and software vulnerabilities (Anjum et al., 2022), because it can identify the most crucial variables, visualize the structure of complex causal relationships, and demands limited data (Soner, 2021).

As previously stated, information sharing between both the public and the private sectors for cyber security in many fields (including maritime) is a tricky issue as how it is done could improve and damage security (Rajamäki et al., 2019). Because public authorities and governments are unwilling to share cybersecurity-related information lest endanger national security or contestability. Private companies are also unwilling to share information about cybersecurity vulnerabilities and consequent losses for fear of jeopardizing sensitive business information, risking their reputation, or violating data protection rules. In this context, US Department of Homeland Security United States Coast Guard (Homeport, 2015) established The Maritime & Port Security Information Sharing and Analysis Organization (MPS-ISAO), which is the Information Sharing and Analysis Center (ISAC) for the Maritime & Port critical infrastructure as a strategic public/private partnership, to advance maritime cyber resilience. Although it is started to build some centers to cope with this issue, trust needs to be strengthened so that public-private partnerships support broader cooperation and knowledge sharing among more sectors, as well as in maritime.

Consequently, fuzzy DEMATEL method, which is an expert-based method is utilized for the purpose of determining the which factors are influence in which level for the occurrence of ransomware incidents in maritime industry. Therefore, this is a pioneering study concerned with ransomware incidents that launched against the maritime industry.

2.2.1 Fuzzy

Fuzzy logic, which began to be used by Zadeh in 1965, is a robust technique for overcoming the fuzziness, inconsistent nature, and ambiguity of human judgment and evaluation (Zadeh, 1965). In order to aggregate different experiences, opinions, ideas, and motives of an individual or group decision-maker, a fuzzy set aims to translate language concepts into fuzzy numbers. While making decisions, fuzzy numbers guarantee that the right results are obtained. Readers who are interested to know more about fuzzy sets and some elementary operations should read (Maiers & Sherif, 1985; Zimmermann, 2010).

2.2.2 DEMATEL

The DEMATEL approach was created by the Geneva Research Center of the Battelle Memorial Institute to address complicated and extensive decision-making issues (Fontela & Gabus, 1976; Gabus & Fontela, 1973). DEMATEL is commonly regarded as an excellent tool for finding the causal relationship among relevant factors (Lin & Tzeng, 2009). To analyze and explore complicated decision-making situations, it is especially advantageous and effective to illustrate the framework of complex causal interactions using matrices and/or charts (Liu & Wu, 2003). The DEMATEL method was included in the current study because it is capable of revealing the dependency link among the factors as well as the values of influence effect. The following sub-section outline the fundamental steps of the fuzzy DEMATEL integration.

2.2.3 Integration of Fuzzy and DEMATEL

Finding the connections among the factors and organizing them according to the type of link and the strength of their influence on the other factors is one of the fundamental advantages of the fuzzy DEMATEL. At the same time, the suggested model's ability to account for fuzziness and handle it in a flexible manner therefore becomes its main strength (Wu, 2012). The fuzzy DEMATEL model under this research has been derived from (Akyuz & Celik, 2015; Başhan & Ust, 2019; Soner, 2021).

Step 1: To receive concrete assessments, it is first necessary to organize an expert group whose members have the necessary expertise in the associated area.

Step 2: To properly analyse and evaluate the subject matter under investigation, it is important to identify key components/factors/parameters throughout second step. The next step is to arrange the linguistic terms in according to the fuzzy numerical scale. Accordingly, the corresponding fuzzy members are procured.

Step 3: The expert group would then execute the pairwise comparisons in accordance with the linguistic terms. Additionally, the defuzzification and aggregation of the corresponding fuzzy numbers are performed to reveal the crisp values. It is therefore possible to create the initial direct relation (Ẽ) matrix.

$$\tilde{E} = \begin{bmatrix} 0 & \cdots & \tilde{E}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{E}_{n1} & \cdots & 0 \end{bmatrix} \tag{1}$$

$$\tilde{e}_{ij} = l_{ij}, m_{ij}, u_{ij} \tag{2}$$

Step 4: The following formulations (3), (4) and (5) are utilized to carry out normalization after obtaining the initial direct-relation matrix.

$$\tilde{\beta}_i = \sum \tilde{e}_{ij} = \left(\sum_{j=1}^{n} l_{ij}, \sum_{j=1}^{n} m_{ij}, \sum_{j=1}^{n} u_{ij} \right) \tag{3}$$

$$\gamma = max\left(\sum_{j=1}^{n} u_{ij} \right) \tag{4}$$

$$\tilde{F} = \begin{bmatrix} \tilde{F}_{11} & \cdots & \tilde{F}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{F}_{n1} & \cdots & \tilde{F}_{nn} \end{bmatrix} \tag{5}$$

where $\tilde{f} = \frac{\tilde{e}_{ij}}{\gamma} = \left(\frac{\tilde{e}_{ij}}{\gamma}, \frac{\tilde{e}_{ij}}{\gamma}, \frac{\tilde{e}_{ij}}{\gamma} \right)$.

Step 5: A total relation matrix is then calculated to confirm $\lim_{\omega \to \infty} f^{\omega} = 0$. The total relation matrix would then be computed in accordance with the subsequent formulas (6)-(10) respectively.

$$\tilde{T} = \lim_{\omega \to \infty} \left(\tilde{F} + \tilde{F}^2 + \cdots + \tilde{F}^{\omega} \right) \tag{6}$$

$$\tilde{T} = \begin{bmatrix} \tilde{t}_{11} & \cdots & \tilde{t}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{t}_{n1} & \cdots & \tilde{t}_{nn} \end{bmatrix} \tag{7}$$

where $\tilde{t}_{ij} = (l"_{ij}, m"_{ij}, u"_{ij})$;

$$\text{Matrix } [l"_{ij}] = F_l \text{ x } (I - F_l)^{-1} \tag{8}$$

$$\text{Matrix } [m"_{ij}] = F_l \text{ x } (I - F_m)^{-1} \tag{9}$$

$$\text{Matrix } [u"_{ij}] = F_l \text{ x } (I - F_u)^{-1} \tag{10}$$

Step 6: It is now feasible to determine the $\tilde{r}_i$ and $\tilde{c}_j$ because the $\tilde{T}$ matrix has been determined. The sum of the rows is shown by the $\tilde{r}_i$, while the sum of the columns is shown by the $\tilde{c}_j$. As previously established, $\tilde{r}_i + \tilde{c}_j$ exemplifies the significance of the factor i whereas $\tilde{r}_i - \tilde{c}_j$ shows the factor's overall influence.

