The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified

Sheetal Temara

Asian Journal of Advanced Research and Reports

Volume 18, Issue 3, Page 1-16, 2024; Article no.AJARR.112469
ISSN: 2582-3248

The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified

Sheetal Temara [a*]

[a] Department of Computer & Information Sciences, University of the Cumberlands, Williamsburg, KY, United States.

Author's contribution

The sole author designed the study, conducted the research, collected and analyzed the data, and wrote the manuscript.

Article Information

DOI: 10.9734/AJARR/2024/v18i3610

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/112469

Review Article

Received: 27/11/2023
Accepted: 02/02/2024
Published: 05/02/2024

ABSTRACT

The pervasive threat of ransomware poses a significant risk to businesses across various scales as cybercriminals continue to exploit vulnerabilities causing severe disruptions and demanding substantial ransom payments. This review conducts a comprehensive literature review delving into recent ransomware attacks to analyze key aspects, including the targeted organizations, attack vectors, threat actors, propagation mechanisms, and the resulting business impact. The study goes beyond a surface examination by exploring the evolving nature of ransomware attacks, encompassing different types, attack vectors, and emerging tactics, such as double extortion, where cybercriminals not only encrypt data but also exfiltrate and threaten to release it publicly unless a ransom is paid. High-profile incidents, including those involving SickKids Hospital, Royal Mail, Dish Network, Five Guys, and ION are scrutinized to glean insights into the intricacies of these attacks. The review also evaluates the effectiveness of existing ransomware defenses and proposes potential strategies for organizations to counteract, identify, and manage ransomware incidents. The findings underscore the critical need for organizations to comprehend the evolving ransomware landscape and implement robust cybersecurity measures to protect both internal and external stakeholders. As ransomware continues to evolve in complexity, this study provides valuable insights emphasizing the importance of proactive defenses to mitigate the risks posed by this growing threat.

**Corresponding author: Email: stemara22276@ucumberlands.edu;*

Keywords: Ransomware; cybercriminals; ransomware incidents; ransomware defenses.

ABBREVIATIONS

API : Application Programming Interface
DLL : Dynamic Link Library
EDR : End-point Detection and Response
ESXi : Elastic Sky X Integrated
FTA : File Transfer Appliance
MFA : Multi Factor Authentication
NMR : No More Ransom
PII : Personal Identifiable Information
RAAS : Ransomware-as-a-service
RDP : Remote Desktop Protocol

1. INTRODUCTION

It has been observed that threat actors wielding sophisticated malware are capable of targeting organizations globally with ease. These attacks can have a devastating impact and disrupt the normal operations of companies and governmental agencies by degrading the accessibility and privacy of confidential data resulting in loss of information, reputational damage, and legal implications [1]. This can also lead to system failure, operational downtime, loss of data integrity, and reduced customer confidence if the data gets compromised.

Ransomware is a type of malicious software that is used by cybercriminals to compromise a computer and subsequently encrypt files ensuring authorized users can no longer access them. After the files have been encrypted, a stipulation for a ransom to be paid is issued from the threat actor in exchange for the keys that can decrypt the files. During some incidents, threat actors may not grant access to the files even after the payment of ransom has been made [2]. Currently, ransomware is considered one of the most rapidly expanding types of cyber-attacks. As ransomware continues to flourish, it generated $20 billion in 2020 with payments for ransomware incidents rising to an average of $570,000 in 2021 [3]. The number of ransomware attacks skyrocketed by 64 percent in 2021 from the year prior. The propagation of ransomware is increasing as a result of its ease of deployment, indiscriminate targeting of organizations in all industries, and the fact that ransomware kits are available at an affordable price on the dark web marketplace.

The initial variants of ransomware were restricted to encrypting the drives on the compromised computer. This could include logical drives created within the operating system or external drives that are physically connected to the computer [4]. However, the newer variants can encrypt network shares to ensure that ransom payment occurs by prohibiting the recovery of files over the network.

The initial ransomware appeared in 1989 during the distribution of the PC Cyborg to people who attended a convention through a physically mailed diskette containing the ransomware [5]. This ransomware encrypted files on the hard drive of the computer system that the diskette was inserted into. Subsequently, a message would be displayed requiring a ransom to recover the files by delivery of $189 to an organization located in Panama [6]. Ransomware did not gain significant attention until the maturation of the Internet. The initial contemporary ransomware surfaced in 2005 at the point that there were over 1 billion connected users.

1.1 Types of Ransomware

Ransomware affects all industries but is particularly effective for targets in the government, aviation, and aerospace organizations. Ransomware attacks are becoming increasingly sophisticated and widespread making it challenging to keep up with the ever-growing documentation describing this malicious software. Within its landscape, ransomware can be categorized into three primary types namely: screen-locking ransomware, data file-encrypting ransomware, and double-extortion ransomware [6]. The ransomware locks screens and inhibits victims from using systems entirely by locking the interface and thereafter requiring disbursement of a release fee to regain access. This type of ransomware makes no effort to encrypt files or data but the computer system continues to be locked after the machine is forced to restart [7]. The data file encrypting ransomware will encrypt data and files by means of a cryptographic algorithm and requires payment to retrieve the decryption keys. This type of ransomware normally integrates asymmetric cryptography for encryption operations and creates a key pair consisting of public and private keys distinctive for the victim and the threat actor [8]. The double-extortion ransomware not only encrypts the data but also will release sensitive information as a consequence of not paying the demanded ransom. A few actors are involved in

the ecosystem of ransomware including the infected systems and the command-and-control servers managed by threat actors processing the encryption keys and ransom disbursements [9]. Additional operators provide auxiliary functions such as ransomware binary delivery and victim identification.

