DIGITAL DEFENCE: BATTLE AGAINST RANSOMWARE ATTACKS IN INDIA

Janani R, School of Excellence in Law, TNDALU

ABSTRACT

"Cybercrime is the greatest threat to every company in the world."

Ransomware attacks in general is considered to be a significant threat to the organizations as well as the individuals across the world. This is due to the advent growth of technology and the increase in use of the internet by almost majority of the population worldwide. These attacks generally involve the employment of malware by the attackers in order to encrypt the critical data and demands ransom payment in exchange for the decryption key. This malicious software is typically spread through phishing emails that pretends to be from trusted source, malicious links, pop-up ads, social engineering tactics, or exploiting unpatched vulnerabilities. There are certain cases in which the victims even after paying the demanded ransom will not be provided with the decryption key. This as a result leads to severe impacts like the loss of revenue, financial loss, business disruption, and reputational damage.

Keywords: ransomware, malicious, exploit, decrypt, extort.

INTRODUCTION

The term ransomware is derived from the two words, ransom and software and it refers to the malicious software that is designed to extort money from a victim, by either holding certain specific files hostage or denying the access of the entire computer until a ransom is paid. Ransomware incidents are experiencing rapid growth with attacks across multiple sectors including the critical infrastructure[1] which poses severe risks to services like oil & gas, transportation, water, electricity etc., Majority of this attack is targeted on essential sectors like IT & ITeS, finance, manufacturing, education, healthcare, transport, energy and others[11] resulting in disruption of services, financial loss and in some extent, it poses risk to public safety also. Ransomware attacks in the finance sector have emerged as a notable issue due to the sensitive nature of the data involved and also their financial resources. The attackers choose certain sectors as prime targets as they know that the victims are likely to pay the demand to get their data's back and have resources to meet the ransom amount. These attacks as a result are found to have severe impacts like loss of finance, data theft, loss of IP, functional disruptions and damage to reputation.

The evolution of ransomware traces back to 20th century when the world was witnessing the growth of internet at a slower rate. The introduction of cryptocurrencies, especially Bitcoin, revolutionized the way that the ransomware was monetized and caused a surge in attacks starting in 2012. The emergence of Ransomware-as-a-Service (RaaS) has further democratized cybercrime by making ransomware attacks accessible to persons with less technological expertise. Attackers frequently use cybersecurity knowledge and human error to encrypt sensitive data, obtain illegal access to financial systems, and demand ransom payments in order to get the data decrypted.

OBJECTIVES OF THE STUDY

1. To understand the emerging concept of the term ransomware, its definition, evolution and technologies behind.

2. To examine the effectiveness of current laws and regulations regulating ransomware

[1] Shmuel Gihon, Ransomware Trends 2023 Report, *available at:* https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report, (last visited on August 08, 2025).

attacks in India.

3. To understand the ethical dilemma of legality of ransom payments made by the victim to the perpetrator.

HISTORY OF RANSOMWARE

Ransomware attacks have increased and evolved substantially over the years and at present has become a major cybersecurity threat globally. It is the fastest growing malware threat, targeting users of all types from the home user to the corporate network. The evolution of ransomware attacks traces back to late 1980's with the AIDS Trojan as one of the first documented ransomware instances[2]. At first, ransomware attacks were relatively uncommon and simple to solve, often demanding payments through mail in order to get decryption keys. But in the early 2000s, criminal organizations began employing more advanced and sophisticated encryption methods, leading to the emergence of new variants and tactics, thus maximizing the impact of those attacks and demanding higher ransom amounts.

The evolution of ransomware continued with the introduction of stronger encryption algorithms and the utilization of cryptocurrencies like Bitcoin for ransom payments[3]. Cryptocurrency and advances in payment techniques and strong data encryption techniques are some of the major factors leading to increased amount of ransomware. This provided the attackers with a safe and untraceable way to accept ransom payments which significantly increased the ransomware incidents thus transforming them from small-time crime to a money- making business for criminals. The sophistication of ransomware attacks has increased over time with variants like Ryuk, Maze, REvil, and LockBit employing advanced techniques like data theft and double extortion to put greater pressure on victims to pay. particularly during COVID-19 pandemic, there has been a notable increase in ransomware attacks that was targeted globally[4].