Step 7: In this stage, the derived $\tilde{r}_i + \tilde{c}_j$ and $\tilde{r}_i - \tilde{c}_j$ are defuzzified using the COA (centre of area), which (Ross, 2005) created to produce BNP (best non-fuzzy performance) values. Thus, the aim of the following formulation is to estimate a convex fuzzy number, $\tilde{\delta}$, a real number z^* that corresponds to its centre of area (Gumus et al., 2013).

$$z^* = \frac{\int \mu_{\tilde{\delta}}(z) z dz}{\int \mu_{\tilde{\delta}}(z) z dz} \tag{11}$$

The formula below may be used to determine $\widetilde{\mathrm{G}} = (l_{ij}, m_{ij}, u_{ij})$, which is a BNP value for a fuzzy number.

$$BNP_{ij} = \frac{u_{ij} - l_{ij} + m_{ij} - l_{ij}}{3} + l_{ij} \tag{12}$$

Step 8: This final stage involves creating a cause-and-effect diagram based on the $\tilde{r}_i + \tilde{c}_j$ and $\tilde{r}_i - \tilde{c}_j$ values that were accomplished. Step 6 provides the necessary formulation.

3. Application and Analysis

To begin with, 22 ransomware attacks against the marine industry have been looked into to determine common contributing factors. The NIST (Barker et al., 2022; NIST, 2021) and CISA (CISA, 2016) recommendations, in addition to that, are also used to determine the factors for ransomware attacks in maritime industry. Next, the interaction between the causal factors evaluated by experts. Four experts, including computer engineers and maritime transportation engineers with in-depth understanding of maritime cyber security, were selected for their expertise in this effort. The assigned judgments by the experts' consensus are shown in Table 3. Using this judgement as a foundation, Table 4 presents the initial direct-fuzzy matrix. Following that, Eqs. (3) through (5) were used to normalize the direct-relation fuzzy matrix, as shown in Table 5. Eqs. (6) through (10) were applied to calculate the total-relation fuzzy matrix after the normalization matrix had been established. In this regard, Table 6 shows a total-relation fuzzy matrix. The fuzzy values of $\tilde{r}_i$, $\tilde{c}_j$, $\tilde{r}_i + \tilde{c}_j$, and $\tilde{r}_i - \tilde{c}_j$ are calculated and shown in Table 7 in accordance with the findings. Eqs. (11) and (12) have been applied in the subsequent step to transform the fuzzy numbers into crisp values. Table 8 contributes to a better understanding of the detailed information and ranking of $\tilde{r}_i$, $\tilde{c}_j$, $\tilde{r}_i + \tilde{c}_j$, and $\tilde{r}_i - \tilde{c}_j$ values.

Table 3 Linguistic assessment of identified ransomware incidents.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25
C1	NO	VH	VL	L	H	VL	VH	VH	VL	VL	VH	VL	L	L	L	L	VL	H	VL	VL	H	L	VL	VH	L
C2	VH	NO	VH	H	VH	VH	VH	VH	VH	H	L	L	L	L	H	VH	H	VL	L	VL	H	VL	VL	H	VL
C3	L	VH	NO	H	VH	VH	VH	VH	VH	VH	VH	H	VH	VH	H	H	L	L	L	VL	VL	H	H	L	L
C4	VH	H	L	NO	VL	VL	L	L	L	L	VL	VL	VL	VL	VH	VH	VH	VL	L	H	L	L	L	H	VL
C5	H	H	VH	L	NO	VH	VH	VH	VH	VH	VH	VH	VH	VH	H	VH	H	VL	VL	VL	VL	L	L	L	L
C6	H	H	VH	L	VH	NO	VH	VH	VH	VH	VH	VH	VH	VH	H	H	H	H	H	H	H	H	H	H	VH
C7	H	H	VH	L	VH	VH	NO	VH	VH	VH	VH	VH	VH	VH	VH	L	H	H	H	H	H	H	H	H	VH
C8	H	H	VH	L	VH	H	H	NO	H	H	H	H	H	H	H	L	H	H	H	H	H	H	H	H	VH
C9	H	VH	VH	VH	VH	H	H	VH	NO	VH	VH	VH	VH	VH	L	H	H	H	L	H	H	H	L	H	VH
C10	VH	VL	L	L	H	VH	VH	VH	H	NO	VH	H	VH	VH	L	L	L	VL	VL	VL	L	VL	VL	L	L
C11	VL	L	H	VL	VL	L	L	L	L	VH	NO	VL	L	L	VH	VH	H	L	VL	L	L	VH	L	VL	L
C12	VH	VL	L	VL	VH	H	H	H	H	L	VH	NO	VL	VL	VL	L	VL	VH	VH	H	VH	VH	H	VH	H
C13	VH	VL	VL	VL	H	L	L	L	VH	H	H	H	NO	VL	VL	L	VL	VL	VL	VL	VL	VL	VL	VL	VL
C14	L	VL	VL	L	H	L	L	L	L	H	H	L	VL	NO	L	L	L	L	L	L	L	L	L	L	L
C15	VL	VH	L	VH	VH	L	L	L	L	L	L	H	L	L	NO	VH	VH	VH	H	VL	VL	VL	VL	VL	VL
C16	VL	VH	L	VH	VH	L	H	H	H	L	L	H	L	L	L	NO	VH	L	VL	VL	VL	VL	VL	VL	VL
C17	VL	VH	L	VH	VH	L	L	L	L	L	L	H	L	L	L	VH	NO	VH	VL	VL	VL	VL	VL	VL	VL
C18	H	H	L	L	VH	H	H	H	H	H	L	H	L	L	H	L	VH	NO	VH	VH	VH	VH	VH	VH	H
C19	VL	VH	VH	VH	VL	L	L	L	L	VL	L	L	VL	H	L	H	H	H	NO	L	L	L	L	L	VL
C20	VL	L	L	H	VL	H	VH	VH	VH	H	H	H	VL	H	L	H	H	H	L	NO	H	H	L	H	L
C21	VL	VH	H	H	VL	H	VH	VH	VH	H	H	H	VL	H	L	H	H	H	L	L	NO	VH	L	VH	L
C22	VH	H	H	VH	VL	H	H	VL	VL	VL	L	L	VH	H	L	L	L	VH	VH	H	H	NO	VL	VH	L
C23	VL	L	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	L	H	VL	H	H	VL	VL	VL	NO	VL	VL
C24	L	VH	L	H	L	H	H	H	H	L	L	L	L	H	H	H	H	H	VH	VH	VH	VH	VH	NO	L
C25	VL	L	H	L	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	H	VH	H	L	VL	VL	VL	L	L	L	NO

Table 4 The direct-relation fuzzy matrix of the causes.

