ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse701022021.pdf
https://doi.org/10.30534/ijatcse/2021/701022021

Security Awareness on Ransomware Threats Detection and their Protection Techniques

Muhammad Waqas[1], Mansoor Ahmed Khuhro[1], Umair Saeed[1], Kamlesh Kumar[2], Naadiya Mirbahar[1, 3], Ruqiya[1]
[1]Department of Computer Science, Sindh Madressatul-Islam University, Karachi, Sindh 74000, Pakistan.
muhammad.waqaspn@gmail.com, makhuhro@smiu.edu.pk, umairsaeedmixit@gmail.com, naadiya.khudabux@yahoo.com, ruqiyaabbasi42@gmail.com
[2]Department of Software Engineering, Sindh Madressatul-Islam University, Karachi, Sindh 74000, Pakistan.
kamlesh@smiu.edu.pk
[3]Department of Computer Science, Benazir Bhutto Shaheed University Lyari, Karachi, Sindh, Pakistan.
naadiya.khudabux@yahoo.com

ABSTRACT

Computing and smart monitoring devices or machines are involved in every organization and sector in present era. These machines have any operating system (OS), software and applications installed based on the requirement. Due to available security vulnerabilities in OS or software and applications, these machines have more chances to become victims of Ransomware attacks. Attacker demands for ransom in any form of cryptocurrency like Bitcoin and other to normalize the files and services. Ransomwares are pandemic threats globally. Paper focuses on this part of the cybersecurity issues, the latest ransomware and their variants. In our research, we tried our best to explained ransomware and millions of dollar damage done by them in the past few years. Further, we have provided different ransomware spreading and detection mechanisms. At the end of the paper, if any machine infected through ransomware so some prevention, protection and recovery tools and techniques have been mentioned.

Key words: Cybersecurity, Cryptocurrency, Ransomware, Security vulnerability, Smart devices.

1. INTRODUCTION

Today, security threats to multiple corporations, businesses with a small or large scale, health care, local or governmental organizations and end users are constantly on target [2]. Hospitals around the world are also facing such types of challenges because of the vast usage of IT equipment in the health sector [12]. These threats are rising day by day as malevolent techniques are getting more powerful since their inception. In Atlanta, approximately one third of users applications were encrypted through SamSam ransomware in 2018 [6] and the cost of restoring the computer network was 17 million dollars [7]. On February 29, 2020, [46] [47] published at their websites that municipal government of City of Cartersville became the victim of ransomware attack on May 6, 2019. Their 3 terabytes were affected over the week by this ransomware attack. Attackers demanded 2.8 million dollars to remove file access limitations. After negotiation, victim paid 380,000 dollars in non-tradable bitcoins with 7,755.65 dollars paid for negotiators and transaction fees additionally. They got access to their files with 48 hours after the payment. Adel Hamdan Mohammad [49] in his work presented the annual earnings of ransomware from 2015 to 2021 and predicted that in 2021, this damage will be up to 20 billion dollars. The cyber and malware attacks are serious threats over the internet to be considered seriously.

This paper highlights one of cybersecurity issue, latest ransomwares with different classes and versions. Further, this paper provides what are the difference between ransomware and other terms? How these are spread? By whom and why these ransomware inserted and how anyone can survive from these attacks?

Malware is a threat which is designed to put any system in an alarming zone by replicating itself in machines like computers, smartphones, smart devices, etc and spreading through all attached directories (USB or Diskettes) or even to the multiple systems attached to the same network. The malevolent coded program, viruses, trojans, crimeware, spyware, ransomware, worms, botnet, and adware, etc all come under the umbrella of malware as described in figure 1, which is an acronym for malicious software. According to a report over 350,000 malware files and potentially unwanted applications find by AV-TEST Institute every day [1]. Malware different versions are designed to steal someone's information to harm financially or reputability.

No matter which operating system an individual or organization is using, they may be involved in the list of victims. An individual and employees of the organization surf hundred of website every day on the internet which involve malicious websites also and their systems have become the victim of malware and viruses without even familiar about it. As the mitigation techniques are improving, scammers also

enhance their software capability with file less malware as an effective method which makes it more difficult to detect by the available anti-viruses software.

