

## The Danger of Ransomware Threats: A Comprehensive Analysis

Pedro Brandao, Full Professor ISTECS, Assistant Professor –  
Universidade Lusíada de Lisboa - FCEE  
Isabel Mendonça, Computer Science Degree Student, Universidade  
Lusíada de Lisboa - FCEE

**Abstract:** *Ransomware is a type of threat to computer security which involves a program that, when executed, holds a computer system or the user's data ransom by making them inactive, encrypted, and hidden from the user. After the user's data is completely encrypted, the attacker will demand a ransom from the victim in exchange for the decryption key. The victim has to obtain and send the payment to the attacker within the given period, or the key will be lost forever. There have been numerous ransomware attacks targeting ordinary users, companies, public sectors, and even high profile medical facilities, to name a few instances [1].*

*What makes ransomware a dangerous threat is the different types that can be built: including file-encrypting, data-hiding, and lockscreen ransomware. Each of these types is designed to target different aspects of a computer system, and they are typically delivered through various methods as well. This makes it difficult for an average user to understand how ransomware works and how to protect against it. Additionally, since the dawn of Bitcoin, these attacks have spiked. Prior to this modern advancement, attackers needed to ask for bank information, which left a traceable paper trail; therefore, criminals were more afraid of being caught.*

*There is always something to take away from a ransomware incident whenever it happens. It is important to think ahead and do the R&D to analyze and understand the threat, know how it infects the system, what kind of ransomware was used, where are the encrypted keys stored, can the attack be stopped at any point, etc., while also being careful about how high-risk fields operate. No organization would ever want to lend itself liable to a lawsuit because of negligence due to insufficient security measures and potential harm to other third parties connected to that particular environment.*

**Keywords:** *Cybersecurity, Ransomware, Malware.*

### 1. Introduction

One of today's most noteworthy topics of interest in the information technology realm involves the up-and-coming threats of ransomware. With such a high frequency, these provocative predicaments are sending numerous organizations and individuals into a calamitate event. As an outcome, this commentary will shed a light on the meaning of ransomware, its alarming statistics, the motivation behind the attacks, and numerous countermeasures to apprehend this growing affinity. It is of

prodigious importance that everyone becomes cognizant of ransomware and what needs to be executed in order to sidestep the catastrophic damage these semblances of malware can cause.

Ransomware's presence on computer systems is an intimidating deficiency that businesses and individuals face on a daily basis. This depiction of malware grips the victims' information and coerces them to make a demanded payment. When the payment is rendered, the data is then decrypted and assigned back to the original possessor. Although, if the payment is not made in a timely manner, the data will be irretrievably deleted. The safety measures of acquiring and retaining the confidentiality, integrity, and accessibility of data can certainly be an apparent factor in which even the most shielded institution can succumb to these defeats due to their obscure peculiarities, their capability and audacity to customize versions having no record from prior ends, and their effectiveness of being difficult to block. Close to 68% of all incidents that involve ransomware require the financial gratification from the prey, whereas the remaining 32% of theatre goers opted to endure and accept the fabricated ending convoked to their information [1]. The great proliferation of the risk provides the ransomware developers a substantial gain without exerting plentiful effort on their behalf. Actually, numerous utilities can be flexed to generate ransomware websites in which the malice can be engendered without encumbering its creator. Furthermore, the most recent variant of this scoundrel displays the prey's confidential matters as an intimidation tactic in the event that they do not consummate the tariff.

## **2. Understanding Ransomware**

Ransomware is a kind of malware infecting end users' devices and restricting them from using it. This malware influences people by different means like: affecting the OS, downloading harmful scripts from malicious websites, or block the program by encrypting its files. People initially have vague information about this kind of malicious infection, but at the same time understanding the fundamentals is essential in order to forestall early threats. This paper elicits the fundamental concepts of ransomware from a variety of perspectives, forming a comprehensive understanding to analyze this new and formidable threat [1].

A clear definition of ransomware is set to commence, followed by operation outlines on how ransomware works. Understanding the purpose and modes of ransomware is crucial knowledge used by other societies in shaping anti-ransomware policies or developing victim recovery approach. In the meantime, differentiations of this new cyber threat are addressed on various dimensions. First, ransomware categorizations by restoration abilities are elaborated, highlighting the disparities between encryptor ransomware and locker ransomware. The inherent disparities between these two kinds of ransomware in implementation encourage differentiations on the OS-level and file-level operation. On the OS-level, differentiations focus on the way they block the user's interface; while on the file-level, comparison is made on how they restore the original data. Second, the evolutionary paths of ransomware since 1989 are disclosed,

focusing on the trend transitions from earlier-to-modern and non-to-CBI-to-CBI. The earlier ransomware era inspires understanding of ransomware-inflicting e-mails, while the encounter of modern ransomware era urges attentions to the proportions, distribution, and geoplots of ransomware attack. Third, the fundamental disparities of ransomware to existing prevalent malwares like botnets and worms are elucidated, highlighting the importance of user interactions and demand patterns in various phases. Understanding these characteristics aids developers or security researchers to identify nascent threats timely, as the behaviors in each victim phase are profoundly rooted in certain operating logics, resulting distinctive footprints between ransomware and prevalent malwares.

### **3. Technical English**

Ransomware, a fusion of ransom and software, presents the colossal and growing threat to organizations and endpoint users. Ransomware is the well-designed malicious software program that aims to attack the targeted systems and hold users as a hostage to restrict accessing their device. Alternatively, it could encrypt user data, making the victim spend hundreds or thousands to retrieve files or data [1]. Typically, ransomware commonly utilizes malware, and mostly, Trojan forms seek out to bypass and infect the planned system software. Certainly, this infected software program emerged such as booby-trapped emails, and once it was executed on the operating system, the system froze, displaying instruction for recovered data or bypass control access state. The basics of ransomware involve

the attackers encrypting critical files, and within the given timeframe, the victim is asked to pay the ransom or lose the files forever.