	C1	**C2**	···	**C24**	**C25**
C1	(0, 0, 0.25)	(0.75, 1, 1)	···	(0.75, 1, 1)	(0.25, 0.50, 0.75)
C2	(0.75, 0.75, 1)	(0, 0, 0.25)	···	(0.5, 0.75, 1)	(0, 0.25, 0.5)
⋮	⋮	⋮	⋱	⋮	⋮
C24	(0.25, 0.5, 0.75)	(0.75, 1, 1)	···	(0, 0, 0.25)	(0.25, 0.50, 0.75)
C25	(0, 0.25, 0.5)	(0.25, 0.5, 0.75)	···	(0.25, 0.50, 0.75)	(0, 0, 0.25)

Table 5 Normalization of the direct-relation fuzzy matrix of the causes.

	C1	**C2**	···	**C24**	**C25**
C1	(0, 0, 0.01)	(0.03, 0.05, 0.05)	···	(0.03, 0.05, 0.05)	(0.01, 0.02, 0.03)
C2	(0.03, 0.05, 0.05)	(0, 0, 0.01)	···	(0.02, 0.03, 0.05)	(0, 0.01, 0.02)
⋮	⋮	⋮	⋱	⋮	⋮
C24	(0.01, 0.02, 0.03)	(0.03, 0.05, 0.05)	···	(0, 0, 0.01)	(0.01, 0.02, 0.03)
C25	(0, 0.01, 0.02)	(0.01, 0.02, 0.03)	···	(0.01, 0.02, 0.03)	(0, 0, 0.01)

Table 6 Total-relation fuzzy matrix.

	C1	**C2**	···	**C24**	**C25**
C1	(0.01, 0.06, 0.36)	(0.05, 0.11, 0.43)	···	(0.04, 0.10, 0.40)	(0.02, 0.07, 0.36)
C2	(0.05, 0.11, 0.44)	(0.02, 0.08, 0.45)	···	(0.04, 0.10, 0.45)	(0.01, 0.07, 0.39)
⋮	⋮	⋮	⋱	⋮	⋮
C24	(0.03, 0.09, 0.46)	(0.05, 0.13, 0.51)	···	(0.02, 0.07, 0.45)	(0.02, 0.08, 0.43)
C25	(0.02, 0.08, 0.42)	(0.03, 0.11, 0.47)	···	(0.02, 0.09, 0.44)	(0.01, 0.06, 0.38)

Table 7 Fuzzy values of $\tilde{r}_i$, $\tilde{c}_j$, $\tilde{r}_i + \tilde{c}_j$, and $\tilde{r}_i - \tilde{c}_j$.

	$\boldsymbol{\tilde{r}_i}$	$\boldsymbol{\tilde{c}_j}$	$\boldsymbol{\tilde{r}_i + \tilde{c}_j}$	$\boldsymbol{\tilde{r}_i - \tilde{c}_j}$
C1	(0,582, 2,047, 9,925)	(0,68, 2,233, 10,451)	(1,262, 4,279, 20,376)	(-9,869, -0,186, 9,245)
C2	(0,848, 2,553, 11,247)	(0,899, 2,65, 11,604)	(1,746, 5,203, 22,85)	(-10,756, -0,098, 10,348)
C3	(0,959, 2,765, 11,811)	(0,777, 2,417, 10,953)	(1,736, 5,182, 22,763)	(-9,993, 0,349, 11,034)
C4	(0,527, 1,943, 9,821)	(0,738, 2,344, 10,919)	(1,265, 4,288, 20,74)	(-10,392, -0,401, 9,083)
C5	(0,923, 2,696, 11,429)	(0,923, 2,697, 11,268)	(1,846, 5,393, 22,697)	(-10,345, -0,001, 10,506)
C6	(1,16, 3,148, 13,041)	(0,829, 2,517, 11,473)	(1,989, 5,664, 24,514)	(-10,313, 0,631, 12,212)
C7	(1,161, 3,149, 12,92)	(0,958, 2,763, 11,999)	(2,119, 5,912, 24,918)	(-10,838, 0,386, 11,961)
C8	(0,949, 2,814, 12,92)	(0,912, 2,774, 11,745)	(1,861, 5,588, 24,665)	(-10,796, 0,039, 12,008)
C9	(1,119, 3,069, 12,817)	(0,859, 2,661, 11,618)	(1,978, 5,729, 24,435)	(-10,499, 0,408, 11,958)
C10	(0,711, 2,293, 10,569)	(0,805, 2,53, 11,359)	(1,516, 4,823, 21,928)	(-10,648, -0,237, 9,764)
C11	(0,555, 1,997, 9,965)	(0,782, 2,667, 11,593)	(1,337, 4,663, 21,559)	(-11,038, -0,67, 9,183)
C12	(0,864, 2,548, 11,323)	(0,458, 2,479, 11,48)	(1,322, 5,027, 22,803)	(-10,616, 0,069, 10,865)
C13	(0,376, 1,654, 8,947)	(0,231, 2,27, 10,304)	(0,606, 3,924, 19,251)	(-9,929, -0,617, 8,716)
C14	(0,483, 1,858, 9,982)	(0,667, 2,473, 11,185)	(1,15, 4,332, 21,167)	(-10,702, -0,615, 9,314)
C15	(0,621, 2,12, 10,111)	(0,053, 2,33, 11,21)	(0,674, 4,45, 21,321)	(-10,589, -0,209, 10,057)
C16	(0,575, 2,034, 10,051)	(0,059, 2,681, 11,96)	(0,633, 4,714, 22,011)	(-11,385, -0,647, 9,993)
C17	(0,55, 1,986, 9,741)	(0,853, 2,474, 11,619)	(1,403, 4,461, 21,36)	(-11,069, -0,488, 8,888)
C18	(1, 2,843, 12,428)	(1,332, 2,332, 11,167)	(2,333, 5,175, 23,595)	(-10,167, 0,512, 11,096)
C19	(0,581, 2,046, 10,259)	(1,707, 2,04, 10,126)	(2,288, 4,086, 20,385)	(-9,545, 0,006, 8,552)
C20	(0,786, 2,469, 11,675)	(2,309, 1,867, 9,753)	(3,095, 4,337, 21,428)	(-8,967, 0,602, 9,366)
C21	(0,888, 2,628, 11,811)	(1,913, 2,093, 10,412)	(2,801, 4,721, 22,223)	(-9,524, 0,536, 9,897)
C22	(0,757, 2,379, 11,076)	(1,047, 2,201, 10,528)	(1,804, 4,58, 21,604)	(-9,77, 0,178, 10,029)
C23	(0,157, 1,238, 7,799)	(1,118, 1,9, 9,867)	(1,275, 3,138, 17,666)	(-9,71, -0,663, 6,681)
C24	(0,93, 2,676, 12,135)	(0,485, 2,269, 10,789)	(1,415, 4,945, 22,924)	(-9,859, 0,407, 11,65)
C25	(0,91, 2,672, 11,337)	(-0,227, 1,964, 9,759)	(0,683, 4,636, 21,096)	(-8,848, 0,707, 11,565)