1.2 Anatomy of a Ransomware Attack

Six stages are involved in a ransomware attack which include reconnaissance, distribution/delivery, installation/infection, communication, encryption, and extortion/payment [6]. The reconnaissance phase discovers a catalog of prospective target computer systems for the ransomware attack. This can be accomplished with techniques such as port scanning, social media discovery, mailing list enumeration, or procurement of lists from other threat actors. With distribution/delivery, the primary goal is to deploy the ransomware to the identified target computer systems [6]. This can be accomplished with techniques such as phishing, website exploitation, or physical file delivery with portable drives. During the installation/infection stage, the ransomware will be configured on the target computer systems. During this deployment of ransomware, many variants will attempt to obfuscate their existence while performing additional reconnaissance to find other computer systems for ransomware propagation [6]. The communication stage entails communications with the command & control server which varies depending on the design selected for encryption. In variants using symmetric key encryption, an encryption key is created for the targeted computer system that is, in turn, maintained locally or transmitted to the ransomware command and control server requiring victims to interact with the server to acquire the keys for decryption. This type of implementation involving local keys puts the ransomware encryption scheme at risk of being blocked by the protection offered by anti-virus software which could also reveal the key to the victim. Due to this potential issue, asymmetric encryption is often used resulting in slower encryption along with a high risk of detection [10]. Through the encryption stage, the malicious software executes encryption operations to encrypt files and/or data or lock access to the victim's computer system. The data is typically deleted along with a message announcing the installation of the ransomware as well as the demand for payment. The extortion/payment stage manages payments of ransom and additional required actions [6]. Note that some ransomware may not provide keys for decryption even after a ransom payment is received.

2. LITERATURE REVIEW

This paper studied the ransomware incidents presented in the following literature: The Evolution of Cryptocurrency and Cyber-attacks by Berry [11], Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Caroscio et al. [6], Some Of The Companies Affected by Ransomware in 2021 by Din [4], Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server by Kiesel et al. [7], The State of Ransomware in 2023 by Robb [12], Royal ransomware claims attack on Queensland University of Technology by Toulas [13], Ransomware Detection and Classification Strategies by Vehabovic et al. [14].

2.1 The Evolution of Cryptocurrency and Cyber-attacks by Berry [3]

Berry [11] examines the relationship between the growth in ransomware attacks and the rise of cryptocurrency. Ransomware can be classified into two types including encryptor ransomware and screen-locker ransomware [11]. Screen-locker ransomware is described as ransomware that locks the user interface while mandating a request for ransom and prohibiting the target from accessing the data as well as the computer system itself [11]. Encryptors ransomware executes encryption to encrypt data in the file system while mandating a ransom payment to obtain the key needed to decrypt the data [11]. It has been determined that ransomware predated cryptocurrency and that the existence of ransomware does not need cryptocurrency as a prerequisite.

2.2 Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk by Caroscio et al. [6]

Ransomware is experiencing massive growth while presenting a significant risk to the public which can impact the targets considerably from both financial and data availability perspectives [6]. A deep examination of a fresh ransomware attack by a ransomware group named Babuk on a police branch was studied by Caroscio et al. [6] to understand damages from both international and regional standpoints. An overview of the

probable steps in the Babuk attack is outlined by Caroscio et al. [6] who argue that malicious software such as ransomware enables cybercriminals to easily attack a variety of organizations with the end goal of receiving paying ransom with techniques that negatively influence sensitive data from a notion of confidentiality, integrity, and availability. Caroscio et al. [6] contend that Babuk shifted to concentrate more on data extortion after the attack on the police department. The ransomware attack methodology employed by Babuk is described as having a few phases including obtaining initial access, maintaining access, performing encryption, and demanding ransom. Lastly, Caroscio et al. [6] present several potential countermeasures including constant penetration testing, maintenance of policies designed to mitigate ransomware attacks, regulation of cryptocurrency, and education and awareness programs regarding phishing and social engineering.

2.3 Some of The Companies Affected by Ransomware in 2021 by Din [4]

Din [4] states that threat actors are performing an ever-increasing number of ransomware attacks by using security vulnerabilities as a primary attack vector resulting in many organizations having their data encrypted. This is further illustrated by Din [4] as she states that more than 200,000 new variants of ransomware are identified every day while they impose significant destruction. The motivation for the threat actors behind ransomware is that organizations provide ransom payments while not announcing the attacks occurred because they are concerned about reputational damage. A list of organizations impacted by ransomware incidents in 2022 and 2023 is provided by Din [4] including impacts, ransom details, and the ransomware involved if identified.

2.4 Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server by Kiesel et al. [7]

Kiesel et al. [7] investigate an attack against the Accellion File Transfer Appliance (FTA) server which is a widely used product that enables the quick and efficient transfer of large amounts of data among numerous computer systems. The threat actors stated they would distribute compromised data if a ransom payment was not received [7]. Defense strategies were created by Accellion and several clients to support compromised organizations. Kiesel et al. [7] determined that although the FTA was sunset, the organizations that were vastly impacted by ransomware would experience consequences possibly for years. Communications from Accellion to their customers regarding the availability of patches did not appear to be adequately conveyed leading to potentially hundreds of customers being affected with the impacts ongoing until mid-2021 [7].

2.5 The State of Ransomware in 2023 by Robb [12]

Robb [12] provides a list of ransomware incidents that have been released to the public. According to Robb [12], there were 33 ransomware incidents released to the public in January 2023 which is the largest number to be ever logged in the first month with the education industry being most impacted with 11 of the incidents. There were 40 ransomware incidents released to the public in February 2023 with the government segment being the most targeted [12]. A detailed list of ransomware incidents was provided by Robb [12] including impacted organizations, actual impacts, and a variety of detailed information about the ransomware, threat actor, and the ransom which will be investigated in greater detail in the following sections of this review study.

2.6 Royal ransomware claims attack on Queensland University of Technology by Toulas [13]

Toulas [13] describes ransomware as software that performs three tasks including compromising computer systems, incapacitating access to data and the file system, and mandating a ransom. Furthermore, Toulas [13] illustrates how trivial ransomware attacks can be enabled because of the affordability of the computer equipment and connectivity, the availability of digital currency, and due to the ease of universally initiating a ransomware attack against any individual or organization. Three reasons have been determined by Toulas [13] to facilitate successful ransomware attacks including phishing, poor cyber education, and weak baseline controls being implemented by targeted organizations. Three different impacts are recognized such as large ransom payments, operational impacts due to system availability, and reputational impacts to the organization’s brand. Toulas [13] lists several security controls that can mitigate the impacts of ransomware including end-point

detection and response (EDR), threat intelligence regarding ransomware attacks, secure management of credentials with privileged access, the implementation of multifactor authentication (MFA), a methodically applied backup strategy, and an up-to-date secure configuration of the information technology systems. Lastly, Toulas [13] provided a list of recent ransomware attack incidents from multiple industries that are explored further in the subsequent sections of this study.

