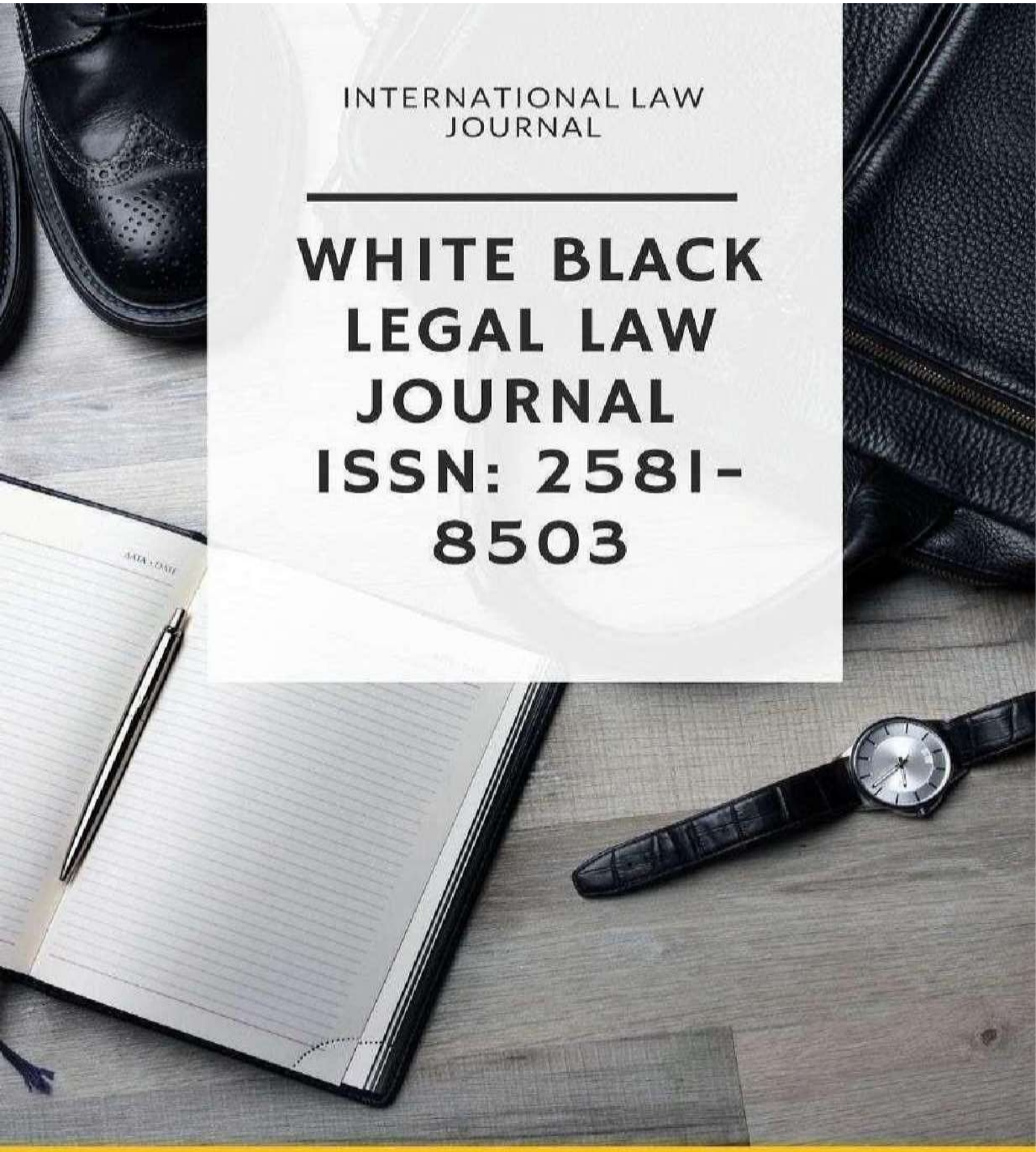

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

UNRAVELING THE DIGITAL ENIGMA: A COMPREHENSIVE ANALYSIS OF CYBER RANSOMWARE TRENDS

AUTHORED BY - ANAGHA MOHAN & T H ALOK NARAYANAN

ABSTRACT

Ransomware is a worldwide cybersecurity menace that has experienced fast growth due to its significant cost-effectiveness and lack of punishment. The proliferation of technology and a wide range of technical capabilities have significantly contributed to the rise in ransomware attacks. In recent years, ransomware has emerged as a prominent fraudulent scheme that poses a significant threat to enterprises. The consequences of a successful attack are significantly broader than solely the financial expense of the ransom. Organizations may experience decreased productivity, loss of business, consumer discomfort, and the potential irreversible loss of data. A ransomware attack constitutes a violation of the fundamental right to personal liberty as provided by the Indian Constitution. Currently, India lacks a comprehensive extradition statute to address cybercrimes. This article examines the rise of cybercrime, the reconceptualization of cybercrime, recent instances, and measures to decrease the impact of ransomware, the importance of cyber insurance and the future of cyber ransomware.

INTRODUCTION

Technology and internet access have had a significant impact on society, improving the efficiency and interconnectedness of individuals. They have revolutionized our lives, becoming them indispensable for our everyday existence. Nevertheless, they have also given rise to the emergence of transnational criminal operations, which are deeply concerning because of their cross-border and clandestine characteristics. The proliferation of cybercrimes is a global phenomenon driven by the growth of internet, where individuals and organizations illicitly collect sensitive information for financial, political, or personal motives. The crimes can be categorized into three primary classifications: cyber crimes targeting individuals, organizations, and society as a whole, based on the targeted groups. Data of a victim is held hostage by ransomware, a type of cybercrime that uses