4. Results

To present better solution about understanding etiologies of the ransomware attacks in maritime and influence loop between them, after producing the influential relation map (IRM), four quadrants are created on it by calculating the mean of $(R + C)$ as in Figure 3. Because, in various DEMATEL studies (Chien et al., 2014; Chuang et al., 2013; Hwang et al., 2016; Si et al., 2018), it is suggested that four quadrants I to IV is created on the IRM in order to classify the factors better in a sophisticated system according to their positions in the diagram. Accordingly, the agents in portion I are defined as essence factors or intertwined supplier because they include high relation and prominence; the agents in portion II are defined as driving elements since they include high relation and low prominence; the agents in portion III are identified as independent elements and relatively disengaged from the system because they involve low relation and prominence; the agents in portion IV are identified as impact factors or intertwined receivers that are affected by other agents and cannot be directly enhanced because they consist of low relation but high prominence. As a result, portions I and IV are identified as powerful “cause” and “effect” agents of asked issued, respectively. On the contrary, portions II and III are identified as powerless “cause” and “effect” agents for asked issues, respectively. By the help of the driving power-dependence diagram in Figure 3, people, who needs to make a decision, can visually ascertain the complicated causal links between agents and attract further attention effective inner vision for decision making.

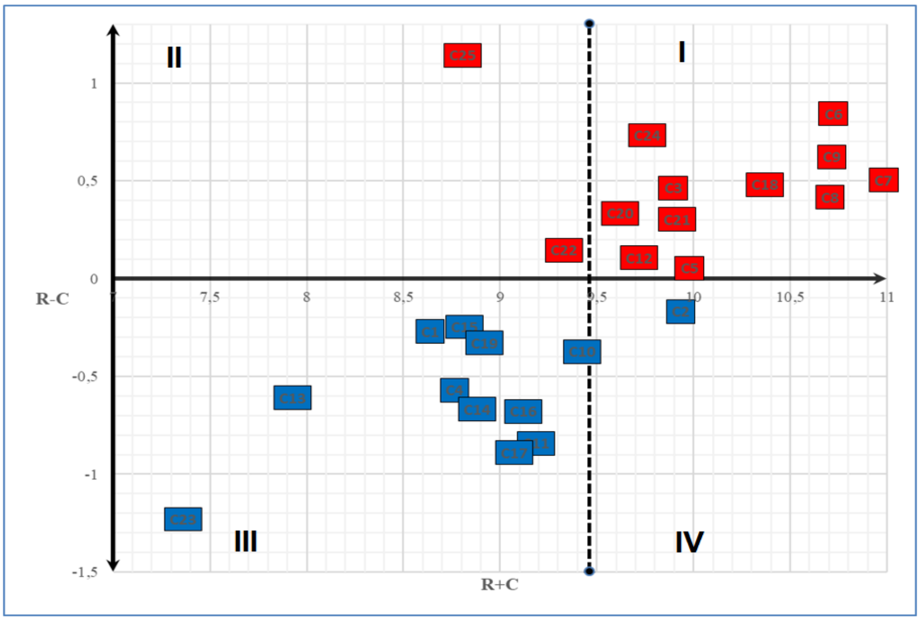

Figure 3 Cause-effect diagram of ransomware cyber-attacks in maritime

In Table 8, the ranking of factors according to several categories are presented. The (R+C) values represent the degree of importance between the elements. The (R-C) values show the relationship between elements where positive values are grouped as cause factors and negative values are grouped as influence factors. The (R+C) values shows the degree of significance of elements in determining the success of ransomware attacks in maritime.

Table 8 Results of the analysis

Factors	**Prominence (R+C)**	**Rank of Factors**	**Relation (R-C)**	**Cause/Effect Groups**	**Quadrant of Factors**	**Rank of factors, according to groups in the same quadrants**
C6	10,72	2	0,84	Cause	I	1
C24	9,76	10	0,73	Cause	I	2
C9	10,71	3	0,62	Cause	I	3
C7	10,98	1	0,50	Cause	I	4
C18	10,37	5	0,48	Cause	I	5
C3	9,89	9	0,46	Cause	I	6
C8	10,70	4	0,42	Cause	I	7
C20	9,62	12	0,33	Cause	I	8
C21	9,91	8	0,30	Cause	I	9
C12	9,72	11	0,11	Cause	I	10
C5	9,98	6	0,05	Cause	I	11
C25	8,81	21	1,14	Cause	II	{1}
C22	9,33	14	0,15	Cause	II	{2}
C15	8,81	20	-0,25	Effect	III	(1)
C1	8,64	23	-0,27	Effect	III	(2)
C19	8,92	18	-0,33	Effect	III	(3)
C10	9,42	13	-0,37	Effect	III	(4)
C4	8,76	22	-0,57	Effect	III	(5)
C13	7,93	24	-0,61	Effect	III	(6)
C14	8,88	19	-0,67	Effect	III	(7)
C16	9,12	16	-0,68	Effect	III	(8)
C11	9,19	15	-0,84	Effect	III	(9)
C17	9,07	17	-0,89	Effect	III	(10)
C23	7,36	25	-1,23	Effect	III	(11)
C2	9,93	7	-0,17	Effect	IV	[1]

According to the results of the analysis, the factors in quadrant I and IV in Figure 3 are strong "cause" and "effect" factors for occurring the ransomware cyber-attacks in maritime, respectively. In this context, in Table 9, the most important causes and the most important impact factors for ransomware attacks in maritime are shown in addition to preference of importance ranking. The column of preference of importance shows the importance level of factors for occurring ransomware cyber-attacks in maritime. These factors have the highest relation to ransomware cyber-attacks in maritime and they are depended each other in this system. On the other hand, C2 is the effect factor for ransomware attacks in maritime, it means that it depends on other factors, which higher than it according to the importance level, owing to its position in impact group.