MODUS OPERANDI

The modus operandi of ransomware attacks involves various factors that the attackers

[2] Kieran Laffan, "A Brief History of Ransomware", *available at*: https://www.varonis.com/blog/a-brief-history- of-ransomware (last modified June 9,2023).
[3] Allan Liska and Timothy Gallo, *Ransomware: Defending Against Digital Extortion* 20 (O'Reilly Media, Sebastapol, 2017).
[4] Andrew Jenkinson, *Ransomware and Cybercrime*, (Taylor & Francis Ltd; India, 1st edn., 2022).

adopt to carry out the malicious activities[5]. This includes; starting from the initiation & setup phase, it passes through infection phase, then encryption phase, extortion phase and finally decryption phase[6].

1. **Initiation & setup phase:** This is the first phase where the hackers identify the target that they are planning to infect and gathers all relevant information required by them to carry out activities. This can eventually be done through phishing emails, software vulnerabilities or by malicious websites. Once the ransomware infiltrates the targeted system, it sets up a communication line back to the attacker in order to install more malware and hold hostage of the files.

2. **Infection phase:** This phase is considered to be the most crucial stage, since the attacker sets the stage to infect or compromise the system. The attacker in this stage introduces the malware into the system. The ransomware searches for the files to encrypt and mainly it infects the victim's backup storage systems.

3. **Encryption phase:** The malware now encrypts the target data, while deleting any backup that may be preserved. This is the stage where the attackers achieved their part goal to encrypt important data and make the system unusable by the victims.

4. **Extortion phase:** The victims usually receive communication for payment of ransom amount in return for a decryption tool key to restore data and the system. Most often, the users come to know that their system compromised when there displays a ransomware note demanding money to decrypt files. The cybercriminals demand payment through cryptocurrencies since it is considered to be a safer and untraceable method due to its anonymity.

5. **Decryption phase:** At this final stage, those victims whoever met with the demands of the attackers will be provided with the decryption key to regain the encrypted data without any guarantee. Without any guarantee means there is a less chance for the files to get decrypted or there may be chances where part of the encrypted files be regained. The

[5] Aditya Mehta, Pritvish Shetty, et.al., "Digital Age Warfare: Ransomware Attacks", available at: https://corporate.cyrilamarchandblogs.com/2022/01/digital-age-warfare-ransomware-attacks/ (last visited on August 8, 2025).
[6] "The 7 Stages of a Ransomware Attack", *available at:* https://www.zerto.com/blog/ransomware-recovery/the-7-stages-of-a-ransomware-attack/ (last visited on August 08, 2025).

following figure depicts the modus operandi deployed by the cyber criminals.

TYPES OF RANSOMWARE

Ransomware attackers use different type of methodology for encrypting the user data and files. Their primary target would be to create fear among the users about the device becoming inaccessible. Differences in each type of ransomware can be due to the algorithms for encrypting data or blocking access of to the device. There are three main variants of Ransomware: Crypto-ransomware, Locker-ransomware and Master Boot Record (MBR)-Ransomware.

1. CRYPTO RANSOMWARE

It is one of the most common strains of ransomware. It encrypts valuable files and data on the target's computer or mobile phone, so that it become unusable by them. This kind of ransomware search silently for the victim's files and data after being injected to user's system. The victim's device continues to work as usual until the malware start targeting the critical operating system files and applications. The malware finds the end user data and files it will encrypt and make them unusable for the user and demand a ransom[7]. The ransom is demanded by the attackers by means of cryptocurrency like bitcoins because of the anonymity.

2. LOCKER RANSOMWARE

Ransomware-locker is another type of ransomware that impacts the computing devices such as end user computer systems or mobile devices. Locker ransomware can also lock the input interface like keyboard and mouse and deny access for the user. It would allow limited functionality for the user such as moving the mouse or keeping the numbers button on the keyboard enabled, for the user to be able to pay the ransom. Unlike crypto ransomware, this malware keeps the data and files untouched. This means the data can be recovered by moving the storage device to another computer[8].

[7]Ali Hoseini, "Ransomware and phishing cyberattacks: analyzing the public's perception of these attacks in Sweden", Department of Information Technology (2022).
[8] A. Bhardwaj, V. Avasthi, H. Sastry, and G. Subrahmanyam, "Ransomware digital extortion: a rising new age threat", 9 IJST pp. 1–5 (2016).

