DS Journal of Digital Science and Technology
Volume 1 Issue 1, 1-9, Jul - Sep 2022
ISSN: 2583-5416/ https://doi.org/10.59232/DST-V1I1P101

Original Article

Detection and Prevention of Ransomware Attacks using AES and RSA Algorithms

K. Raja

School of Information Science, Annai College of Arts and Science, Kumbakonam, India.

viceprincipal@annaicollege.com

Received: 31 March 2022; Revised: 14 June 2022; Accepted: 22 June 2022; Published: 08 July 2022;

Abstract - At the moment network security is the vital role for all the administrations and also for the government offices. Ransomware attack is one of the most wide spread attacker in grid or network environment and increasing the every year very heavily. This ransomware attack is the blackmail based attack and it locks the victim users of source of content and demands the money to release. Over the last rare years many number of high profile ransomware attackers are observing here. in this paper we proposed the detection and prevention technique using advanced encryption standard algorithm from Ransomware attack. It is very difficult to recover the information which is attacked using cryptographic based approaches. It will show to reduce the network traffic and increases the efficiency whenever compare to proposed approaches.

Keywords -Ransomware attacks, Detection, Prevention, AES and RSA Cryptographic algorithms.

1. Introduction

Attack is executes the harm on the computer. There are different kinds of attacks are available. Those are active attack and passive attack. Ransomware attack is gentle of malware and that is pointing the key data. This Ransomware attack is fastest growing malware and pointing to all kinds of users. These Ransomware attacks mostly generates the terror in the mind for the holder of the system of losing their serious files or canceling the document information. We need to detect the various types of ransomware attacks and protected from ducking the financial loses.

Ransomware is the largest peril to the corporate network and private networks as well. Due to these danger of attacks, there is huge loss in all the business sectors. This Ransomware attack is stealing the filesand it's not possible to access the files until to know the exact key of information which is available with hijackers. Ransomware attackers are enter into the system in the various ways like downloading of files, attachments and spam emails and from the ports and so on of the different ways. This is very very imputable in business side.

Earlier approaches are detecting the ransomware attacks passively and control the attacks with different mitigation techniques and secure the system. All the existing approaches are ineffective and data is in risk only and many of the privacy issues.

In this paper proposed a detection and prevention techniques using advanced encryption standard algorithms. These techniques are helpful for reducing the ransomware attacks and decreases the network traffic effectively.

2. Literature Survey

In this segment presents the literature about ransomware research. The researcher collected all the potential threats modeled by the malware which consist of system shutdown due to septicity, files loss and economic cost and occasionally damage of life.