encryption. It employs encryption techniques to safeguard important data, thereby restricting unauthorized access to files, databases, and applications. The ransom is requested in exchange for granting access. Ransomware has the ability to propagate over networks and specifically attack database and file servers, which has the capacity to completely incapacitate an entire enterprise. Ransomware assaults inflict severe repercussions on their targets, encompassing tiny enterprises, major businesses, and even entire nations. Highly targeted industries such as energy, healthcare, and transportation have significant pressure to restore their systems, making them vulnerable to attacks that can cause widespread repercussions. Although most assaults have been perpetrated by criminal entities, there have also been instances where rogue nation-states have conducted such attacks with the intention of causing disruption in countries they perceive as unfriendly or to conceal their espionage operations.

EMERGENCE OF CYBER CRIMES

The emergence of cybercrime can be attributed to the expansion of the internet, particularly with the introduction of email in the late 1980s and internet browsers in the 1990s. Social media platforms in the early 2000s facilitated the occurrence of identity theft and financial fraud. Transnational criminal groups are currently focusing on individuals who have an internet presence, employing well-established techniques. The origins of cybercrime can be traced back to phone phreaking, an illicit practice that arose in the 1970s with the aim of obtaining telecommunications services at no cost or at a discounted price. Ransomware attacks have emerged as a significant worry, as fraudsters demand bitcoin ransoms from companies in return for restoring access to the cryptocurrency.

The progression of human civilization has resulted in the emergence of cyber crimes, as cyber criminals adjust their strategies to match technological advancements. Criminals possessing sophisticated technology skills tend to favor conducting their activities in the digital domain because of the anonymity it affords and the potential for substantial financial profits. On a global scale, there has been a consistent increase in the reported incidents of cybercrimes. This rise can be attributed to the growing number of individuals connected to internet networks, which in turn makes them more vulnerable to dangerous software, viruses, and phishing attempts.

During the 1980s, email communication became commercially feasible and effective, but, personal computers were heavily targeted by spam. Perpetrators employed deceptive identities to get personal

data or commit identity theft. During the 1990s, there were sporadic outbreaks of viruses that caused significant damage to governments, organizations, and individuals. Web browsers served as channels for delivering malware to victims' systems.

