Study on Prevention and Solution of Ransomware Attack

[1]Tiu Yan Lin and [2]Zolkipli, Mohamad Fadli
[1]School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah Darul Aman, Malaysia
[2] School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah Darul Aman, Malaysia
Email: [1]tiu_yan_lin@soc.uum.edu.my, [2] m.fadli.zolkipli@uum.edu.my

Date received: 9 May 2021
Date accepted: 24 September 2021
Date published: 1 November 2021

Abstract - *The development of science and technology in this era brought many advantages for peoples, organizations, enterprises, and companies merely a lot of cyber threats are occurring nowadays. Ransomware is one of the families of malicious software that spread quickly and cause a critical impact around the world. Ransomware attacks the victim by infecting the malicious file into the device; they will encrypt and deny the victim to access it. A ransom demand message will prompt the user so that they will gain the money anonymously. The victims are only allowed to access after pay the demand using crypto-currencies such as Bitcoin. There is a lot of reason that cause the ransomware attack around the world, for example, the vulnerability of the system. Otherwise, the weaknesses of security knowledge also become one of the causes. However, many preventions allow the user to avoid the ransomware propagate but the system is not fully free from the ransomware attack. Thus, a lot of solutions are giving out by the researcher to overcome the problem after the attack.*

Keywords: malware, ransomware, prevention, prevention approach, solution.

1 Introduction

The use of the internet and application are widely used in these technology eras. People always connecting the internet and installing the application on their devices for working, education, social, and other purposes. There is a lot of useful application and program are build-up by the programmer and used by entire sector in global. The technology of the internet and application program have highly increased the life quality, economic status, healthcare, and more. However, a computer program named Malicious Code is created as a tool for the malware writer to attack computers, data networks, or any digital devices. Malicious code is a program that might bring a big impact on the device or sector. The most popular symptom of it on a device is the appearance of strange files, programs, or an icon on the desktop. The attack can be propagated through few methods, for example, viruses, worms, script attack, and so on. Currently, the security programmer in the different sectors is facing a lot of challenges in malware detection. Zero-day attacks are one of the malware detection challenges that difficult to detect and prevent due to its characteristic that is a severe threat. This cyber-attack targets unknown programs or software vulnerabilities. The malware writer or a hacker might exploit it to damage the software program, database, other digital device or impact on network connection before the mitigation. The chance of suffering from a Zero-day attack might be reduced with early awareness and avoid the development of program vulnerability.

Ransomware is malicious software that uses protection methods, for example, crypto graphing user data and related information. The attacking are possible happen on every single person, enterprise, or organization since it will spread from the internet network. Currently, attacking of ransomware has become a scary cyber threat for organizations and the most popular incident that always appears in global news (Byrne & Thorpe, 2017). The attacker will require the victims to make payment via bitcoin transaction or cryptocurrency to unencrypt and get back the data. Victims might also face a big amount of losses and critical financial problems if the attacker requests a big amount of payment. The data and file might not able to unlock until the end and destroy if they are not possible then make the payment. Thus, ransomware is divide into two main groups, which are Encrypting Ransomware and Locker Ransomware (Shah & Farik, 2017). Encrypting Ransomware is malicious software that using the encrypting method to deny the user for file accessibility, payment for the attacker is the only way to decrypt the file. "CyproLocker", "Locky", "CryptoWall" are the example for this category and come with the most popular ransomware that spread worldwide in 2017, which is called "WannaCrypto" or "WannaCry". The spreading of the WannaCry attack cause $4 billion. of financial losses worldwide. Next, Locker Ransomware will not encrypt the program or victim's file, the file will still in a safe condition but it will take an action with locked the victim device. Generally, Locker Ransomware only encrypts the user interface of the device. The victim is not able to use their device after the attack. Examples for this ransomware are "Reveton" and "Winlocker", "Locky", "TorrentLocker" etc. In some of the cases, the attacker won't unblock the user's device even the ransom demand has been paid.