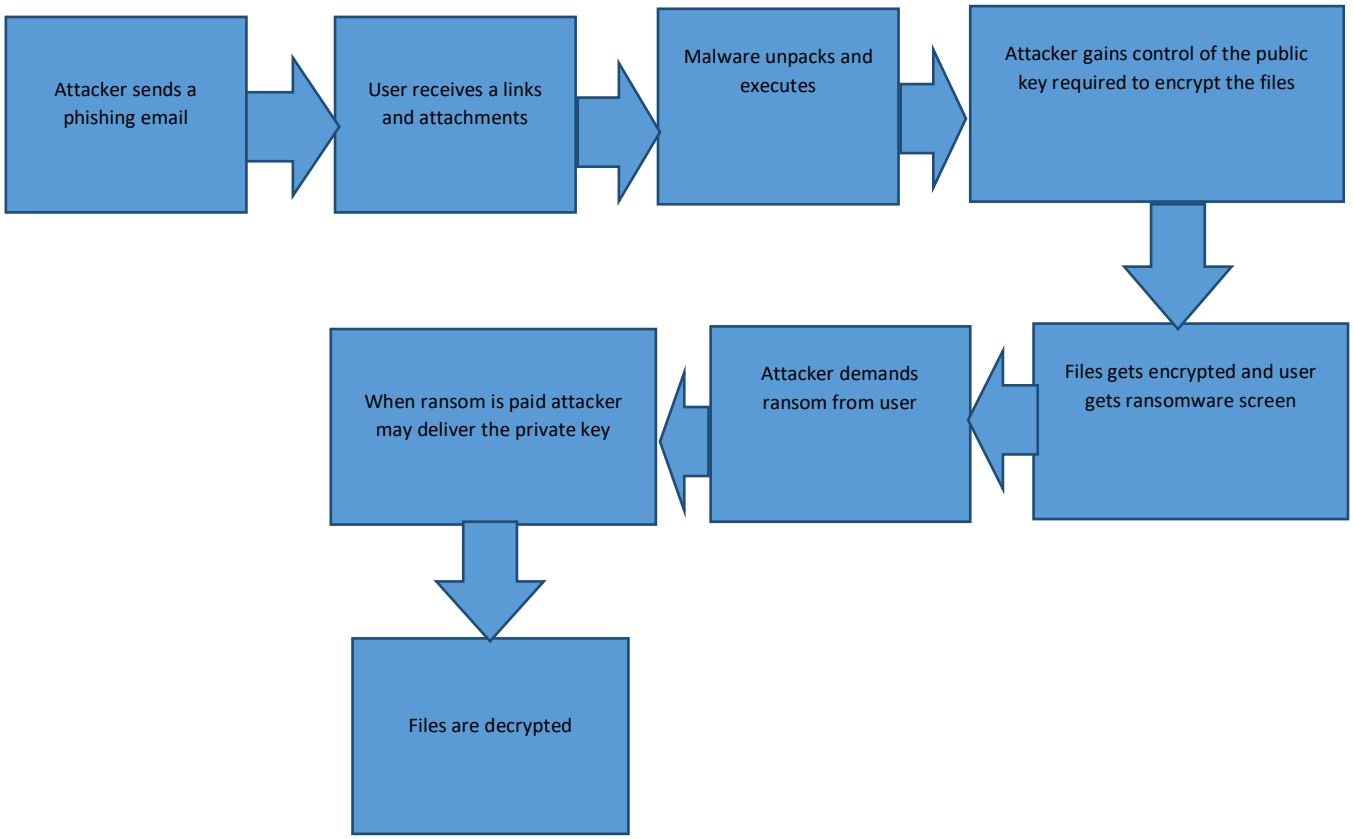

Fig. 1 Ransomware attack flow

The prevention techniques concentration on shunning damage and tentative the attack. Regular backup technique is the best prevention technique to reduction the loss from ransomware attacks. Backups data can be encrypted and decrypted the files is fairly complexlacking of the decryption key. Identifying or guessing decryption key is very complex from crypto analysis techniques and it is very impossible thing. Data backup technique are not sufficient for control the ransomware attacks effectively. Detecting ransomware attacks with various techniques and control the damage.

Researcher proposed a situational parameters to identify the ransomware attacks. Those situational parameters are mapped to ransomware attacks, those parameters are sensitivity, conception, prediction, choice and action. These approaches are also not help to identify the ransomware attacks effectively.

Author proposed a windows based ransomware discovery and stoppage techniques. These resolutions are helpful in these main categories only. Those are delivery, deployment, destruction and dealing. Those categories solutions are mainly focused on user behavior and policies. These approaches are also not working accurately to notice the ransomware attacks efficiently.

Author proposed a ransomware exposure approaches for mobile systems in android environments. It designed with deep learning and big data techniques. Those are detect and prevent the ransomware attacks bit effectively, but not accurate. This deep learning technique are performing the dynamic analysis process.

All the above exiting approaches are discussing the different aspect of solutions for detection of ransomware attacks and threat modeling and prevention things. Those all the approaches are mitigate the different kinds of ransomware attacks. Those are not working up to mark.

