Sri Lanka Institute of Information Technology

Module: IE2022

Introduction to Cyber Security

Year 2, Semester 1

Aazaf Ritha. J – IT23151710

B.Sc. (Hons) in Information Technology

Specialized in Cyber Security

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

Ransomware attacks, their Evolution, and Mitigation strategies

Contents

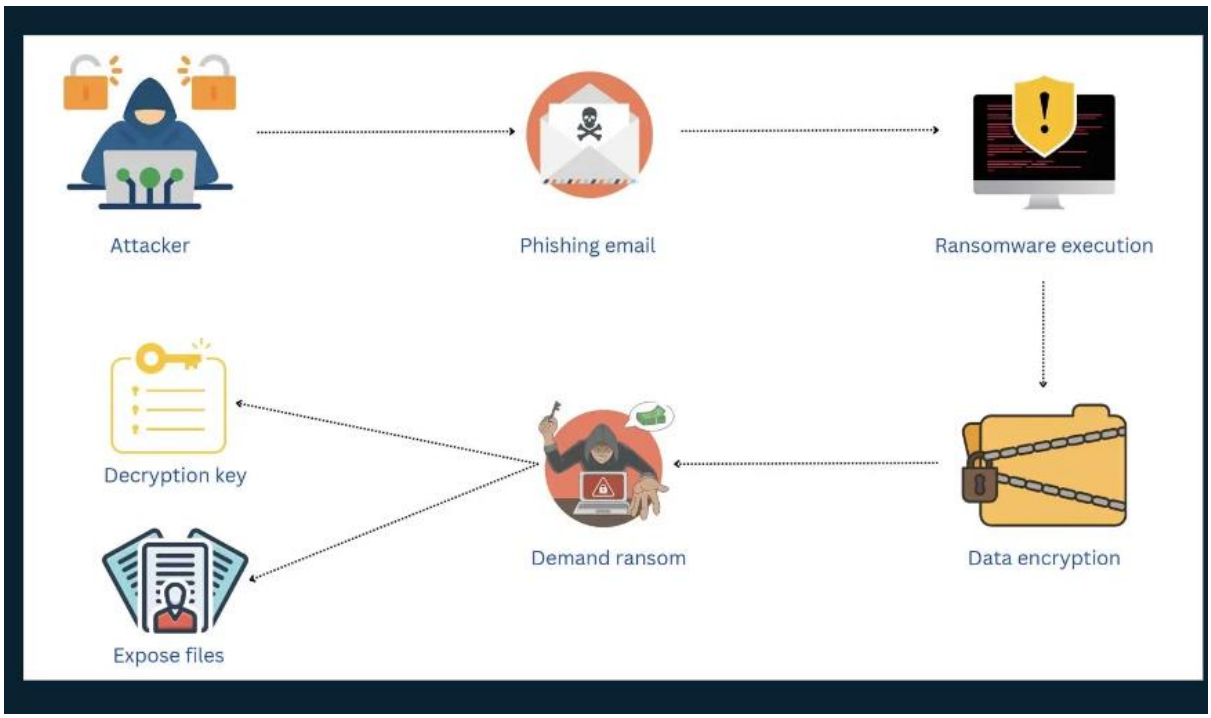
1. Abstract

Ransomware is a subtype of cybercrime and has become one of the most dangerous types of threats for individuals, companies, governments, and essential facilities globally. In this paper we discuss how ransomware started with AIDS Trojan in 1989 and has evolved over the years to Crypto Ransomware, Locker Ransomware and Ransomware-as-a-Service (RaaS). The history of ransomware lays out that ransomware becomes more complex in terms of encryption, delivery, and payment system like cryptocurrency that makes ransomware even more dangerous and challenging to contain. The report also looks at the direction that ransomware is taking in the future in terms of developments such as the polymorphic ransomware and the AI ransomware. Furthermore, it outlines key mitigation strategies, including prevention techniques like software updates and employee training, detection mechanisms such as Endpoint Detection and Response (EDR), and network monitoring. Last but not the least, it addresses response strategies, for example, the formulation of incident response procedures and the need to strengthen private and public partnership along with threats posed by ransomware. The study concludes that there is a need to keep developing new and better cybersecurity measures especially given the ever-changing security threats.