In practice, ransomware consists of two major types. The first, lockers, prevents the user from purchasing the entire system; rather, only the malicious program presents the graphical user interface (GUI) or message within the system. The blocker message takes over the system, making it impossible to access the current, and limits users with trivial instructions. The second type is the growing crypto-ransomware, which has different operational and device tactics. Crypto-ransomware maliciously encrypts the user files and requests payments to decrypt the files, rather than finishing. Scareware, disguising as the triangle anti-virus and providing misleading diagnostic messages, may not actually compel the open system to be at risk. Doxware ransomware, similar to the crypto-ransomware, encrypts user data, but threatens to release private or sensitive information if payment is not completed. Cerber ransomware is known as ransomware-as-a-service (RaaS) and actively upkeeps with new and untalented variations on malware as well as the customer service facilities. Tonsee, the remarkable Android Trojan, infects the victim and switches the device seeking the user overall control. Jigsaw, an older caution, pays the user a few files initially, but continues to delete the user files as they do not satisfy the ransom demands. The 2016 Locky first uses the current loader that substitutes the infected doc for the binary file; thereby, this automatically downloads and installs a variety of malware depending on your Windows version. The 2016 Locky distributed Zepto encrypts the victim's file; once the payment

goes through, it then provides the decryption key unique to the attacked system. The globe crypter ransomware malware encrypts user files with the strong AES instructions and, following the ransom demand, is tasked with decrypting it. Similarly, there is the Kpv\_Nemucod\_RinceLocker, also infect the host with the RinceLocker sample, prevents user accessing the system. In contrast, the Petna-Raas entirely wipes the hard disk sectors in the master boot record and demands payment.

#### **4. Key Characteristics**

Ransomware attacks continue to be a prevalent threat and unique from those that have posed risks to individuals and organizations. In response to its elevated profile, this section attempts to provide a comprehensive analysis of ransomware threats. To this end, the key characteristics that define ransomware attacks are delineated along with those that differentiate them from other types of cyber threats. This analysis elucidates the tactics employed by ransomware adversaries, which have continued to evolve in such a way as to make these attacks difficult to detect, mitigate, and recover from. To effectively defend against ransomware, both organizations and individuals must therefore be informed about these attacks and recognize their signs and vulnerabilities. The goal of this analysis is to offer detailed information to this end. In addition to enumerating the attributes that define them, this section reviews the history of ransomware attacks and their development alongside defensive efforts.

Among the most common attack vectors in ransomware threats attempts to exploit

software vulnerabilities, with which this essay finds relatively large numbers of potential attack vectors, so they are discussed here in greater detail. In addition to software vulnerabilities, ransomware attacks often exploit weaknesses in cybersecurity practices, including insufficient security awareness, non-compliance with IT security standards, password reuse, and lack of e-mail filtering. Due to the complexity and continuously evolving nature of ransomware threats, this analysis argues that unauthorized access points have also been identified by the attackers, which is an unprecedented analysis finding. Additional notable features of these attacks concern the tactics used to restrict notification of the infection and the methods for social engineering attacks. Ransomware attacks are highly prepared for the intrusion, which includes the exploitation of up to twenty different mitigations of system vulnerabilities. Ransomware actors have also used zero day exploits as early as in 2017, which further emphasizes the need for software patching and updating. Given wide coverage, ransomware attackers use all types of attachment files and employ a variety of techniques to bypass e-mail filtering systems for spamming the phishing e-mails. Since 2018, there has been a significant rise in e-mail filtering bypass methods, with the use of unusual file extensions being most successful. Individual firms constantly adapt to changing risks, with population estimates annually correlating to strategic analysis for years following major incidents. A fortnight period before the peak in hiring of information security professionals is observed, at which point the salaries are highest ( [2] ).

## **5. Evolution of Ransomware Threats**

Ransomware has not emerged yesterday. By tracing its history, it becomes apparent that ransomware dates back to the late 1980s with one of the known first victims being the very early version of Microsoft MS-DOS. The first ever observed ransomware style malware - named the "AIDS-trojan" - circulated in the wild in 1989. That malware was a trojan which would encrypt the names of the files stored on the target machine's hard drive and set the password. After the noted password was changed, newly booted computer would display a message stating that all files on the disk had been encrypted, and a ransom of allegedly 500 US Dollars needed to have the files back. Ransomware had a few minor outbreaks in the 1990s, and a couple of them used email to infect the victim's machine. However, during the whole decade of 2000, the number of recorded ransomware attacks was below twenty which indicates that the ransomware was not "paying off" that much. In 2005, the ransomware did change its tactic by including the ability to encrypt the files stored on the victim's machine. While there were multiple versions of the ransomware dealing with locked victim's screen, it took years for the ransomware to use the reprehensive encryption method. First of the modern versions of the ransom using the file encryption were the GPCoder and its variant FileCoder which

appeared in the end of 2005 and during 2006. However, the GPCoder/FileCoder saga quickly ended after the responsible trojan/worm was deleted for unknown reasons. In 2006, the Archiveus was spreading in the wild. After the whole hard drive of the victim was encrypted, the program would give the ransom of 10 US Dollars to a charity. This ransomware was undermined ten days ago by a programmer who managed to decrypt holding files. That actually interrupted "business model" until the next spring when new CryptorBit type of ransomware appeared in the wild. In the meantime, in 2007 small scale ransomware campaign called GPCoder.K was keeping the ransomware itself in the headlines.

## **6. Impacts of Ransomware Attacks**

The rapid evolution of 21st-century technology is in no small part due to the ubiquity of the internet. With the world now synched online for most activities, businesses are often at the receiving end of cyber threats. In 2020, ransomware assaults induced in many businesses worldwide \$20 billion in financial harm, with normal recovery expenses amounting to an extra \$24 billion [3]. The financial outlay of ransom fines has been the top known effect recorded by business casualties of such events. However, ransomware assaults have a cascading array of ramifications for the group touched, making it a worldwide risk to shared and

financial security. Organisations will continue to confront unhealthy circumstances whether defrayal or restoration policies are pursued, with insolvencies, ransomware assaults and ransomware fines decreased belief suffered over the mid-to-long duration. For institutions, the multiple unfortunate externalities growing from ransomware assaults are manifest in a cascade fashion that can guide to decreasing trust, reduced customer or investor satisfaction, increased stakeholder apprehensions, and decreasing market competitiveness. Casualties also indicated many effects that were frequently under the surface but could guide to concrete repercussions for an enforcing organization. Positive ransomware data reports are generally determined by factors that provide to a mix of adversarial conditions most frequently experienced, together with a combination of unpreparedness, a sophisticated cyber danger background to which the industry has limited sway, and empirical phenomena that make ransomware occurrences, and the consequences thereof, more likely. A framework for ransomware risk preparedness, which accounts for the multifaceted impacts of such incidents, is guaranteed henceforth. This prominently comprises investing in wide-ranging, all-body technology and network threat prevention methods, including shielding organizations and victims from malware propagation, facilitating transparent awareness and transparency on ransomware solutions for counterparts in alliance-

networks, and seeking post-attack collaboration and damage containment. Analytics of the key vulnerabilities and behavioural frailties discovered in the consequences on the number and types of ransomware claims produced in numerous business groups is the system's foundation, demonstrating how a considered comprehension of likely spills can help to minimize losses post-attack after this comprehensive analysis.