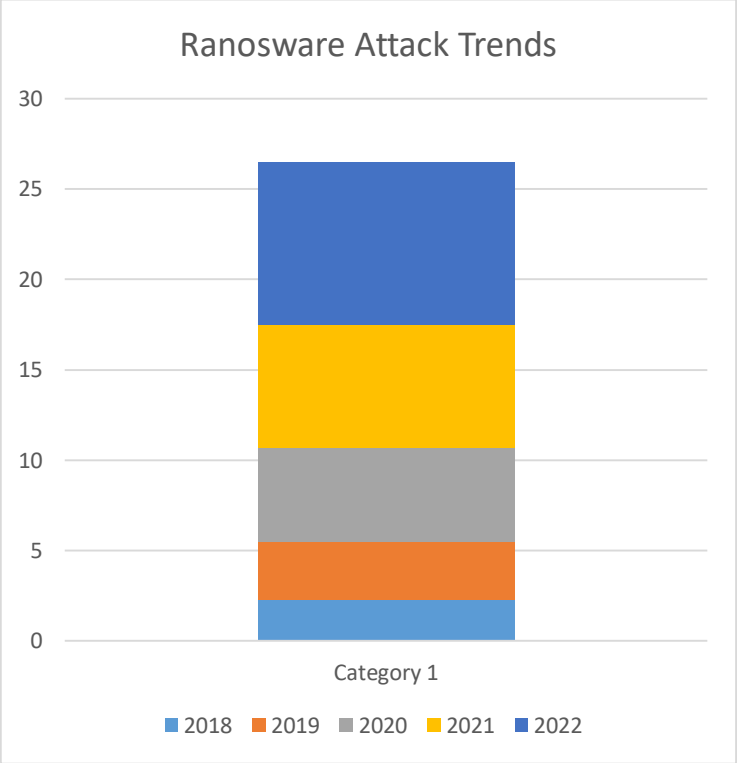

Fig. 2 Ransomware attack trends

the above graph represents number of ransomware attacks are increasing from one year to another (2018 - 2022). Every year numbers of ransomware attacks are increasing and need to control effectively using detection and prevention techniques.

3. Prevention Techniques for Ransomware

A fruitful ransomware attack can be a harmful to a business and administrations needs to paying a ransom demand and lettering off the whipped data entirely. Several actions need to be taken by administrations to reduce their exposure and probable effects of ransomware attacks.

- ✓ Robust Data backup
- ✓ Cyber awareness Training
- ✓ Strong secure user authentication
- ✓ Up to date patches
- ✓ Anti Ransomware Solutions

1.1. Robust Data Backup

The Robust Data Backup solution is an operative way to diminish the impact of ransomware attacks. If the systems are backed up frequently then the data harm to a ransomware attack is very slight. This Robust Data Backup solution should not be encrypt the data and data is kept in read only format to avoid the range of ransomware to drives containing recovery data.

3.2. Cyber Awareness Training

Phishing emails are one of the widely held directions to feast ransomware attacks. User is clicking on the nasty links and opening the attachment, automatically cybercriminals get the access to computers and then start installing and executing the ransomware program on the computer.

Cyber awareness training programs are vital to guarding the organizations against the ransomware attacks. Training programs should share the below information to all the employees in the organizations.

- Don't click on the malicious links
- Don't open the untrusted and unexpected attachments
- Don't reveal the personal and sensitive information to the phishers
- Software legality before downloading it
- Don't plugin the USB
- Use VPN when connecting the public Wi-Fi.

3.3. Strong Secure User Authentication

Cybercriminals may install the remote desktop protocols and similar tools in the organization computers to get the remote access of systems and get the guessed sensitive information and whipped login credentials. Here introduces the strong password policy as a multi factor authentication mechanism and this will helpful to employees to reduce the phishing attacks.

3.4. Up to Date Patches

Many of the organizations are not applying the patches in time and resulting the ransomware attack spread inside the organization due to that most of the computers are affected. Keeping the computers are updated with latest patches, those will helpful to limit the vulnerability to ransomware attacks in organizations.

3.5. Anti Ransomware Solutions

Earlier many prevention techniques are not helpful to provide perfect protection. Protecting against the ransomware attacks, anti ransomware solutions monitor the programs running on a systems for suspicious behaviors, if any suspicious behaviors are observed and automatically need to detect without encryption of files and damage on the same.

The above all ways are helpful to protect the organizations from Ransomware attacks.

4. Types of Ransomware Attacks

There are double types of Ransomware attacks, one is Sealed ransomware attacks and another one is the crypto ransomware attacks.

4.1. Sealed Ransomware Attacks

Sealed Ransomware attack is curls the computer from system logged in process by the victim. When the above issue is occurred need to perform the rebooting in safe mode and then automatically restore the original settings. This kind of Locky Ransomware attacks occur less frequently and also resolved the issues very easily.

4.2. Crypt Ransomware Attacks

Crypto Ransomware Attacks can perform the encryption of specific file types which are prized to the victim. These file types are encrypt like documents, spreadsheets, pictures and databases. Whatever the files are encrypted, renamed, relocated, it is impossible to difficult to of stalking and restoring the files.