Table 9 Preference of significance for factors

Net Group	Causal factors: C6, C24, C9, C7, C18, C3, C8, C20, C21, C12, C5 Effect factors: C2
Preference of importance	C7>C6>C9>C8>C18>C5>C2>C21>C3>C24>C12> C20

5. Discussions

According to the results, “having the vulnerabilities of OS or software against ransom malwares (C6)” is the most important causal factor for ransomware attacks in maritime as expected results. Because for an attack to be successful, the ransomware file requires to be executed on a computer. For this purpose, an exploit kit or a phishing email is usually used. Malware in the phishing mail or the malicious toolkit is used to exploit vulnerabilities in the operating system or software applications to spread malware – it refers to C6. Even the ranking of the importance of the factors is C7, C6, C9, C8, respectively, the prominence values of them (10.98, 10.72, 10.71, 10.70) are close each other. Accordingly, they can be evaluated as a whole factor in terms of making any ransomware attacks more possible to be successful. Therefore, “lack of patches for supported versions of OS (C7)”, “lack of anti-malware tool on the systems and software (C9)”, and “lack of updating the system and software (C8) in addition to C6 are the most significant driver agents for ransomware attacks in maritime. Starting from this point of view, maritime companies should consider specifically the factors of C6, C7, C9, and C8 for ensuring cyber hygiene against ransomware attacks on their shipping or other informational and operational systems in the critical level. Because for instance, when it comes to CryptoLocker malware, the preferred method is the Angler exploit kit, as with many exploit kits, to gain execution. The security holes used by the Angler exploit kit usually exist in Internet Explorer and Adobe Flash based on Microsoft Windows. There are vulnerabilities in Windows' Server Message Block (SMB) protocol or Oracle WebLogic Server vulnerability CVE-2019-2725 for Sodinokibi ransomware that are used in maritime area commonly. Furthermore, for Ryuk ransomware, which is the most common ransomware in maritime area according to the above-mentioned incident table, the vulnerabilities CVE-2017-0144 and CVE-2017-0143 are exploited by External Blue. CVE-2017-0144 / 0143 / 0145 / 0146 / 0147, which are found in Microsoft products, are vulnerable against Ryuk ransomware. Ryuk infection and other types of ransomwares cause an interruption of physical access control systems, interruption of the whole enterprise IT network, and loss of critical process control monitoring systems in the maritime companies. Accordingly, in maritime sector, where the payment for ransomware reach from $500.000 to $1.2 billion (Stone, 2019), these obtained prominence factors should be considered as a persistence layout for ransomware attacks as suggested in "T1059 - Command and Scripting Interpreter: Windows Command Shell" in MITRE ATT&CK mapping (MITRE ATT&CK, 2022), which is used as a basis for the designing models and approaches for particular threats in the government, private sector, and the community for cybersecurity service and product, as well. Accordingly, to quarantine suspicious files automatically, antimalware tools can be utilized. With endpoint behavior prevention in Windows 10, Attack Surface Reduction (ASR) rules can be enabled to prevent JavaScript and Visual Basic scripts derived from executing potentially malicious downloaded content. It can remove or disable unused or unnecessary interpreters or shells with the uninstall program functionality. Application control can be used where appropriate with the execution prevention function.

Flowing that, as above-mentioned, the malicious kits or phishing e-mails as well as portable devices such as USB sticks are the common ways to execute the malicious ransomware on the system for several targeted sectors. Outdated or insecure software applications run on users' computer are targeted by these kits, phishing e-mails, or portable devices. Additionally, spam mails need some kind of act by the user to be successful. This step refers "opening a malicious any kind of electronic messaging (C2)". As it can be seen from the mathematical analysis as a proof, for resulting successful ransomware attacks, the function of C2, as being an effect factor, depends on the presence of more important factors (C7, C6, C9, C8, C18, C5), which are the causal factors for ransomware attacks in maritime. On the other hand, it is understood from preference of importance in Table 9 that in maritime area, "using several USB without pre-scanned (C5)" is more preferred way than C2 for downloading or infiltrating the payload to the system. However, the most preferred method for deploying ransomware in maritime sector is to use RDP ports by the attacker due to "leaving open RDP ports used by the company to the internet (C18)". As the default listening port, RDP utilizes port 3389. This is known by threat actors and a script can be run to scan port 3389 that has been left open to the internet. The attacker must capture the login credentials when an exposed port is found. Once inside, they can leave backdoors for future access or distribute ransomware. For instance, ransomware variants such as Maze and Ryuk, which are the common attacks in maritime, attack the victim's entire network, often via a back door opened by exploiting RDP. Although there is no detail information about starting point of ransomware attacks in the exist incidents in maritime, the result of this study is also an indicator for that using RDP ports by the attacker to deploy ransomware to the system can be the most used method. The implication is that in maritime sector the intrusion point is more network based (RDP) rather than C5 or C2. To prevent that using VPN while RDP ports open to internet, using an allow list, which only confirmed IP addresses is allowed in order to access to the RDP server, creating an implementation on the network firewall to prevent RDP from accessing the Internet from any system behind the firewall (C21), using network traffic monitoring and tracking system (C24), using multi factor authentication (C12), using network segregation (C20), and limiting failed logins attempts are the best mitigations.

In addition to all of them, running up-to-date end-point security and anti-virus software (C3) provides sustainability of cyber security against ransomware attacks in case of using both phishing or portable devices and RDP ports.

Consequently, this study provides an optimum map for overall cyber hygiene against ransomware by building influence loop based upon mathematical analysis in a security framework consisting of demonstration vulnerable points and protection methods. The overall influence diagram for successful ransomware cyber-attack in maritime is shown in Figure 4.