In the nutshell, we can conclude that ransomware, a cyber-attack that is spread widely around the world is the most critical threat for all the community. It brings a lot of impact and losses that might cause a worse condition to the economy, management, security, or politic. The reason for this is because the attack might influence the spread or steal of sensitive data from the community and it might be a threat for them. The way of prevention and solution after ransomware attack might be solved with the approach discussed in this paper. This introduction will be Section 1 for this paper. Then, follow with Section 2, literature review on prevention approach and solution for a ransomware attack. Besides, Section 3 is the prevention approach that might avoid from hit of ransomware. Thus, Section 4, a discussion about the solution that can be used by victims after or once they suffer from a ransomware attack. Lastly, ended with Section 5 includes discussion, acknowledgment, and reference.

2 Literature Review

As we know, the case of a cybercriminal from day to day due to the attack from the hacker to gain the money by using malicious code as one of the tools. Ransomware is an example of malicious software that will harm and damage a device no matter it is personnel, enterprise, organization, or other else. It will bring a critical impact and a lot to the victim in both financial, privacy and management aspect. The target that ransomware love to target is user-wise and system-wise (digital device) (Maurya, 2018). An example for user wise, the healthcare organization especially hospital become the popular target to trigger ransomware attack due to the reason: patient's information and digital medical report and the vulnerability of security system. The attacking rate of ransomware on patient information and record are gain from 55% to 64% within a year (Paul III et al., 2018). The hospital that hit by the attack of ransomware is necessary to make payment because it is the most effective way to get back all of the sensitive data such as patient's medical record even though the payment that requires are in a big amount (Humayun et al., 2020). The hospital has the responsibility to protect the privacy of the patient.

2.1 Ransomware Prevention Techniques

In nowadays, the victim who has been attacking by ransomware are looking for more approach to prevent the attack. It can directly control the loos of economic that might be the most critical threats in cyber-crime. Based on the statistics analyzed by the researcher, over half of malware attack reports in 2017 are ransomware and the newbie of cyber-crime might the ransomware when the victim access the service of the website (Alam et al., 2020). Science and technology researchers are researching and developing better prevention methods so that people will not be attacked. They also shared many previous preventive measures by publishing the research paper. However, a few methods that can be used to overcome the attack of ransomware. In this section, the author will discuss the prevention technique and solution from previous research that might reduce the chance of ransomware attack. Ransomware prevention technique can be separate into few ways, which is user behavior and system.

2.1.1 User Behavior

The behavior of a device user and careless of them are always the causes of getting attack from ransomware. Some of the users in an organization might share their account of a software or application with others people and set an easy password for it. Sharing an account with others might explore the weakness and the attacker might hack into the system via the account. The attacker might take the chance to attack the system and ransom the data if the employee is not aware of their account security that logged in by using the device in the organization. So the user is highly recommended to set a strong password with a different character and do not connect to an unknown public network because it may gain the chance and risk for hackers to hack into the device. The organization may be asked the IT department to prepare a talk that related to a ransomware attack or education in cybersecurity for all employees. The content of the talk related to the dangers of ransomware, how it spread from a phishing attack, and its role on data security in the organization (Tamburello, 2017). Therefore, the risk after the attack must be informed to all the employees due to the safety of the organization are depends on their internet usage behavior.

2.1.2 Prevent the Clicking on Links or Attachments

Ransomware can be disseminated through many approaches, the most familiar approach that known by people is phishing attack (Richardson & North, 2017). The attacker will create a crafted email to the victim and trick them to click on the attachment or links that contain malicious code. Those malicious content can be send together, in many form with the link or attachment, for example, PDF, ZIP, Word Doc or JavaScript (*.exe, *.pdf, *.doc, *.cmd, *.scr, *.jar file). After the victim has a click on the links or attachments, they will redirect to the malicious site. The harmful file will spread into the device before the victim realize they are clicking on a weird malicious site and started the trigger action such as locked device, encrypt file and program, stealing information and so on. In case the user is an employee from an organization, they suggest to visit and access the safety site based on the "whitelist" which allow the specific program to run on the device and block others disallowed program to avoid the malicious attack (Sittig & Singh, 2016).