5. Proposed System

Check point anti ransomware detection and prevention solution is helpful to restore the files from regular backups. Here mainly ransomware attacks is based on cryptographic algorithm such as Advanced Encryption Standard and RSA algorithms. These algorithms are perform the readable text converted into unreadable text format that is called untidy format. Using again another key convert the unreadable text to readable text format that is called decipherable format. Attackers are attack the systems or files and encode the victim user's files. Victim users wants to decrypt the files, they need key information that information is not with victim users. to get the decryption key from attackers or cybercriminals, they are expecting to pay the amount for the key. Cryptographic algorithms are very robust in landscape and it is not possible to crack the key for decrypt the files which are sealed due to crypto ransomware attacks.

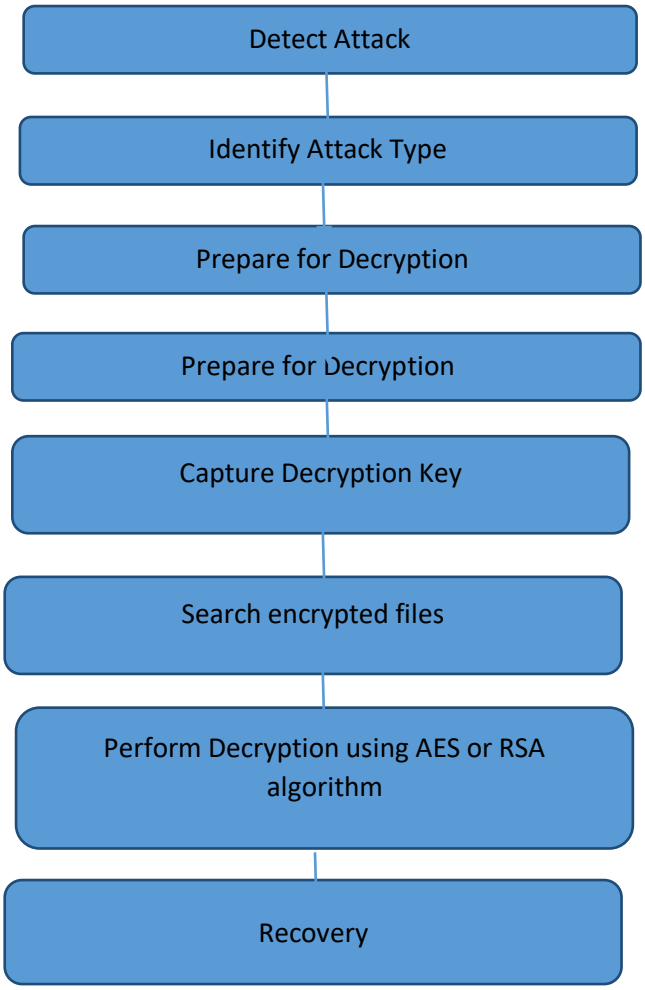

Fig. 3 Proposed system

The above architecture represents the detection and prevention technique and it will process of vindication of recovery from ransomware attack. It will recover and able to decrypt the file and use the file information as required format.

We will implement the monitoring and detecting techniques for identify the possible attacks or malicious code or any malicious attachments whenever transfer the packets to target system. the packet catching mechanisms are perform the analyzation and detecting from likely attack. Those analyzation techniques are wireshark and PCAP. These all the tools are identifying the likely attack information and also identifying the network traffic. One more technique is called sniffing, this will helpful filter the attacked packets and recovery the same. This all the techniques are helpful for reducing the HTTP traffic.

6. Results Discussion

As a result of proposed methodology of detection and prevention measures is best tactic to evade the danger of ransomware attacks. We will apply this kind of prevent measures to reduce ransomware attacks.

Cyber security ventures imagines the business will drop victim to ransomware attack every 13 sec in 2021, every 24 sec in 2019 and every 45sec in 2016. Ransomware attacks are in the upswing and have been getting extra risky in modern years. An attacker is attack the business network that encode the superficial info can cost hundreds and even in million and billions of hundreds. Total number of universal ransomware gossips increased by 486% year finished by year.

