DECODING RANSOMWARE ATTACKS: UNMASKING LEGAL SOLUTIONS IN THE IT ACT OF 2000

BY *NAVANEETHAKRISHNAN. T*,[1] *MANOHAR. R*[2] and *VISWAJIT SRINIVASAN*[3]

ABSTRACT

Cybercrime is a widespread issue in the globe today. Crimes including identity theft using computers and the internet, unauthorized imports, and harmful software. Cybercrime is simply any crime in which a computer is either the weapon or the victim. Cybersecurity is what we have to guard against this. Attacks using ransomware have become a common and profitable menace in today's digital environment. An extensive summary of ransomware attacks is given in this abstract, including information on how they have developed, how they affect people and businesses, and what countermeasures are being implemented in order to mitigate the threat. This article examines a case study of assaults and analyses the vulnerability or cause of the affected system primarily assaults using ransomware.

Keywords

Ransomware, Scareware, Encryption, Doxware

I. INTRODUCTION

Cybercriminals are aware that the growth of any organization or daily working operations depends heavily on data, files, networks, and other digital resources. The fastest and best method to make a lot of money is to hold all of these digital assets at hostage since they are so valuable to the company. Thus, the development of ransomware, a type of virus that often encrypts all files and demands payment in order to provide the victim with the key to decode them.[4]

[1] Advocate, Madras High Court Madurai Bench, Madurai

[2] Advocate, Madras High Court Madurai Bench, Madurai

[3] *Student, NALSAR University, Hyderabad.*

[4] Popli N, Girdhar A, Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In Verma, Nishchal K, Ghosh, A. K. (eds) Computational

The "Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanack" states that one of the biggest problems facing humanity over the next 20 years is cybercriminal activities. The fastest-growing type of crime in the world is cyberattacks, which are also getting bigger, more sophisticated, and more expensive.[5] Additionally, they project that by 2021, cybercrime losses would cost the global economy $6 trillion annually, and that over 70% of all bitcoin transactions will include illicit behavior.

Transportation, healthcare, financial services, manufacturing, and government have been the top five industries targeted by cyberattacks in the last five years. "Cybersecurity Ventures" predicted that the top 10 industries for 2019 to 2022 will include teaching, retail, gas and natural gas, media and entertainment, and law. For many years, hacking tools and equipment for identity theft, ransomware, virus, and other malicious purposes have been available on the internet for as little as $1, making it almost free to engage in cybercrime.

Ransomware is a class of malicious software that locks down user files and related resources using security methods like cryptography. It then demands bitcoin in return for the unlocking of the data. While some ransomware attempts to find holes to exploit it, using open ports or a backdoor to get inside, others use social engineering, malicious adverts, spamming, and drive-by downloads. As a result, vulnerability testing, the identification of security flaws, and public awareness of these types of exploitation mechanisms are required.

As a result, ransomware has grown in popularity among attackers and become a lucrative vocation. The widespread use of ransomware has given rise to an incredible network of hackers. The financial impact of the ransomware outbreak is directly related to encryption technologies and virtual currency. Encryption works well and is virtually unbreakable. Cybercurrency that is anonymous can avoid tracing. Simple access to ransomware code makes it simple to enter the

Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[5] https://www.researchgate.net/publication/339326833_Ransomware_Prevention_and_Mitigation_Techniques

realm of criminality. When they are combined, hackers have an alluring avenue to operate, leading to the emergence of expert cyber criminals.