2. Introduction

The world is at the cutting edge of technology. The technology industry has many advantages, but they have a main dark side. That is called “Cybercrime”. Here is an important cybercrime Ransomware. Ransomware is a type of malicious software (malware), it’s blocks or locks that access a victim’s files, systems, or networks by encrypting data. The attackers demand a ransom payment to release the data and unlock or release the victim’s items making them inaccessible without a decryption key provided by the attacker after payment.

Ransomware mostly spreads through the use of phishing emails, infected attachments, as well as through infected websites. The main payment is made by cryptocurrencies like bitcoin-in exchange. This type of attack can target individuals, businesses, governments, and organizations, causing both financial and reputational damage.



There are many types of ransomwares, each have unique characteristics and way of compromising the systems. The most common types of ransomwares are:

1. **Crypto Ransomware or Encryptors**

This type locks or encrypt a computer’s files and data and demands a ransom be paid to receive the code for unlocking the system. Such are WannaCry and Crypto Locker [1].

2. **Lockers**

Locker lock the system so the user cannot open any file or application on the computer at all. An intermediary, called a ransom note or screen, is displayed to the victim because of the encrypted data. [1]

3. Scareware

Scareware imitates system alerts, in one way or another telling the user that the system is already infected or changed and that it is necessary to pay to correct it. Thus, although many scareware programs 'freezes' the monitor, it does not really harm anything. [1]

4. Doxware or Leakware

This ransomware demands the money be paid with the data being released or remaining private. At times it assumes the identity of a law enforcement agency, informing the user that he or she has engaged in unlawful acts. [1]

5. Ransomware as a service (RaaS)

This is a model in which the hackers offer ransomware kits for sale or for rent to other attackers, who take care of the technicalities in the process in exchange for a percentage of the ransom. [1]

The objective of this report is to define the evolution of ransomware, study some of the most known attacks, understand the countermeasures used to mitigate them and explore potential future development on it.

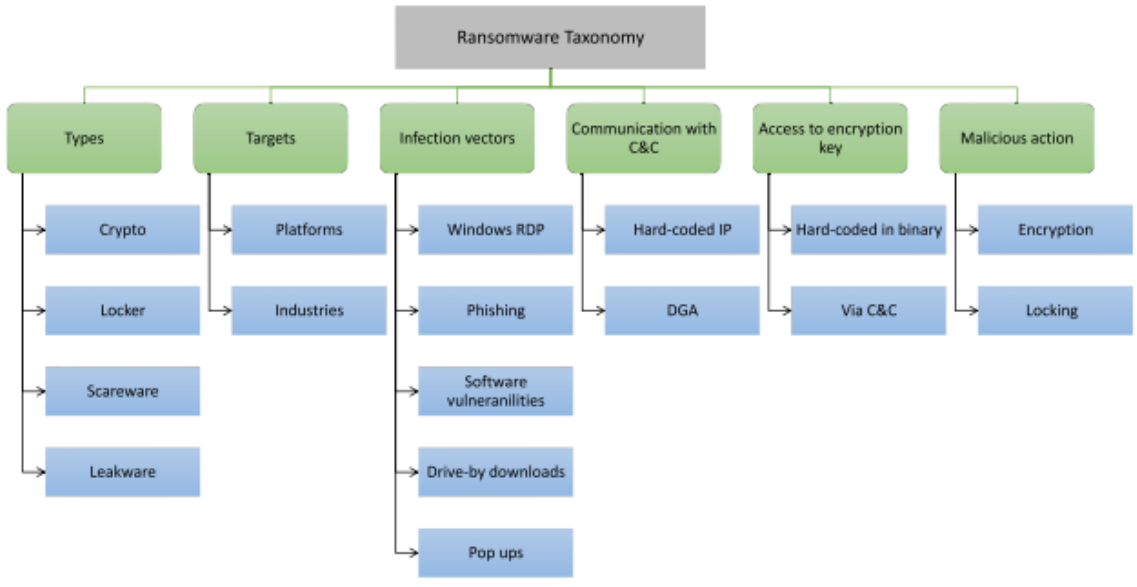


Figure 1. Taxonomy of Ransomware

3. Evolution of Ransomware

3.1. History of Ransomware

Ransomware is not the new cybercrime that developed and changed a lot over the years. Initially, it was a basic threat that implied personal attacks, but it evolved into a highly dangerous threat to businesses, governments, and critical infrastructure. According to history and key events, the first ransomware was reported to arrive in the late 1989s.