## **7. Financial Losses**

Due to the surge in ransomware attacks, financial losses incurred from the threat are surging as well [3]. Financial losses associated with ransomware are twofold: the first includes direct costs which occur as a result of the ransom payment needed to regain access to encrypted data; the second comprises of indirect costs arising out of the attack i.e. downtime, recovery operations, and the multitude of efforts invested in the handling of the incident. A statistically significant correlation between the number of days of downtime and net overall cost, as well as net overall cost and recovery time objective, has been reported. By delaying the beginning of the response to a ransomware incident, additional costs in terms of response endeavours are likely to be incurred. On average, victims necessitate five days of downtime to recover after experiencing an attack. On average, organizations spent recovering from a ransomware attack. It was emphasised that organizations of all

sizes are targeted by ransomware threats and are exposed to the risk of extortive attacks. What distinguishes one from the other, however, is their preparedness to a wide array of threats, their financial stability, and the measures in place dictating their reaction to a security incident. Recovery from a ransomware attack can cost up to billion. Imminent financial strain arising out of the attack may lead to layoffs, and if no external support is available, even spell bankruptcy. Given its devastating consequences, it is vital to have a comprehensive understanding of the complete spectrum of ransomware harms and to implement the necessary remediation strategies. This is to better understand the present and long-term financial implications of extortive threats and to establish financial strategies to prevent, detect, and respond to ransomware acts.

## **8. Operational Disruption**

Ransomware attacks pose significant operational disruptions which affect the functionality of targeted organizations, potentially paralyzing critical processes and services. This can result in significant downtime in the targeted company. In many cases, it is found that the productivity of employees can be impacted in recovery efforts; there is often an inability to effectively perform core duties when systems have been locked or lost [3]. This can be significantly exacerbated if a major effects chain reaction in organisation occurs: such a sudden stop can be

observed in wider customer service and the resultant satisfaction stakeholders receive. When this impacts an entire city or region and has effects on wider infrastructure, the ultimate chain reaction can be seen to be severe and local government services were still affected in an attendant ransomware infection over years later. The colonial pipeline ransomware infection and subsequent recovery efforts exacerbated fuel delivery network operations across the entire East Coast of the US and the surrounding colonies of regions, with long-lasting consequences that can still be discerned today. Similarly, the ransomware infection of JBS S.A. halted beef processing plants in the US, Australia, and Canada, and supplier notices of “JBS has experienced an unauthorized intrusion” had impacts on the global meat supply chain that were still noted seven days later. These highlighted cases offer a clear warning of the immediate effects that ransomware attacks can have on many large organizations. The immediate and comprehensive disruptions they cause following infection, even after many millions of dollars have been paid by the victims, serve to reiterate the urgent need for these organizations to develop effective recovery plans. Moreover, it is perceived that the long-term costly harrowing symptoms that would subside if these large companies do not have adequate planning, resources and simulation exercises will be suffering. Instead, they are on-the-back-foot and “getting

wheeled into the theatre” in a rush every time without condemnation. In many instances, the standard operations have therefore been to offer equivalent everyday public offerings; at their peak, it was noted that they “do not yet something” to restore businesses to usual conditions. This shortcoming cascades significant operational issues.

## **9. Reputational Damage**

A further, less quantifiable, type of damage that is possible to measure might also befall a victim organisation - yet still be just as severe as any financial impact. This type of harm is reputational, and such damage can take considerable resources, time, and effort to redress. Public, official raised, and international agencies, society, the media, and shareholders may all look upon an impacted organisation with disfavour. A good example of this was the ransomware attack faced by Foxtel. Out of all cases profiled here, Foxtel’s ransomware attack might have been the worst in terms of negative press coverage of the impacts borne by the victimised organisation. Consumer sentiment toward Foxtel soured significantly when many of their shows and general viewing services were taken offline. This was echoed in frequent news articles and media coverage of the event, with accusations levelled of Foxtel neglecting their existing commitments and the campaign run to rectify the situation labelled as ‘half-hearted’. It would seem that two

crucial mishandlings of the situation were any official public announcement from Foxtel regarding the attack and the consequent impacts, as well as how Foxtel was unable to adequately restore the normal viewing services to its customers for a considerable amount of time in the wake of the event. Even after the release of a free ‘recovery package’ of viewing services, along with insurance claiming forms, this was still perceived poorly, with many consumers expressing anger that the recovery package was of minimal value. [3]

A key issue that can excavate a colossal footing in the industry, in addition to dear expense, is the security and contractual standing between various bodies. Channel 7 suffered a fairly notable financial impact, though the harm this dealt to the entity was significantly attenuated due to the indefinite expiration of the television broadcast rights contract the organisation was withholding. Instead, it may have eluded substantial damages due to there no longer existing any applicable penalties incurred; however it was subsequently unable to secure another further contractual accord, as these more recent contracts now included stipulations holding targets responsible for any damages stemming from ransomware events that might befall them. Analysis of the available data could not ascertain both how commons this manner of ‘self-defence’ was currently, or whether this practice was going to extend into other areas of industry in

the near-term. Counterbalancing the relatively broad nature of this analysis, it was observed that corporate giants the likes of Vodafone and Google were not engaging in such a practice yet, and instead, as per the initial precautionary advantage of such a stance, were arranging more and more stringent biannual third-party reviews of their respective cybersecurity systems. This indicated, however, that until a standardised, independent guideline was arrived at en masse, implementing this preventative procedure was both more onerous and restrictive than simply adding a clause into an affected contract. Nevertheless, the lesson learned was that defending according to traditional business practice and establishment was no longer a viable endeavour.

Reputational damage as a consequence of a ransomware event is an underexamined and often-sidelined field, regrettably so, as it can potentially undo an organisation where direct financial losses were otherwise manageable. In broader considerations of this type of harm, a comparison of statistics after the WCRY outbreak across the numerous industries that suffered therefrom found the most hard-hit were those characterised by absolutely far-reaching impacts in the event of data unavailability. This was, notably, the medical and banking industries in the saga (but in stark comparison to previous situations, not only). A later analysis

of the far-reaching fallout from these attacks revealed that no less than 17.3K adults suffered yet poorly elucidated grievous eventualities ensuing from a lack of patient records at 31 of the afflicted medical facilities. Similarly, the attacks at JP Morgan and Goldman Sachs were not characterised by an especially in-depth analysis of the occurrences there, yet the relatively brief impact of consumer confidence towards both entities resulted in the former losing \$4.3 billion in assets, and the latter being purchased at a pittance of its actual value by a rival. Another overlooked facet of such fallout across sectors was the adroitness of external 'downstreamers'. Following the initially discussed attack on News South Wales Historic Buildings, the digitised visitor database was taken hostage. This successfully led to 1750 government workers' commissions surreptitiously redirecting potential tourists keen on finding more about said buildings to commence investigative excursions exclusively to rival structures.