2.7 Ransomware Detection and Classification Strategies by Vehabovic et al. [14]

Ransomware impacts users by utilizing encryption routines that transform data into an inaccessible state inflicting harm on individuals and organizations including governments and private firms [14]. Contemporary ransomware identification and categorization mechanisms as well as services and utilities to examine ransomware were studied by Vehabovic et al. [14] to strengthen network and system controls to mitigate the effects of ransomware. Two categories of ransomware detection schemes were described by [14] including network-based detection which examines traffic transmitted between systems for behaviors characterized by ransomware and host-based detection which detects ransomware by observing behaviors occurring locally on computer systems. Forensic analysis which concentrates on retrieving, collecting, and investigating data from systems infected with malware to uncover the properties of ransomware is also studied [14]. Another ransomware analysis technique reviewed by Vehabovic et al. [14] is malware authorship attribution which examines the primary aesthetic traits of ransomware code to discover its origins. There are two methods to perform authorship attribution including source code analysis and binary analysis [14]. Four tools used to identify ransomware are presented by Vehabovic et al. [14] as studied by

Table 1. Datasets in Literature Review

Literature/Study	Dataset Used	Purpose/Focus
The Evolution of Cryptocurrency and Cyber-attacks	Network Traffic Logs	Examining the relationship between the growth in ransomware attacks and the rise of cryptocurrency.
Analyzing the Ransomware Attack on D.C. Metropolitan Police Department	User-behavior Analytics	Analyzing a ransomware attack by the Babuk group on the D.C. Metropolitan Police Department, focusing on damages, attack methodology, and countermeasures.
Some Of The Companies Affected by Ransomware in 2021	Security Events and Alerts	Highlighting the increasing number of ransomware attacks, using security vulnerabilities as a primary attack vector, and listing impacted organizations.
Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server	Email and Web Traffic	Investigating a multi-vector ransomware attack on the Accellion File Transfer Appliance (FTA) server, discussing defense strategies, and consequences.
The State of Ransomware in 2023	Threat Intelligence feeds	Providing a list of publicly released ransomware incidents in 2023, including impacted industries, organizations, and detailed information about the attacks.
Royal ransomware claims attack on Queensland University of Technology	Security Information and Event Management data	Describing ransomware attacks and their impacts, outlining reasons for successful attacks, and suggesting security controls to mitigate ransomware impacts.
Ransomware Detection and Classification Strategies	Endpoint data	Studying contemporary ransomware detection and classification mechanisms, including network-based and host-based detection, forensic analysis, and malware authorship attribution.

other researchers including malware repositories in which ransomware datasets are collected, raw trace captures in which ransomware is analyzed in a sandbox with specialized tools, a preprocessing/feature extraction technique in which machine learning with massive data is used to train software to search and identify ransomware behaviors, and several open-source packages with machine learning capabilities.

Drawing upon the discussion in the existing literature, this scholarly review employed search tools such as Google Scholar, IEEE Xplore, MDPI, and the Grover Hermann Library at UC to identify relevant scholarly journal entries and articles. Supplementary to these academic sources, reputable independent news articles and blog posts were also consulted. The research process involved a meticulous evaluation of each identified source, with a focus on its relevance to the chosen topics encompassing ransomware, security incidents, and the timeliness of publication.

The table summarizing the publicly used datasets mentioned in the surveyed literature is listed Table 1.

3. METHODOLOGY

This section outlines the systematic methodology on the procedural and methodological context employed in conducting the study including a comprehensive analysis of the fundamental elements of a ransomware attack as well as the identification of key contributors to such attacks which served as a foundation of laying the groundwork for further research.

3.1 Analyzing the Roots of a Ransomware Attack

In most cases, the fundamental motivations and characteristics underlying ransomware attacks with a primary focus on the monetary drivers and instances where nation-states may diverge from financial motives. Ransomware can be highly compensated with substantial amounts of money and in many cases, this involves digital currencies with the additional benefit of anonymity.
Beyond motivations, the subsection acknowledges that various factors play a role in the successful initiation of a ransomware attack. These factors can include technological, socio-economic, and geopolitical elements that contribute to the evolving landscape of ransomware threats [15]. The complex interplay of these factors underscores the dynamic nature of ransomware attacks, necessitating a nuanced understanding to develop effective countermeasures.

3.1.1 Monetary incentives

In the majority of cases, ransomware attacks are motivated by financial gain. Cybercriminals deploy ransomware with the primary objective of extorting monetary compensation from their victims. The encrypted files and data are held hostage and the attackers demand a ransom often in the form of digital currencies. The use of digital currencies provides an additional layer of anonymity, making it challenging for authorities to trace the transactions back to the perpetrators [16].

3.1.2 Non-monetary motivation behind nation-states incidents

Contrastingly, there are instances where ransomware attacks conducted by nation-states are not solely driven by financial motives. In these cases, the motivation may be rooted in geopolitical or strategic objectives rather than seeking compensation [17]. Nation-state actors may deploy ransomware as a tool for espionage, disruption, or coercion, utilizing the chaos caused by the attack for political advantage.

3.1.3 Digital currencies and anonymity

The prevalent use of digital currencies in ransomware transactions such as Bitcoin are favored by cybercriminals due to their pseudo-anonymous nature. The use of digital currencies allows cybercriminals to receive substantial sums of money while maintaining a level of anonymity that complicates law enforcement efforts [18]. The complex interplay of these aspects underscores the dynamic nature of ransomware attacks necessitating a nuanced understanding to develop effective countermeasures.

3.2 Identifying the Contributors to a Ransomware Attack

The success of a ransomware attack is determined by a few different factors:

One primary factor would be the ease of conducting a ransomware attack. From the context of a financial perspective, the affordability

of a decent computer and reliable internet connectivity is widely achievable [6]. Also, digital currency can be received by everyone. Due to this inherent nature of ransomware, perpetrators can launch an attack from any geographic location against any victim without regard to physical or jurisdictional boundaries resulting in a persistent and ever-evolving global threat landscape.

A second factor would be inadequate cybersecurity education. The personnel of an organization may lack appropriate recognition of phishing attempts, risks involved with cybersecurity, and understanding of ransomware concepts.