2.1.3 Identify Ransomware with Different Approach

Currently, many approaches take place to avoid the attack of ransomware on the device. The first approach that is used in avoiding ransomware is the Signature-based approach. This approach is the most common technique for detecting malware include ransomware. The process will be going on by detecting the unique characteristic of it such as a series of bytes in ransomware script, functions, and message of required demand (Ashwin et al., 2019). The antivirus is involved in this approach to detect a footprint of known malicious software in a device. The mistake ratio is quite low and an alarm will trigger if a well-known pattern appears. However, the antivirus is not able to solve completely the problem of malware, it can only detect the ransomware but the action can't be stopped once it is taking over (Mohammad, 2020). Next, the behavior-based approach also the popular approach used by people nowadays due to the efficient tools to protect the attack from threats. It will estimate the object depends on the expected actions before the actual behavior observation. The actions that will be triggering by a behavior-based approach are file access and file system activity and network behavior (Alshaikh et al., 2020).

The others approach that might use to identify the occurrence of ransomware is heuristic detection techniques. The heuristic detection technique is a process of analyzing malicious code. It will evaluate the command in the software or system that are not often occurring in the application. The engine of the heuristic technique can search for the function of the malicious file. There are three sub-analysis under the heuristic detection technique that are file-based analysis, weight-based heuristic analysis, and rule-based heuristic analysis (Ashwin et al., 2019). The file-based analysis will investigate the file path and understand it. The file will be categories as malicious if the command in it includes a delete or harmful file. The weight-based analysis will be analyzing all functionality on weight with the rate of danger that may cause. The file considers as malicious if the total weight same or over. Last, rule-based analysis focused on analyzing the malicious file where getting rule from the file, then measure up the previous rule with the initial rule. If both of the rules are the same, then it will send a warning to the user.

2.2 Solutions after Ransomware Attack

Attacking from ransomware to the vulnerability of a program or device is an unexpected incident even the prevention is made and detection technique always used to avoid it. The victim for sure desires to reduce the losses to the minimum, get back the information data, and trying to recover. Based on the advice from the FBI, the first thing to do is make sure you never pay the demand for an attacker after you confirm that you are infected and attack by ransomware on your device. This is because ransomware attacks are considered cybercriminal that spread quickly globally. The case of ransomware attack might be gain due to attackers will gain money through the way, they know that the victim or their company are willing to pay the demand to get back all the important information (Lee et al., 2021). However, the data and information that encrypt might not completely get back from the attacker. This section will review commonly used solutions in others research after ransomware.

2.2.1 Back Up and Unplug the Infected Device

The value of data and the appearance of crypto-currencies is the reason that makes ransomware effective nowadays. This situation creates a road for the attacker to receive the demand payment anonymously. The user must back up all the significant ad useful data in an offline approach. During the process of backup, the user must ensure that the backup set is not connected to the computer, this will save the data from stealing or destroying if the device is hit by the attacking again (Sittig & Singh, 2016). For an example in organization or healthcare center, once you have realized your device are infect by the ransomware, please immediately unplug the device to reduce smash up of file and program. Besides, inform the IT professional to immediately secure the important data, copy an offline backup, and store it in another safety device. The administrator needs to take responsibility to turn off the network that connects to the infected device to minimize the spreading of ransomware (Zetter, 2016).

Nevertheless, the time taken and cost to recover or back up are always the problems faced by the organization, some of the back-ups will use huge of storage of a device and cause the slowdown of the system. However, they must concern about the cost and the time needed to maintain the dependable backup data (Morris, 2021). The backup solution is not recommended and is considered the last strategy after the attack of ransomware.

2.2.2 Insurance Policy in Cybercriminal

Currently, the attack of ransomware has become the trend of a cybercriminal and spreading widely globally. Many organizations, enterprises, and companies are unfortunate hitting by the attack. The high cost of financial losses will lead them to a critical condition such as bankruptcy, divestment of investors, and be in a financial strait. There is a trend that springs up within organizations, enterprises, and companies to overcome the financial problem faced after an attack by ransomware. Most of them are looking for the cybercrimes insurance policy that can help them to cover the financial losses that cause by ransomware attack. A few processes that similar to normal insurance claiming will going on to claim the losses from the cybercriminal insurance policy. The victim needs to file the document, which includes the evidence of attacking, demand payment, losses list, and so on. However, the expected losses of a ransomware attack can be defined into few categories: break of business, expenses to clear the infecting file from the device, and expenses for recovery (Narain, 2018). The payment of demand is not a good way after attacking. The attacker might take chance to attack again if the demand is paying immediately to get back the data, it will also cause the rise of criminal cases from time to time.