In rest of the other as mentioned above, this study focuses on the ransomware[2,5] because these are global pandemic and more harmful since its inception up to date. The term ransomware is a combination of ransom and malware [50], although it is the subcategory of malware but with a huge hazardous impact. It is launch to target an individual, whole organization at small or large scale and local government (because of less training to face these attacks), power grid and even hospitals [2] [12] [22]. In result, empowers the attackers to get full access control to the system and blocks access of the owner by either lock the whole system and show screen lock at startup or encrypt the confidential, official and personal data files by cryptographic techniques. After encryption, a popup message or an email is released mostly a windows API which is used to make payment demand in the form of cryptocurrency because of its high privacy parameters and worldwide acceptance such as Bitcoin [3,5], Monero [5], Ethereum [5], DASH [10] and other formats of payment which remains the attacker anonymous [4] and no decryption key will be issued until ransom is paid. The demand is made for the short time duration with the threat to double the ransom amount or destroy the decryption key if the ransom is not paid within the timeline. In March 2020, some of ransomware attackers announced that as the world is suffering from Coronavirus outbreak, they will not attack health care sectors [48].

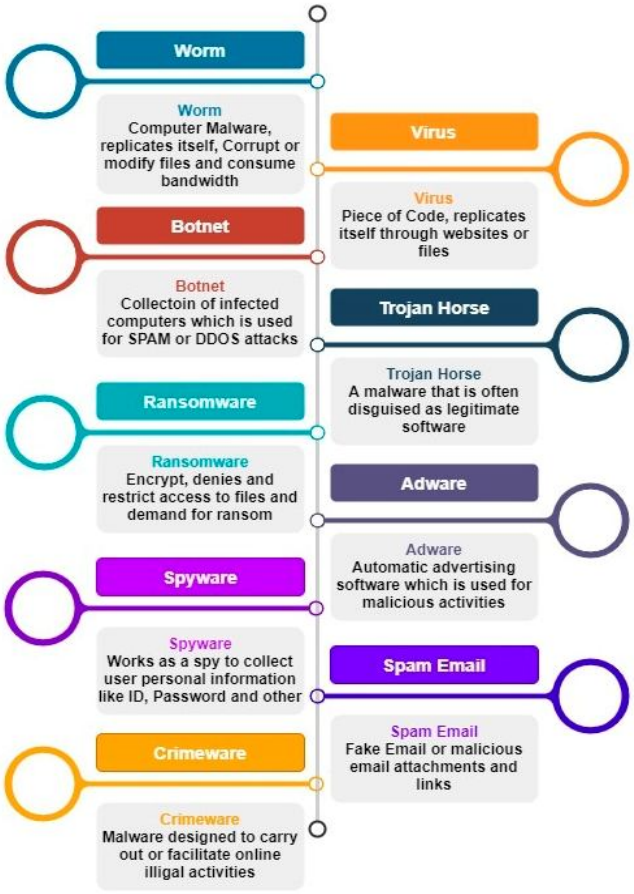

Figure 1: Types of Malware

The rest of the paper has been designed as the section II highlights the literature review about the ransomware since it first infection and number of variants with passage of time, section III describes the how the ransomware spread and number of tricks use to spread it, section IV explains the detection and protection techniques and what parameter should take in case of infection. In the end section V, defines the conclusion and future work.

2. LITERATURE REVIEW

This section highlights the prominent amount of related materials in ransomware evaluation, injection into the machine, encryption, detection, protection and mitigation methods. Ransomware is not a new threat which is facing by many organizations globally. In 1989, the first ever ransomware named PC Cyborg or AIDS Trojan was released by Dr. Joseph Popp, who was an anthropologist and distributed 20,000 copies of 5.25 diskettes via postal mail to the attendees of World Health Organization conference [50]. The Trojan in disk infected the AUTOEXEC.BAT file, which encoded the files after every 90 reboots and a ransom of $189 for the normalization of computer operation at mailing address in Panama has been demanded [8][9][10].