A third factor is related to the lack of training which is the ability of cybercriminals to launch successful phishing campaigns. In this case, email filtering may be inoperable in addition to the previously discussed training deficiencies. When a successful phishing incident occurs, the ransomware will encrypt files and data while it spreads across an organization's network infecting servers and personnel computers at a rapid rate. Cybercriminals can also succeed with ransomware due to another reason which is an organization's inadequate implementation of cybersecurity best practices [8]. One such unhygienic security control that enables ransomware attacks to succeed is insufficient controls for password protection.

The fourth contributing factor related to the success of ransomware attacks is cybercriminals performing attacks from within locales offering shelter from the international legal system.

A fifth purported factor influencing ransomware attacks is payments via cryptocurrencies which are not regulated by governmental agencies.

A sixth critical factor that has an impact on the success of ransomware attacks is that some organizations agree to pay the ransom while also concealing the occurrence of the ransomware incident.

Another factor is the prosecution rate for cybercrime which is less than 1 percent of all transgressions making it a favorable risk-reward ratio for criminal activity.

The eighth factor contributing to the success of ransomware attacks is the emergence of ransomware-as-a-service (RaaS) capability. RaaS offers a turnkey operation to cybercriminals planning to install malicious software against vulnerable computer systems without requiring any technical expertise regarding the implementation of malicious software resulting in the seamless execution of a ransomware attack [7]. Furthermore, RaaS also allows for the ransom of encrypted data which is rendered inaccessible as a consequence of the attack. The prevalence of RaaS has contributed to an escalating trend of ransomware attacks emphasizing the imperative necessity for comprehensive and proactive cybersecurity measures to counteract its increasingly disruptive and detrimental effects [4].

The ninth and final factor driving the success of many ransomware attacks is large deficiencies in patching vendor-supplied software.

Ransomware attacks succeed due to a confluence of factors including the accessibility of conducting attacks globally supported by the affordability of basic computing resources and digital currency transactions; insufficient cybersecurity education within organizations leaving personnel vulnerable to phishing and other cyber threats; weaknesses in email filtering and inadequate training, enabling the rapid spread of ransomware within organizational networks; cybercriminals operating from jurisdictions with limited international legal oversight; unregulated cryptocurrency payments providing anonymity to attackers; the willingness of some organizations to pay ransoms discreetly; a low prosecution rate for cybercrime, creating a favorable risk-reward ratio for criminals; the emergence of ransomware-as-a-service (RaaS), simplifying attacks for individuals without technical expertise; and large deficiencies in patching vendor-supplied software, emphasizing the crucial need for proactive cybersecurity measures [19].

4. RESULTS

Since the beginning of 2023, many well-known businesses in several industry sectors such as government, healthcare, and education have been targeted with malware. There were a variety of attack vectors and exploits exercised to introduce the malware into the targeted organization and trigger the execution. A compilation of these attack vectors and exploits is included here to educate personnel and organizations to provide the background needed to deploy compensating controls in the environment so that the risk of exploitation can be diminished.

The cybercriminals that make use of ransomware generally make use of three different attack vectors. The first attack vector is a type of social engineering attack known as phishing in which an adversary delivers malicious emails intended to deceive targeted individuals into disclosing sensitive information including credentials, financial data, and other types of personally identifiable information (PII). The second main attack vector used during ransomware is known as a credential stuffing attack which takes advantage of the predisposition of people to reuse the same passwords in a variety of different applications including websites. This is further problematic because employees will repeatedly sign up for external services while making use of their business email address and even set up the same password for these external services that is used for their login credentials at work. If the external service is compromised, the login credentials could be used by adversaries deploying ransomware to acquire unauthorized access to the same account used by the employee or other legitimate websites. People reuse passwords due to ease of use as it is difficult to remember passwords of the many websites they interact with. The third attack vector commonly used for ransomware attacks involves exploiting well-known vulnerabilities. This attack vector makes use of software flaws to obtain a foothold in a network [20]. Usually, the associated vulnerabilities have had a patch released that the target organization has not applied. In some cases, this could be caused by poor patch management practices or the attackers could immediately start using the exploits as soon as they are made available which may not provide adequate time for the patch to be applied.

4.1 Recent Ransomware Attack Vectors and Exploits

The following list will focus on specific attacks that occurred in late 2022 and early 2023 including the targeted organization, threat actor, attack vector, and the business impact as a result of the ransomware attack:

Hospital Hack – LockBit Strikes SickKids: The first ransomware attack that will be discussed is the attack that occurred on January 1, 2023, against the Hospital for Sick Children (SickKids) in Toronto, Canada. The threat actor used the LockBit ransomware which is recognized to regularly attack VMware Elastic Sky X integrated (ESXi) to exploit well-known vulnerabilities. This attack vector has not been confirmed for the attack against the hospital for SickKids but the free decryption mechanism provided by LockBit was identified to be related to Linux/VMware ESXi [21]. Several different operational technologies were affected including internal hospital phone infrastructure, internet-facing website, as well as other internal systems. Note that patches for the vulnerabilities in VMware ESXi were offered by VMware in early 2021 [21].

Educational Disruption – Royal Ransom at Queensland University: Another ransomware attack that occurred on December 22nd, 2022, targeted Queensland University of Technology with a threat actor making use of the Royal ransomware [22]. The impact of the attack against the Queensland University of Technology included the shutdown of all IT systems shortly after the attack as well as the HiQ website, 'Digital Workplace', 'eStudent', and Blackboard system [22]. It was also necessary to reschedule a large number of examinations and courses to February. The university additionally inactivated its VPN access, network printing infrastructure, and network drives. In addition, the Royal ransomware group leaked a variety of data claiming (while not verified) email communications, files from the HR department, identification cards, and related information, as well as documentation associated with financial and administration activities [22]. The Royal ransomware group has been known to obtain an initial foothold into a targeted network through a variety of different techniques including harvesting credentials related to VPNs, sending phishing emails with malicious content, malicious advertising, accessing open remote desktop protocol ports with stolen passwords, and by exploitation of well-known vulnerabilities in internet-facing applications.

Royal Mail Paralyzed – LockBit's Shipping Standstill: On January 10, 2023, Royal Mail was subjected to a ransomware attack facilitated by LockBit ransomware. The impact was direct on shipping services as Royal Mail ceased international shipping which was not restored until six weeks later because of a critical interruption of service [12]. The ransomware incident resulted in printers printing ransom notes and devices related to international shipping being encrypted. Another impact of this ransomware attack was the publishing of stolen data from Royal Mail which did not contain financial data or sensitive customer information. Royal Mail states that

their research indicates most of the stolen data is comprised of administrative information and technical program files [12]. While the exact attack vectors for Royal Mail ransomware incident were not revealed, the ransomware deployed makes use of phishing, email compromise, exploitation of well-known vulnerabilities in internet-facing applications, brute force using passwords, and making use of credential stuffing to gain a foothold through entry points such as Remote Desk Protocol (RDP) attacks by retrieving access to sensitive and confidential information.