3. MASTER BOOT RECORD RANSOMWARE

Master boot record-ransomware is one of the types of ransomware that encrypts the MBR by replacing it with malicious code, that holds the information on how the logical partitions, containing file systems, are organized[9]. Usually, a ransom note demanding the ransom in order to regain the access and control of the system is displayed once the attackers locks the user out. This type of ransomware is particularly dangerous as it prevents the operating system from loading properly, making it challenging for users to access their files or use their computers until the ransom is paid.

TECHNOLOGIES EMPLOYED

The most common approach employed by the ransomware attackers to compromise computers, encrypt data, and demand a ransom is done by combining several technologies and methodologies. At first, the ransomware file is transmitted to the victims by the threat actor through attack vectors such phishing emails, software vulnerabilities, and remote desktop protocol penetration. Once the user is tricked to install the malicious malware into the system, the ransomware starts to work by searching the files and encrypts them. These encrypted files may appear to be important and it could be documents, spreadsheets, pictures, videos etc., [10].

The victim gets warned about the intrusion of their device only when the ransomware has sufficiently encrypted the files. Only after the user is locked out of the system by the ransomware, the victims acknowledge that they are unable to access their files. This notice is followed by payment instructions that require payments to be made in Bitcoin which typically cost anywhere from hundreds to thousands of dollars. The perpetrators assure that the key that is required to decrypt the files will be provided as soon as the demanded ransom is met. In certain circumstances, the case is not similar because once the decryption key is provided, some victims face the difficulty to decrypt the files and some may be able to

[9] J. S. Aidan, H. K. Verma, and L. K. Awasthi, "Comprehensive survey on petya ransomware attack," ICNGCIS pp. 122–125 IEEE (2017).
[10] Hoplite Technology, "Technologies most vulnerable to Ransomware attack", *available at:* https://www.hoplite- tech.com/blog/top-technologies-most-vulnerable-to-ransomware-attack (last visited on August 09,2025).

decrypt a part of the encrypted files[11].

FRAMEWORKS REGULATING RANSOMWARE ATTACKS IN INDIA

As far as India is concerned, it does not have explicit provisions for ransomware attacks in its legislations, but certain laws have provisions that can be applied to ransomware attacks. These laws provide for compensations, penalties in case of breach of sensitive personal data and Critical Information.

➢ THE CONSTITUTION OF INDIA, 1950

Privacy issues in ransomware attacks are a significant concern in cybersecurity. Traditionally, ransomware attacks focused on encrypting data, compelling organizations to either pay the ransom or rely on backup data to restore their systems. In the event of encrypting the personal data, it signifies a breach of that data, resulting in the loss of immediate access to the information. As a result of that attack, the victims are made to face the risk of permanent loss of personal data, relinquishing control over their information, becoming susceptible to social engineering tactics utilizing compromised data and potential malicious exploitation of their personal data by cybercriminals. However, recent trends have seen cybercriminals use their advanced tactics, now routinely copying data before encrypting it. This modification in ransomware attacks presents an extra level of danger, compelling organizations to fight with the added threat of data breach, which further worsen the consequences of a ransomware attack. Ransomware attacks threaten the unity, integrity, security and sovereignty of India and also can be targeted to strike terror in people, causing significant harm.

The Indian Courts recognized right to privacy as an intrinsic part of the Right to life and personal liberty and made it as a fundamental right under Article 21 of the Indian Constitution, 1950[12]. In India, ransomware attacks are considered as a breach of Fundamental Right to Privacy guaranteed under the Constitution.

[11] Steve Brown," How Does Ransomware Work and What Technologies Best Prevent It?", *available at:* https://www.rutter-net.com/blog/how-does-ransomware-work-and-what-technologies-best-prevent-it#:~:text=Ransomware%20works%20by%20leveraging%20one,ransomware%20file%20to%20their%20victims (last visited on August 09, 2025).