Monika et al [11] published the evaluation of ransomware till March 2016 in windows and android platforms. 25 different families of ransomware have been taken in which 17 were related to windows and 8 were for android. To remain unbiased, 3 variants from each family have been analyzed and observed that every variant behavior was the same but with different payloads to carry attack. They collected ransomware samples from multiple resources such as 90% from Virus total [11] [22], 8% from public malware repository by crawling [11] and 2% by security forums through browsing. In android analysis, if any application is asking for irrelevant information and access then it is suspicious. In windows analysis, if machines get infected by any spam email, malicious email attachment or link and malicious website and malware propagate from there. Some of the ransomware encrypts the file locally and some contacts with C2 (command and control) server, they forward the information like pc user, pc name, pc group, pc language, pc keyboard, pc IP, os major, os bit, ransom id, public key, private key, version[10]. Once they get the encryption key, they search files and folders to encrypt and some of the variants delete backup and volume shadow copy with no option left to the victims except payment. In results, paper demonstrated that ransomware detection is possible in Windows environment by timely analysis of abnormal filesystem and registry key activities while in the case of android, installation of applications requires proper attention.

Ibrahim and Taimur [8] described some of the variants of multiple ransomware families like CryptoWall, CryptoDefence, Reveton, Cryptolocker, Lockerpin, TeslaCrypt, and other. Paper identified the damage done by the multiple variants till 2017. Further, paper defined the techniques used by attackers for the propagation of ransomware like spam mailing, exploitation kit, malware advertising and affiliating programs and also the methods of payment for the restoration of

encrypted data. At the end of the paper, some mitigation techniques like recovery of data from backup, level of control access/authorization and online resources for data recovery, etc has been provided. Further, ransomware infects the machines through some of these available possible steps illustrated in figure 2.

Figure 2: Ransomware Infection Process

Vlad Constantin Craciun et al [12] analyzed the development of ransomware and provided an overview of ransomware design, about 50,000 samples selected from 150 variants in 2017 and 100 variants till October 2018. In 250 families, paper chose the crypto-locker due to its outstanding performance. Binary threats can contain both analysis either static or dynamic but in their work they performed static analysis either to guide the threat to execute the encryption or provide the path to victims to pay the ransom. Further, paper presented the extent of total evaluation of ransomware families in which the big percentage of encrypted files have the additional extensions, whole file name has been changed by small percent and very small portion did nothing with the file name. Spreading mechanism like exploitation kits, spam email, OS exploit, RDP brute-force and BotNet/RaaS of 250 selected families and standard algorithms for encryption (RC4, RSA, AES, Blowfish) and hashing (MD5, SHA256) have been declared also. Dean F.Sittig and Hardeep Singh [13] also disclosed the problems and prevention techniques to protect an electronic health record (ECR) about patient health history.

Ross Brewer and LogRhythm[14] explained about the ransomware families (like TeslaCrypt, CryptoWall, CryptoLocker and other) and mentioned that till second quarter of 2015 there were 4 million ransomware samples in which 1.2 million were new. Most of them hit the windows environment because the number of users is higher for its user-friendly environment. Paper described the two types of attacks, 1) Mass distribution attack (Without human intervention and takes about 15 minutes from infection to show ransom note) and 2) Targeted attack (same as an advanced persistent threat and takes more time than mass distribution). Further, paper presented the different phases of ransomware attack from enter into the machine for infection to ransom notification and handling mechanisms.

Yassine Lemmou and El Mamoun Souidi [10] published a deep analysis over the behavior of Gandcrab ransomware on 2 subversions (v1.0 and v2.2r) out of 7 (v1.0, v1.1, v2.1, v2.1r, v2.2r, v2.3r, and v2.3.1r) subversions while Oleg Kolesnikov [17] mentioned the v4.1 has detected in July 2018 and it reached up to v5.2 March 2019 and observed all the versions have same payload with little changes. Gandcrab owner mentioned that they ceased their business on June 2019 [21]. Gandcrab kill the running process to avoid detection except antivirus, monitoring tools and some programs of operating system. It does not encrypt the files which are installed on removable media. It counts the number of antiviruses is installed on machine without any disturbance. Gandcrab avoids targeting CIS countries and it is checked by the function if the language of computer is Russian then the loop exit and marks the value 0 for CIS countries. This paper describes the overall steps taken by the Gandcrab from file restoration in folder, communication with C2, etc and declared some detection and prevention mechanism also.