Public Transit Infiltrated – Vice Society Hits Bay Area Rapid Transit: A successful ransomware attack was performed against the Bay Area Rapid Transit in San Francisco. Most of the data leaked is associated with the agency's police department which included highly sensitive data containing employee information and police reports. The threat actor was a ransomware group called Vice Society [23]. The Bay Area Rapid Transit has not revealed the attack vector used to obtain the initial foothold into their network. Vice Society uses a variety of attack vectors to obtain initial access to a target organization's infrastructure [23]. These include the same techniques that were discussed above including phishing, exploitation of known vulnerabilities, and credential stuffing.

Financial Firm in Distress – ION's Derivative Platform Disrupted: On January 31, 2023, the financial firm known as ION was subjected to a ransomware attack using LockBit. The impact included service disruption to the Cleared Derivatives platform for at least 42 banks, hedge funds, and brokerages [13]. This outage required the impacted organizations to manually process derivative trades as well as track data in spreadsheets and also impacted these organizations' capabilities to retrieve quotes [13]. The ransomware group stated that the ransom was paid. While not clear, the ransomware group reported that data was stolen during the incident. It is unknown which attack vector was used in the ION ransomware incident but the common attack vectors for LockBit were previously described.

Satellite Service Sabotage – Dish Network's Black Basta Nightmare: One of the largest satellites pay-to-use service companies which also has a wireless phone business unit known as Dish Network was recently subjected to a ransomware attack on February 28, 2023, which resulted in outages of websites, customer service operations, and other applications for a few days [24]. Also, some internal servers and their information technology telephony systems experienced an outage. The company has stated that the data that has been exfiltrated could include PII information from customers. Some customers have been reporting complications in or with contacting the company's customer service and others have complained that their service has been disconnected after they had experienced difficulties with paying their bills [14]. Some reports claim that the Black Basta ransomware group was responsible for this attack. However, this has not been confirmed. It has also been reported that the attack vector was a vulnerability in Dish's windows
domain controllers.

Auto Dealer Debacle – Play's Double Extortion at Arnold Clark: Another recent high-profile ransomware attack occurred against a large United Kingdom car dealer named Arnold Clark on December 23, 2022. The ransomware used was the Play double extortion ransomware [11]. During this attack, the impact led to sales personnel making use of pen and paper to document sales as employees were locked out of their applications and computer systems. In addition, the dealer was unable to transfer cars to customers due to the system's unavailability [11]. The threat actor leaked 15 gigabytes (GBs) of customer data including customer names, dates of birth, vehicle information, driver's license and bank account details, insurance policies, mailing addresses, and passport information [11]. The attack vectors most often associated with Play ransomware is the use of credential stuffing or attacking and exploiting Fortinet SSL VPN vulnerabilities that have not been patched.

Electronic Manufacturing Espionage – Fujikura Global's LockBit Leak: In Japan, a major electronic manufacturing company named Fujikura Global was attacked with LockBit resulting in 718 GB worth of data containing confidential and critical information being leaked [2]. Financial records, certificates, employee PII, accounting, internal documentation, and report information were all included in the information exposed. Some of the report information included HR data, sales invoices, goals, cost reduction proposals, financial statements, emissions data, and supplier evaluation information [2]. This attack made use of LockBit

ransomware which has several attack vectors that were previously discussed.

Fast Food Fiasco – BlackCat Targets Five Guys: BlackCat ransomware was used in the recent attack against the Five Guys restaurant chain [5]. The threat actor claimed to exfiltrate payroll information, names, social security numbers (SSNs), driver's license numbers, financial data, recruitment information, and audit data. The data exfiltrated due to this incident would be useful for mule recruitment activities, identity theft, credit card theft, and phishing attacks. This attack took place on September 17, 2022.

The incident was centered around the company's employment process. Five Guys may be facing legal action as a law firm is requesting anyone receiving a notification of breach letter from Five Guys to contact the legal firm regarding potential legal action [5]. A variety of attack vectors have been seen with the BlackCat ransomware including vulnerabilities with Microsoft Exchange Server, credential stuffing, and compromise of remote desktop
applications.

Agricultural Attack – Dole Food Company's Production Shutdown: A large supplier of vegetables and fruit named Dole Food Company recently had to cease production in their facilities located in North America due to a ransomware attack that occurred on February 22, 2023 [25]. Not only was production halted but grocery store deliveries were also hampered. In addition, the threat actors procured data regarding employees. It was also noted by the company that they had executed their crisis management protocol to restart normal business operations while making use of their manual backup program which may result in slower production and deliveries [25]. The incident was noted to be especially impactful to the fresh vegetable operations in Chile. The type of ransomware used during this incident is currently unknown as Dole has not revealed this information as of the writing of this study.

The tabular data below summarizes the ransomware incidents including details such as the targeted organizations, threat actors involved, attack vectors employed, and the resulting business impacts. Each row in the table represents a specific incident providing a concise overview of the circumstances surrounding each cyber-attack. The incidents range across various domains including healthcare, education, logistics, public transportation, finance, satellite services, automotive, electronic manufacturing, and fast-food chains. The diverse attack vectors such as phishing, exploiting vulnerabilities, credential stuffing, and exploiting VPN credentials underscore the adaptability and sophistication of ransomware tactics. The business impacts vary widely from compromised internal systems and operational technologies to service disruptions, data leaks, and even

Table 2. Ransomware Incidents: A Comprehensive Overview of Targeted Organizations, Threat Actors, and Business Impacts

Incident	Targeted Organization	Threat Actor	Attack Vector	Business Impact
Hospital Hack – LockBit Strikes SickKids	Hospital for Sick Children	LockBit	Uncertain; potential use of VMware ESXi vulnerabilities	Affected operational technologies; internal systems compromised; patches for vulnerabilities available since early 2021
Educational Disruption – Royal Ransom at Queensland Univ.	Queensland University of Tech.	Royal ransomware	Multiple techniques including VPN credential harvesting, phishing, and exploiting vulnerabilities	Shutdown of IT systems, website, and various services; data leaked by the ransomware group
Royal Mail Paralyzed – LockBit's Shipping Standstill	Royal Mail	LockBit	Not specified	International shipping ceased for six weeks; ransom notes printed; data published, mostly administrative information