3.2. Early Ransomware (1989 – 2005)

The first recorded ransomware with the name AIDS Trojan had come into existence in 1989 and was also famous as a PC cyborg virus. Joseph L. Popp (The father of ransomware) had created this virus and had distributed it on a floppy disk to attendees of an AIDS research conference, and it encrypted filenames on infected systems, and demanded a ransom of $189 to be sent to the P.O. box in Panama through mail. [2] [3]

The AIDS Trojan used the symmetric encryption (use a key for encryption and decryption), it set the precedent for future ransomware attacks.

However, the attack was not widespread because there was poor internet infrastructure and the low use of digital payment methods at the time. Moreover, early ransomware efforts lacked sophistication in both distribution and encryption, reducing their overall impact.

The period between 1990 and 2005 had a relatively low number of ransomware attacks. The primary reasons for this were:

1. Lack of Anonymous Payment Methods
2. Limited Internet Use [4]

Although the AIDS Trojan was not very successful, it set the foundation for future ransomware attacks.

3.3. Rise of Crypto Ransomware (2005 – 2015)

The new significant evolution phase of ransomware is discussed to have started about 2005 when new advanced encryption techniques were introduced. Crypto ransomware was become from these techniques. In this phase, the attackers were not only using simple encryption format but shifted to asymmetrical encryption (use two keys (public key and private key) for encryption and decryption) such as **RSA** and **AES** encryption algorithms. Some of these algorithms were so designed that victims couldn't access their files unless they agreed to pay the demanded ransom.

Key developments at this stage:

1. **GPCode and Archievus (2004 -2006)**
   These attacks were different from today's ransomware, as the attackers requested a low ransom because they preferred targeting a high volume of victims, rather than targeting a smaller number of high value victims. GPCode, which surfaced in 2004, used two

infection vectors to attack victims, namely phishing emails and malicious website links. By 2006, Archievus marked a shift in the evolution of ransomware as it was the first strain to use Rivest-Shamir-Adleman (RSA) encryption. [5]

2. **WinLock (2006)**

   In 2006, the WinLock introduced a new type of method, that called locker ransomware, utilizing a new method that didn't encrypt files but rather locked the user's screen, displaying pornographic content. Victims were compelled to send a $10 premium-rate SMS to receive an unlock code. This malware spread through a deceptive mechanism that mimicked the Windows Product Activation notice, tricking victims into making costly international calls. By 2010, authorities in Moscow had arrested ten individuals responsible for the scheme, which had grossed over $16 million, mainly affecting users in Russia and Eastern Europe.

3. **CryptoLocker (2013)**

   In 2013, the most malicious malware threat called CryptoLocker emerged. By December of 2013, this potent form of ransomware had impacted roughly 250,000 Windows-based computers. It was also during this time that security researchers learned that cybercriminals were not only targeting professionals but also home-based internet users. The primary source of infection during this year seemed to be phishing emails that contain malicious attachments. [5] it's used RSA-2048 encryption algorithm to lock files. The victims were forced to pay in bitcoin, a clear indication that ransomware attacks would increasingly use cryptocurrencies for payment. It's become a major milestone in the evaluation of ransomware.

3.4. Introduction of Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service or RaaS is a form of business through which expert hackers or cybercriminals develop ransomware and then sell it to others, who then use it for criminal activities. Think of ransomware as a service as a variation of software as a service (SaaS) business model [6]. This model makes ransomware easily available and does not require the attacker to have a high level of computer expertise to launch a complex attack.

Ransomware was more accessible after 2015, and it is hitting larger organizations. Cyber criminals observed that targeting health care centers, government units, and schools were easier, and these organizations are likely to pay ransoms to avoid operational disruptions. The RaaS platforms are most often located on the dark web since here the attackers can purchase the ransomware kits and start their attacks easily. The increasing frequency of ransomware attacks in recent years has been largely attributed to the widespread adoption of the ransomware-as-a-service (RaaS) model. **TeslaCrypt** was one of the early examples of RaaS.