The analysis of ransomware was first issued by the Alexandre Gazet [15] in February 2010 with no detection method. Amin Kharraz et al [16] presented the result of observation on ransomware from 2006 to 2014. They

investigated the different 15 ransomware families with 1,359 samples and suggested the detection technique to avoid the ransomware attack by paying attention on abnormal file system. Ransomwares emerge on daily basis while it growth increased in past few years and some of prominent ransomwares have been shown in figure 3.

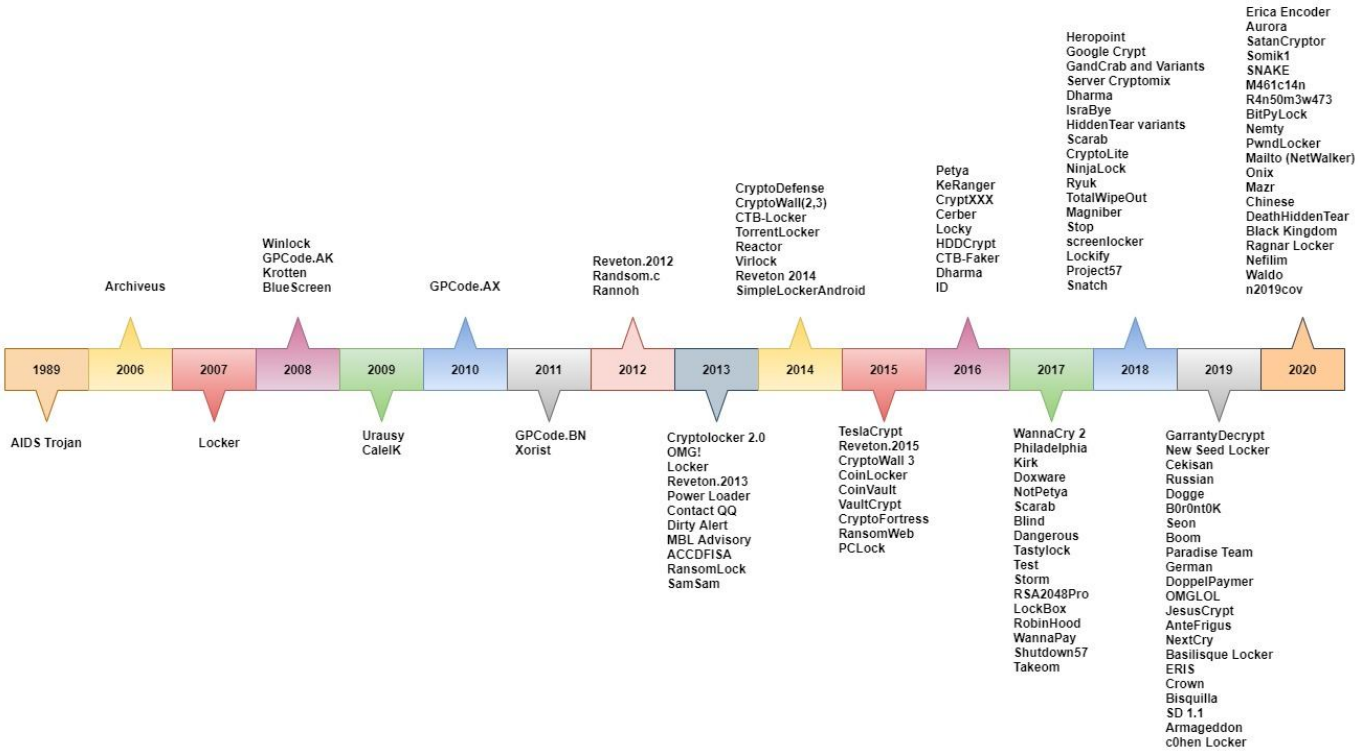

Figure 3: Ransomware Evaluation Timeline

3. SPREADING MECHANISM

This section provides the spreading mechanism through which the ransomware enter, regulate, survive and move from machine to machine. There are varieties of phases through which ransomware attacks are launched.