Throughout history, the utilization of computers has posed risks to persons that engage with the internet. The emergence of electronic crimes is influenced by legislation and the global nature of internet, enabling potential offenders to commit crimes discreetly across many geographical areas. In order to tackle this issue, nations must cooperate to adopt uniform cyber laws and efficiently combat cyber threats originating from remote areas.[1]

OVERVIEW ON RANSOMEWARE ATTACKS

Ransomware is a form of malicious software that employs encryption to extort a payment in exchange for a victim's data. It secures sensitive information by encrypting files, databases, and software. The ransom is requested in order to grant access. Ransomware has the ability to instantly halt large enterprises by propagating over networks and attacking file servers and databases. It produces billions of dollars in illicit payments made by cybercriminals and causes enormous harm to businesses and governments.

It is a form of malicious software that use asymmetric encryption to encode and decode files. The assailant creates a distinct set of public-private keys, utilizing the private key to decipher files saved on the assailant's server. Without the private key, file decryption is practically impossible and is only feasible once the ransom money is paid by the victim. Ransomware can be disseminated by spam mail campaigns or focused assaults, and necessitates a form of attack to establish its existence on an endpoint. Following a triumphant breach, the virus proceeds to execute a malevolent binary on the compromised machine, scanning and encrypting valuable assets such as Microsoft Word documents, photos, and databases. The ransomware can also utilize system and network weaknesses to propagate to additional computers and organizations. After the data are encrypted, the user is prompted to pay a ransom within a timeframe of 24 to 48 hours in order to decode them. Failure to comply may result

[1] Sauvik Acharjee, “The Evolution of Cyber Crime: An Easy Guide”(u-next,13-02-2021) <https://u-next.com/blogs/cyber-security/evolution-of-cybercrime/#:~:text=Although%20there%20was%20cyber%2Dcrime,continuum%20came%20in%20the%2090s.>accessed 28 March, 2024

in permanent loss of the files.

Ransomware attackers frequently request cryptocurrency because they are subject to less regulation and are more challenging to monitor under Anti-Money Laundering rules. The decentralized and anonymous nature of these digital currencies complicates the implementation of "know Your Customer" and other customary customer identification processes. Ransom attempts impose time limits, and if victims fail to meet them, attackers may escalate the ransom amount or erase the encryption key. Remitting the ransom may not terminate the operation, as certain programs have the capability to contaminate further network devices or infect individuals with malicious software such as Trojans.

According to SOPHOS, 46% of ransomware-encrypted firms paid ransoms in 2021, with 11% paying a sum of at least one million dollars. These funds contribute to the criminal organization that supports ransomware, so encouraging more assaults. Nevertheless, providing compensation to each individual affected by a crime is a financially logical decision as it transfers the burden of expenses and mitigates the adverse impact on society.[2]

The European Union Agency for Cybersecurity (ENISA) has identified ransomware's rising frequency and complexity as a significant danger to enterprises across all industries. The agency asserts that we are currently experiencing the "golden period of ransomware," which is considered a matter of utmost national security importance, since its full impact has not yet been realized.

RECONCEPTUALIZING THE OFFENSE OF RANSOMWARE

As Russia prepared to start its war of aggression against Ukraine, President Biden made a mistake when he talked about the difference between Russia's "minor incursion" and "more severe invasions." The international society reacted with dismay at this, as aggressiveness is universally acknowledged as a criminal act. A war of aggression is prohibited under UNGA Resolution 3314 as a crime against international peace, and no territory gained or benefit gained as a result of aggression is accepted as legitimate. Therefore, any form of violence cannot be justified by any political, economic, military,

[2] Amit Gopal Thakre, “CYBER CRIMINOLOGY & CYBER FORENSICS” (2020) & lt;https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001742/M027880/ET/1521179572E-textCybercrime-HistoryandEvolution.pdf>accessed on 7 April 2024

or other factors. Aggression is inherently wrong and is characterized by being fundamentally illegal. There are three distinct categories of these crimes: maritime piracy and the slave trade, the act of taking hostages and hijacking aircraft, and the organized criminal activities that span multiple countries and involve terrorism. Crimes spanning three generations can be classified into three categories: maritime piracy and slave trade, hostages-taking and airplane hijackings, as well as organized transnational terrorist activity.