As of present lack of goodwill towards the channel, public services or industry commonality would be most significantly impacted within the finance and utilities sectors, and also, to a lesser extent, amusements and betting (though this momentarily harmed agents in these sectors by no means made themselves more alluring to their corporate betters; they are already notorious for having abhorrent interest rates and legality). Depending on established business standing, the perceived loss of

goodwill with no small interest parties encompassing dropped prices and/or unworkability in collaborations could of itself be too damaging to risk continued hostaged holding of valuable resources. An alternate fabric of perception waging would see the infiltratee as possessing little-to-no financial stock of value, yet still quite agreeable to inform on all tainted competitors towards a rival, thereby delegating the diminishing attention and ransomware developments to the inquiry of others. Public postal services would likely be seen as an easy vector of attack, that, whilst they still entailed the possibility of damaging state unrest, did not have the same level of direct association with the unmitigated triumph of competing personal prosperity as would be the case with, e.g., certain lesser agreed upon private corporations. Livelihood or the capacity to fund the same was a non-entity here, with few of these destitute entities statewide even possessing the requisite resources of legal standing to instigate a most basic and hasty grand jury.

## **10. Key Industries Targeted by Ransomware**

Healthcare, finance, and education are among several industries that face increased threats from ransomware. The recent ransomware attack on Allscripts illuminates growing concerns about the healthcare industry's vulnerability to ransomware attacks [1]. This comes

at a time when healthcare organizations are digitizing patient data in efforts to improve the efficiency of healthcare. The sensitivity of patient data makes the industry an easy target for ransomware actors. Paying ransom is particularly appealing to these organizations since data recovery can be a life or death situation. The Pittsburg Medical Center, for instance, paid \$40,000 to decrypt its systems after a ransomware attack disrupted its operations.

In the meantime, the finance sector has also become an increasingly targeted industry with no signs of slowing down. Unlike the healthcare industry, the finance sector is familiar with cybercrimes and is investing more in cybersecurity than other industries but is still failing to safeguard from ransomware attacks. Conventional ransomware emerges in the form of phishing attacks, effectively penetrating the industry. Cybercriminals used cryptomining to breach networks and execute ransomware before instantly connecting to a C&C center. This demonstrates that hackers are aiming for high returns from the finance sector and are coming prepared with advanced attacks. For these reasons, recognizing key industries that ransomware actors attack is crucial, as companies can adjust their cybersecurity defense strategies accordingly.

Healthcare, finance, and education industries are the top three industries most frequently attacked by ransomware. To discover insights

into these targeting patterns, industry-specific trends of ransomware attacks against each industry were analyzed, as were the forms of ransomware attacks on these industries. For a more holistic approach towards the understanding of industries, it is necessary to first establish that different industries are likely to have unique patterns of ransomware attacks.

## **11. Techniques and Tools Used by Ransomware Actors**

Ransomware is rapidly becoming an increasingly prevalent threat in the realm of cyber security. It has been estimated that over a billion dollars have been paid out to ransomware actors since 2013. These actors are employing a wide array of methods and technologies to execute ransomware attacks and are continually evolving new tactics to evade countermeasures. This paper will delve into these methods and technologies, covering how ransomware actors are getting into systems, the makeup of their ransomware, and how they are executing their campaigns. Furthermore, this paper will also investigate the very latest ransomware exploitation techniques to assist cyber security professionals and help preserve the integrity of their services. It is absolutely vital to understand how these knobs are being turned in order to enhance defensive measures [1]. Each day, a tenacity to perfect these ransomware

tools is growing, to remain one step ahead.

For a cost exceeding \$2000, it is quite easy to stand up an operational and effective ransomware campaign. Phishing remains the most common method to infiltrate a system with ransomware. It is still considerable that ransomware actors are able to profit from outdated patches and unsecured systems. This can include all commonly used strain of ransomware and there are many. Although many ransomware actors are not credited for their programming, ransomware is no easy tool to craft. It is merely steeped with complications. It is these factors that have resulted in the development of ransomware toolkits. Such cyber tools greatly assist those who have no previous knowledge in ransomware and wanting to explore this tactic. Ransomware service kits are even available for free on the clearnet. Once a commission is taken from the funds extorted, the rest of the payment made by the individual who initiated the campaign is taken by the ransomware distributor responsible for performing decryption. Assisting the operation of ransomware on computers, a ransomware administrator account is commonly employed. Automation has facilitated the employment of many ransomware campaigns and tasks by simply pointing, clicking, and possibly copy and pasting. One possible hurdle for emerging ransomware actors is the crafting of their own ransomware. As a consequence, a complimentary or

service can be found on the dark web. One such service allows for patterned ransomware custom-built based on a series of choices. Its output is 64bit print modules that load into the CryptoLocker codebase. But perhaps the biggest helping hand for ransomware actors is the ransomware as a service model. It typically involves a conjugal ransomware server, a ransomware panel that manages campaigns, and a buyer and a seller. The buyer is responsible for selecting the type of ransomware they wish to distribute on the server. From there, the buyer is provided with a payload associated with the ransomware executable.

The seller is responsible for the upload of the buyer's payload to the server. The seller shall receive 6% - 20% of the ransom payouts. Such a union provides the opportunity for any individual with minimal monies to mount an operational ransomware campaign. The Prism Ransomware Wrangler represents a possibility for emerging ransomware workforce. They can work with detection avoidance techniques and avoid the more common strains to their irregular activities. Numerous ransomware stockpile splash screens will be cooped up. Nonetheless, the DanaBot ransomware, for instance, primarily being employed only in European nations and hasn't coxtosed to be bonamous. As always in the realm of cyber security, one who would aspire to wager a step to outmanoeuvre ransomware attacks requires a similar basis and a creative perspective. As ransomware

operations witnessed advancing improvements, so too must an operant have sharpened its cyber tools. Ransomware removal techniques are a few cryptocurrencies intelligence sharing observable metastasis behaviour in the limiting of cryptocurrency trade directories. To decimate plot symmetry in a ransomware splash screen image. To actualize a calamity mitigation strategy at a conspicuously time to end the cosmic rangle. Brill be aless and well.