3.1. Spam and Phishing Email

This is the easiest and very cheap mode for any ransomware to enter into the machine [8] [9]. Attackers use social engineering techniques which attract the victims for viewing the malicious email or malicious attachments. In 2016, 24% in the first quarter while 69% in second quarter were the Locky out of all attacks which were launched through email attachments [8]. In 2019, [12] also mentioned that different ransomware families used spam email. Botnet or Distributed denial-of-service (DDoS) attack is done by this technique [18].

3.2. Exploitation Kit

Exploitation kits make victims to those operating system, applications or software, etc, which are not updated, vulnerable or insecure. CryptoLocker used Angler exploitation kit, which when found the vulnerabilities to execute itself in internet Explorer and Adobe Flash [14]. Cerber used RIG, GandCrab used Fallout, RIG and grandsoft, while Magniber used Magnitude exploitation kit [12].

3.3. Remote Desktop Protocol (RDP)

Remote Desktop Protocol is a popular method through which attackers can easily infect the victims. When machine run with open 3389 port so attackers enter into the machine and by applying brute-force attack with help of some available tools. Attackers can access administrator privileges with multiple password attempts. Once attackers accessed administrator rights then they can encrypt or delete files. LockCrypt, SamSam, GlobeImposter, Lowlevel04 and Crysis ransomware use this method [19] [12].

3.4. Malicious Websites

Malicious websites are also a critical method which is used by the attackers when a user visits such skepticism websites for downloading software/application then it falls under the radar of cyber attack. Downloading software from such websites provides an entry level to ransomware without user knowledge. Reference [18] referred malicious sites as first step to start of ransomware kill chain. According to [19] CryptoWall, PrincessLocker and CryptXXX while in [21] GandCrab uses this method to deliver attack.

3.5. Botnet/RaaS

Botnet is a network which works as a pandemic virus and when finding any vulnerability in machine software it enters and starts its execution as per the instruction of command and control server. Organizations which are manufacturing AI bots should also focus on the security parameters and dark side of these AI bots [20]. Cyber attackers started a scheme as ransomware as a service (RaaS) against some percent of revenue and also keep safe to expose themselves [12]. GandCrab, Corebot, UIWIX, Scarab, Satan use these tactics to launch attack [12] [21].

3.6. Removable or Portable Media

The first ever Trojan was launched by PC Cyborg organization through 5.25 diskette [8] [9] [10]. Australian police informed about malware program to the citizen distributed through USB drives in 2016.

3.7. Affiliated Program

The affiliated program works similar manner as ransomware as a service (RaaS). Attackers with no past experience can utilize available malwares and developed infrastructure to launch an attack with simplicity and effectively [8].

3.8. Operating System (OS) Exploit

Operating system (OS) exploits represent the zero day exploit. Practically no software is design without any vulnerability and security hole. Attackers find out these vulnerable holes to patch the malware code in the software and circulate the ransomware through it.

Table 1 showed the summary, through which ransomwares spread.

Table 1: Ransomware Spreading Mechanism

Serial	Spreading Mechanism	Ransomware
01	Spam and Phishing Email	Nemucod, Cerber, Spora, GoldenEye, Petya and GandCrab
02	Exploitation Kits	CryptoLocker, Cerber, GandCrab, Spora and Magniber
03	Remote Desktop Protocol (RDP)	LockCrypt, SamSam, GlobeImposter, Lowlevel04, Dharma and Crysis
04	Malicious Websites	CryptoWall, PrincessLocker, BadRabbit, GandCrab and CryptXXX
05	Botnet/RaaS	GandCrab, Corebot, UIWIX, Scarab and Satan
06	Removable and Portable Media	AIDS Trojan and Spora
07	Affiliated Program	Cerber and GandCrab
08	Operating System (OS) Exploit	WannaCry, NotPetya, SynAck and BadRabbit

4. DETECTION AND PROTECTION MECHANISM

This section expresses some of the available techniques to detect, prevent, protect and recover from the malware infection. As the accuracy and efficiency of machine learning and deep learning algorithms have been improved and achieved popularity in various domains like health care, banking sector, cybersecurity and others. Besides from aforementioned fields, Cyber researchers are also utilizing these algorithms and designing models for the detection of ransomware patterns.