[12] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

➢ THE INFORMATION TECHNOLOGY ACT, 2000

The Parliament of India enacted The Information Technology (IT) Act[13] on 9th June 2000 and it was subsequently amended in the year 2008. This Act is the primary legislation in India that governs cybersecurity, data protection, and cybercrime. The Information Technology (Amendment) Act of 2008[14] does not explicitly deal with ransomware but it significantly enhances the legal framework for addressing cybercrimes, including those related to ransomware attacks. The IT Act along with the rules framed thereunder, deals with electronic governance and cybercrimes and has an overriding effect over any other law for the time being in force. A ransomware attack frequently leads to concealment, alteration, disruption, theft, deletion of data, tampering of computer code, programs, systems, or networks. It also encompasses the introduction and propagation of viruses within them. The IT Act includes relevant provisions addressing ransomware attacks.

Section 43 read with Section 66: In general, the Act does not explicitly mention ransomware, it covers activities related to unauthorized access and damage to computer systems, which can include ransomware attacks. These section 43 read with 66, pertain to causing damage to computer or computer system without the owner's consent. This offence carries penalties of imprisonment for a maximum of three years and a fine of up to five lakh rupees or with both.

Section 43 of IT Act states that if any person without permission or beyond the scope of his authorization, accesses or secures access to a computer, computer system or computer network; downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network, including information or data held or stored in any removable storage medium; introduces or causes to be introduced any computer contaminant or computer virus; damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer; disrupts or causes disruption of any computer, computer system or computer network; denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or

[13]The Information Technology Act, 2000 (Act 21 of 2000).
[14] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

affects it injuriously by any means; steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage; he shall be liable to pay damages by way of compensation to the person so affected[15].

Section 43A of IT Act, 2000 in India deals with the compensation for failure to protect data. Even though Section 43A does not specifically refer ransomware, its emphasis lies on the responsibility of organizations to safeguard sensitive personal data or information stored within computer systems. Any body corporate that holds, manages or processes sensitive personal data or information on a computer system under its ownership, control, or operation is mandated to ensure a reasonable level of security for the protection of such data. This section is pertinent in cases of ransomware attacks, which frequently cause unauthorized access, disclosure, destruction, modification, or alteration of sensitive personal data or information. A corporate entity that does not establish and maintain reasonable security measures and processes to safeguard such data or information may be held responsible for paying damages to those affected by the breach[16].

Section 65 of IT Act is relevant in the context of ransomware attacks as it pertains to tampering with computer source documents. This section specifies that tampering with computer source documents is punishable with imprisonment of up to three years or with a maximum fine of Rs. 2,00,000/-. In the event of ransomware attack where there is unauthorized access, alteration or destruction of computer source documents, Section 65 can be invoked to address such criminal actions and impose penalties on the perpetrators involved in tampering with computer source documents[17].

Section 66C of IT Act that gives punishment for identity theft, may not be broadly relevant to ransomware attacks but is does in some circumstances, which involve the use of encrypted data to gain unauthorized access to a computer system or network. But typically, ransomware attacks involve the encryption of victim's data and demand for ransom to restore access to data. This offence punishable with an imprisonment that extends to three years or one lakh rupees fine[18].

[15] The Information Technology Act, 2000 (Act 21 of 2000), s.43.
[16] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.43A.
[17] The Information Technology Act, 200 (Act 21 of 2000), s.65.
[18] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.66C.

Section 66D of the Act relates to the punishment for cheating by personation by using computer resource and in the case of ransomware attacks, the perpetrators often use deceptive tactics to gain unauthorized access to computer system or network. In short, the cyber criminals impersonate themselves to be a trusted source in order to execute their malicious attacks. The perpetrator shall be made liable to fine up to 1 lakh rupees or imprisonment for a term extending 3 years[19].

Section 66F of the Information Technology Act, 2000 provides punishment for cyber terrorism. It states that anyone who threatens India's unity, integrity, security, sovereignty or strikes terror in the people or any section of the people shall be punished. In the context of ransomware attacks, it may be relevant if the attack is carried out with the intent to threaten India. Whoever commits or even conspires shall be punishable with imprisonment for life[20].

Section 70 of the Information Technology Act, 2000 deals with protected system. This section in the context of ransomware attacks can be invoked as it focuses on safeguarding critical information infrastructure that comprises computer resources that have impact on national security, economy, safety or public health. Ransomware attacks can target this infrastructure, disrupting essential services and causing significant damage[21].