## **11. Preventative Measures and Best Practices**

As new technologies and services are developed and adopted, the cybersecurity landscape is becoming increasingly complex and sophisticated. Implementing proper prevention and detection programs is imperative for organizations to protect themselves from the range of cyber risks they face on a daily basis. All the technology in the world will not help if basic good practices are not in place. In preparing for the worst recognized attack scenarios, an organization can tailor incident response plans that are comprehensive yet simple in the prototypical case. Below is a collection of best practices and methodologies that can be implemented to mitigate the danger of ransomware threats.

The most effective method to protect data is to use cryptographic algorithms for security during the transmission and storage of data [4].

The data is encrypted using cryptography and a key remains with specific users. To read the data, the user requires a key and the data is decrypted accordingly. Consequently, the role of access controls and strong password policies are also needed. Invalid access is prevented with a mechanism involving technology and data processing. Access and modification of crucial data should be introduced for monitoring with appropriate logging. Procedures ensure logs are monitored on a regular basis and any changes are understood and authorized. This introduces the concept of network segmentation and the need for strong password policies for network devices. Ideally, remote desktop should not be open and a VPN should be configured so as to access a limited amount of data from a touch device.

Ransomware is an ongoing business that can only succeed if no one is willing to pay any more. Client awareness and education programs regarding basic cyber security and phishing are important. Many of the victims became victims because the wrong link was clicked on and the wrong email was opened. Encourage employees to concern and report any suspicious activity as well as to take a more conservative approach in their day-to-day activities. Set up formalized reporting agreements and communication to address most security queries early before compensation is invested.

## **12. Employee Training**

As evidenced by the scale and scope of ransomware incidents across public and private enterprises, education is crucial. Employee awareness and behaviors can directly impact the cybersecurity posture of a company, highlighting the necessity for comprehensive, frequent and genuine training programs covering the most prevalent attack vectors [5]. The topics of training content have been widened through sustained devastating attacks on hospitals, the most notable being WannaCry. This global menace to the healthcare industry underscores the necessity for re-examination of training programs in place.

An effective training program needs to visit multiple facets of potential attack vectors. While ransomware is of primary concern, the training should focus on the avenues by which ransomware is generally delivered. Users should frequently examine emails for tell-tale signs of phishing, especially with the growing prevalence of whaling attacks. Stressed in training should be that no government or private institution demands money wired through services for a fine. These are clearly public services that would not take payment for a criminal act on the behalf of a government agency. Additionally, infected removable media should never be plugged into a company machine and remnant paper invoices faxes or voicemail messages should also never execute an unknown file [6]. It is important to run drills like email with hazardous attachment or link deliver to 30

clients and then the responsiveness of the users check. Summation of knowledge gained from all users and possible methods to evade the email should then be distributed. Subsequently, the training program should encompass simulated attacks in the form of real-life examples in order to educate and increase awareness. Falling under the guise of educating the user, a fake ransom demand payment may be received, and then the subsequent results used as teaching tools. Along with emails a fake call from a “vendor” inquiring about late invoice payment may occur. This supposed vendor will then try to get the rep to navigate to a phony copy of the vendor’s site. The instructive data gleaned from a failed attack should be used to enlighten and prevent subsequent failure.

### **13. Regular Data Backups**

Recently, a significant increase in ransomware attacks has been seen targeting various organizations, including hospitals, government institutions, and industry. Ransomware is a type of malware encrypting files on infected devices, and the victim must pay a ransom to get them back. Ransomware attacks have malicious patterns, such as deletion recovery points in Windows OS, and they largely have the effects of preventing users from accessing data. As huge amounts of important data are damaged by these attacks, data backups are often considered to be the most effective defense mechanism. Following a ransomware attack, files are automatically

recovered from backup copies, but this approach requires a significant amount of extra storage, and their clever authors know how to locate and delete the backup copies of the infected files.

Backup is not a single type of method. The backup may be executed by a differentiated strategy, such as backing up all files, adding new files, or backing up modified files. The strategies are the full backup strategy, the incremental backup strategy, and the differential backup strategy. Full backup needs more store space, but it has the advantage of faster recovery. Incremental backup only copies data that has not been backed up since the last full backup. It can back up more frequently, but many incremental changes lead to higher data loss. Differential backup is similar to incremental backup, except it copies data that changed since the last full backup copy. Differential backup retains a complete copy of all changes while the last full backup was done. In this way, full recovery can be made faster since it is potentially necessary to use only the last full backups. The critical data, such as the data owned by the organization, are in offline environments or isolated environments, because ransomware usually focuses on environments that are connected to networks and backing up hardware. Backup copies shall be as updated as possible, which allows the gap between the ransomware infected file and the backup copy of the file to be minimized and thereby lesser data

damage. People easily consider only backup data is appropriate. However, a simple backup system may have a storage limit and it may fail to perform backup operations or errors may occur in backup operations. Regardless of the reason, if the backup does not work as intended, the file can be the original file. A consistent backup is the element to restore a non-encrypted file after a ransomware attack; therefore, a stock pony is a prime device for the organization to take into account careful considerations.

#### **14. Network Segmentation**

Ransomware, a type of malware that locks a victim's computer or encrypts its files until a ransom is paid, can have catastrophic consequences for individuals, businesses, and government agencies. Unlike many forms of malware, ransomware is designed for immediate financial gain. Ransomware developers often hold the victim's files "hostage" until a predetermined payment is made. Encrypted data by ransomware is unrecoverable until a cryptographic key is obtained. Ransomware developers can encrypt only a small part of the file or have the ability to upload the victim's files to the remote server. If there is no fair way of recovery the damage is even bigger, especially for companies or governmental institutions that may lose the production data or intellectual property. Criminals behind the ransomware threat are constantly improving their product; thus, it's a challenge to design

effective countermeasures. Although the ransomware can be detected, full data recovery is almost impossible [7].

Partitioning a network into smaller subnetworks is recognized as a valuable strategy for thwarting ransomware actors. Network segmentation involves dividing the network infrastructure into smaller segments. This approach can greatly decrease the attack surface for the ransomware actors. Segmentation limits the ability of an intruder that has routes to only a portion of a target network to move laterally across the rest of the networked environment. Therefore, even if an intruder can access sensitive information, network segmentation reduces the probability they can exfiltrate the recovered data. For optimal security, critical data assets and systems should be prioritized during network segmentation. Subsequently, the most sensitive parts must be isolated in a way that would limit access to only selected employees with business needs. There must be a system consisting of firewalls, policies and switches capable of traffic flow control between the segments to ensure that lateral movement involves only authorized personnel and the strictly necessary systems. However, one of the main challenges that organizations face when implementing and maintaining a network segmentation is the difficulty in designing an initial network architecture. Consequently, network segmentation should be carefully planned and should involve

a continuous assessment during further maintenance. Regularly updating the network architecture and configuration could thus thwart intruders trying to gain the necessary control over a segment to successfully conduct ransomware activities.