II. HISTORY OF RANSOMWARE ATTACKS

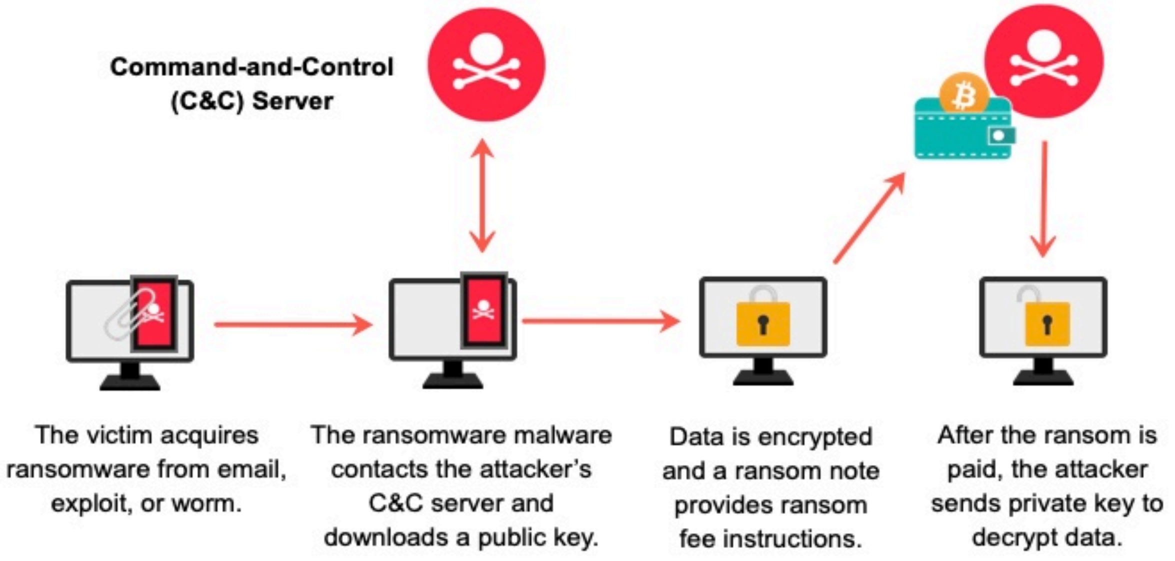
The history of ransomware dates back to 1989, when victims were tricked into paying ransomware developers using the "AIDS virus." After money for the assault was mailed to Panama, the user received a decryption key back. Columbia University researchers Moti Yung and Adam Young first described "cryptoviral extortion" ransomware in 1996. This concept, which originated in academics, demonstrated the development, power, and invention of contemporary cryptography instruments. The first crypto virology attack was presented in 1996 at the IEEE Security and Privacy Conference by Young and Yung. Their malware encrypted the victim's data and contained the public key of the attacker. The virus then requested payment from the victim to the attacker in order for them to decode the asymmetric ciphertext and deliver the decryption key. Over time, attackers have become more inventive by demanding payments that are almost hard to track down, which helps cybercriminals stay anonymous. For instance, victims of the well-known mobile ransomware Fusob are required to use Apple iTunes gift cards as payment methods rather than fiat money like dollars. The rise in popularity of ransomware attacks coincided with the emergence of cryptocurrencies like Bitcoin. Cryptocurrency is a type of virtual money that controls the creation of new units and verifies and secures transactions using encryption techniques. In addition to Bitcoin, victims may be encouraged to utilize other well-known cryptocurrencies like Ethereum, Litecoin, and Ripple by attackers. Organizations in almost every industry have been targeted by ransomware; the attacks on Presbyterian Memorial Hospital are among the most well-known examples.

III. WHAT IS RANSOMWARE?

Malware known as "ransomware" encrypts a user's files and demands payment of a ransom to unlock them. Ransomware attacks often occur when a user opens a malicious email attachment or clicks on a malicious link. The ransomware will begin encrypting the user's data as soon as it is installed on their machine. The individual will subsequently get a notification requesting payment of a ransom to unlock their files.[6]

Attacks using ransomware can cost their victims a lot of money. The requested ransom in certain situations may amount to hundreds or even thousands of dollars. The victim can be forced to pay the ransom in order to recover their files if they don't have a backup of them. Attacks using ransomware are become increasingly frequent. They pose a severe risk to people and companies alike. It's critical to understand the dangers of ransomware and take precautions against these assaults.

IV. RANSOMWARE WORKING MECHANISM


Command-and-Control (C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware malware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends private key to decrypt data.

Source: https://www.hideipvpn.com/vpn/what-are-ransomware-attacks-2022/

A kind of malware known as a ransomware assault involves hackers breaking into a victim's computer and encrypting crucial data. The data are then encrypted, and the victim is requested to pay a ransom—typically in cryptocurrency—to unlock them. Attackers using ransomware have several methods for getting on a victim's computer. Phishing emails are one popular technique.

[6] What are Ransomware Attacks, Hide IPVPN, (Oct 23, 2023, 01:30 PM), https://www.hideipvpn.com/vpn/what-are-ransomware-attacks-2022/

These emails frequently include links or attachments that, if opened, cause the ransomware to be downloaded onto the victim's computer. Malicious websites are another means. Phishing websites with malicious content can be made by hackers and appear authentic. The malware may unintentionally be downloaded onto users' PCs when they visit certain websites.

The ransomware will start encrypting crucial data as soon as it gets onto the victim's PC. The attacker will then send a message to the victim requesting payment of a ransom to unlock the data. Typically, ransom payments are paid with cryptocurrencies like Bitcoin. This is due to the challenge of tracking down bitcoin transactions. The attacker will send the victim a decryption key so they may unlock the encrypted data if they pay the ransom. But there's no assurance that the assailant will truly provide.

V. TYPES OF RANSOMWARES[7]

- **Scareware**

This prevalent kind of ransomware trick consumers by pretending to be a warning message that says the victim's machine has virus on it. These attacks typically take the form of antivirus software that requests payment in order to eliminate malware that doesn't exist.