Qian Chen et al [21] designed a tool, which extracts patterns of malware and performs early detection. They mentioned in their research that manually analysis of malware is time killing and not as much accurate as designed tool. They used three machine learning algorithms, ET (extra trees/extremely randomized trees), TF-IDF (term-frequency inverse document frequency) and Fisher's LDA (linear discriminant analysis) and tested on seven different ransomware families. Experimental results provided that ET performed well in terms of time-efficiency while TF-IDF outperformed other two methods in discriminating features extraction.

Sajad Homayoun et al [22] implemented four classification algorithms like J48 (decision tree), random forest, bagging, MLP (Multi-layer perceptron) over 1624 ransomware samples including 220 benign applications Such as Windows Portable and Executable (PE32). They used sequential pattern mining (SPM) for finding which sample belongs to which ransomware family through maximum frequent patterns (MFP). They calculated the accuracy through Confusion matrix, precision, recall, F-score, Roc and AUC. Their model achieved 99%

accuracy for detecting the ransomware as compare to benign sample while 96.5% accuracy for detecting the correct family of the ransomware with less than 10 seconds in time.

Daniel Morato et al [23] proposed a framework named REDFISH (Ransomware Early Detection from File Sharing traffic) for the early detection of ransomware over NAS (Network Attached storage) when ransomware tries to encrypt file in shared network volume. They tested it on 19 different ransomware families and received 99% detection accuracy in less than 20 seconds with more than 10 files encrypted which can be recovered easily. Fairuz Amalina Narudin et al [24] applied 5 classification algorithms like J48 (decision tree), random forest, Bayesian network, KNN (K-nearest neighbor) and MLP (Multi-layer perceptron) over 2 datasets including MalGenome (1,000 samples taken from 49 malware families) and self-collected (30 samples from 14 malware families) for the detection of malware in mobile applications. Random forest and Baysian network provided 99.97% TPR while 84.57% TPR achieved by KNN to detect Android malware. Lorenzo Fernandez Maimo et al [25] used deep learning algorithms for the detection of anomaly and botnet through analyzing the network traffic.

To protect the system from security threats, vulnerabilities should be as low as possible. Emrah Yasasin ei al [26] predicted IT security vulnerabilities for operating system, browser and applications. They presented post-release vulnerabilities through statically approaches like ARIMA (Autoregressive Integrated Moving Average) and Croston's Methodology and neural network algorithm on National Vulnerabilities Dataset (NVD). They calculated the Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) and mentioned ARIMA and Croston' methodology better for vulnerabilities prediction, it will help the software developer in decision making and reduce the damage.

Pedro Tubio Figueira et al [27] performed the risk assessment for future threats occurrence based on past data. They calculated the probability by logistic and SVM regression on Magerit and achieved accuracy more than 70% while they mentioned logistic regression is better because of its simplicity in tuning and time efficiency.

4.1. Updating Operating System and Software

Updating system software applications regularly are the best protection to fight against the ransomware attack. Even Zero-day vulnerabilities when became public, so the attackers have more chances to exploit it. If the system is updated with all available patches so the system has more chances to remain in safe zone [8] [50].

4.2. Data Redundancy

Good data backup strategies can protect any organization or individual to minimize the effect of the ransomware attack [8] [28] [29] [30] [31] [32] [50]. Unfortunately, attackers target the firms and individuals who have no security issues awareness and technically strong enough [22]. Jason E. Thomas et al [9] published the importance of back system for the assessment of security risk to combat against the ransomware attack. They illustrated 3 ways to maintain backup (traditional, continuous data protection (CDP) and replication) with 2 strategies 1) time required to restore the data and 2) time point from which data need to be restored before encryption. There are many solutions available to maintain daily backup like cloud services, data warehouse and offline server. The best defense against the ransomware attack which make it useless to maintain backup to machine which is not connected to network. Some can retrieve data up to 14 days, 21 days and 13 months to 7 years prior (conservative and aggressive approaches) [9].

4.3. Safe Browsing

Organizations can protect themselves through proper training of their office staff. Training should include the awareness of the cyber threats and entry point of these attacks. Utilization of available tools like Microsoft SmartScreen [33], Google Safe Browsing [34], Malwarebytes [35] and others should be activated in browser which will block the blacklist websites and provide multi-layers of protection.