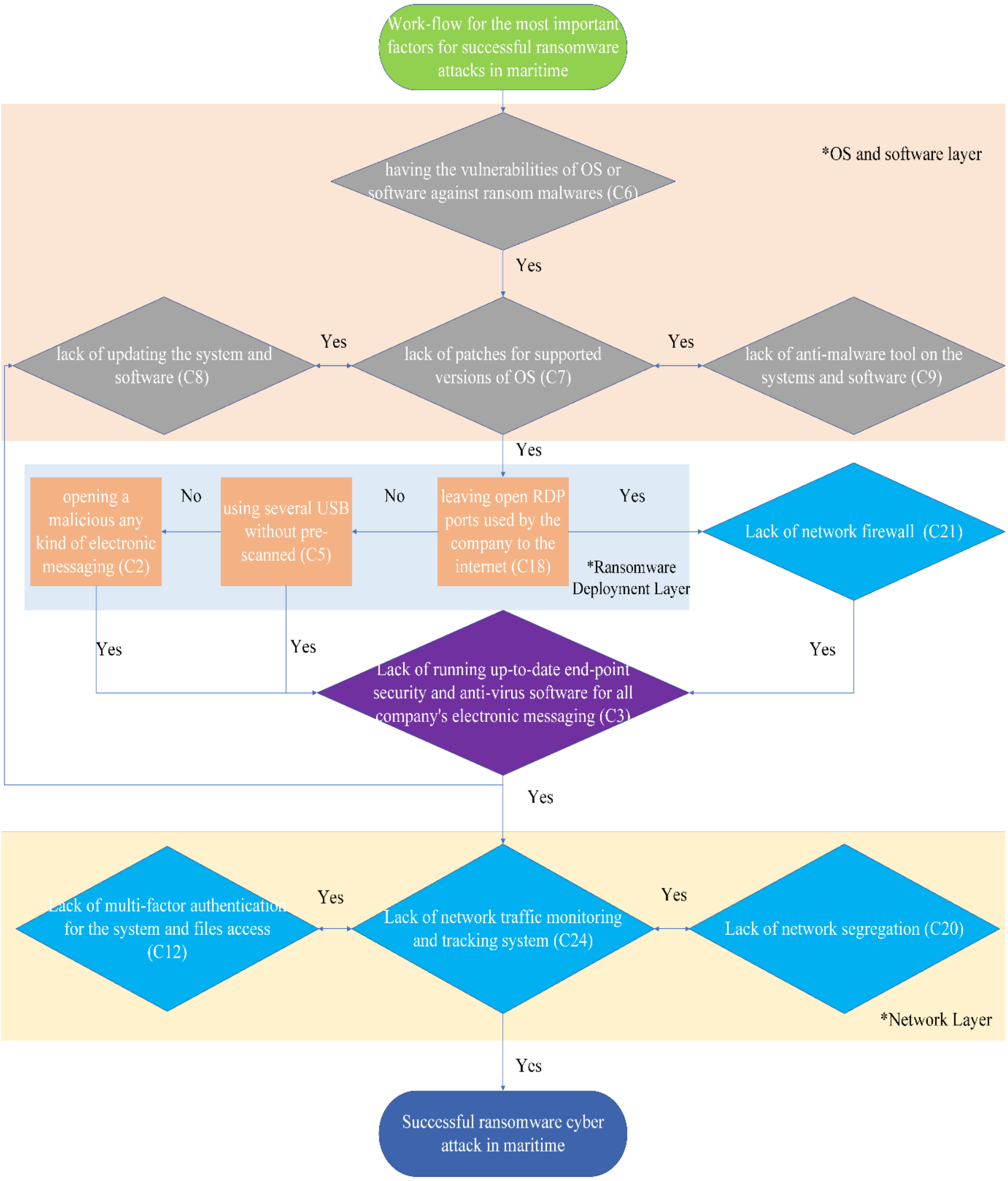
Work-flow for the most important factors for successful ransomware attacks in maritime
*OS and software layer
having the vulnerabilities of OS or software against ransom malwares (C6)
Yes
lack of updating the system and software (C8)
Yes
lack of patches for supported versions of OS (C7)
Yes
lack of anti-malware tool on the systems and software (C9)
Yes
opening a malicious any kind of electronic messaging (C2)
No
using several USB without pre-scanned (C5)
No
leaving open RDP ports used by the company to the internet (C18)
Yes
Lack of network firewall (C21)
*Ransomware Deployment Layer
Yes
Yes
Yes
Lack of running up-to-date end-point security and anti-virus software for all company's electronic messaging (C3)
Yes
Lack of multi-factor authentication for the system and files access (C12)
Yes
Lack of network traffic monitoring and tracking system (C24)
Yes
Lack of network segregation (C20)
*Network Layer
Yes
Successful ransomware cyber attack in maritime

Figure 4 Flow diagram for successful ransomware cyber-attack in maritime according to analysis results

Accordingly, the factors are positioned on the diagram according to their importance level for successful ransomware attacks in maritime sector. The obtained result is that ransomware attacks can be only successful if there are vulnerabilities on the OS and software layer, which attacker can exploit as a security hole. This layer defines the working principle of considered ransomware. Then, the created ransomware by the attacker needs to intrusion to system by using RDP protocols, or utilizing unconscious human error including using portable devices without pre-scan or opening phishing mails. Lastly, the in running ransomware moves to network layer if above mentioned mitigations are not existed and encrypt accessed files and system, which are perhaps recoverable against ransom.

6. Conclusions

The prevention of digital incidents and the confidentiality, integrity and availability (CIA) of valuable assets are the main goals of accident/incident analysis, which is a crucial component of cyber risk management. Ransomware is often listed as one of the top cybersecurity threats in annual threat reports, but despite that public and private organizations still often are reluctant to report their cybersecurity vulnerabilities/incidents, so it is critical to conduct such cybersecurity research and develop strategies to either prevent such attacks or better handle them.

To look at the sector wide threat, this study focuses on the 22 public maritime ransomware incidents in order to determine their causes and create preventive measures for each of the major elements that significantly influenced the incidents which have been performed against the maritime industry and have substantial consequences. For this purpose, fuzzy sets and DEMATEL are combined in the present research to analyze the cause elements and, ultimately, avoid future ransomware incidents by creating efficient safety measures.

The study's findings clearly reveal that there are several key steps that maritime organizations should take in order to become cyber-resilient against ransomware attacks. The first and most critical step is to prioritize cyber security investment for OS and software layers. Then, it's crucial to concentrate on the strategies for utilizing RDP protocols securely that are outlined in detail in the discussion section. Another primary consideration that has been emphasized is giving serious attention to network layer cyber security mitigations. In light of the findings, it is absolutely critical for organizations to be proactive against this cyber threat since, unlike other cybersecurity risk, ransomware attacks have a direct immediate impact on daily operations. Therefore, implementing comprehensive and consistent incident analysis methods and techniques is a prerequisite for continuously improving cyber risk management strategies, in addition to fostering transparency among stakeholders and educating users of cyber systems about the steps to take to prevent and handle potential compromises. This has emerged as a fundamental principle of cyber risk management given the frequency and sophistication of strategies and techniques used in cyberattacks. This will make it possible to offer a proactive baseline for sector-specific cyber risk management strategies.