3 Prevention

The advancement of science and technology has brought people a lot of conveniences and improved the quality of life, especially the internet. The huge rate of internet usage during the pandemic within 2020 to 2021 proved the statement above, in which people used the internet and technology to overcome the impact that causes by Covid-19. The employee continues their work with the use of the internet on a work-from-home basis, the student continues their studies with online class are the great example for it. Although the advancement of science and technology has brought a lot of conveniences, it has also brought a lot of harm to the community, such as cybercrime and cyber-attacks. The cyber attacker will try to steal, encrypt the file of the user to gain money from demand by using malicious software. Users can re-access their device or file after paying the demand via crypto-currency such as bitcoin (Aurangzeb et al., 2017). The worst cyber-attack that happen within the year was "WannaCrypto" or known as WannaCry, it was happening in May 2017. WannaCry Ransomware is one of the malware that encrypts and locks the file, program or data hostage of the user in a device, the user is only allowed to access the encrypted file after they pay the ransom demand (Mohurle, & Patil, 2017). This attack has attack around 230,000 devices all over the world. However, the infection of ransomware can be carry on with the entire prevention. This section will discuss the prevention method proposed by the authors.

3.1 Update Operating System and Security Software

There is an entire user that not aware of the damage of out date operating system and software. These operating systems and software will no longer to against the attack due to the weak defense system and protection. The operating system that out of date is not allowed to support the latest update that release by the vendor. The attacker would like to hit the victim if they found that the security vulnerability occurred. Operating system, explorer, and defender application must always keep it in the latest version, the third-party plug-ins application are strongly recommended installing in the device to increase the safety of device if the device is allowed to support it (Richardson & North, 2017). The example of the third-party plugins is Java and Flash Player. This is one of the ways to protect the device from attack but not to escape from unharmed.

3.2 User Awareness

The occurrence of tricky email, link, and attachment in the browser always the initial point of spreading ransomware. The user plays an important role in protecting the device, file, or data from a ransomware attack and always aware of the news related to cyber. The user is encouraged to attend and study more about the malware attack, which is the trend for now. The best practice that can be started for the user is to set a strong password for an account on their device including software, email, and financial account. For example, did not open and view an email from an unauthorized sender and scan the email before review. Categories the email as spam if suspected file as malicious. They have to aware when connecting to a public network. Thus, the installation of paid software is always needed for the user for a specific purpose. Most of the user are prefer to install the cracked paid software from the free website due to fee for some paid software are expensive and the cracked software are cheaper compare to it. However, they did not realize that some of the websites or buttons to download the cracked software might contain malicious files that can harm their device. User has to think twice before their take action to download.

For the organization, they might hold a talk for the employee to be more aware while they access the network during work. In preventing the system of organization hit by ransomware, the employee must understand the risk once the ransomware attacks them. One of the useful suggestions for the employee is avoiding logging their email and not to browser an unknown website on the machine. This is because the malicious attacker would like to create a crafted email that including the malicious file with an interesting title. The harmful file will infect and spread in the machine once the employee attracts by the tricky email (Paul III et al., 2018).l file will infect and spread in machine once the employee attract by the tricky email (Paul III et al., 2018).

3.3 Test Software on an Isolated Computer or Operating System

Software that is downloaded from the entire website has a chance containing the malicious software or file to install together in a device. No one of the users can predict all the software downloaded is completely free from malware. To avoid installing together with the malicious file, the user can try to install the software in an isolated computer that has not to connect to other devices and networks. The infection will not spread to another device or network if the software containing a ransomware file. If the user realizes that the software is installed with the ransom file, they can uninstall whole the operating system or reformat the device. This prevention might reduce the rate of infection, saving time for recovering the data in the device and avoid financial losses.

4 Solution of Ransomware Attack

Updating operating systems, software and using antivirus of a device are the best and effective ways to prevent ransomware attacks. It can detect all the stranger activities in a device and observe it. The warning message will prompt to tell the user if some stranger activity is detected in the device so that the user might take action to avoid it. There is no guarantee that all the data, files, and programs will be completely safe from attack although the prevention is doing at the early stage. Once the machine or device is attacked by ransomware, they need to decide which solution must use to save another device from infection. However, the data that recovery from the attack might not completely recover. Moreover, there are not many of choose to select as the solution to overcome the problem.

