Review Article

The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified

Abstract

The Ransomware epidemic continues to be a grave threat to businesses of any magnitude. Cybercriminals target and attack organizations causing widespread damage while demanding substantial compensation. The impacts of ransomware attacks can be catastrophic including temporary or permanent loss of information, monetary damages, and reputational harm. This research performs a holistic assessment of recent ransomware attacks including the targeted organization, the attack vectors, threat actors, propagation mechanisms, tools and techniques used by the attackers, and the business impact resulting from the attacks. The in-depth examination also studies the evolving nature of ransomware attacks through its different types, attack vectors, exploits, and contributors to ransomware attacks such as the use of double extortion by cybercriminals to not only encrypt but also exfiltrate data and threaten to release the encrypted data publicly unless the ransom is paid. The research explores recent high-profile ransomware incidents, such as SickKids Hospital, Royal Mail, Dish Network, Five Guys, and ION. The effectiveness of current ransomware defenses is also investigated along with potential strategies that organizations can utilize to counteract, identify, and manage ransomware attacks. The findings of this analysis provide meaningful insights into the ransomware epidemic, its implications on organizations, and the defensive measures that can be taken to mitigate the risks of ransomware attacks. As ransomware continues to evolve and become more complex, it is critical for organizations to understand the threat landscape and implement robust cybersecurity measures to

protect customers as well as organizational users both internally and externally from this growing threat.

Keywords: Ransomware, cybercriminals, double extortion, ransomware incidents, ransomware defenses

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 [6]. 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 [1]. 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 [5]. However, the newer variants have the ability to 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 [12]. 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 in order 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 [4]. 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 [10]. 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 [11]. 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 [13]. Additional operators provide auxiliary functions such as ransomware binary delivery and victim identification.

1.2 Anatomy of a Ransomware Attack

There are six stages that are involved in a ransomware attack which include reconnaissance, distribution/delivery, installation/infection, communication, encryption, and extortion/payment [4]. 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 [4]. 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 [4]. 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 & 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. 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 [4]. 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: Ransomware Detection and Classification Strategies by Vehabovic et al. [4], The Evolution of Cryptocurrency and Cyber-attacks by Berry [11], Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk by Caroscio et al. [10], Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server by Kiesel et al. [13], Royal ransomware claims attack on Queensland University of Technology by Toulas [9], The State of Ransomware in 2023 by Robb [6], Some Of The Companies Affected by Ransomware in 2021 by Din [1].

Ransomware Detection and Classification Strategies by Vehabovic et al. [4]

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 [4]. Contemporary ransomware identification and categorization mechanisms as well as services and

utilities to examine ransomware were studied by Vehabovic et al. [4] in order to strengthen network and system controls to mitigate the effects of ransomware. Two categories of ransomware detection schemes were described by [4] 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 in order to uncover the properties of ransomware is also studied by [4]. Another ransomware analysis technique reviewed by Vehabovic et al. [4] is malware authorship attribution which examines the primary aesthetic traits of ransomware code in order to discover its origins. There are two methods to perform authorship attribution including source code analysis and binary analysis [4]. Four tools used to identify ransomware are presented by Vehabovic et al. [4] as studied by 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 in order to search and identify ransomware behaviors, and several open-source packages with machine learning capabilities.

The Evolution of Cryptocurrency and Cyber-attacks by Berry [11]

Berry [11] examines the relationship between the growth in ransomware attacks and the rise of cryptocurrency. Ransomware can be classified into two types including encryptors ransomware and screen-locker ransomware [11]. Screen-locker ransomware is described as ransomware that locks the user interface while mandating a request for ransom while 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 in order 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.

Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk by Caroscio et al. [10]

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 [10]. A deep examination of a fresh ransomware attack by a ransomware group named Babuk on a police branch was studied by Caroscio et al. [10] 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. [10] who argues that malicious software such as ransomware enables cybercriminals to easily attack a variety of organizations with the end goal of receiving pay of ransom with techniques that negatively influence sensitive data from a notion of confidentiality, integrity, and availability. Caroscio et al. [10] contends 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. [10] presents 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.

Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server by

Kiesel et al. [13]

Kiesel et al. [13] investigates 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 [13]. Defense strategies were created by Accellion and several clients to support compromised organizations. Kiesel et al. [13] determined that although the FTA was being 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 [13].

Royal ransomware claims attack on Queensland University of Technology by Toulas [9] Toulas [9] 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 [9] 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 [9] 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 [9] 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 [9] provided a list of recent ransomware attack incidents from multiple industries that are explored further in the subsequent sections of this research paper.

The State of Ransomware in 2023 by Robb [6]

Robb [6] provides a list of ransomware incidents that have been released to the public. According to Robb [6], 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 [6]. A detailed list of ransomware incidents was provided by Robb [6] 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.

Some of The Companies Affected by Ransomware in 2021 by Din [1]

Din [1] 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 [1] as she states that more than 200,000 new variants of ransomware are identified everyday 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 are provided by Din [1] including impacts, ransom details, and the ransomware involved if identified.

3. Methodology

This section expands on the procedural and methodological context employed in conducting the study including a detailed 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 for further research.

3.1 Analyzing the Roots of a Ransomware Attack

In most cases, ransomware attacks are driven by monetary reasons. However, there are certain incidents involving nation states in which compensation is not the driving force of the attack. Ransomware can be highly compensated with substantial amounts of money and in many cases, this involves digital currencies with the additional benefit of anonymity. There are several factors that can influence the successful instigation of a ransomware attack.

3.2 Identifying the Contributors to a Ransomware Attack

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

1. 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 [4]. Also, digital currency can be received by everyone. Due to this inherent nature of ransomware, perpetrators can launch the 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.
2. 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.

3. 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 [11]. One such unhygienic security control that enables ransomware attacks to succeed is insufficient controls for password protection.
4. 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.
5. A fifth purported factor influencing ransomware attacks is payments via cryptocurrencies which are not regulated by governmental agencies.
6. 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.
7. 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.
8. 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 [10]. 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 [5].

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

4. Results

Since the beginning of 2023, many well-known businesses in several industry sectors such as government, healthcare, and education were targeted with malware. There were a variety of attack vectors and exploits exercised in order to introduce the malware into the targeted organization and trigger the execution. A compilation of these attack vectors and exploits are included here to educate personnel and organizations in order 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 in order 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 the ransomware attacks involves exploiting well-known vulnerabilities. This attack vector makes use of software flaws in order to obtain a foothold into a network. 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:

1. 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) in order 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 [15]. 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 [15].
2. Another ransomware attack that occurred on December 22nd, 2022, targeted Queensland

University of Technology with a threat actor making use of the Royal ransomware [8]. The impact to 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 [8]. It was also necessary to reschedule a large number of examinations and courses to February. The university additionally inactivated their 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 [8]. The Royal ransomware group have 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.

3. On January 10, 2023, Royal Mail was subjected to a ransomware attack facilitated by LockBit ransomware. The impact was directly to shipping services as Royal Mail ceased international shipping which was not restored until six weeks later because of a critical interruption of service [16]. 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 [16]. 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.

4. 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 [17]. 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 [17]. These include the same techniques that were discussed above including phishing, exploitation of known vulnerabilities, and credential stuffing.
5. 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 [21]. This outage required the impacted organizations to manually process derivative trades as well as track data in spreadsheets and also impacted these organization's capabilities to retrieve quotes [21]. 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.
6. One of the largest satellite 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 [18]. 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 [22]. Some reports are claiming that the Black Basta ransomware group has responsibility for this attack. However, this has not been confirmed. It has also been reported that the attack vector was through a vulnerability in Dish's windows domain controllers.

7. 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 [3]. 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 unavailability [3]. 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 [3]. 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.
8. 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.