## **15. Incident Response and Recovery Strategies**

Ransomware remains a potent threat capable of destroying or disrupting organizations. Thus, it is paramount to understand the threat landscape, evaluate the risk, and deploy protection measures commensurate with the identified risk. These measures shall encompass facets beyond mere technical preparations, extending into administrative measures and best practices within operations [8].

Prior to an incident, organisations must develop an effective incident response plan. The plan should include not only a technical checklist to inform containment and recovery actions but also well-defined roles and responsibilities and a communication plan [3]. Perhaps imperatively, engagement of IT, legal, and communications teams before an incident is necessary to navigate the complexities of a ransomware attack. Incident response and recovery procedures must be practised and contingent upon legal and cybersecurity professionals who understand the peculiarities of ransomware incidents.

Immediate detection and communication are required during a ransomware incident. It is observed that time is of the essence, and immediate swift action can prevent further damage caused by the ransomware or mitigate existing damage. Detection of encrypted files or a compromised system sets forth a series of actions leading to the containment and eventually the investigation into the incident by forensicators to determine the malware's type of execution or deletion pattern. Pieces of compromised hardware must be collected for further analysis providing a list of actions to be conducted by first responders and alluding to hard disk clean room services.

There are various methods to enable the recovery of systems once made unavailable due to a ransomware infection. Most importantly, it is crucial to have in place tested and working backups that may be restored offsite. Nevertheless, organizations must be prepared for the worst, and in the case of a full production environment compromise, it is crucial to give investigative teams the availability to system-wide images or other forensic artifacts. These will allow retrospective analysis of the incident to assess how it took place and define lessons to be learned for future incident prevention. Continuing recovery actions is outlined such as service containment, user credentials analysis, and securing detection of the malware.

Due to the nature of the ransomware threat, recovery steps must be parallel with a negotiation of the decryption key. Currently, there are no public decryption keys for most ransomware families, but advocating for not using ransoms implies avoiding payment to organized crime. Moreover, the re-execution of encrypted files requires for them to be subject of a thorough investigation to understand the encryption employed. Such actions suggest ethical grey zones, e.g. payment to criminals, and advise to be rehearsed by any organisation prior to an incident.

## **16. Legal and Ethical Considerations in Dealing with Ransomware**

Ransomware is a substantial danger, and it is crucial for all businesses, executives, and managers to learn about the danger. Not merely the high-level functioning and prevention tactics of ransomware, but also the regulatory and ethical elements of ransomware and ransomware settlement. Paying off ransomware agrees with keeping the adversary of a felony inside the eyes of the law.

There can be serious fines and consequences from legal organizations if there is information on ransomware cases. This can deter search organizations from preserving the money and even compensate otherwise required bills [9]. But there are additional likely critical challenges of paying ransomware that may include more than simply

money. It perpetuates illegal behavior by rendering offenders financially thriving. It's the same as providing the financing for the next ransomware as crooks generate capital [3]. One (false) assertion to settle up the ransomware criminals creates "a mentality then." But when crooks learn they can get away with the ransomware, assaults will only grow. This has led various school zones to cancel a score disputes with CPAs in order to refrain from deploying teenagers.

## **17. Case Studies of Notable Ransomware Attacks**

Ransomware is a form of malware that typically locks electronic files until a sum of money is paid. Often targeting large organizations, ransomware has the potential to disrupt daily operations of industries such as healthcare, critical infrastructure, and many others. Some ransomware actors have used the added incentive of threatened data release to extort money. As time passes without payment, the ransomware actor may increase the total payment demanded, or manufacture a new penalty to increase pressure on the victim. Ransomware can have several additional impacts on a victim to encourage them to make the payment. Both onerous and costly to investigate, the heavy burden on organizational responders can cause business disruption through IT forensics, rebuilds, and recovery processes. If data is not adequately

protected, data leaks in tandem with ransomware incidents are common, and can have severe consequences, including: PI (personally identifiable) data being exposed, significant GDPR & CCPA fines, and significant reputational damage. Finally, as a result of data leaks, ransomware incidents suffered UCI (unauthorised access, exfiltration, & publication) [3].

In the domain of ransomware, different organizations can be involved based on the approach taken by the ransomware actors. Regarding the several impacts on a victim, working exclusively from a third-party forensic provider's perspective would come with a deep understanding of the data, process, and victimology of 180 separate ransomware incidents in 2021. Before a ransomware incident hits, there are often multiple vulnerabilities and misconfigurations that ransomware actors can exploit to gain deep access to an organization's internal data network. The initial access point usually either employs public facing services, for example, VPN or RDP, to gain entry; and/or social engineering tactics, often through unsolicited emails. However, common in every analysed case was the exploitation of known CVEs (common vulnerabilities and exposures). After gaining access, and establishing persistence, the ransomware actors thoroughly explore the network and systems to assure their tooling will have the desired destructive impact unless the ransom is paid. There is typically a

gap between the time of the initial compromise and the deployment of the successful ransomware payload. By the time they found out about the attack, most victims had little time before the full deployment of a successful ransomware encryption payload. The ransomware actor then explicitly instructs victims to engage or withhold particular third-party services during the containment, rebuild, and recovery process. Victims are discouraged from carrying out their own investigation. Victims are also routinely pressured not to negotiate the ransom, or to wait until the deadline after which the price will increase, and/or new penalties will be added.

## **18. Case Studies of Notable Ransomware Attacks**

Ransomware is a form of malware that typically locks electronic files until a sum of money is paid. Often targeting large organizations, ransomware has the potential to disrupt daily operations of industries such as healthcare, critical infrastructure, and many others. Some ransomware actors have used the added incentive of threatened data release to extort money. As time passes without payment, the ransomware actor may increase the total payment demanded, or manufacture a new penalty to increase pressure on the victim. Ransomware can have several additional impacts on a victim to encourage them to make the payment. Both onerous and costly to

investigate, the heavy burden on organizational responders can cause business disruption through IT forensics, rebuilds, and recovery processes. If data is not adequately protected, data leaks in tandem with ransomware incidents are common, and can have severe consequences, including: PI (personally identifiable) data being exposed, significant GDPR & CCPA fines, and significant reputational damage. Finally, as a result of data leaks, ransomware incidents suffered UCI (unauthorised access, exfiltration, & publication) [3].