Popular Ransomware-as-a-Service Variants

- **DarkSide**

The DarkSide is perhaps the most lethal ransomware variant we have faced recently. First seen in August 2020, the DarkSide Ransomware-as-a-Service quickly spread to more than 15

countries, targeting organizations across a variety of industries, including financial services, legal services, manufacturing, professional services, retail and technology. The DarkSide ransomware group was behind the Colonial Pipeline ransomware incident that occurred in May 2021. The incident forced the company to temporarily shut down the 5,500-mile pipeline for several days, impacting consumers and airlines on the East Coast of the United States [7].

- **LockBit**

LockBit, previously known as ABCD ransomware, is malicious software designed to block users from accessing their computers. LockBit is a highly advanced ransomware that automatically scans for valuable targets, deploys the malware and encrypts all possible computer systems. The LockBit ransomware gang launched its Ransomware-as-a-Service in 2019. The group promoted their service on the dark web, provided support on Russian-language hacking forums and recruited wannabe cybercriminals to breach and encrypt networks [7].

- **REvil**

REvil or Sodinokibi is another Ransomware-as-a-Service variant responsible for extorting large amounts of money from organizations globally. Sodinokibi spreads in several ways, including through unpatched VPNs, exploit kits, remote desktop protocols (RDPs) and spam mail. REvil or Ransomware Evil is also known for double extortion. The group would threaten its victims to publish the stolen information in public if ransom is not paid. The REvil gang is believed to have been shut down by Russian authorities at the request of U.S. government agencies [7].

- **WannaCry**

The WannaCry ransomware worm that caused a worldwide cyberattack in May 2017 when it targeted Microsoft Windows operating systems-based computers, encrypted files and blocked users from accessing their computers and demanding ransom payments in Bitcoin to decrypt the files until the ransom payment was made. It's spread using an exploit called **EternalBlue**, developed by the U.S. National Security Agency (NSA) and leaked by a group known as The Shadow Brokers [8] [9]. This exploit targeted vulnerability in the Windows Server Message Block (SMB) protocol. The attack affected over 300,000 computers across 150 countries [8]. Infected systems displayed a ransom note demanding payments of $300 to $600 in Bitcoin [8]. The North Korean Lazarus Group was behind the WannaCry ransomware attack [7].

- **Ryuk**

Ryuk is used in targeted attacks against healthcare organizations in late 2020. Ryuk is commonly spread by other malware (e.g., Trickbot and Emotet) or through email phishing attacks and exploit kits [7] [10]. In this attack $100,000 to $500,000 ransom amount paid by Bitcoin method.

Figure 2. Evolution of Ransomware

4. Future Developments in Ransomware

4.1. More Advanced Attacks

Polymorphic Ransomware (Changing Ransomware)

Polymorphic ransomware is an evolved form of malware, it can constantly change the code while maintaining its original function. The ransomware evolves, and produces its variants, thereby bypassing static security measures. As new forms of polymorphic malware are being created, protecting organizational systems will become even more difficult.

For example, **VirLock** is one of the first polymorphic ransomware that infect shared applications and cloud storage. It locked users out of their systems and demanded a ransom for access restoration. VirLock not only makes encrypted files but also copied them and changed their format, making it a versatile and persistent threat. This polymorphic nature allowed it to effectively evade traditional detection methods. [11]

Similarly, **CryptoWall** is another notorious polymorphic ransomware that encrypts files on the victim's computer and demands a ransom for their decryption. The polymorphic engine behind CryptoWall generates a unique variant of the malware for each target, making it difficult for traditional antivirus solutions to detect and block. This ransomware has caused significant financial losses and operational disruptions for many organizations [11].

Better Encryption

The future of ransomware will also see improvements in the encryption methods used. Encryption is the primary element of ransomware attacks because it allows attackers to lock down the files and demand ransom for decryption keys. At the present time, ransomware uses

standard encryption algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) [12] [13]. However, there are more advanced encryption techniques that might leverage multi-level encryption, hybrid cryptosystems, and even combinations of symmetric and asymmetric encryption [5]. These encryption methods will decrease the possibility of hacking into the encryption and getting the files without paying the ransom [14].