Section 70A of the Information Technology Act, 2000, is particularly relevant in the context of cybersecurity and ransomware attacks, with a specific focus on safeguarding critical information infrastructure. This section empowers the government to authorize designated agencies to monitor, collect or analyze information in response to emergencies[22].

Section 70B of IT Act is related to Indian CERT which serves as nodal agency for incident response. This provision establishes the National Critical Information Infrastructure Protection Centre (NCIIPC) tasked with safeguarding critical information infrastructure from cyber threats including ransomware[23].

Section 72 of the Act deals with the penalty for breach of confidentiality and privacy

[19] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.66D.
[20] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.66F.
[21] The Information Technology Act, 200 (Act 21 of 2000), s.70.
[22] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.70A.
[23] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.70B.

of information. In the case of ransomware attacks involving unauthorized access or disclosure of confidential information, Section 72 of the IT Act serves as a critical legal framework to address privacy violations and impose penalties on offenders. This section reinforces the importance of upholding data confidentiality and protecting against ransomware threats to preserve information integrity and privacy[24].

- **THE INFORMATION TECHNOLOGY RULES**

The following are some of the rules and intermediary guidelines of the IT Act to regulate different aspects of cyber security and combat cybercrimes including ransomware.

The Central Government Vide power under section 87 of the IT Act has framed Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. The Rules endowed CERT with the following functions: the administrative role to collect, analyse and disseminate information on cybersecurity incidents, and take emergency response measures. These rules made some obligations for intermediaries and service providers to report occurring cybersecurity incidents immediately to the CERT-In[25].

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI rules) require companies that handle sensitive personal data or information in any stage of processing, collection, storage or transfer are obliged to establish and maintain reasonable security measures and procedures to ensure protection of such data[26]. Rule 8 provides for compensation and penalties in case of negligence or failure of duty by the body corporate and are punished with an imprisonment that extends to 3 years or fine of 5 lakh rupees or with both[27].

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021) require intermediaries to establish and maintain reasonable security practices and procedures to safeguard their computer resources and information, thus ensure safe harbour protection. Additionally, intermediaries are obliged to report any

[24] The Information Technology Act, 200 (Act 21 of 2000), s.72.
[25] "A comparison of cybersecurity regulations: India", *available at*: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html.
[26] Ministry of Communications and Information Technology," Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"; G.S.R. 313(E).
[27] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s.72A.

cybersecurity incidents to the Indian Computer Emergency Response Team (CERT-In)[28].

Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, require companies with secured systems as outlined in the IT Act, to implement designated information security measures[29]. At present, in India protected systems are confined to all government functions.

Thus, the Information Technology Act (IT Act) plays an essential part in the fight against ransomware attacks by establishing a legal foundation to prosecute cybercrimes. Even though, it does not have provisions that deal with combating ransomware attacks explicitly, it criminalizes computer-based activities, including ransomware incidents. This Act aims to safeguard computer systems from malicious activities and is considered to be essential in deterring and holding ransomware perpetrators accountable for their actions, ultimately contributing to a more secure digital environment.

- **THE INDIAN PENAL CODE, 1860[30]**

Due to the technological development and emergence of new concept of crimes, it is need of the hour to enact new as well as amend the existing laws considering those cybercrimes. In many countries, there is lack of specific legislations addressing the concerned crimes like ransomware attacks. Even though there are no specific laws, these crimes are addressed under the traditional criminal laws since it resembles the traditional form of crimes such as forgery, theft, extortion and fraud. As a result, in many jurisdictions where there are no specific laws on ransomware, the existing penal and criminal laws are most preferably applied to address those criminal activities.

Under IPC, the ransomware attacks are charged as a crime under following provisions. This includes extortion (Sec.383), cheating (Sec 415-420), mischief (Sec.425), criminal conspiracy (Sec.120A,120B), criminal intimidation (Sec.503) and theft (Sec.378). The Supreme Court of India in a recent case of Jagjit Singh v. State of Punjab[31] held that the

[28] Ministry: Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021"; G.S.R. 314(E).
[29] MeitY," Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018" *available at:* https://www.MeitY.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf (last visited on February 10, 2025).
[30] The Indian Penal Code, 1860 (Act 45 of 1860).
[31] [Special Leave Petition (Criminal) No. 3583 of 2021].

offences like hacking and data theft will not be addressed as an offence only under the IT Act of 2000, but it can also be filed as an offence under the way older Indian Penal Code.