Maritime piracy, taking hostages, aerial hijackings, organised international crime, terrorist activity, especially ransomware pose risks to the domestic shipment of commodities, services, and individuals. These crimes depend on the legal systems of individual countries to punish the perpetrators. They have elements that go beyond national borders, involve actions that violate fundamental human rights and universal principles of freedom, can be carried out with minimal expenses, and cause widespread suffering due to the inequitable nature of the attacks, which greatly shocks the international community.

Hence the illegality of ransomware on an international scale can be attributed to the three preceding iterations, therefore establishing it as the fourth iteration in the digital era of international criminalization and prohibition of individuals deemed as "enemies of humanity." The collective efforts of the global community for the suppression of these crimes showcased the influence and extent of the global legal system. By employing time travel, ransomware protection measures can be firmly linked to other established frameworks. Studying previous and current instances of crimes that are considered enemies of all mankind and are universally condemned is essential for regulators. This allows them to gain valuable knowledge about emerging crimes that have similar origins.[3]

TYPES OF RANSOMWARE

- **Locker ransomware** : is a version that infiltrates computer systems via social engineering and compromised credentials, preventing users from accessing them until a ransom is paid.
- **Crypto ransomware**: is a prominent and comprehensive type of ransomware that encrypts data on computers and requests a ransom in return for a decryption key. The computer

[3] Asaf Lubin , "The Law and Politics of Ransomware" (2022) Indiana University Maurer School of Law (Vanderbilt journal of transnational law) vol 55 issue 5

malware has the ability to infiltrate shared, connected, and cloud drives and propagates itself by means of fraudulent emails, websites, and downloaded files.

- **Scareware:** is a way for perpetrators to trick people into thinking their devices have malware on them. The scam typically employs pop-up windows that display scary messages, frequently pressuring victims to make a payment or buy software in order to resolve the infection issue. Occasionally, the software itself may harbor malware, which can surreptitiously pilfer data and propagate other ransomware.
- **Extortionware**: is a sort of malicious software that takes data and threatens to publish it unless a ransom is paid. It is also referred to as leakware, doxware, and exfiltrationware. Extortionware increases the pressure on victims to pay the ransom before the material is made public.
- **Wiper malware**: alternatively referred to as wiperware or data wipers, deletes data from the systems of its victims, similar to ransomware. The objective is not to achieve financial profit, but rather to eradicate incriminating evidence, undermine a target, or disrupt operations in the context of a cyber conflict. A multitude of wiperware variants utilize methods commonly associated with ransomware.

THE MOST NOTABLE RANSOMWARE ATTACKS

WANNACRY ATTACK, 2017

In May 2017, the highly devastating ransomware attack known as WannaCry affected a total of 7,000 systems and 110,000 unique IP addresses within a span of two days. This attack had a significant impact on multiple businesses, including Renault and Honda. The malware is delivered through a deceptive email and rapidly spreads like a self-replicating program, taking advantage of the vulnerability in the Windows Server Message Block (SMB) protocol. The assailants requested a sum of $300 in bitcoins to be paid within a timeframe of three days, and subsequently raised the ransom amount to $600 over a span of six days. WannaCry specifically targets file extensions commonly associated with office documents, compressed files, multimedia files, databases, as well as files used by graphic designers and photographers. The malware inserts itself into a randomly named directory within either the 'ProgramData' or 'C:\Windows\' folder.

TESLACRYPT, 2015

TeslaCrypt, a widely-known ransomware that was first identified in 2015, has gone through several iterations, with each release incorporating novel functionalities and tactics to avoid detection. The strategy initially involved employing social engineering techniques to deceive consumers into clicking on phishing links and incorporating harmful files. The malware was disseminated via exploit kits such as Angler and Nuclear, which take advantage of vulnerabilities in widely-used web technologies such as Internet Explorer, Adobe Reader, Microsoft Silverlight, and Oracle Java. TeslaCrypt employs encryption algorithms to secure user files and thereafter demands a payment of $500 in bitcoins as a ransom in exchange for decrypting them. Curiously, the individuals responsible for TeslaCrypt made the master decryption key available to the general public in 2016, therefore terminating their business model.