In summary, the contributions of the study are as follows: (i) identification of overall vulnerabilities for any of ransomware attack comprehensively and systematically with the help of analysis of ransomware incidents in specifically maritime sector and examining frameworks of various kind of ransomware; (ii) performing fuzzy DEMATEL methodology in order to understand influence loop between factors for ransomware attacks within the maritime industry; (iii) developing mitigations and strategies about cyber security for ransomware by focusing on most important factors; (iv) providing insights to maritime companies about ransomware cyber security investment precedencies; (v) the findings of this study may be helpful for other industries where ransomware attacks occur. To sum up, this study provides a pioneering application of the fuzzy DAMETAL approach in ransomware incident analysis in maritime cyber systems.

As a result, the model used enables maritime cyber resilience to be improved by developing realistic and adaptable steps that may be taken based on actual incidents. However, it should be worth mentioning that the present study has some flaws, including its theoretical nature and reliance on expert opinions. Consequently, future studies may be extended to cover a systematic and transparent process for data collection and analysis to overcome to mentioned limitations.

Acknowledgements

This study is partially funded by The Scientific and Technological Research Council of Turkey (TÜBİTAK) - 2214-A - International Research Fellowship Programme for PhD Students [REF: 53325897-115.02-152823] (Grant No: 1059B142100581).

This study is also supported by University of Plymouth, Cyber-SHIP Lab Research Team.

Author Contributions

The authors confirm contribution to the paper as follows: study conception and design: O. Soner; data collection: G. Kayisoglu; analysis and interpretation of results: O. Soner, G. Kayisoglu, P. Bolat, K. Tam; draft manuscript preparation: O. Soner, G. Kayisoglu, P. Bolat, K. Tam. All authors reviewed the results and approved the final version of the manuscript.

References

Akyuz, E., & Celik, E. (2015). A fuzzy DEMATEL method to evaluate critical operational hazards during gas freeing process in crude oil tankers. *Journal of Loss Prevention in the Process Industries*, *38*, 243–253. https://doi.org/10.1016/j.jlp.2015.10.006

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, *8*(10), 776. https://doi.org/10.3390/jmse8100776

Anjum, M., Kapur, P. K., Agarwal, V., & Kumar, V. (2022). Analyzing Interrelationships Among Software Vulnerabilities Using Fuzzy DEMATEL Approach. In *Reliability and Maintainability Assessment of Industrial Systems* (pp. 291–300). Springer Cham. https://doi.org/10.1007/978-3-030-93623-5_13

August, T., Dao, D., & Niculescu, M. F. (2019). Economics of ransomware attacks. *Available at SSRN*.

Aziz, S. M. (2016). Ransomware in High-Risk Environments. In *Information Technology Capstone Research Project Reports 1*.

Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. (2022). Ransomware Risk Management: A Cybersecurity Framework Profile. In *National Institute Of Technology*. https://doi.org/10.6028/NIST.IR.8374

Başhan, V., & Ust, Y. (2019). Application of fuzzy dematel method to analyse s-CO2 Brayton power systems. *Journal of Intelligent & Fuzzy Systems*, *37*(6), 8483–8498. https://doi.org/10.3233/JIFS-191133

Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. *Expert Systems with Applications*, *209*, 118299. https://doi.org/10.1016/j.eswa.2022.118299

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology*, *9*(14). https://doi.org/10.17485/ijst/2016/v9i14/82936

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2015). *Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics*. https://arxiv.org/ftp/arxiv/papers/1611/1611.08294.pdf

Chien, K.-F., Wu, Z.-H., & Huang, S.-C. (2014). Identifying and assessing critical risk factors for BIM projects: Empirical study. *Automation in Construction*, *45*, 1–15. https://doi.org/10.1016/j.autcon.2014.04.012

Chuang, H.-M., Lin, C.-K., Chen, D.-R., & Chen, Y.-S. (2013). Evolving MCDM Applications Using Hybrid Expert-Based ISM and DEMATEL Models: An Example of Sustainable Ecotourism. *The Scientific World Journal*, *2013*, 1–18. https://doi.org/10.1155/2013/751728

Chubb, N. (2022). *Cyber attacks: who targets the maritime industry and why?* Thetius. https://thetius.com/cyber-attacks-who-targets-the-maritime-industry-and-why/

CISA. (2016). *Protecting Your Networks from Ransomware*.

Dadiani, D. (2018). *The Maritime Commons : Digital Repository of the World Cyber-security and marine insurance*. World Maritime University.

Fayi, S. Y. A. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. In *In: Latifi, S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham.* (pp. 93–100). https://doi.org/10.1007/978-3-319-77028-4_15

Fontela, E., & Gabus, A. (1976). *The DEMATEL Observer, DEMATEL 1976 Report*.

Gabus, A., & Fontela, E. (1973). *Perceptions of the world problematique: communication procedure, communicating with those bearing collective responsibility*.

Goodell, J. W., & Corbet, S. (2023). Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. *Finance Research Letters*, *51*, 103329. https://doi.org/10.1016/j.frl.2022.103329

Gumus, A., Yayla, A., Çelik, E., & Yildiz, A. (2013). A Combined Fuzzy-AHP and Fuzzy-GRA Methodology for Hydrogen Energy Storage Method Selection in Turkey. *Energies*, *6*(6), 3017–3032. https://doi.org/10.3390/en6063017

Homeport. (2015). *The Maritime and Port Security Information Sharing & Analysis Center*

(MPS-ISAO). US Department of Homeland Security United States Coast Guard. https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=45422&Source=/Lists/Content/DispForm.aspx?ID=45422

Hwang, W., Hsiao, B., Chen, H.-G., & Chern, C.-C. (2016). Multiphase Assessment of Project Risk Interdependencies: Evidence from a University ISD Project in Taiwan. *Project Management Journal*, *47*(1), 59–75. https://doi.org/10.1002/pmj.21563

HYPR. (2022). *NotPetya*. HYPR Corp. https://www.hypr.com/security-encyclopedia/notpetya

Kang, S., Lee, S., Kim, S., Kim, D., Kim, K., & Kim, J. (2021). A Study on Decryption of Files Infected by Ragnar Locker Ransomware through Key Reuse Attack and Its Applications. *Journal of the Korea Institute of Information Security & Cryptology*, *31*(2), 221–231. https://doi.org/https://doi.org/10.13089/JKIISC.2021.31.2.221

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, *190*, 116198. https://doi.org/10.1016/j.eswa.2021.116198

Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models. In *Master thesis* (Issue July).