9. BlackCat ransomware was used in the recent attack against the Five Guys restaurant chain [12]. 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 [12]. 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.
10. 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 [7]. Not only was production halted but also 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 [7]. The incident was noted to be especially impactful to the fresh vegetables' 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 paper.

5. Discussion

Many precautionary tactics and strategies can be implemented to identify and address ransomware attacks in order 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 [9]. The EDR solution provides a capability to discover and disrupt ransomware activities. Threat intelligence can also be implemented in order 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 [9]. 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 [9]. Backups with a meticulously planned approach can be considered a primary element of an organization's security strategy to manage ransomware attacks. In order to have a resilient backup strategy, an organization needs to ensure that their 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 on a regular basis 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 prior to transmitting it further

into the organization's network. This capability can be represented in multiple different ways making all of them equally valuable [6]. The first is network-based detection methods which scrutinize network traffic for suspicious actions that could indicate ransomware activity. Another would be host-based detection mechanism which 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 [4]. Lastly, another piece of mitigation strategy would include malware authorship origin identification which reviews aesthetic characteristics of ransomware computer code to determine the authors [10].

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 are periodically audited against [11]. Also, a reliable incident response plan should be created and routinely validated in order 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 [13]. 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 in a timely manner. 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 [10]. 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 attacks mitigation. Another important security control for a ransomware strategy is to perform regular penetration testing of systems and applications in order 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 [20]. This initiative provides free decryption tools and supplementary sources of information to ransomware victims in order to decrypt their files without having to pay a ransom to cybercriminals [19]. 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 [14]. The Crypto Sheriff tool available on the NMR website is intended to help victims of ransomware in discovering 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.

6. Conclusions

Ransomware attacks are continuing to evolve to become more advanced and pervasive with an ever-increasing number of organizations and individuals being impacted by these incidents. These attacks have three common attack vectors including phishing, credential stuffing using previously compromised credentials, and exploitation of well-known vulnerabilities that have remained unpatched. 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. There are several security controls that can help with either stopping ransomware attacks altogether or reducing the impact when a ransomware attack occurs. The primary security control would be education of users regarding phishing attacks. Other security controls would be a robust patching program, password management policy and education to drive better password hygiene within an organization to ensure passwords are changed on a regular basis and encourage employees to not reuse passwords, the implementation of multi-factor authentication, robust backup process, implementation of a mature privilege access management program, and an EDR solution for end-point computing devices. Another recent control that could assist with managing a ransomware incident is called the No More Ransom (NMR) project which is a global program led by Europol, several governmental bureaus and private cybersecurity organizations to prevent ransomware. 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.

7. List of Abbreviations

Table 1 : below provides an explanation for the abbreviations and acronyms used in the paper.

Acronym/Abbreviation	Meaning
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

References

[1] Din A (2021) Some Of The Companies Affected by Ransomware in 2021. Heimdal Security Blog. Available via https://heimdalsecurity.com/blog/companies-affected-byransomware. Accessed: 04-02-2023.

[2] Khaitan A (2023) Fujikura Global: LockBit Ransomware Group's Latest Victim. The Cyber Express. Available via https://thecyberexpress.com/lockbit-fujikura-global-cyberattack-ransom/. Accessed: 04-02-2023.

[3] Scroxton A (2023) Arnold Clark cyber attack claimed by Play ransomware gang. ComputerWeekly. Available via https://www.computerweekly.com/news/252529566/Arnold-Clark-cyber-attack-claimedby-Play-ransomware-gang/. Accessed: 04-02-2023.

[4] Vehabovic A, Ghani N, Bou-Harb E , J Crichigno, and Yayimli A (2022) Ransomware Detection and Classification Strategies. In: 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). doi: 10.1109/blackseacom54372.2022.9858296.

[5] Kay B (2021) ServiceNow BrandVoice: The Destructive Rise Of Ransomware-As-AService. Forbes. Available via https://www.forbes.com/sites/servicenow/2021/06/09/thedestructive-rise-of-ransomware-as-a-service/?sh=7c1eb6661e16/. Accessed: 04-02-2023.