- **THE DIGITAL PERSONAL DATA PROTECTION ACT (DPDP), 2023**

DPDP Act of 2023[32] is the recent legislation that provides provisions for processing of digital personal data. The data fiduciary is a person who themselves or in conjunction with other person determines the purpose for which the personal data is processed. The data principal is one whose personal data is being processed[33]. In relevance to ransomware attacks, this Act of 2023 mandates the data fiduciaries to adopt required security measures to prevent data breaches and also implement robust cyber security practices to protect sensitive data. The Act also requires the organisations and data fiduciaries to notify to the Data Protection Board of India (DPBI)[34], the data principal and individuals too in case of data theft which includes ransomware attacks.

- **CERT-In**

The India Computer Emergency Response Team (CERT-In or ICERT) was formed in the year 2004 under the IT Act, 2000. It is a nodal agency under MeitY to deal with cyber security incidents including ransomware attacks in India. This agency presents its report twice a year on ransomware attacks in India based on reported incidents.

According to 'India Ransomware Report' by CERT-In, ransomware incidents in India have increased by 51%[35] in first half year of 2022 (H1) than the previous year and in H2 it has seen an increase by 53%[36]. A majority of attacks were observed in IT & ITeS sector followed by Finance and Manufacturing sectors as per the 2022 report. They have predominantly targeted critical infrastructure organisations including Oil & Gas, Transport and Power to disrupt their operations and extract ransom. This report also mentioned the prominent ransomware families, Lockbit which was majorly seen variant in the Indian context followed by Makop and Djvu/Stop ransomware. Based on the analysis made by CERT-In on ransomware attacks, it made recommendations to organisations to carry out risk

[32]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[33] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(i).
[34] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), Chapter-v, s.18.
[35] CERT-In, India Ransomware Report H1-2022.
[36] CERT-In, India Ransomware Report 2022.

assessment and vulnerability tests, implement policies, disconnect the infected system, report immediately to CERT-In and other regulatory authorities and lodge FIR with law enforcement agencies. This agency also recommends not to negotiate or pay ransom when demanded.

The CERT-In recently on 23rd July, 2023 has warned about the newly emerged ransomware group 'Akira', which targets Windows and Linux based systems. This ransomware would initially steal and encrypts the victim's data and conducts double extortion to force ransom from the victims. Sometimes they would steal data and release it on their dark web page[37].

Figure 3. 1: Majorly impacted sectors 2022.

Figure 3. 2: Majorly observed ransomware variant 2022.

The above figure 3.1 depicts the ransomware trends in India in the year 2022. This statistic is regarding the majorly impacted sectors of the ransomware attack. Majority of the attacks are observed in IT & ITeS followed by Finance and Manufacturing sectors.

The above figure 3.2 depicts the majorly seen variant in the Indian context and also many new variants observed in 2022. LockBit was majorly seen variant followed by Makob and Djvu/Stop ransomware.

[37] Economic Times," Govt warns of ransomware Akira which steals & encrypts vital data to conduct extortion", *available at:* https://government.economictimes.indiatimes.com/news/secure-india/govt-warns-of-ransomware- akira-which-steals-encrypts-vital-data-to-conduct-extortion/102054419 (last visited on August 10,2025).

NOTABLE RANSOMWARE INCIDENTS IN INDIA

➢ AIIMS RANSOMWARE ATTACK

The All India Institute of Medical Sciences (AIIMS) in Delhi, India, experienced a cyber threat on November 23, 2023 that completely made their operations and services still. The attack was caused due to improper network segmentation and resulted in operational disruption due to the non-functionality of critical applications[38]. The attack was the most sophisticated form of the ransomware attack so that a case of extortion and cyber terrorism was registered by the Delhi Police on November 25. The attack disrupted the hospital's operations and compromised patient data, highlighting the potential risks to public health and safety that cyberattacks pose. Patient records were inaccessible, leading to delays in treatment and potential privacy breaches. The incident raised questions about the resilience of the healthcare infrastructure and the need for proactive measures to prevent cyberattacks. Regular data backups, robust security solutions, and incident response plans are crucial for healthcare organizations to mitigate the impact of ransomware attacks[39]. The AIIMS cyber attack also highlighted the need for cybersecurity awareness training for healthcare employees and the importance of creating a secure, cyber-savvy culture in the organization. The attack on AIIMS is a grave wake-up call for India's safety, especially in the healthcare sector, which is increasingly vulnerable to cyberattacks due to growing reliance on digital infrastructure. The incident underscores the need for robust cybersecurity measures and a thorough reassessment of existing measures to safeguard critical institutions like healthcare facilities.