NOTPETYA,2017

A ransomware epidemic that affected businesses around Europe and was first detected in Ukraine on June 27, 2017, is estimated to have cost $10 million. The infection propagated via MeDoc, a Ukrainian accounting program, by exploiting update servers and creating a counterfeit update patch. NotPetya caused the victims' machines to restart, encrypted the master file table of the hard drive, and made the master boot record unable to function. The perpetrator illicitly obtained the victim's Windows login information and the specific location on the physical drive. Upon infecting a single computer, the malware proceeds to scan the immediate network and then infects all other machines connected to it. This particular attack stands out as one of the largest and most destructive in the history of ransomwares.[4]

CYBER RANSOMWARE NEGOTIATIONS

Cyber ransomware discussions are an essential component of addressing a cyber assault, in which a hostile individual encrypts or steals valuable information and demands payment in exchange for its return. The negotiating process commonly entails communication between the victim, frequently a company or organization, and the ransomware offenders, who are normally unidentified hackers aiming to obtain financial profit. The conversations are intricate and sensitive, as both parties

[4] " 5 Biggest Ransomware In History" (Swiss Cyber Institute, 2020) <https://swisscyberinstitute.com/blog/5-biggest-ransomware-attacks-in-history/#1_WannaCry> accessed on 5 April 2024

maneuver through the unpredictability of the circumstance and the possible repercussions of their decisions.

During a cyber ransomware negotiation, the victim must thoroughly evaluate their alternatives and make a deliberate choice between engaging with the attackers or seeking help from law enforcement or cybersecurity experts. Various factors, including the monetary worth of the encrypted data, the organization's reputation, regulatory obligations, and the probability of data recovery without ransom payment, all influence the decision-making process. The victim should also evaluate the reliability of the attackers and confirm their ability to decrypt the data upon payment of the ransom.

Effective communication is crucial in cyber ransomware negotiations, as it enables both sides to share information and discuss terms in a manner that reduces the likelihood of misunderstandings and miscommunication. The victim may be required to create a means of communication with the attackers, typically via anonymous email accounts or chat platforms, in order to discuss payment specifics, decryption keys, and any other negotiating terms. Effective and succinct communication is crucial for achieving a mutually agreeable solution and guaranteeing the secure recovery of data.

The process of determining the ransom amount is a vital component of cyber ransomware discussions, as the victim must carefully consider the financial implications of paying the ransom in relation to the worth of the encrypted data and the potential harm to their reputation. The assailants may initially request a substantial sum of money as ransom, but by engaging in negotiations, the target may have the opportunity to reduce the amount or arrange a more feasible payment schedule. It is crucial for the victim to comprehend the potential dangers and advantages of making the ransom payment and to carefully consider these variables while engaging in the negotiating process.

During cyber ransomware talks, it is crucial for all parties to uphold a certain level of trust and goodwill to ensure a smooth procedure and successful data recovery. The victim may be required to prove their readiness to pay the ransom in order to secure the safe release of their data, while the attackers must fulfill their part of the agreement by giving decryption keys or other methods to access the encrypted material. Establishing trust in high-stakes situations can be challenging, but fostering open communication and openness can facilitate the development of rapport between the two parties.