In the domain of ransomware, different organizations can be involved based on the approach taken by the ransomware actors. Regarding the several impacts on a victim, working exclusively from a third-party forensic provider's perspective would come with a deep understanding of the data, process, and victimology of 180 separate ransomware incidents in 2021. Before a ransomware incident hits, there are often multiple vulnerabilities and misconfigurations that ransomware actors can exploit to gain deep access to an organization's internal data network. The initial access point usually either employs public facing services, for example, VPN or RDP, to gain entry; and/or social engineering tactics, often through unsolicited emails. However, common in every analysed case was the exploitation of known CVEs (common vulnerabilities and exposures). After gaining access, and establishing persistence, the

ransomware actors thoroughly explore the network and systems to assure their tooling will have the desired destructive impact unless the ransom is paid. There is typically a gap between the time of the initial compromise and the deployment of the successful ransomware payload. By the time they found out about the attack, most victims had little time before the full deployment of a successful ransomware encryption payload. The ransomware actor then explicitly instructs victims to engage or withhold particular third-party services during the containment, rebuild, and recovery process. Victims are discouraged from carrying out their own investigation. Victims are also routinely pressured not to negotiate the ransom, or to wait until the deadline after which the price will increase, and/or new penalties will be added.

## **19. Global Efforts to Combat Ransomware Threats**

Ransomware has quickly emerged as one of the most prevalent and damaging cyber threats across the globe. The advent of Bitcoin and anonymous cryptocurrency payment systems has been a big enabler to the criminals perpetrating the ransomware. This has made the threat an attractive option for a large, increasingly international community of cyber criminals. Hence, international collaboration is required to address both the sources and the effects of ransomware

attacks. Countries such as the U.S., U.K., and European Union are calling for a united international front against the attackers. EUROPOL has also initiated Operation Ransom to pool together resources from law enforcement and cybersecurity firms with the goal of creating a concerted, global response against the actors. The U.S. has also initiated efforts such as the Ransomware Task Force which leverage public-private partnerships to tackle the problem of ransomware attacks. Efforts by countries to increase and facilitate the sharing of intelligence to address ransomware are expected to enhance the ability to tackle the threat [1].

Some of these initiatives include platforms for the exchange of information on threats and intelligence, as well as the development of guidance for both public and private parties. There is also a trend globally towards establishing joint government task forces to develop and implement an aggressive threat-based strategy to respond to ransomware attacks. Due to their nature, these attacks frequently need a coordinated and international response. It has long been established that the deterrence policy against cyber threats cannot be achieved based on a national cyber security, defense strategy alone, but also requires close international cooperation. Attacks over the internet don't recognize borders and affect all countries equally, and in some case those most affected are the less advanced economies in the matter. Ransomware is no exception. For a

concerted approach against ransomware, taking account of its international nature, threats and victims, questions of international cooperation, information exchange, and mutual assistance are essential. Training, awareness raising campaigns or "table top exercises" are organized to address good practices about preparedness, response and recovery, technical responses or international cooperation and mutual assistance in the context of legal frameworks for such a response. Legislation and regulations are being set in place to cater for the deterrence of ransomware attacks. A coordinated approach is necessary since the singular response of nations could exacerbate the problems.

## **20. Future Trends and Emerging Technologies in Ransomware Defense**

Ransomware has quickly emerged as one of the most prevalent and damaging cyber threats across the globe. The advent of Bitcoin and anonymous cryptocurrency payment systems has been a big enabler to the criminals perpetrating the ransomware. This has made the threat an attractive option for a large, increasingly international community of cyber criminals. Hence, international collaboration is required to address both the sources and the effects of ransomware attacks. Countries such as the U.S., U.K., and European Union are calling for a united international front against

the attackers. EUROPOL has also initiated Operation Ransom to pool together resources from law enforcement and cybersecurity firms with the goal of creating a concerted, global response against the actors. The U.S. has also initiated efforts such as the Ransomware Task Force which leverage public-private partnerships to tackle the problem of ransomware attacks. Efforts by countries to increase and facilitate the sharing of intelligence to address ransomware are expected to enhance the ability to tackle the threat [1].

Some of these initiatives include platforms for the exchange of information on threats and intelligence, as well as the development of guidance for both public and private parties. There is also a trend globally towards establishing joint government task forces to develop and implement an aggressive threat-based strategy to respond to ransomware attacks. Due to their nature, these attacks frequently need a coordinated and international response. It has long been established that the deterrence policy against cyber threats cannot be achieved based on a national cyber security, defense strategy alone, but also requires close international cooperation. Attacks over the internet don't recognize borders and affect all countries equally, and in some case those most affected are the less advanced economies in the matter. Ransomware is no exception. For a concerted approach against ransomware, taking account of its international nature, threats and

victims, questions of international cooperation, information exchange, and mutual assistance are essential. Training, awareness raising campaigns or "table top exercises" are organized to address good practices about preparedness, response and recovery, technical responses or international cooperation and mutual assistance in the context of legal frameworks for such a response. Legislation and regulations are being set in place to cater for the deterrence of ransomware attacks. A coordinated approach is necessary since the singular response of nations could exacerbate the problems.

## **21. Future Trends and Emerging Technologies in Ransomware Defense**

Ransomware is an increasing threat as a form of malware attacks, which encrypts files and data from users' devices to demand payment for their recovery. This chapter outlines an increase of future trends in this area, so researchers and practitioners are better prepared to enhance their defenses or to detect and respond to such threats more successfully. It describes the carrying out and detail a roadmap of adopting techniques applied by ransomware developers at different stages of malware execution, highlighting possible opportunities to thwart them. Researchers and practitioners are called upon to consider the feature-based roadmap and focus their effort

and resources on the proposed novel approaches.

Efforts to prevent and recover from ransomware attacks that have shifted the focus from infected files to ransomware behaviors and activities, seeking new methods of detecting malicious intentions before encryption takes place. Security vendors and organizations have stressed the importance of running up-to-date IT systems and maintaining frequent backups. Since early 2016, a project called “No More Ransom” has been released, offering a collection of legitimate tools to help victims recover their files, including a number of encryption tools [10].