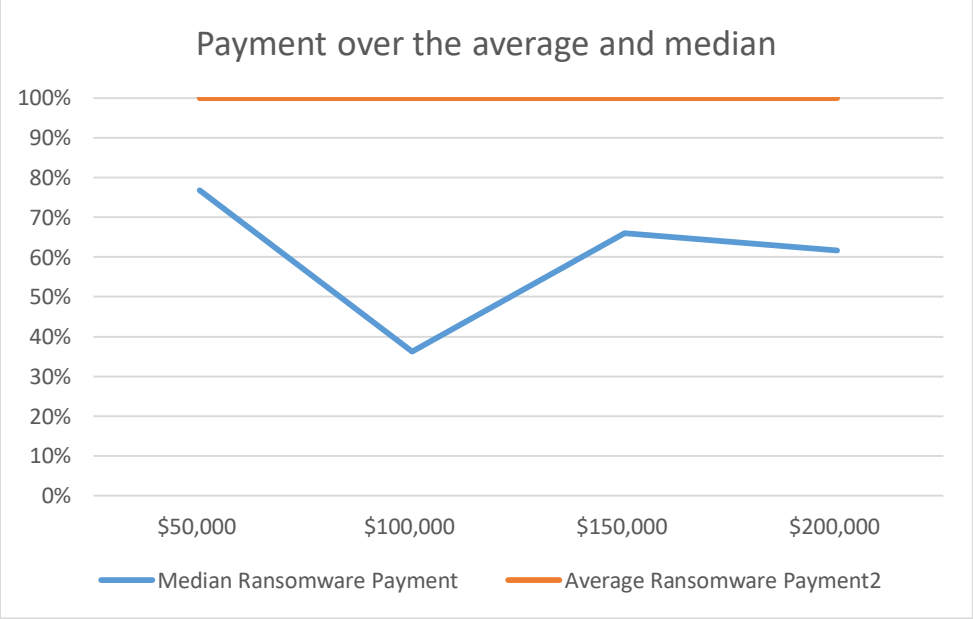

Fig. 4 Payment over the average and median

The graph explain about the average ransomware payment and median ransomware payment. Demands of cybercriminals has been increased year over year in the form of dollar. With this ransomware attacks affects all the industries. These ransomware attacks are pointing other industries like health care sector, and followed by profession services and followed by public sector.

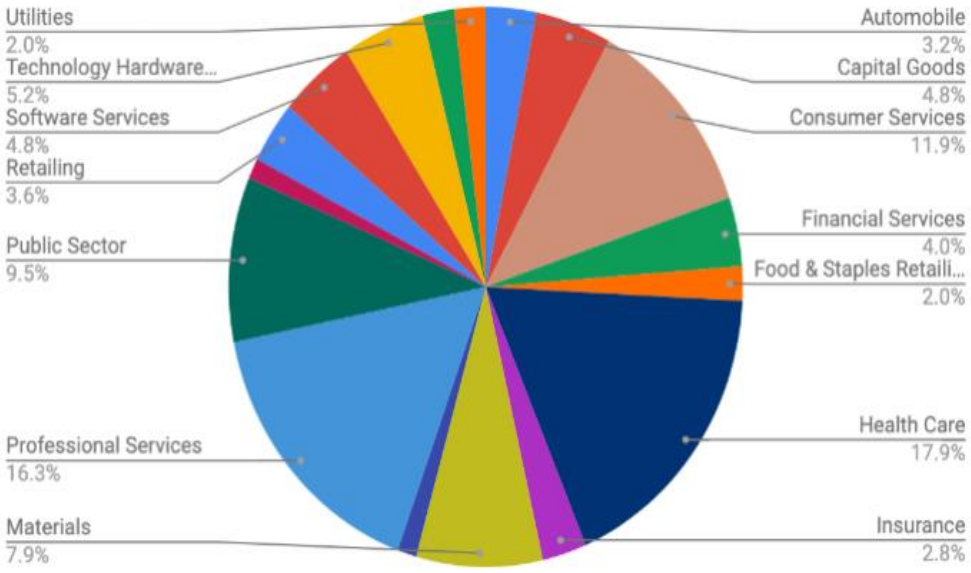

Fig. 5 All different industries pointing by ransomware attacks[Courtesy: Coveware]

We could see the above pie chart represents ransomware attacks percentage on the different industries.

Now we could see the comparison of ransomware attacks detection and preventions in the below chart.