Incident	Targeted Organization	Threat Actor	Attack Vector	Business Impact
Public Transit Infiltrated – Vice Society Hits BART	Bay Area Rapid Transit (BART)	Vice Society	Techniques include phishing, exploitation of vulnerabilities, credential stuffing	Leaked sensitive data from the police department; attack vector not revealed
Financial Firm in Distress – ION's Derivative Platform	ION	LockBit	Not specified	Service disruption to Cleared Derivatives platform; manual processing of trades; ransom reportedly paid
Satellite Service Sabotage – Dish Network's Black Basta	Dish Network	Black Basta (unconfirmed)	Vulnerability in Dish's Windows domain controllers	Outages in websites, customer service, and applications; reported data exfiltration; impacts on customer service and billing
Auto Dealer Debacle – Play's Double Extortion at Arnold Clark	Arnold Clark	Play double extortion	Credential stuffing or exploiting Fortinet SSL VPN vulnerabilities	Sales personnel resorting to pen and paper; inability to transfer cars to customers; data leaked by the threat actor
Electronic Manufacturing Espionage – Fujikura Global	Fujikura Global	LockBit	Not specified	718 GB of leaked data, including financial records, certificates, employee PII, and internal documentation
Fast Food Fiasco – BlackCat Targets Five Guys	Five Guys	BlackCat	Vulnerabilities in Microsoft Exchange Server, credential stuffing, compromise of remote desktop applications	Exfiltration of sensitive data including payroll information, names, SSNs, financial data; potential legal action
Agricultural Attack – Dole Food Company's Shutdown	Dole Food Company	Not specified	Not specified	Production halted; grocery store deliveries hampered; employee data compromised; crisis management protocol initiated

international shipping standstills. This comprehensive summary serves as a reference to understand the breadth and depth of recent ransomware attacks across different industries highlighting the urgency for robust cybersecurity measures.

5. DISCUSSION

Many precautionary tactics and strategies can be implemented to identify and address ransomware attacks to defend a targeted organization. Some ransomware prevention techniques involve the deployment of security controls and process enhancements. One such control is endpoint detection and response which would protect end-user desktops and laptops [26]. The EDR solution provides the capability to discover and disrupt ransomware activities. Threat intelligence can also be implemented to provide alerts regarding the propagation of ransomware in peer organizations in the same industry. Another potential prevention method would be the secure management of privileged credentials [26]. This is important because many ransomware implementations target privileged credentials. By securely managing the credentials for privileged accounts, many ransomware attack incidents can be prevented. In addition to securely managing the passwords,

organizations should have policies requiring the implementation of strong passwords. One other prevention technique is the introduction of MFA as a security control to protect access for all personnel, especially to critical applications, file systems, and other data stores [26]. Backups with a meticulously planned approach can be considered a primary element of an organization's security strategy to manage ransomware attacks. To have a resilient backup strategy, an organization needs to ensure that its entire attack surface is secured including cloud environments as well as any contemporary storage devices. This strategy should guarantee that the storage is immutable and that backups are offline. Backups should be validated basis regularly to ensure that they are functioning properly and the recovery process is reliable.

As much malware is transmitted to an organization's ingress points (mainly email), it is important to deploy a capability to deconstruct, scan for malicious content including malware and ransomware, remove malicious instructions, and then rebuild the file before transmitting it further into the organization's network. This capability can be represented in multiple different ways making all of them equally valuable [1]. The first is network-based detection methods which scrutinize network traffic for suspicious actions that could indicate ransomware activity. Another would be a host-based detection mechanism that observes activities on a local computer system to identify ransomware activities such as operations on the file system and in memory, function calls from application programming interface (API), or dynamic link library (DLL) calls. Also, forensic analysis is another security control that concentrates on restoring, collecting, and evaluating data from computers infected with ransomware to understand its properties [6]. Lastly, another piece of mitigation strategy would include malware authorship origin identification which reviews aesthetic characteristics of ransomware computer code to determine the authors [7].

Another important consideration is to make sure that the configurations of all critical systems and infrastructure follow industry best practices and have defined guidelines for which the configuration of the critical systems is periodically audited against [8]. Also, a reliable incident response plan should be created and routinely validated to diminish the negative repercussions of ransomware attacks. This plan should include creating a strategy regarding whether to pay a ransom which is highly discouraged. As part of the overall ransomware prevention strategy, maintaining a strong patching cadence can act as a powerful tool to prevent ransomware attacks. It is important to have a frequent system patching or regular patch cycle for all operating systems, as external files can be introduced into the environment through many different paths such as browsers and email [9]. It is also important to have a regular update cycle for these types of software which should make sure that the security updates are performed on time. As has been emphasized, an organization's readiness to respond to a ransomware attack is critical. This readiness can be tested with regular ransomware tabletop exercises, execution of cyber crisis awareness exercises with senior leadership, and participation in cyber incident planning and response training sessions [7]. Training personnel regarding fundamental cybersecurity preparedness specifically including anti-phishing and social engineering training is also a key part of the overall organizational strategy of ransomware attack mitigation. Another important security control for a ransomware strategy is to perform regular penetration testing of systems and applications to identify vulnerabilities using ransomware-specific penetration testing tools.

A project initiative known as No More Ransom (NMR) was launched in collaboration with the Dutch National Police, Intel Security, Kaspersky Lab, and additional partners with the support of Europol in July 2016 [27]. This initiative provides free decryption tools and supplementary sources of information to ransomware victims to decrypt their files without having to pay a ransom to cybercriminals [28]. The NMR project website hosted at nomoreransom.org is currently sustained by 188 partners worldwide and provides over 100 decryptors that assist victims with 165 different types of ransomware variants to restore their encrypted data and recover their files [29,30]. The Crypto Sheriff tool is available on the NMR website and is intended to help victims of ransomware discover a free decryptor. Users are asked to upload two encrypted files along with additional information such as the email and website URL related to the ransom demand. This information is then validated against the list of available tools and if a match is found between the ransomware variant and the uploaded information, a decryptor for the encrypted files will be shared along with comprehensive instructions on how to unlock and

recover the information. The primary objective of the NMR project is to provide ransomware victims with the required tools and guidelines regarding the recovery procedures of their encrypted files, directions on how to report an incident using easy-to-follow links regardless of the circumstances surrounding the occurrence, and to raise public awareness on how ransomware attacks work and the preemptive measures that can be taken to prevent future attacks.