➢ WANNACRY

The WannaCry ransomware attack also known as WannaCrypt was a global cyberattack that occurred in the month of May 2017[40]. It was caused by the WannaCry crypto ransomware, which targeted computers running on Microsoft Windows operating system by encrypting data and demanding ransom payments by way of Bitcoins. The major target of this ransomware attack was the US healthcare system and a well-known car manufacturing firm

[38] Aashish Aryan," AIIMS cyber attack took place due to improper network segmentation: Govt in RS", *Economic Times,* Feb. 10, 2023.
[39] PTI," AIIMS cyber attack suspected to have originated in China, Hong Kong", *Economic Times*, Dec. 14, 2022.
[40] Tirth Patel, *WANNACRY RANSOMWARE ATTACK* (Notion Press, 1st edn., 2017).

belonging to France. The attack propagated by using EternalBlue[41], an exploit developed by the United States National Security Agency (NSA) for Windows systems, which was stolen and leaked by a group called the Shadow Brokers, a month prior to the attack. The attack affected more than 300,000 computers across 150 countries, with damages ranging from hundreds of millions to billions of dollars. The attack was halted by the registration of a kill switch, which prevented already infected computers from being encrypted or further spreading WannaCry. Investigators found that the attack was carried out by a North Korean hacker collectively called The Lazarus Group. The group exploited a Windows vulnerability discovered by the United States National Security Agency (NSA) and leaked by the Shadow Brokers in April 2016, one month after Windows released patches for the exploit. The attack highlighted the importance of keeping software up to date with the latest security patches and the potential risks of vulnerabilities in widely used software.

India was also affected by this attack and based on the reports, it is found to be third worst-hit nation by WannaCry ransomware. It affected more than 2 lakh computer systems. During the first wave of attacks, this ransomware attack had targeted and attacked the financial institutions in India including few enterprises in Tamil Nadu and Gujarat. The attack targeted various industries and organizations across the nation, including government-run hospitals, power utilities, and customer care centres of State electricity distribution companies. The ransomware locked user's devices and prevented them from accessing data and software until a certain ransom was paid to its creators.

The attack affected at least 48,000 systems across various organizations, but not many came forward raising doubts whether possible ransomware attacks were being properly reported. The MCA21[42] system is under the administration of Infosys. It provides for making electronic filings related to compliances under the Companies Act and Limited Liability Partnership Act, 2008 and as a result this was also subjected to the WannaCry ransomware attack. By May 12, the systems that were infected were retrieved and proactive measures were undertaken to prohibit the incidence of such attacks in the future.

The attack highlighted the need for stronger cybersecurity measures and the

[41] Kaspersky, "What is WannaCry ransomware?", *available at*: https://www.kaspersky.co.in/resource-center/threats/ransomware-wannacry (last visited on August 12, 2025).
[42] Mail Today Bureau," WannaCry did hit India and even central govt portal. So why did Centre downplay the ransomware attack?", *available at:* https://www.indiatoday.in/mail-today/story/ransomware-wannacry-cyberattack-global-ransomware-attack-india-983427-2017-06-19 (last visited on August 12, 2025).

importance of updating systems to prevent future attacks. The Indian Computer Emergency Response Team (CERT-In) issued a red alert and advised organizations to update their systems with the latest security patches and to avoid opening suspicious emails and attachments. The government also directed all affected organizations to follow the Indian Computer Emergency Response Team's (CER) advisory to handle the attack.