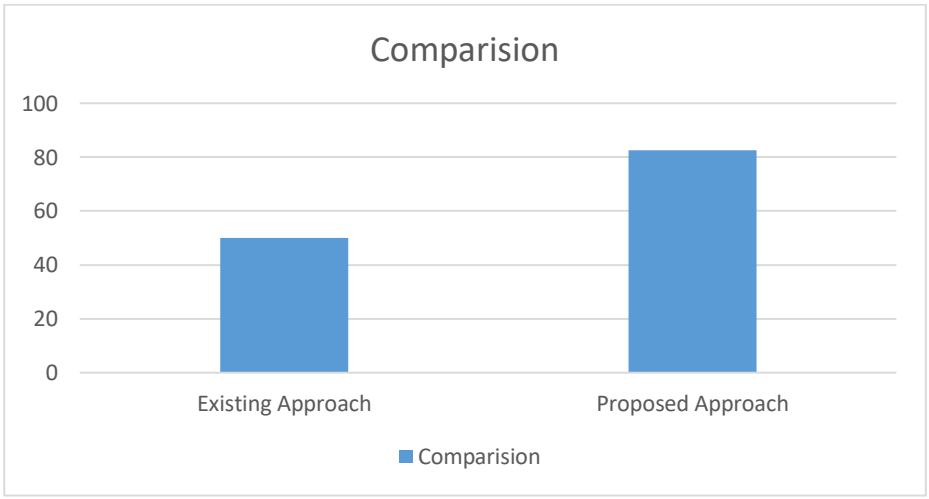

Fig. 6 Comparison performance

We could see the comparison performance of existing approach and proposed approach. Existing approach is able to discover and stop the ransomware attacks as a 50% and it is not that much efficient, however our proposed approach is increases the discovery and stop of ransomware attacks to 82.5. Hence this is best approach, we would need to design some more efficient approaches.

7. Conclusion and Future Work

In this paper first explain about ransomware attacks and types of ransomware attacks and then background of ransomware attacks and then discussed about the prevent techniques. We proposed a detection and prevention techniques that can be control the ransomware attacks using cryptographic algorithms like advanced encryption standard algorithm and RSA algorithms. We have compared the existing and proposed approaches efficiency and proposed approach is control the ransomware attacks efficiently when compare to existing systems.

New methods needs to be designed for cyber profiling and crypto analysis schemes and those schemes are helpful to detect and prevention of ransomware attacks. These new crypto analysis schemes will helpful to increases the recovery of ransomware attacks are more in future. in future some more machine learning techniques are also help to increases the recovery of ransomware attack failures.

References

[1] Xin Luo, and Qinyu Liao, "Awareness Education as the Key to Ransomware Prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195-202, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[2] Amin Kharraz et al., "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," *Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 3-24, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] Philip O'Kane, Sakir Sezer, and Domhnall Carlin, "Evolution of Ransomware," *IET Networks*, vol. 7, no. 5, pp. 321-327, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[4] Alexander Gostev et al., "It Threat Evolution in Q1 2016," Kaspersky Lab, 2016.

[5] U.S. Depatment of Justice, I-062315-PSA, "Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes," 2015. [Google Scholar]

[6] SH Kok et al., "Ransomware, Threat and Detection Techniques: A Review," *International Journal of Computer Science and Network Security*, vol. 19, no. 2, pp. 136-146, 2019. [Google Scholar] [Publisher Link]

[7] R. Surendiran, and K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp. 2217-2224, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] Peter D. Haas, "Ransomware Goes Mobile: An Analysis of the Threats Posed by Emerging Methods," *Proquest LLC*, New Jersey, 2015. [Google Scholar] [Publisher Link]

[9] Helen Jose Chittooparambil et al., "A Review of Ransomware Families and Detection Methods," *Advances in Intelligent Systems and Computing*, pp. 588-597, 2018. [CrossRef] [Google Scholar] [Publ isher Link]

[10] Monika, Pavol Zavarsky, and Dale Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," *Procedia Computer Science*, vol. 94, pp. 465-472, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] Nolen Scaife et al., "Cryptolock (and Drop It): Stopping Ransomware Attacks on User Data," *2016 IEEE 36th International Conference on Distributed Computing Systems*, pp. 303-312, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[12] J. Scott, and D. Spaniel, "*The ICIT Ransomware Report*," 2016.