The following flowchart diagram illustrates a comprehensive framework for mitigating ransomware attacks through a strategic alignment of preventive, protective, and deterrent measures. The components are organized into three key categories: "Prevent" focusing on initiatives that directly impede ransomware incidents, "Protect" encompassing tools and strategies designed to safeguard against attacks and minimize potential damage, and "Deter" outlining measures that discourage and respond effectively to ransomware threats. The relationship between these categories forms a holistic approach addressing vulnerabilities across various layers of an organization's cybersecurity posture. This framework aims to provide a nuanced understanding of the multifaceted strategies required to effectively combat the evolving landscape of ransomware threats.

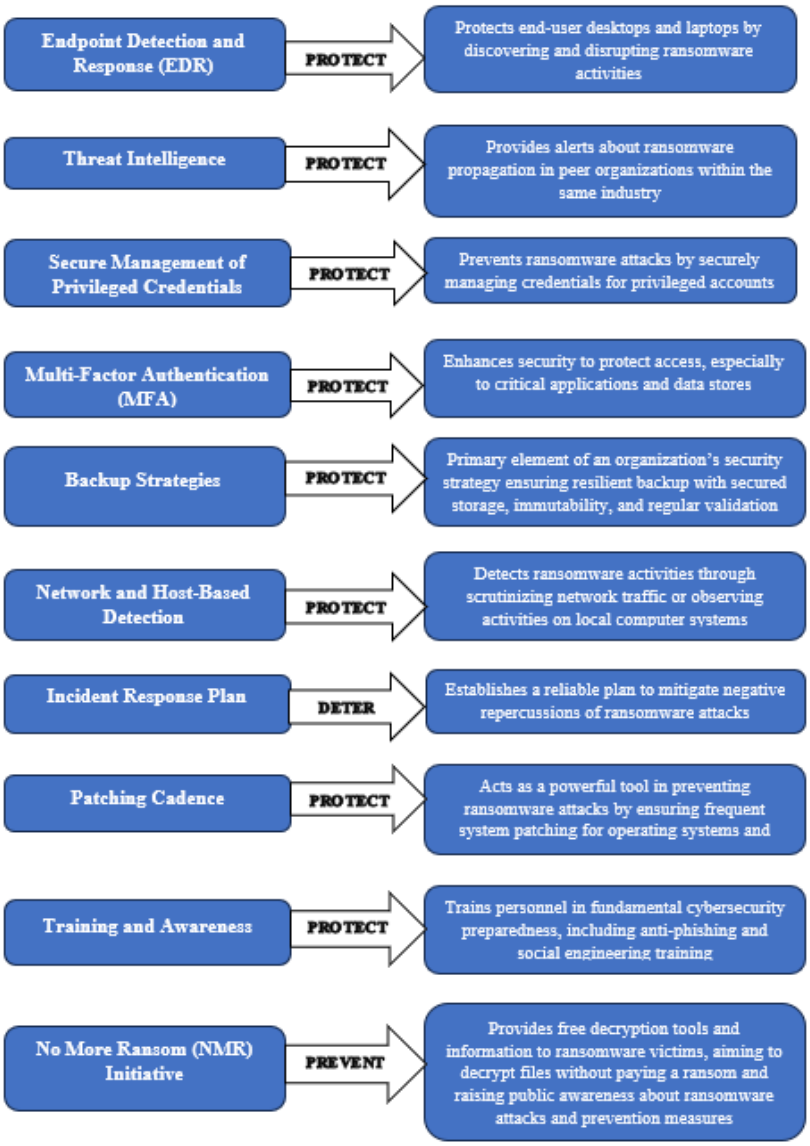

Fig. 1. Comprehensive Strategies for Ransomware Mitigation

6. CONCLUSIONS

The evolving landscape of ransomware attacks poses a formidable challenge to organizations and individuals with a growing number falling victim to these sophisticated incidents. The review has highlighted three predominant attack vectors including phishing, credential stuffing, and the exploitation of unpatched vulnerabilities underscoring the multifaceted nature of these threats. Organizations are impacted in several different ways including operational outages caused by system lockouts or encryption of information resulting in financial loss, sensitive data exfiltration which could include customer PII as well as financial information, exposure to legal risk, reputational impact with customers and suppliers as well as direct monetary loss if the ransom is paid. The consequences of ransomware attacks span operational outages, financial losses, data exfiltration, legal risks, and reputational damage. Security controls play a crucial role in either preventing or mitigating the impact of such attacks. There are several security controls that can help with either stopping ransomware attacks altogether or reducing the impact when a ransomware attack occurs. Key measures include user education on phishing, robust patching programs, effective password management policies, the implementation of multi-factor authentication (MFA), a mature privilege access management program, robust backup process, and the integration of Endpoint Detection and Response (EDR) solutions. Notably, the No More Ransom (NMR) project emerges as a recent control initiative led by Europol and various cybersecurity entities contributing to global efforts in ransomware prevention. However, the review also brings attention to existing challenges in the realm of review articles related to the subject emphasizing the need for improvement in terms of classifiers, utilized datasets, and features. While ransomware is an ever-expanding threat, organizations can mitigate and reduce the impact of ransomware incidents by investing adequate time and resources into planning for and implementing controls to manage the introduction of ransomware prior to an event occurring.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Chris Howser who played a crucial role throughout the research process. Chris generously shared his time and expertise by providing critical feedback on my research question and approach. His insightful feedback and suggestions challenged me to strengthen my arguments and delve deeper into the research. He inspired me to push myself to do my best work and I could not have completed this research without his unwavering support and guidance.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Kapko M. Ransomware attack exposes california transit giant's sensitive data. Cybersecurity Dive; 2023. Available:https://www.cybersecuritydive.com/news/ransomware-attack-exposes-california-transitgiants-sensitive-data/640121/ Accessed: 01-27-2024.
2. Abrams L. Royal mail cyberattack linked to lockbit ransomware operation. Bleeping computer; 2023. Available:https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-tolockbit-ransomware-operation/. Accessed: 01-27-2024.
3. Abrams L. Ransomware gang apologizes, gives SickKids hospital free decryptor. Bleeping Computer; 2023. Available:https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-givessickkids-hospital-free-decryptor/. Accessed: 01-27-2024.
4. Din A. Some of the companies affected by ransomware in 2021. Heimdal security Blog; 2021. Available:https://heimdalsecurity.com/blog/companies-affected-byransomware. Accessed: 01-27-2024.
5. Limited CMA. Ransomware resources - How to prevent ransomware. Cyber management Alliance; 2023. Available:https://www.cm-alliance.com/ransomware. Accessed: 01-27-2024.
6. Caroscio E, Paul J, Murray J, Bhunia S. Analyzing the ransomware attack on D.C.