- **Screen lockers**

The purpose of these programmes is to lock the victim out of their computer so they cannot access any files or data. Usually, a notification appears requesting money in order to unlock it.

- **Encrypting ransomware**

This popular ransomware, often known as "crypto-ransomware," encrypts the victim's files and requests money in return for a decryption key.

- **DDoS extortion**

If the ransom is not paid, the perpetrator threatens to conduct a Distributed Denial of Service (DDoS) assault against the victim's network or website.

[7] What is Ransomware, Proof Point, (Oct 24, 2023, 01:35 PM), https://www.proofpoint.com/us/threat-reference/ransomware

- **Mobile ransomware**

Mobile ransomware, as its name implies, targets tablets and smartphones and demands money in order to unlock the device or decode the data.

- **Doxware**

Though less frequent, this advanced kind of ransomware threatens to release private, explicit, or sensitive data from the victim's machine unless a ransom is paid.

- **Ransomware-as-a-Service (RaaS)**

Ransomware programmes are sold by cybercriminals to other hackers or cyber-attackers who use them to target victims.

VI. METHODS TO PREVENT RANSOMWARE ATTACKS

- **Early detection and reduction of risks**[8]

  Businesses should evaluate their vulnerability to ransomware attacks on a regular basis and take preventative action to lower that vulnerability. This covers procedures like intrusion detection systems, vulnerability scanning, and patch management.

- **Awareness and training for employees**

  Personnel must to be informed on the dangers of ransomware attacks, typical attack avenues, and cybersecurity hygiene recommended practices. To keep staff members informed about the changing danger landscape, organizations should regularly hold training sessions, workshops, and awareness campaigns.

- **Planning and testing for incident response**

[8] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/ransomware-attacks-on-the-rise-in-india-the-need-for-a-global-culture-of-crisis-management

In order to effectively respond to ransomware attacks, organizations should have a thorough incident response plan that defines roles, responsibilities, and procedures. To make sure the strategy works, it should be evaluated often.

- **Strong catastrophe recovery and backup plans**

  Critical data and systems should be regularly backed up by organizations. To make sure the backups are accessible and intact, they should be examined on a regular basis. A clear disaster recovery strategy that describes how to restore systems and data in the case of a ransomware attack should also be implemented by organizations.

- **Cross-functional teams with a collaborative approach**

Companies ought to promote a collaborative and cross-functional teaming culture. Participation in the formulation and implementation of incident response procedures should come from representatives of IT, security, legal, communications, and other pertinent departments.

- **Analysis following the incident and lessons realized**

Organizations should carry out a comprehensive post-incident study following a ransomware attack in order to determine areas for improvement, assess the efficacy of response measures, and comprehend the underlying reasons. The organization's security posture should be strengthened and future assaults should be avoided by documenting and implementing the lessons gained.

- **Periodic assessments and audits of security**

To analyze the efficacy of current security procedures and pinpoint areas for improvement, organizations should regularly perform security audits and assessments. It is possible to hire outside auditors or consultants to offer an objective evaluation of the company's security procedures and recommend corrective actions.

VII. IMPACT OF RANSOMWARE[9]

[9] What is the possible impact of Ransomware, UC Berkley Edu, (Oct 23, 2023, 2:45 PM), https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware

Businesses are also susceptible to ransomware infections, which may have detrimental effects on them in addition to affecting individual individuals.

- loss of private or sensitive data, whether temporary or permanent,
- interference with daily operations,
- monetary losses sustained when restoring files and systems, and
- possible damage to the standing of an organization.

The payment of the ransom simply ensures that the malicious actors will receive the victim's money and, in certain situations, their banking details; it does not guarantee that the encrypted files will be unlocked. Furthermore, the removal of the virus infection is not guaranteed even after files have been decrypted.

VIII. WHAT HAPPENS IF ALREADY AFFECTED?

Disconnecting your computer from the internet should be your first step if you have already fallen victim to ransomware, since this will prevent it from infecting other computers. After that, report the crime to police enforcement and explore what choices are available to you by consulting a technical expert with a focus on data recovery. Don't give up if there aren't any; perhaps in the future, new security technologies will be available to unlock your data. If you have no backups and the encrypted files are precious, it would make sense to pay a ransom in some severe circumstances. However, since WannaCry is involved, individuals should absolutely not pay the extortion. This is due to the fact that victims are reportedly flooding the hackers with demands for the release of their data, and many of those who have paid the ransom are not getting a response.