[13] Ross Brewer, "Ransomware Attacks: Detection, Prevention and Cure," *Network Security*, vol. 2016, no. 9, pp. 5-9, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ibrar Yaqoob et al., "The Rise of Ransomware and Emerging Security Challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444-458, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sumith Maniath, Prabaharan Poornachandran, and V. G. Sujadevi, "Survey on Prevention, Mitigation and Containment of Ransomware Attacks," *Communications in Computer and Information Science*, pp. 39-52, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] R. Surendiran, and K. Alagarsamy, "A Crtitical Approach for Intruder Detection in Mobile Devices," *SSRG International Journal of Computer Science and Engineering*, vol. 1, no. 4, pp. 6-14, 2014. [CrossRef] [Publisher Link]

[17] Ronny Richardson, and Max M. North, "Ransomware: Evolution, Mitigation and Prevention," *International Management Review*, vol. 13, no. 1, pp. 10-20, 2017. [Google Scholar]

[18] L. Constantin, "Widespread Exploit Kit, Ransomware Program, and Password Stealer Mixed Into Dangerous Malware Cocktail," *Pcworld*, 2015.

[19] Daniele Sgandurra et al., "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection," pp. 2-4, 2016. [Google Scholar]

[20] S. Gavaskar, R. Surendiran, and E. Ramaraj, "Three Counter Defense Mechanism for TCP SYN Flooding Attacks," *International Journal of Computer Applications*, vol. 6, no. 6, pp. 12-15, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[21] Shweta Sharma, Rakesh Kumar, and C. Rama Krishna, "Ransom Analysis: the Evolution and Investigation of Android Ransomware," *Proceedings of International Conferenceon IotInclusive Life* (ICIIL 2019), NITTTR Chandigarh, India, pp. 33-41, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Daniel Gonzalez, and Thaier Hayajneh, "Detection and Prevention of Crypto Ransomware," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, pp. 472-478, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Steve Mansfield-Devine, "Ransomware: Taking Businesses Hostage," *Network Security*, vol. 2016, no. 10, pp. 8-17, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[24] Sharifah Yaqoub A. Fayi, "What Petya/Notpetya Ransomware is and What Its Remidiationsare," *Advances in Intelligent Systems and Computing*, pp. 93-100, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] R. Surendiran, and K. Alagarsamy, "A Novel Tree Based Security Approach for Smart Phones," *International Journal of Computer Trends and Technology*, vol. 3, no. 6, pp. 787-792, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[26] Juan A. Herrera Silva et al., "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters," *Remote Sensing*, vol. 11, no. 10, p. 1168, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] S. Gavaskar, E. Ramaraj, and R. Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography," *International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp. 137-140, 2012. [Google Scholar] [Publisher Link]

[28] J. Petters, "Cerber Ransomware: What You Need to Know Varonis," *Inside Out Security*, 2020. [Online]. Available: https://www.varonis.com/blog/cerberransomware/

[29] Aaron Zimba, Luckson Simukonda, and Mumbi Chishimba, "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of Wannacry for Network and Information Security," *Zambia ICT Journal*, vol. 1, no. 1, pp. 35-40, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[30] Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, vol. 1, pp. 113-124, 2019. [CrossRef] [Google Scholar]

[31] Kenneth Kraszewski, "SamSam and the Silent Battle of Atlanta," *2019 11th International Conference on Cyber Conflict*, pp. 1-16, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[32] Zimbaand M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures,"*International Journal of Computer Network and Information Security*, vol. 11, no. 1, pp. 26-39, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[33] Axel Wirth, "The Times They are A-Changin': Part One," *Biomedical Instrumentation & Technology*, vol. 52, no. 2, pp. 148-152, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[34] "Samsam Ransomware Campaigns," Secureworks.Com, [Online]. Available: https://www.secureworks.com/research/samsamransomware-campaigns

[35] Zimbaand M. Chishimba, "On the Economic Impact of Crypto-Ransomware Attacks: the State of the Art on Enterprise Systems," *European Journal for Security Research*, vol. 4, no. 1, pp. 3-31, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[36] M. Midler, K. O'Meara, and A. Parisi, "*Current Ransomware Threats*," Carnegie Mellon University, 2020.

[37] J. Schultz, "Sodinokibi Ransomware Exploits Weblogic Server Vulnerability," Blog.Talosintelligence.Com, 2020. [Online]. Available: https://blog.talosintelligence.com/2019/04/Sodinokibiransomware-Exploits-Weblogic.html

[38] L. Tung, "VPN Warning: Revil Ransomware Targets Unpatched Pulse Secure VPN Servers Zdnet," *Zdnet*, 2020. [Online]. Available: https://www.zdnet.com/Article/Vpn-Warning-Revilransomware-Targets-Unpatched-Pulse-Secure-Vpnservers/