[6] Robb B (2023) The State of Ransomware in 2023. BlackFog. Available via https://www.blackfog.com/the-state-of-ransomware-in-2023/. Accessed: 04-02-2023.

[7] Toulas B (2023) Fruit giant Dole suffers ransomware attack impacting operations. BleepingComputer. Available via https://www.bleepingcomputer.com/news/security/fruit-giant-dole-suffers-ransomwareattack-impacting-operations/. Accessed: 04-02-2023.

[8] Limited CMA (2023) Ransomware Resources - How to prevent Ransomware. Cyber management Alliance. Available via https://www.cm-alliance.com/ransomware. Accessed: 04-02-2023.

[9] Toulas B (2023) Royal ransomware claims attack on Queensland University of

Technology. BleepingComputer. Available via https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-onqueensland-university-of-technology/. Accessed: 04-02-2023.

[10] Caroscio E, Paul J, Murray J, Bhunia S (2022). Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk. In: 2022 IEEE International Systems Conference (SysCon), Montreal, Canada, April 2022, pp. 1-8, doi: 10.1109/SysCon53536.2022.9773935.

[11] Berry HS (2022), The Evolution of Cryptocurrency and Cyber-attacks. In: 2022 International Conference on Computer and Applications (ICCA), Cairo, Egypt, December 2022, pp. 1-7, doi: 10.1109/ICCA56443.2022.10039632.

[12] Lapienyte J (2023) Five Guys allegedly hit by ransomware. Cybernews. Available via https://cybernews.com/news/five-guys-ransomware/, Accessed: 04-02-2023.

[13] Kiesel K, Deep T, Flaherty A and Bhunia S (2022) 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, July 2022, pp. 1-6, doi: 10.23919/SpliTech55088.2022.9854275.

[14] Kaspersky (2022) No More Ransom helped more than 1.5 million people decrypt their devices. Corporate News, Available via https://www.kaspersky.com/about/pressreleases/2022_no-more-ransom-helped-more-than-15-million-people-decrypt-theirdevices/. Accessed: 04-02-2023.

[15] Abrams L (2023) Ransomware gang apologizes, gives SickKids hospital free decryptor. BleepingComputer. Available via

https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-givessickkids-hospital-free-decryptor/. Accessed: 04-02-2023.

[16] Abrams L (2023) Royal Mail cyberattack linked to LockBit ransomware operation. BleepingComputer. Available via https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-tolockbit-ransomware-operation/. Accessed: 04-02-2023.

[17] Kapko M (2023) Ransomware attack exposes California transit giant's sensitive data. Cybersecurity Dive. Available via https://www.cybersecuritydive.com/news/ransomware-attack-exposes-california-transitgiants-sensitive-data/640121/. Accessed: 04-02-2023.

[18] Marcelline M (2023) Dish Network Hit With Multi-Day Outage, Suspected Ransomware Attack. PCMag. Available via https://me.pcmag.com/en/tvs/15036/dish-network-hitwith-multi-day-outage-suspected-ransomware-attack/. Accessed: 04-02-2023.

[19] NMR (2022) Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files. Europol. Available via https://www.europol.europa.eu/mediapress/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-torescue-your-files/. Accessed: 04-02-2023.

[20] NMR (2019) The No More Ransom Project. Nomoreransom.org. Available via https://www.nomoreransom.org/en/index.html. Accessed: 04-02-2023.

[21] Satter R (2023) Hackers who breached ION say ransom paid; company declines comment. Reuters, Available via https://www.reuters.com/technology/hackers-sayransom-paid-case-derivatives-data-firm-ion-company-declines-comment-2023-02-03/. Accessed: 04-02-2023.

[22] Staff SC (2023) Dish Network ransomware attack information remains sparse. SC Media. Available via https://www.scmagazine.com/brief/ransomware/dish-network-ransomwareattack-information-remains-sparse/. Accessed: 04-02-2023.