There are trends to develop and improve machine learning (ML) models, using new methodologies and improving algorithms and infrastructure for better features generation and engineering. Moreover, there is a discussion about advancements on adversarial ML models for detecting attacks, advocating a transition to the use of Recurrent Neural Networks (RNNS) rather than Convolutional Neural Networks (CNNs). Next to the development of executable-based security solutions and memory guards to prevent file-less attacks, there are findings that those can detect ransomware with 100% accuracy in a few minutes of propagation, but with the limitation that those could not handle pre-execution or early propagation states because takeover of other services would break the synchronization and logging. Among others, ransomware

has also evolved its mechanisms such as trying to encrypt files very quickly by using known encryption software and mitigate any possible solution for file recovery, encrypting more DJN files with most recent attacks or using transmedia information by stealing digital data, to outline an increase the need for lighter encryption algorithm. Back-and-forth trends and an arms race between ransomware developers’ offense and defense efforts by security researchers and practitioners may be facing probabilistic encryption that ransomware sends the key of local files and has time of exposure requirements, which under discussion of file size of more than a few KB. Additionally, ransomware mostly leverage RSA-2048AK/PK encryption that conventional technology should not theoretically break before many years or so, even with the most powerful installation in the world. Due to the centralization nature and the concentration of many eggs in a single basket, the distributed Ledger Technologies (DLTs) may change how organizations and personal computers manage and therefore defense against ransomware. There are findings that ransomware seems to be the first large-scale malware exploiting DLTs solution that prices and drills itstonesandk7 node is currently around \$1000k/month or \$10k/month. With 2% of all confirmed attacks that targets control technology and 64% of all manufacturing intermediary applications, the ICS sector will soon surpass the health sector in terms of

entities being targeted or at risk. Other critical infrastructure sectors are also increasingly targeted by ransomware, as prior identified in trend number five. Government services are currently hit less frequently compared to pay-perishing (PPD) by ransom writes so the potential for decentralized cryptocurrencies to lower ransomware incentive of isolated incidents. Moreover, there is a pronounced increase in the recent spread of through the entire attack chain, and one adversaries move later workflows. Organizations are advised to anticipate such attacks and consider employing a shift left of frameworks (e.g., attack forgings), increase defense systems, and monitoring the right empowered or as a cloud services through MSPs. Due to the broad technological landscape associated with healthcare, there is a likelihood of incorporating smart devices, firmware, and IoT sensors. This large and hgrial landscape can be challenging to properly secure, leading to an increase in clinical infrastructure elements and further well-exploitation services. Finally, there is an almost infinite supply of cyber threats that argue: "R&D in the cybersecurity industry must be continuous because the bad guys never seem to rest". As rejected, has a staggering and unpredictable set of potential future trends and threats. Nonetheless, one is to side-separation with all the ransomware defense strategy. Required researchers and practitioners to try one step ahead by increasing awareness of recent ransomware developments and the

efficacy of been and emerging defense technologies. With a market that is anticipated to grow stronger by 2021, the risky betransit ransomware trends ranked ransom ahead of class-based variants (RV, SG, CM) targeting IT companies and then provide cybersecurity firms at high addressing by conducting ransomware probability expertise and providing required training to improve infection and has omping malware. On the other hand, bank and blockchain empowers focused allocate resources and continuous ongoing training to maintain relevant developments. Organizations find an insightful understanding of future trends from different angles and the attack chain, potential sector targets, and DRI/ERL ramifications, as well as five separate additional funding to decrease the risk and following through with the duty regulations mechanism. These can guide more informed research into emerging ransomware threats and targeting defense mechanisms. Throughout this write-up document, there are researchers and practitioners are not only better prepared to enhance their defense, but also be able to more successfully detect and respond to this growing malware. Keep in view the negative comments, a ransomware defense awareness that it fell short on just in the making deployment and review of ransomware detected bypass using the end-of-the-employment.

## **22. Conclusion**

A number of strategies have emerged to remove ransomware attacks. While ransomware is a varied and complex cybercrime, there are simple methods that victims can follow to remove such cyber-attacks. Troubleshooting or launching safe mode with networking is an action plan. This action plan allows researchers to investigate all types of files, extensions, or applications inserted by the ransomware, which have created changes in the system registry. It is paramount that victims obtain an understanding of how the ransomware infection occurred. This can be beneficial for researchers to design custom-made removal tools proficient in removing the malware. After the infection is analyzed, the decryption key of the ransomware is essential for victims to decrypt their files. Obtaining the decryption key guarantees victims will not lose money and can remove the ransomware effectively. There is a need for governments to work on laws and regulations for cyber laws that can deal with ransomware cyber-attacks and bring cybercriminals to justice [1].

An imposed ransomware removal solution in the concept is an installation of an operating system wildly on any device, creating an overall perspective. As a result, the affected partition is not amongst the erased data. This broadens the removal solutions to conflicting and severely attacked ransomware. Protection plans for organizations and individuals are presented in a friendly way with the cyber environment and an understanding of ransomware. This paper provides an explanation of a “ransomware removal kits” concept, with a systematical measure that individuals and organizations can apply to remove the ransomware, and how the government can approach on enact

laws or regulations to deal with ransomware cyber-attacks and collaborate.

## 23. References

- [1] S. M Aziz, "Ransomware in High-Risk Environments," 2016. [\[PDF\]](#)
- [2] A. Zimba, M. Chishimba, and S. Chihana, "A Ransomware Classification Framework Based on File-Deletion and File-Encryption Attack Structures," 2021. [\[PDF\]](#)
- [3] N. Pattnaik, J. R. C. Nurse, S. Turner, G. Mott et al., "It's more than just money: The real-world harms from ransomware attacks," 2023. [\[PDF\]](#)
- [4] J. Ahn, D. Park, C. G. Lee, D. Min et al., "KEY-SSD: Access-Control Drive to Protect Files from Ransomware Attacks," 2019. [\[PDF\]](#)
- [5] N. Dugan, "Security awareness training in a corporate setting," 2018. [\[PDF\]](#)
- [6] C. J.W. Chew and V. Kumar, "Behaviour based ransomware detection," 2019. [\[PDF\]](#)
- [7] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics," 2016. [\[PDF\]](#)
- [8] H. Ghayoomi, K. Laskey, E. Miller-Hooks, C. Hooks et al., "Assessing resilience of hospitals to cyberattack," 2021. [ncbi.nlm.nih.gov](https://ncbi.nlm.nih.gov)
- [9] A. Laszka, S. Farhang, and J. Grossklags, "On the Economics of Ransomware," 2017. [\[PDF\]](#)
- [10] J. Pont, O. Abu Oun, C. Brierley, B. Arief et al., "A Roadmap for Improving the Impact of Anti-Ransomware Research," 2019. [\[PDF\]](#)