Legal factors are also relevant in cyber ransomware discussions, as both the victim and the perpetrators need to address the legal consequences of their acts. Providing monetary compensation to cybercriminals could be considered unlawful in many legal countries, and individuals who fall victim to such attacks may encounter regulatory repercussions for their involvement with the perpetrators. In addition, law enforcement agencies may participate in the negotiating process, offering direction and assistance to the victim while endeavoring to discover and apprehend the culprits. Navigating the delicate balance between legal obligations and ethical considerations is a complex task in the realm of cyber ransomware negotiations.[5]

RECENT INCIDENTS OF RANSOMWARE ATTACKS

ION Cleared Derivatives RANSOMWARE ATTACK, 2023

ION Cleared Derivatives, a subsidiary of ION Markets, experienced a ransomware assault on January 31st, 2023, resulting in the disruption of its systems. As a result, finance companies were compelled to manually verify trades and had difficulties in submitting data. It is recommended that large trading businesses make initial estimates of commodity prices and then update them later to prevent any delays in reporting.

COSTA RICA RANSOMWARE ATTACK,2022

In 2022, Costa Rica experienced two instances of ransomware attacks, resulting in a national emergency due to the severe disruption of essential systems. The initial assault focused on the digital tax service and IT systems associated with customs control, resulting in the disruption of 800 servers and the compromise of many gigabytes of data within the finance ministry. The import and export activities between countries were severely hampered, resulting in projected daily losses ranging from $38 million to $125 million. The ransomware organization known as 'Conti' has acknowledged their involvement and is demanding a payment of $10 million in order to avoid the release of sensitive data. The second assault was aimed at the Costa Rican Social Security Fund, resulting in the disruption of more than half of the servers and compelling doctors to reschedule their appointments. The second attack has been attributed to a group utilizing the 'HIVE' ransomware, which has certain connections to Conti.

[5] Pavan Duggal,Cyber Law - An exhaustive section wise Commentary on The Information Technology Act(Third Edition,2023)

AIIMS DELHI CYBER ATTACK,2023

The AIIMS Delhi facility had a cyberattack in 2023, resulting in the deliberate shutdown of servers and the disruption of healthcare services. The security of patient data was potentially breached, highlighting the inherent risks associated with cyberattacks targeting the healthcare sector. This latest event in India highlights the necessity for more robust cybersecurity measures.

IMPORTANCE OF CYBER INSURANCE

Cyber insurance is essential for reducing the financial risks linked to cyber ransomware attacks. In the current digital environment, characterized by the widespread presence of ransomware, businesses and organizations are consistently exposed to the danger of cybercriminals compromising their data and extorting them. Cyber insurance offers financial protection and assistance to these organizations in the case of a ransomware occurrence, serving as a safety net.

A primary advantage of cyber insurance in addressing cyber ransomware is its provision of coverage for ransom payments. In the event of a ransomware attack, cyber insurance policies might provide financial coverage for the expenses incurred in paying the ransom requested by hackers to decrypt encrypted data. Providing financial aid to enterprises dealing with extortion demands can serve as a crucial support, allowing them to regain access to their data and restore normal activities without having to shoulder the entire financial responsibility.

In addition, cyber insurance policies frequently provide coverage for other expenses associated with a ransomware attack, including forensic investigations, legal bills, public relations charges, and losses incurred due to business interruption. This extensive coverage guarantees that firms possess the essential tools to handle the consequences of a cyber event and reinstate normalcy to their operations.

Businesses can protect themselves from the financial consequences of a ransomware attack and show their dedication to managing cybersecurity risks by investing in cyber insurance. Cyber insurance offers both financial protection and encourages firms to adopt strong security measures and protocols to reduce the risk of cyber threats, hence promoting a proactive cybersecurity approach.

LEGAL FRAMWORK FOR RANSOMWARE ATTACKS

Ransomware attacks are not significantly restricted by international law, which includes regulations on sovereignty, nonintervention, and the prohibition of the use of force. The reason for this is that there are stringent criteria that need to be met in order to breach these regulations, and the majority of illegal ransomware actions do not match these criteria. The majority of ransomware attacks do not meet the criteria for uses of force as outlined in Article 2(4) of the United Nations Charter, as they must be on par with a non-cyber physical use of force. Nevertheless, the majority of ransomware attacks primarily result in financial losses and have a restricted impact. Furthermore, the majority of ransomware assaults do not contravene the customary prohibition on interference, as stipulated by the International Court of Justice in Nicaragua. This ban specifically pertains to interventions that are carried out under coercion. Ransomware assaults, which seldom qualify as coercive intrusions into the exclusive domain of the state where the target is located, are not subject to this prohibition. During the majority of ransomware attacks, the victims are typically private persons and enterprises, and there is no compulsion for any government to intervene.