Lawrence, C. (2022). *Securing the seas when the maritime industry's drowning*. The Next Web TNW. https://thenextweb.com/news/martime-industry-drowning-from-cybercriminal-threat

Lazarovitz, L. (2021). Deconstructing the SolarWinds breach. *Computer Fraud & Security*, *2021*(6), 17–19. https://doi.org/10.1016/S1361-3723(21)00065-8

Lin, C.-L., & Tzeng, G.-H. (2009). A value-created system of science (technology) park by using DEMATEL. *Expert Systems with Applications*, *36*(6), 9683–9697. https://doi.org/10.1016/j.eswa.2008.11.040

Liu, Z., & Wu, Z. (2003). The human element in ship collisions at sea. *Asia Navigation Conference*.

Logan, M., Mendoza, E., Maglaque, R., & Tamaña, N. (2021). *The State of Ransomware: 2020's Catch-22*.

Maiers, J., & Sherif, Y. S. (1985). Applications of fuzzy set theory. *IEEE Transactions on*

Systems, Man, and Cybernetics, *SMC-15*(1), 175–189. https://doi.org/10.1109/TSMC.1985.6313408

Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments*, *5*(2), 67–89. https://doi.org/10.1007/s40860-019-00080-3

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security*, *2019*(3), 8–10. https://doi.org/10.1016/S1361-3723(19)30028-4

McIntosh, T. R., Jang-Jaccard, J., & Watters, P. A. (2018). Large Scale Behavioral Analysis of Ransomware Attacks. In *In: Cheng, L., Leung, A., Ozawa, S. (eds) Neural Information Processing. ICONIP 2018. Lecture Notes in Computer Science(), vol 11306. Springer, Cham.* (pp. 217–229). https://doi.org/10.1007/978-3-030-04224-0_19

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

MITRE ATT&CK. (2022). *Ryuk*. MITRE ATT&CK. https://attack.mitre.org/software/S0446/

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940.

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Nicols, S. (2022). *SonicWall: Ransomware attacks increased 105% in 2021*. TechTarget. https://doi.org/https://www.techtarget.com/searchsecurity/news/252513538/SonicWall-Ransomware-attacks-increased-105-in-2021

NIST. (2021). *Tips & Tactics: Preparing Your Organization for Ransomware Attacks* (Issue May).

NJCCIC. (2022). *Maritime Threat Analysis*. Threat Analysis Report - New Jersey Cybersecurity and Communications Integration Cell. https://www.cyber.nj.gov/threat-analysis-reports/maritime-threat-analysis

Pen Test Partners. (2022). *Maritime Cyber Security Testing*. Pen Test Partners Security Consulting and Testing Services. https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/

Rajamäki, J., Tikanmäki, I., & Räsänen, J. (2019). CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain. *Information & Security: An International Journal*, *43*(2), 215–235. https://doi.org/10.11610/isij.4317

Ross, T. J. (2005). *Fuzzy logic with engineering applications*. John Wiley & Sons.

Saketh, V. S. R., & Puppala, H. (2023). *Assessment of Smart City Indicators from ICT Framework in an Indian Context: A Fuzzy DEMATEL Approach* (pp. 927–935). https://doi.org/10.1007/978-981-19-4040-8_75

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2015). Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection. *Cornell University Cryptography and Security*, *1*(11), 203–206.

Si, S.-L., You, X.-Y., Liu, H.-C., & Zhang, P. (2018). DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications. *Mathematical Problems in Engineering*, *2018*, 1–33. https://doi.org/10.1155/2018/3696457

Sittig, D., & Singh, H. (2016). A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied Clinical Informatics*, *07*(02), 624–632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

Soner, O. (2021). Application of fuzzy DEMATEL method for analysing of accidents in enclosed spaces onboard ships. *Ocean Engineering*, *220*, 108507. https://doi.org/10.1016/j.oceaneng.2020.108507

Stone, J. (2019). *Coast Guard says Ryuk ransomware hit systems that monitor cargo transfers at maritime facility*. Cyberscoop. https://www.cyberscoop.com/ransomware-australia-task-force/

Svilicic, B., Rudan, I., Frančić, V., & Doričić, M. (2019). Shipboard ECDIS cyber security: Third-party component threats. *Pomorstvo, 33*(2), 176–180. https://doi.org/10.31217/p.33.2.7

Svilicic, B., Rudan, I., Frančić, V., & Mohović, D. (2020). Towards a Cyber Secure Shipboard Radar. *Journal of Navigation*, *73*(3), 547–558. https://doi.org/10.1017/S0373463319000808

Tam, K., Chang, B., Hopcraft, R., & Jones, K. (2023). Quantifying the econometric loss of a cyber-physical attack on a seaport. *Frontiers Computer Science*.

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., . . . Jones, K. D. (2022). Case Study of a Cyber-Physical Attack Affecting. *Journal of Transportation Technologies*, 1-27.

Thavi, R. R., Narwane, V. S., Jhaveri, R. H., & Raut, R. D. (2022). To determine the critical factors for the adoption of cloud computing in the educational sector in developing countries – a fuzzy DEMATEL approach. *Kybernetes, 51*(11), 3340–3365. https://doi.org/10.1108/K-12-2020-0864

Trellix. (2022). *THE THREAT REPORT Fall 2022*. Trellix Advanced Research Center. https://www.trellix.com/en-us/advanced-research-center/threat-reports/nov-2022.html

TREND MICRO. (2022). *What Is RYUK Ransomware?* https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

Vinodh, S., & Wankhede, V. A. (2021). Application of fuzzy DEMATEL and fuzzy CODAS for analysis of workforce attributes pertaining to Industry 4.0: a case study. *International Journal of Quality & Reliability Management*, *38*(8), 1695–1721. https://doi.org/10.1108/IJQRM-09-2020-0322

Wagner, P. (2021). Third Party Breaches - A Survey of Threats and Recommendations. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3782822

Wang, Z., Liu, C., Qiu, J., Tian, Z., Cui, X., & Su, S. (2018). Automatically Traceback RDP-Based Targeted Ransomware Attacks. *Wireless Communications and Mobile Computing*, *2018*, 1–13. https://doi.org/10.1155/2018/7943586

Wu, W.-W. (2012). Segmenting critical factors for successful knowledge management implementation using the fuzzy DEMATEL method. *Applied Soft Computing*, *12*(1), 527–

535. https://doi.org/10.1016/j.asoc.2011.08.008

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

Zimmermann, H.-J. (2010). Fuzzy set theory. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(3), 317–332. https://doi.org/10.1002/wics.82