4.1 Law Enforcement

Ransomware is considered a critical threat and harmful cybercrime; it causes many people, organizations, businesses, and companies to fall into crisis. There is the implementation of cybercrime law globally to protect the victim and information. Once the victim is attacked, he/she can immediately notify the relevant authorities and take action so that no more people will be victimized. The special law enforcement and method will be used by the leg of the law to the attackers. They apply for the international law enforcement partner to trace the malicious attackers. The result of this action will reduce the rate of cybercrime in the future and rise of arrest rate. Before these, the Federal Law enforcement will take investigate in considering the operation of the victim then cooperate with the related authorities. All the progress of law enforcement with the victim is going on privately to avoid the spoiled of information. The attacker that is arrested will be sue with the related law such as cybercrime law, procedural law, and each other else.

Once the victim is recovering from the cybercrime incident, they need to do more prevention such as back up, updating their device's operating system, software and gain knowledge related to cybersecurity and also cybercrime. The Department of Cyber Security of a state needs to implement and do more repetition to avoiding the same thing happens in the future. In the addition, the victim is going to evaluate their response during the incident and the advantage and disadvantages of the response plan.

4.2 Isolation and Rescue

In previous, malware is categorized as a threat over the world, but compared to ransomware it becomes less rate of threat due to the characteristic of ransomware that it is more attacking and demand (Aurangzeb, 2021). The cybersecurity personnel is facing a critical challenge to overcome and wipe out the ransomware during the recovering process. It will be spreading quickly, infect the device, and network connection before forwarded to the user. If there is one of the devices infected, the user must quickly turn off the power of the device and isolate it from the other. Then, check which network that it connects to and shut down the network immediately to avoid more infection to the whole network. The user should also immediately rescue the data by novel practice to the offline device. Novel practice can protect files and systems from the ransomware attack, back up all files to prevent data losses (Mohurle & Patil, 2017). They need to make sure that the offline device is free from malware and does not have a connection with the infected network. Thus, changing of account, the network password is required if it is possible. Process rescue data also can get on with the decryption tools that offering by the No More Ransom Project (Narain, 2018). The decryption tools that offering by this project are around 52 tools that cover hundreds of ransomware families.

4.3 Network Separation

All of the victims for sure will scare of the threat from ransomware and feel afraid if they are hit by it again. One of the solutions after the ransomware attack to the victim is network separation. Network separation is known as a very useful method to decrease the rate of attack. Network separation will divide the connecting network of the device into subnetwork due to the separation of network traffic that operates and work independently. This technique will enable the attacker to access or entry the device via the network connection. Most of the organization prepare the newest prevention approach to reduce the attack from ransomware via their network. For example, the Company of Cisco had designed a particular security system called Advanced Malware Protection (AMP) to scan and avoid ransomware attacks. AMP can be used for file reputation, observe file activity and evaluate the level of threat.

5 Discussion

In this article, we can know that ransomware is malicious software that will harm, stealing and encrypt the file of the victim make the victim unable to access it (Nardone et al., 2016). The encrypted file is only allowed to access after the victim makes the payment of demand. It is a threat that everyone is scared of especially the sector that operates with sensitive data, such as healthcare centers, state government, organizations, and so on. The rate of cybercrime related to a ransomware attack can be reduced if the law enforcement and solution are used correctly. Many preventions that can find from the internet and research can temporarily escape from the target of a ransomware attack. The prevention discusses in this article can be divide into two, which are artificially or machine. The prevention with updating operating system and software is the potential preventing method. The built-in antivirus and window defense program of an operating system can effectively prevent ransomware from quickly attacking users' devices. Once traces of the virus find out, the anti-virus on the device will send a system notification to let the user notice. Then, the updated operating system has patched the existing system vulnerabilities and leaving the attacker with no trace.