Ransomware is a type of cybercrime that causes severe disruptions in political, social, or economic spheres, resulting in serious consequences. Even if a public entity is compelled to pay the ransom, it does not qualify as a coercive intervention because the authority to make the decision to pay is not within their jurisdiction. In order for ransomware to be classified as an internationally wrongful act, it must be proven that a state is responsible for it, supported by substantial evidence. However, this is difficult to establish due to the unclear connection between these criminal groups and the countries in which they operate. Moreover, there is a lack of consensus among states over the precise extent of sovereign equality in cyberspace, which diminishes the effectiveness of this theory in effectively limiting the impact of ransomware. The philosophy currently lacks the ability to effectively limit the impact of ransomware. The issue of whether ransomware can be considered a suitable means of violating sovereignty is intricate, as it involves challenging problems regarding interpretation and implementation that do not have a global agreement. The current international legal regulations concerning cyberspace are still in their early stages and developing. States have been reluctant to give up their ability to act by implementing or promoting particular international laws that could restrict ransomware activities. This has resulted in an apparent absence of laws in the realm of cyber activity, where all offensive and defensive actions are assumed to be legal, even if they prevent the regulation of enemies' use of these tools to cause harm. While a limited number of very destructive and

sensational ransomware assaults may be subject to the laws against the use of force, intervention, or violation of sovereignty, the bulk of ransomware incidents will not be covered by international regulations. Specific regulations may be developed to govern extremely malicious ransomware attacks, such as the UN Group of Governmental Experts (UNGGE), with a focus on prohibiting ransomware attacks on key infrastructure.

The United States has implemented laws and regulations to address the issue of cyber ransomware. One such step is the Computer Fraud and Abuse Act, which specifically outlaws unauthorized access to computer systems. The Federal Trade Commission is responsible for enforcing legislation related to the protection of data and for conducting investigations into occurrences involving ransomware. The Cybersecurity and Infrastructure Security Agency offers materials and guidance to help prevent and respond to ransomware attacks. The Department of Justice engages in the prosecution of cybercriminals who are implicated in ransomware attacks. The Cybersecurity Information Sharing Act promotes the exchange of information to effectively address and counteract ransomware threats. In addition, firms are required to adhere to state data breach notification rules and regulations related to their industry. The objective of these endeavors is to protect data and mitigate the consequences of cyber ransomware in the United States.

In the UK, cyber ransomware is governed by the Computer Misuse Act 1990, which criminalizes unauthorized access to computer systems. The Data Protection Act 2018 sets standards for protecting personal data from ransomware attacks. The National Cyber Security Centre provides guidelines and support to combat ransomware threats. Additionally, the Cyber Security Breaches Survey helps assess and address cybersecurity risks. Law enforcement agencies, such as the National Crime Agency, investigate and prosecute ransomware incidents. Organizations must comply with the GDPR for data protection.[6]

In India, Cyber Ransomware is governed by the provisions of IT ACT, 2000:
Section 43 of the IT Act outlines the penalties and compensation for unauthorized access or damage to a computer, computer system, or network. It covers actions such as accessing a computer without

[6] M. Robles-Carrillo and P. García-Teodoro, "Ransomware: An Interdisciplinary and Technical Approach" (2022) Hindawi < https://www.hindawi.com/journals/scn/2022/2806605/> accessed on 3 April 2024

permission, downloading or copying data, introducing viruses, causing damage to computers or networks, disrupting access, providing assistance for unauthorized access, tampering with billing, altering or deleting information, and stealing or altering computer source code with the intention to cause harm.