However, as newer and more advanced encryption techniques are likely to soon be employed in future ransomware releases, the situation is going to worsen [15] [14]. These advancements could include the use of multi-level encryption, which applies several layers of encryption to files, making it exponentially harder to break [12]. Moreover, hybrid cryptosystems which combine both symmetric and asymmetric encryption, could be used to make the encryption process faster and more secure. For example, symmetric encryption could be used to lock the files within a short time and then asymmetric encryption could be used to protect the encryption key as well, adding an additional layer of security [12] [14].

Furthermore, AI increases ransomware's capability to evade past encryption methods, and uses new methods such as multi-level encryption and hybrid cryptosystems to encrypt files. From the victim's system, AI-driven encryption algorithms can change dynamically so that the encryption type is both fast and secure and cannot easily be reverse engineered [15] [14]. For instance, AI may evaluate the defense of the system and then pick the type of encryption that will be hard to crack without opting for the ransom [12].

Furthermore, polymorphic encryption methods driven by artificial intelligence AI could be incorporated into future ransomware descendants, which enable the malware to switch the encryption forms during the attack. This would make it more difficult for the cybersecurity tools to detect and prevent the encryption done by malware. These encryption modes when used in consonance with AI make decryption without paying the ransom relatively very hard making ransomware attacks very effective.

4.2. AI in Ransomware

Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems [12]. AI is increasingly being integrated into multiple types of technology, and cybercriminals are no exception to using AI for malicious purposes. Nowadays, attackers or cybercriminals are using AI in ransomware to minimize the risk of their attacks being cracked. By integrating AI into ransomware, attackers can make their malware more sophisticated, adaptable, and harder to detect, increasing the success rate of these attacks. Below are some ways AI is being used in ransomware attacks.

This main factor of ransomware attack is phishing attack. Nowadays AI based phishing attack is evolving. Attackers use AI to create highly convincing phishing emails, which are more likely to deceive victims into downloading malicious attachments or clicking on malicious links. AI can analyze social media, emails, and other publicly available data to craft personalized phishing messages [13] [14].

Another method is automated vulnerability scanning technique in which ransomware powered by AI scan prospective targets working to unveil vulnerabilities like outdated software or misconfigurations. This makes it easier for attackers to target the vulnerabilities with higher accuracy to ensure the effectiveness of their ransomware delivery [15] [13].

A step further in the polymorphic ransomware development is a technique that uses AI. Polymorphic ransomware uses AI to dynamically change its code with each infection, creating unique variants that make detection by traditional security systems nearly impossible. Each time Ransomware penetrates a new system, it can alter its Code, Signatures and Behaviors patterns to slip past signature-based security mechanisms [16]. AI helps ransomware change its code frequently, making it harder for security systems to detect and stop it. This constant change makes traditional methods, like using known virus signatures, less effective [17] [18].

AI is also applied in enhancing the encryption technique used by ransomware in this case. AI can choose which file to encrypt first, or it can adapt encryption strategies according to the defenses of the system, and thus deal as much damage as possible while keeping its victims paying the ransom [19]. Furthermore, ransom demands can be dynamically adjusted by AI so that it can set a ransom demanding enough to be paid by the victim, but still reasonable enough that the payment will be made [17].

Regarding communication, it is possible for AI-based chatbots to control all the contacts with victims, as well as the negotiations about the ransom and the instruction of the payment. This makes the entire process of extortion smoother as there are less individuals that can interfere on the attacker's side. In addition, AI extension for malware evolution means that ransomware can learn from failed attacks and improve its tactics in future, so it is very challenging to defend against it for security systems [19] [13].

Lastly, AI is incorporated into Ransomware-as-a-Service (RaaS) to bring the costs of the tools down for the attackers. AI helps guide less-skilled attackers through the process of launching sophisticated ransomware attacks, enabling them to target and infect systems without needing advanced technical expertise [20] [13]. Such adaptation increases make ransomware more adaptive, harder to detect, and more destructive, posing a growing challenge to traditional security defenses [19].

4.3. Attacks on Important Infrastructure

Targeting the critical infrastructure organizations, ransomware attacks are one of the biggest threats in the modern world. These attacks frequently target essential services such as healthcare, energy, transportation, and government institutions, they are essential to society's operation. As these sectors become more digitized, they increasingly rely on outdated technology and insufficient cybersecurity measures, making them highly vulnerable to ransomware attacks.