- **JAWAHARLAL NEHRU PORT CONTAINER TERMINAL**

The Jawaharlal Nehru Port Container Terminal (JNPCT) in Mumbai was hit by a suspected ransomware attack on February 21, 2022. The attack affected the terminal's management information system (MIS), causing it to shut down the operations. The port authorities were working restlessly to restore the critical operating systems, and no official updates regarding the source and type of attack have been issued by JNPCT. Following the attack, JNPCT diverted one of its scheduled vessels to a nearby terminal and stopped accepting ships. The other private terminals at the port were functioning normally as if nothing seems to be happened. The Jawaharlal Nehru Port Trust (JNPT) at Navi Mumbai is India's premier container handling port, handling nearly half of the total containerised cargo volume in the country. It is connected to more than 200 ports globally and currently runs five container terminals[43].

- **SPICE JET AIRLINE RANSOMWARE ATTACK**

SpiceJet, a low-cost Indian airline, experienced an attempted ransomware attack on May 25, 2022, which impacted some of its systems and caused delays in flight operations. The IT team of SpiceJet managed to prevent the attack, but the incident still had a cascading effect on flights, leading to delays and cancellations. Some passengers reportedly experienced delays of up to five hours, and the airline's customer service via phone was unreachable for some time and this caused serious distress to the customers. The attack did not affect the flight status tables, which were accessible and showed massive delays on all destinations checked. SpiceJet is the second-largest airline in India, operating a fleet of 102 aircrafts to serve over 60 destinations, and it has more than 14,000 employees and holds about 15% of the local market share. The attack had a significant impact on the airline's operations,

[43] Ship Technology, "India's Jawaharlal Nehru Port Container Terminal hit by cyberattack", *available at:* https://www.ship-technology.com/news/jawaharlal-nehru-port-container-terminal/ (last visited on August 15, 2025).

affecting a large number of passengers across India and international destinations, and resulting in significant financial losses due to the multi-hour delays. BleepingComputer reached out to SpiceJet for more details about the ransomware attack, but the company did not provide any further information at the time of writing.

SpiceJet is not alone in experiencing cyber attacks in the aviation industry. In 2020, the airline confirmed a data breach incident that allowed an unauthorized individual to access a database backup file containing unencrypted information of 1,200,000 passengers who had used SpiceJet's services in the previous month. The file contained passengers' full names, flight information, phone numbers, email addresses, and dates of birth.

CONCLUSION

It is concluded that due to the advent growth of internet and technology, there is increase in prevalence of ransomware attacks throughout the territory of India. As India continues to grow rapidly in its digital economy, the organizations should conduct regular risk assessment and patch vulnerabilities to avoid exploitation. Looking into the legislations that regulate the threat of ransomware attacks in India, there are no specific laws. However, there are certain legislations that implicitly deal with this concept. The legislations like the IT Act, 2000 and IPC, 1860 in India provides punishment for those who indulge in activities that are relevant to the ransomware attacks. Beyond this, there are also certain Information Technology Rules as well as guidelines provided by the Government. But these existing Indian legislations should be amended and new enactments to be made with the context of ransomware offences explicitly. The entities must adopt robust cybersecurity measures to prevent themselves from being vulnerable.

SUGGESTIONS

1. The concept of ransomware itself is still a vague phenomenon. The awareness on the ransomware attacks is still not prevalent among individuals as well as the organizations. Thus, the Indian Government can consider defining the term ransomware attacks in any of the existing or new legislations as a cyber offence. This will provide a basis for the enactment of new legal framework addressing the ransomware attacks.

2. Initiatives can be made by the Government and private sectors to educate individuals as well as the organizations about the consequences of ransomware attacks by means of conducting awareness campaigns. These campaigns can provide knowledge on how to prevent and tackle ransomware attacks and what to do immediately after coming to know that the attack has occurred.

3. Due to the increase in frequency and sophistication of ransomware attacks, the attackers use cryptocurrencies as a mode to receive ransom payments which is difficult to trace. It is suggested that the Government shall regulate the use of cryptocurrency to prevent it from being used for ransomware attacks. This can be done by mandating the cryptocurrency exchanges to implement anti-money laundering measures and report immediately in case of suspicious transactions.

4. Measures can also be taken by the Government to invest in Research & Development to develop new cybersecurity tools and techniques to detect the incidence of ransomware attacks. The cybercriminals use anonymity to commit crimes, advancement in technologies can be brought to detect the perpetrators.

5. Backup of data shall be regularly done by the organizations and has to be stored in offline to prevent the incidence of ransomware attacks. The risk assessment and vulnerability tests shall also be conducted frequently to detect and patch the vulnerabilities.