Computer source code refers to a compilation of programs, commands, design, layout, and program analysis related to a computer resource. It is legally mandated to be preserved or upheld according to the current laws. Individuals who deliberately hide, damage, modify, or induce others to hide, damage, or modify this code are subject to a maximum prison sentence of three years, a fine of up to two lakh rupees, or both. It is covered under Section 65 of the Act.

Section 66 of the Information Technology Act, 2000 pertains to computer-related offensescommitted by individuals who engage in dishonest or fraudulent conduct as defined in Section 43. The terms "dishonestly" and "fraudulently" are defined in the Indian Penal Code (45 of 1860). The penalty prescribed under section 66 is a maximum prison sentence of three years, a fine of up to five lakh rupees, or both.

FUTURE OF CYBER RANSOMWARE

Modern cybercriminals are employing sophisticated technology and strategies to intentionally disrupt computer systems, blackmail victims, and avoid conventional security measures. An example of a potential danger is ransomware that utilizes artificial intelligence (AI) capabilities. This type of ransomware has the ability to process large quantities of data, adjust its tactics to overcome security barriers, and create personalized ransom demands tailored to the victim's characteristics. This highly sophisticated and adaptable ransomware presents a substantial danger due to its ability to constantly grow and surpass conventional defense methods.

Quantum ransomware, created in response to the emergence of quantum computing, has the ability to encrypt data at far faster speeds and with greater complexity compared to conventional encryption techniques. This presents a significant issue for cybersecurity experts as it makes existing encryption

measures ineffective and necessitates the development of new strategies to neutralize its power.[7]

Cloud-based ransomware attacks pose a growing threat by specifically targeting cloud storage services and infrastructure. These attacks involve encrypting data stored in the cloud and causing widespread disruption to operations. In order to effectively counteract these emerging ransomware threats, cybersecurity experts need implement sophisticated security measures and technologies, such as strong encryption protocols, multi-factor authentication, threat intelligence tools, and AI-powered security solutions. Implementing proactive defense methods, such as conducting regular cybersecurity assessments, providing comprehensive employee training programs, and developing incident response plans, is crucial in order to be well-prepared and able to respond promptly and efficiently to ransomware events.

CONCLUSION

Ransomware has become a prominent cyber security concern in recent years. From the criminal's viewpoint, the Internet is a substantial boon, not only for ransomware, but also for malware in general. The Internet has facilitated the emergence of a criminal ecosystem that enables the creation, distribution, and financing infrastructure for malware. With the increasing complexity of cyberattacks, it is necessary to adopt a comprehensive and targeted approach to cybersecurity and cyber resilience. The Information Technology Act is a measure aimed at safeguarding the data and sensitive information that is held with online intermediaries. The legislation provides a range of provisions that offer advantages to the citizens and safeguard their data from potential misuse or loss. There is a substantial security risk associated with ransomware, and it is anticipated that this risk will continue to increase as more devices are connected to networks. When it comes to preventing oneself from being impacted by malicious software, preventative steps are absolutely necessary, and fostering shared responsibility is absolutely necessary in order to battle ransomware. Behavior on the part of users and training are essential components in the process of preventing infections in businesses, organizations, and individuals. Ransomware may be fought with a variety of tools, the most important of which are education, response measures, prevention strategies, and being vigilant. The conclusion is that ransomware is a rising worry that calls for the development of creative

[7] Anastasiia Yevdokimova, “What is Quantum Ransomware?” (SOCPRIME,23-07-2023) <https://socprime.com/blog/what-is-quantum-ransomware/>accessed 2 April, 2024

solutions as well as the continual monitoring of activities in the file system and registry. The implementation of preventative measures, the promotion of shared responsibility, and the implementation of proactive approaches are all ways in which we may assist in protecting ourselves and our networks from being attacked by ransomware.[8]

[8] R.Thanmayi,"Ransomware: A Cyber Threat to the Business Community"(2022),Vol 5 Issue 6,<https://www.ijlmh.com/wp-content/uploads/Ransomware-–-A-Cyber-Threat-to-the-Business-Community.pdf>,accessed on 30 March,2024