Healthcare Sector

Amongst the most notable ransomware attacks on critical infrastructure, the WannaCry attack in the year 2017 is known for nearly paralyzing the National Health Service (NHS) in the UK. As per the district's timetable, it encrypted the hospital's systems and shut down patients' access to their records and crucial systems. This attack crippled hospitals rendering essential services out of reach and putting lives at risk [13] [14].

One example is the 2020 ransomware attack of the University of Vermont Medical Center that held up critical operations for weeks. Some cancer patients were forced to delay their treatments, which proved that attacks of this nature are potentially fatal. It is especially true for healthcare institutions that are often targeted by ransomware attackers at best and that still heavily rely on outdated systems at worst as they can't at any rate afford operation stoppages [5].

Energy and Utilities Sector

Ransomware also poses a grave threat to the energy sector. The Colonial Pipeline attack in 2021 disrupted fuel supplies along the U.S. East Coast, leading to widespread shortages and economic disruption. The pipeline operator paid a ransom of $4.4 million to restore operations, highlighting the critical nature of these attacks [15]. Energy infrastructure, particularly Industrial Control Systems **(**ICS**)**, which are often outdated and difficult to secure, are prime targets for ransomware due to their critical role in national infrastructure [14].

The NotPetya ransomware attack in 2017 further demonstrated the global risks posed by such malware. It affected several sectors, including energy, and crippled the operations of Maersk, a global shipping company. This incident, alongside the Ukraine power grid attack in 2015, illustrates how ransomware can cause both digital and physical damage by disrupting essential services [14] [5].

Government Institutions

Government institutions have also become frequent targets for ransomware. The Baltimore ransomware attack in 2019 encrypted critical city systems, including email and payment processing services. The attack severely disrupted municipal services for weeks, costing the city over $18 million in recovery efforts [5]. Similarly, the Atlanta ransomware attack in 2018 crippled the city's IT infrastructure, impacting court systems, utility payments, and law enforcement. Recovery costs for Atlanta exceeded $17 million [5].

5. Mitigation Strategies

Ransomware attacks are on the rise and while they are dangerous, there are steps that organizations can take to identify and mitigate them. Below, we explore key techniques and methods to handle ransomware attacks.

5.1. Prevention Techniques

Ransomware prevention strategies should cover all types of risks, starting with technical vulnerabilities and human factors. Three of these are critical techniques that include software updates, employee training, and network segmentation.

Software updates

The first and probably the most effective prevention measure is to ensure that the software and operating system is frequently updated. They elaborated that weak points in outdated software are the points of entry for ransomware attacks. Vendors regularly release patches and updates to address and fix such vulnerabilities in the software. Some of the important policy include, Organizations should ensure that all systems should be patched regularly. Notably, the WannaCry ransomware outbreak capitalized on unpatched Windows systems that were vulnerable to the EternalBlue exploit, which had been addressed by Microsoft months earlier [16] [4]. Organizations should ensure that all systems are patched regularly to avoid similar attacks [17].

Employee Training

Human error remains a significant entry point for ransomware, with phishing emails being a primary method of infiltration. Phishing emails deceive users into downloading malicious files or clicking on harmful links [17] [2]. Therefore, regular employee training is crucial. Employees should be taught how to recognize phishing emails, suspicious attachments, and social engineering tactics [4]. Training sessions and simulated phishing attacks can help employees stay vigilant [18].

Network Segmentation

Network segmentation involves dividing a larger network into smaller, isolated segments, limiting the spread of ransomware in case of an infection [17] [5]. By isolating critical systems and sensitive data, organizations can reduce the risk of large-scale damage. For example, if customer data is separated from the internal administrative network, an attack targeting the latter might not affect customer data [13]. Regular backups, preferably offline, along with robust firewalls, Intrusion Detection Systems (IDS), and endpoint security solutions, further strengthen defenses [16].

5.2. Detection Mechanisms

Detection mechanisms are crucial for identifying ransomware before it can cause significant damage. Two key detection tools include Endpoint Detection and Response (EDR) systems and network monitoring.