In many cases of ransomware attacks, users are the main reason for the attacks. For example, when a user randomly browses an unknown webpage or links, it is likely to bring ransomware with the malicious file into the device. The author strongly recommends that users use authenticated browsing web pages, such as URLs with HTTPS. This type of URL is more secure than the other else. Thus, connecting to an unknown or public network may also bring the risk of being attack. The attacker may hack into the public network to wait for the victim to connect with their device, but the user unknowingly the attacker already implant the malicious software. In the expectation of attackers, victims will pay the ransom demand to exchange the encrypted file.

Otherwise, the solution after the ransomware is also discussed in the previous section, which is law enforcement, isolation, and rescue. In the author's opinion, isolation and data rescue are the most effective way to solve the problem after the attack. This is because, some of the time, the attacker is difficult to arrest due to they are knowledgeable in hidden track and run from the trace of legal authorities. Isolation of infected devices after unplugging can reduce the chance of infecting more devices. Back up all of the data files are not recommended here due to it might take a long time to restore, occupy spaces and spend more and more cost on it.

Lastly, initial prevention that has been made by the user can effectively avoid the propagation from the ransomware attack. Every man has their responsibility to protect themselves from cybercrime that always happens wisely. If someone is unfortunately hit by the ransomware, they are encouraged to report the incident to the legal authorities and share their experience with others. So that there are, no one will have the chance to become the next victim of the cases. The cooperation between victim and authorities is important to increase the chance of attacker arrest.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conduct for the purpose of System and Network Security Research Project. This work was support by the Ministry of Higher Education Malaysia and University Utara Malaysia.

References

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Paul III, D. P., Spence, N., Bhardwa, N., & PH, C. D. (2018). Healthcare Facilities: Another Target for Ransomware Attacks.

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, *7*(2), 624. Krause,

Tamburello, L., Mulvaney, M. D., & Carpenter, L. L. P. (2017). Your Money or Your Data: Ransomware and Modern Health Information Technology.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: a survey and trends. *Journal of Information Assurance & Security*, *6*(2), 48-58.

Byrne, D., & Thorpe, C. (2017, June). Jigsaw: an investigation and countermeasure for ransomware attacks. In *European Conference on Cyber Warfare and Security* (pp. 656-665). Academic Conferences International Limited.

Shah, N., & Farik, M. (2017). Ransomware-Threats Vulnerabilities and Recommendations. *International Journal of Scientific & Technology Research*, *6*(06), 307-309.

Mohammad, A. H. (2020). Ransomware evolution, growth and recommendation for detection. *Modern Appl. Sci*, *14*(3).

Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware: Evolution, target and safety measures. *International Journal of Computer Sciences and Engineering*, *6*(1), 80-85.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2020). Internet of things and ransomware: evolution, mitigation and prevention. *Egyptian Informatics Journal*.

Alam, M., Sinha, S., Bhattacharya, S., Dutta, S., Mukhopadhyay, D., & Chattopadhyay, A. (2020). Rapper: Ransomware prevention via performance counters. *arXiv preprint arXiv:2004.01712*.

Aurangzeb, S., Rais, R. N. B., Aleem, M., Islam, M. A., & Iqbal, M. A. (2021). On the classification of Microsoft-Windows ransomware using hardware profile. *PeerJ Computer Science*, *7*, e361.

Lee, S., Park, M., & Kim, J. (2021). Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator. *Electronics*, *10*(1), 16.

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, *975*, 8887.

Zetter, K. (2016). 4 ways to protect against the very real threat of Ransomware. Retrieved from Security, http://www.wired.com/2016/05/4-ways-protect-ransomware-youre-targe

Narain, P. (2018). *Ransomware-Rising Menace to an Unsuspecting Cyber Audience* (Doctoral dissertation).

Ashwin, K. H., Deepika, S., Priyanka, G. A, & Bindinganavalle, N. (2019). Detecting Zero Day Malware. *International Journal of Engineering Research & Technology (IJERT)*, *8*(05), 591–595.

Morris, J., Lin, D., & Smith, M. (2021). Fight Virus Like a Virus: A New Defense Method Against File-Encrypting Ransomware. *arXiv preprint arXiv:2103.11014*.

Nardone, V., Santone, A., & Visaggio, C. A. (2016). Ransomware Steals your Phone. Formal Methods Rescue it.