metropolitan police department by babuk. In: 2022 IEEE International Systems Conference (SysCon), Montreal, Canada, April. 2022;1-8.
DOI: 10.1109/SysCon53536.2022.9773935

7. Kiesel K, Deep T, Flaherty A and Bhunia S. Analyzing multi-vector ransomware attack on Accellion File Transfer Appliance Server. In: 2022 7th International conference on smart and sustainable technologies (SpliTech). Split / Bol, Croatia. 2022;1-6.
DOI: 10.23919/SpliTech55088.2022.9854275
8. Lapienyte J. Five guys allegedly hit by ransomware. Cybernews; 2023.
Available:https://cybernews.com/news/five-guys-ransomware/, Accessed: 01-27-2024.
9. Marcelline M. Dish network hit with multi-day outage, Suspected ransomware attack. PCMag; 2023.
Available:https://me.pcmag.com/en/tvs/15036/dish-network-hitwith-multi-day-outage-suspected-ransomware-attack/. Accessed: 01-27-2024.
10. Zubair B, Mekala SH, and Zeadally S. Ransomware attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. IEEE Xplore. 2023;25(5):37-44.
11. Berry HS. The evolution of cryptocurrency and cyber-attacks. In: 2022 international conference on computer and applications (ICCA), Cairo, Egypt. 2022;1-7.
DOI: 10.1109/ICCA56443.2022.10039632
12. Robb B. The state of ransomware in 2023. BlackFog; 2023.
Available:https://www.blackfog.com/the-state-of-ransomware-in-2023/. Accessed: 01-27-2024.
13. Toulas B. Royal ransomware claims attack on Queensland University of Technology. BleepingComputer; 2023.
Available:https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-onqueensland-university-of-technology/. Accessed: 01-27-2024.
14. Vehabovic A, Ghani N, Bou-Harb E, Crichigno J, Yayimli A. Ransomware detection and classification strategies. In: 2022 IEEE International Black Sea Conference on communications and networking (BlackSeaCom); 2022.
DOI: 10.1109/blackseacom54372.2022.9858296
15. Yahye AA, Huda S, Bander AS Al-rimy, Alharbi N, Saeed F, Ghaleb FA, and Ali, IM. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. Sustainability. 2022;14(3):1231.
16. Zahoora U, Rajarajan M, Pan Z, Khan A. Zero-day ransomware attack detection using deep contractive autoencoder and voting based ensemble classifier. Applied Intelligence. 2022;52(12):13941-13960.
17. Zandile M, Botha RA. Preventing and mitigating ransomware: A systematic literature review. In information security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17 (pp. 149-162). Springer International Publishing; 2019.
18. Zesheng C, Ji C. An information-theoretic view of network-aware malware attacks. IEEE Transactions on Information Forensics and Security. 2009;4(3):530-541.
19. Zheyu S, Tian Y, Zhang J. Similarity analysis of ransomware attacks based on ATT&CK Matrix. IEEE Access; 2023.
20. NMR. Hit by ransomware? No more ransom now offers 136 free tools to rescue your files. Europol; 2022.
Available:https://www.europol.europa.eu/mediapress/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-torescue-your-files/.
Accessed: 01-27-2024.
21. Zimba A, Wang Z, Chen H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express. 2018;4(1): 14-18.
22. Kay B. Service now brand voice: The destructive rise of ransomware-As-AService. Forbes; 2021.
Available:https://www.forbes.com/sites/servicenow/2021/06/09/thedestructive-rise-of-ransomware-as-a-service/?sh=7c1eb6661e16/. Accessed: 01-27-2024.
23. Satter R. Hackers who breached ION say ransom paid; company declines comment. Reuters; 2023.
Available:https://www.reuters.com/technology/hackers-sayransom-paid-case-derivatives-data-firm-ion-company-declines-comment-2023-02-03/. Accessed: 01-27-2024.

24. Scroxton A. Arnold clark cyber-attack claimed by play ransomware gang. ComputerWeekly; 2023.
Available:https://www.computerweekly.com/news/252529566/Arnold-Clark-cyber-attack-claimedby-Play-ransomware-gang/. Accessed: 01-27-2024.

25. Kaspersky. No more ransom helped more than 1.5 million people decrypt their devices. Corporate News; 2022.
Available:https://www.kaspersky.com/about/pressreleases/2022_no-more-ransom-helped-more-than-15-million-people-decrypt-theirdevices/. Accessed: 01-27-2024.

26. Khaitan A. Fujikura global: LockBit ransomware group's latest victim. The Cyber Express; 2023.
Available:https://thecyberexpress.com/lockbit-fujikura-global-cyberattack-ransom/. Accessed: 01-27-2024.

27. Toulas B. Fruit giant dole suffers ransomware attack impacting operations. BleepingComputer; 2023.
Available:https://www.bleepingcomputer.com/news/security/fruit-giant-dole-suffers-ransomwareattack-impacting-operations/. Accessed: 01-27-2024.

28. Staff SC. Dish network ransomware attack information remains sparse. SC Media; 2023.
Available:https://www.scmagazine.com/brief/ransomware/dish-network-ransomwareattack-information-remains-sparse/. Accessed: 01-27-2024.

29. NMR. The no more ransom project. Nomoreransom.org; 2019.
Available:https://www.nomoreransom.org/en/index.html. Accessed: 01-27-2024.

30. Zhang X, Wang J, Zhu S. Dual generative adversarial networks based unknown encryption ransomware attack detection. IEEE Access. 2021;10: 900-913.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/112469