Endpoint Detection and Response (EDR)

EDR solutions continuously monitor and gather data from endpoint devices, such as computers and servers [18]. These tools detect ransomware by analyzing behavioral patterns rather than relying solely on known virus signatures. EDR systems can detect unusual file encryption or unauthorized system modifications, signaling a potential ransomware attack [16] [4]. Early detection allows EDR systems to isolate infected devices and prevent malware from spreading further [13].

Network Monitoring

Network monitoring tools observe traffic and behavior across the organization's entire network, detecting anomalies like unusual spikes in data encryption or suspicious traffic to external servers [18]. IDS and Intrusion Prevention Systems (IPS) are effective in identifying these anomalies and can automatically block access to suspicious addresses, reducing the risk of ransomware infiltration [17] [13].

5.3. Response Strategies

In the event of a ransomware attack, an organization's ability to respond quickly and effectively is crucial in minimizing damage. Key response strategies include incident response plans and collaboration with law enforcement.

Incident Response Plans

An incident response plan (IRP) outlines the steps an organization should take during a ransomware attack, including identifying the attack, isolating infected systems, notifying key stakeholders, and initiating recovery procedures [2] [13]. The IRP should be regularly updated and tested through simulation exercises. Once an attack is detected, the first step is isolating affected systems to prevent the malware from spreading further [4]. Cybersecurity teams and third-party vendors should be notified, and if backups are available, affected systems can be restored [16] [13].

Collaboration with Law Enforcement

Law enforcement agencies play a crucial role in mitigating ransomware attacks. Reporting incidents to authorities such as the FBI or Interpol allows these organizations to investigate and track cybercriminal groups [4]. In some cases, law enforcement may possess decryption tools

to help victims recover their data without paying the ransom [13]. Establishing protocols for engaging with law enforcement is essential for a comprehensive response plan [18].

5.4. Future Mitigation Trends

As ransomware evolves, so too must mitigation strategies. Emerging trends include the use of artificial intelligence (AI), cyber insurance, and public-private collaboration.

Artificial Intelligence (AI)

AI is increasingly deployed to detect and prevent ransomware attacks [19] [20]. By analyzing large datasets, AI can recognize patterns indicative of ransomware behavior before traditional systems detect them. Machine learning models can predict ransomware actions based on previous data, enabling more proactive defenses [21].

Cyber insurance

Cyber insurance is becoming a popular mitigation strategy, covering costs related to data recovery, legal fees, and sometimes even ransom payments. However, organizations should not rely on cyber insurance as a substitute for robust security measures [4] [22].

Public-Private Collaboration

As ransomware threats become more complex, public-private collaboration is essential [17]. Governments and private organizations need to work together to share intelligence, develop countermeasures, and respond to ransomware incidents [13]. Such collaboration ensures that best practices are widely disseminated across industries [16].

6. Conclusion

Ransomware has become one of the most serious cyber threats in today's world. Starting from the simple AIDS Trojan in 1989, it has evolved into much more advanced forms like Crypto Ransomware, Locker Ransomware, and Ransomware-as-a-Service (RaaS). These attacks can affect individuals, companies, governments, and critical infrastructures, causing serious damage both financially and operationally.

As ransomware continues to develop, it is becoming more complex, with stronger encryption techniques and the use of artificial intelligence (AI) making it harder to detect and defend against. Cybercriminals are constantly improving their methods, and future ransomware will likely be even more difficult to stop.

However, there are ways to fight back. Prevention strategies like keeping software updated, training employees, and using network segmentation can help reduce the chances of an attack. Detection tools like Endpoint Detection and Response (EDR) and network monitoring are also crucial for spotting ransomware early. Additionally, organizations need to have a clear plan for responding to attacks, and working with law enforcement can provide extra support.

In conclusion, ransomware is a growing threat, but with proper prevention, detection, and response strategies, we can limit its damage. The key is to stay informed and keep improving cybersecurity measures to protect against these evolving attacks.

7. References

[1] K. Baker, "CrowdStrike," 30 01 2023. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/types-of-ransomware/. [Accessed 13 10 2024].

[2] A. K. Maurya, N. Kumar, A. Agrawal, R. A. Khan, "Ransomware: Evolution, Target and Safety Measures". *International Journal of Computer Sciences and Engineering · January 2018.*

[3] A. K. Muslim, D. Z. M. Dzulkifli, M. H. Nadhim and R. H. Abdellah, "A Study of Ransomware Attacks: Evolution and Prevention.," *Journal of Social Transformation and Regional Development.,* vol. 1, no. 1, pp. 18-25, 2019.