IX. RANSOMWARE ATTACKS IN INDIA[10]

- Hackers assaulted AIIMS Delhi in 2023, resulting in server shutdowns and interruptions to medical services. Potential compromise of patient data underscores the risks that

[10] Cyber security center of excellence, (Oct 23, 2023, 2:00PM) https://ccoe.dsci.in/7-biggest-ransomware-attacks-in-india/#:~:text=AIIMS%20Attack%3A%20In%202023%2C%20hackers,measures%20to%20protect%20sensitive%20information.

hackers pose to the healthcare industry. The necessity for more robust cybersecurity procedures to safeguard sensitive data was highlighted by this malevolent attempt. The whole healthcare sector was rocked by one of the most recent ransomware assaults in India.

- Assaulting on the power utility systems of Telangana and Andhra Pradesh: Last year, a ransomware assault was launched against the power utility systems of Telangana and Andhra Pradesh, two southern Indian states. All servers were brought down by the dangerous virus until the issue was fixed. The virus propagated swiftly since the two states' computer systems were connected, which resulted in the total shutdown of every system.

- Attack by UHBVN Ransomware, Uttar Haryana Hackers breached the computer systems of Bijli Vitran Nigam, a power utility in Haryana, taking customer billing information with them. In exchange for the returned stolen material, the attackers wanted a huge ransom payment of Rs. 1 crore, or $10 million.

- WannaCry: Over two lakh computer systems were impacted by the WannaCry ransomware outbreak. India's banks as well as a few businesses in Tamil Nadu and Gujarat were affected by this ransomware assault.

- Mirai Botnet Malware Assault: The Mirai botnet malware assault was another startling ransomware incident that occurred in India. This botnet malware especially targeted residential routers and Internet of Things (IoT) devices, impacting 2.5 million IoT devices, many of which were Indian computer systems. Unpatched vulnerabilities were utilised by the virus to gain entry into systems and networks.

- Petya: India is now the tenth country to have been affected by the ransomware attack Petya as a result of the latest attack. One of the terminals of India's main seaport experienced work interruptions and a computer lockdown as a result of this ransomware assault.

- BSNL Malware assault: Almost 2,000 broadband modems were affected by a serious malware assault that targeted the state-owned telecom provider BSNL. Following the Telecom Circle malware assault, sixty thousand modems stopped working.

X. LEGAL REMEDIES AVAILABLE IN INFORMATION TECHNOLOGY ACT 2000[11]

- **Tampering with Computer Source documents – Section 65[12]**

  Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both

- **Hacking with Computer Systems, Data Alteration – Section 66**

  If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

- **Publishing obscene information – Section 67**

  Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with

[11] Shriji Pandey, iblog Pleaders, (Oct 23, 2023, 01:45PM), https://blog.ipleaders.in/ransomware-attack/

[12] Information Technology Act 2000

imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

- **Un-Authorised access to protected system – Section 70**

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Explanation. –For the purposes of this section, ―Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

- **Breach of Confidentiality and Privacy – Section 72**

Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

- **Publishing false digital signature certificates – Section 73**

  (1) No person shall publish a [electronic signature] Certificate or otherwise make it available to any other person with the knowledge that– (a) the Certifying Authority listed in the certificate has not issued it; or (b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a [electronic signature] created prior to such suspension or revocation. (2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to one lakh rupees, or with both.

XI. CONCLUSION

In conclusion, the rise of ransomware attacks in the digital age has posed a significant threat to individuals, organizations, and even critical infrastructure. This evolving landscape of cyber threats demands a multi-faceted approach to combat and mitigate the risks associated with ransomware. As highlighted in the extensive discussion provided, there are several critical points to consider.

First, the historical evolution of ransomware demonstrates the ever-growing sophistication and adaptability of cybercriminals. The utilization of cryptocurrency as a means of ransom payment and the diverse methods of intrusion reveal the need for robust cybersecurity measures and continuous vigilance. Preventing ransomware attacks demands a proactive approach, including early risk assessment, employee awareness and training, incident response planning, robust backup and recovery systems, and continuous security assessments. Collaboration across various departments within an organization is vital to effectively respond to such threats.

Furthermore, the impact of ransomware extends beyond monetary losses, with potential damage to an organization's reputation and the loss of sensitive data. It is essential to consider the legal remedies available, such as those outlined in the Information Technology Act 2000, to hold cybercriminals accountable. In light of the ransomware attacks in India and their far-reaching consequences, it becomes evident that strengthening cybersecurity infrastructure is of paramount importance. As technology advances, so too do the tools and methods employed by cybercriminals, necessitating ongoing adaptation and resilience in the face of these ever-present threats.

In essence, ransomware is a pervasive and evolving cybersecurity concern, demanding collective efforts, awareness, and preparedness to mitigate its impact on society. The lessons learned and actions taken today will play a crucial role in safeguarding the digital landscape of the future.