[4] A. B. T. D. A. S. H. a. M. K. K. C. Beaman, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers & Security,* vol. 111, pp. 1-22, 2021.

[5] C. F. C. M. A. G. W. M. B. C. M. F. a. C. A. S. Razaulla, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access,* vol. 11, pp. 40698-40712, 2023.

[6] K. Baker, "CrowdStrike," 30 January 2023. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

[7] "UNITRENDS," A Kaseya Company, [Online]. Available: https://www.unitrends.com/blog/ransomware-as-a-service-raas#:~:text=What%20are%20some%20examples%20of%20Ransomware-as-a-Service%3F%201%20DarkSide,globally.%20...%204%20WannaCry%20...%205%20Ryuk%20.

[8] W. contributors, "WannaCry ransomware attack," Wikimedia Foundation, [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

[9] D. L. Johnson, "WannaCry explained: A perfect ransomware storm," CSO Online, 20 May 2017. [Online]. Available: https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html.

[10] Wikipedia, "Ryuk (ransomware)," Wiki Media, [Online]. Available: https://en.wikipedia.org/wiki/Ryuk_%28ransomware%29.

[1] C. McCart, "What is polymorphic malware? Staying Vigilant in 2024," Comparitech, 20 May 2024. [Online]. Available: https://www.comparitech.com/antivirus/what-is-polymorphic-malware-staying-vigilant/.

[2] L. Craig, "What is AI? Artificial Intelligence explained," TechTarget, [Online]. Available: https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

[3] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. M. Fung, and C. Assi, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access,* vol. 11, pp. 40697-40705, April 2023.

[4] M. A. Mos and M. Chowdhury, "The Growing Influence of Ransomware," *IEEE International Conference on Technology, Management, and Operations (TEMO),* pp. 643-647, 2020.

[5] H. V. V. e. al, "Enhancing AI-Powered Malware Detection by Parallel Ensemble Learning," *RIVF International Conference on Computing and Communication Technologies,* pp. 503-507, 2023.

[6] S. Aurangzeb, M. Aleem, M. A. Iqbal, and M. A. Islam, "Ransomware: A Survey and Trends," *National University of Computer and Emerging Sciences,* June 2017.

[7] A. O. Imaji, "Ransomware Attacks: Critical Analysis, Threats, and Prevention Methods," 5 March 2019.

[8] K. Khaliq, K. Hamid, M. U. Ullah, M. Ibrar, N. Z. Ab Rahim, and U. Ahmad, "Ransomware Attacks: Tools and Techniques for Detection," *2nd International Conference on Cyber Resilience (ICCR),* pp. 89-96, 2024.

[9] H. V. Vo, P. H. Nguyen, H. T. Nguyen, D. B. Vu, and H. N. Nguyen, "Enhancing AI-Powered Malware Detection by Parallel Ensemble Learning," *2023 RIVF International Conference on Computing and Communication Technologies (RIVF),* pp. 503-510, 2023.

[20] J. von der Assen, A. Huertas Celdrán, J. Luechinger, P. M. Sánchez Sánchez, G. Bovet, G. Martínez Pérez, and B. Stiller, "RansomAI: AI-Powered Ransomware for Stealthy Encryption," *2023 IEEE Global Communications Conference: Communication & Information Systems Security,* pp. 2578-2585, 2023.

[21] J. von der Assen, A. Huertas Celdrán, J. Luechinger, P. M. Sánchez Sánchez, G. Bovet, G. Martínez Pérez, and B. Stiller, "RansomAI: AI-Powered Ransomware for Stealthy Encryption," *2023 IEEE Global Communications Conference: Communication & Information Systems Security,* pp. 2578-2585, 2023.

[22] Y. Tezcan, "Ransomware, Threat, and Detection Methods," *Beykent University,* 2024.

[23] J. Kahriman, "The Future of Ransomware," HORNETSECURITY, 30 05 2024. [Online]. Available: https://www.hornetsecurity.com/en/blog/the-future-of-ransomware/#:~:text=The%20future%20of%20ransomware%20will,dark%20web%20auctions%2C%20and%20more..