4.4. Trustworthy Anti-Virus

Kevin Savage et al [36] explained about extortion based attacks and emergence of fake anti-virus software in 2008. These fake anti-virus software showed bogus errors to victims and offered to fix them in $40 to $100 payment while someone offered lifetime membership [9]. Reliable anti-virus can detect attacks for which ransomware signatures are already present while now some have machine learning techniques which can classify between benign or malicious activities based on previous signatures [8]. Some of the available reliable anti-virus softwares in 2020 are Bitdefender, Nortan, Nortel, Avast, Kaspersky and others [37] [38].

4.5. Trustworthy Application

Installation of benign applications from trustworthy websites can play a vital role to combat ransomware attacks. Jason E. Thomas et al [9] defined in their research work that proceeding of ransomware was begun in 2005 through misleading applications. These types of applications presented them as removal of spyware or to enhance the performance of the system. Windows OS and Mac OS X became target to such applications as SpySheriff and PerformanceOptimizer. They asked $30 to $90 ransom to fix the bugs which even did not exist. System administrators should recognize the application which can make changes in program and files [8] [13] [39]. Especially in case of Android environment, if any applications after the completion of installation ask for administrative rights so it should not be granted. Such types of applications open the door for the ransomware entry which can encrypt data or can steal personal data. According to [11], they focused on source code of an application and AndroidManifest.xml which have

such characteristics. They mentioned in their work through following security parameters at the time application installation from apps store can reduce ransomware attack.

4.6. Limited Access Control

In an organization privileges to make changes such as read, write, update, remove files and other authorization should be held by the IT professionals, it can be helpful to protect data and prevention from ransomware attacks. IT professionals should be responsible for granting the shared resources to other staff according to their level [8]. An intrusion detection and prevention system (IPS) installation at the main data server can perform well because an expert can also make mistakes.

4.7. Email Filtering

Email is the easiest method to spread ransomware as mentioned above in section 3.1. Due to the simplicity and success rate, this method outperformed all other techniques. Most of the available email servers have machine learning algorithms installed which perform classification between spam or non-spam email based on some attributes and features. According to [40], if the mailing servers have such type of filtering technique or algorithm then it can perform well against ransomware attacks.

4.8. Online Available Tools

Once the data of any organization captured, encrypted or deleted by any ransomware and demand for the ransom to return or decrypt the data although there is no guarantee that organization will retrieve its data back. There is an example in case of WannaCry ransomware in which it had not linked the ID after encryption and no way to decrypt data back [41]. There are number of online decryption tools are available free of cost such as Avast, Kaspersky, Window defender and other. These types of tools provide decryption if the encryption of data is not enough strong (decryption possible if encryption key below 1024 bit AES) [8]. Some tools can decrypt up to 1024 bit AES encryption. There are websites available also, which operated by law enforcement agencies globally and deal with these cases. Some of websites are “No More Ransom project” [42], “FBI Ransomware Information” [43], “Internet Crime Complaint Center (IC3)” [44], “National Cybercrime Security Center (NCSC, U.K.)” [45].

5. Conclusion

The growth of ransomware attacks increasing day by day because it has become a lucrative business with less effort. Nowadays, every Field and sector has involved digital and computing devices for the process of their daily operation. As the researcher are improving security technique on daily basis, hence the attackers are also learning from their previous mistakes and with the launching of every version of such ransomware, they are becoming more powerful to hit hard. This paper has tried best to explain about the ransomware, ransomware types and their working and infection procedure. This paper also provided the most popular spreading mechanism and recent published and available detection and protection techniques. This study provided us some of the available ransomware datasets and we will apply deep learning algorithms in the investigation and detection of ransomware hidden pattern in our future work.

Acknowledgment

The authors are thankful to faculty members of computer science department, Sindh Madressatul Islam University, Karachi Sindh Pakistan, for their kind support throughout the research work.

References

[1] Comtact: “What are different types of malware?” https://www.comtact.co.uk/blog/what-are-the-different-types-of-malware.
[2] B. Dobran, “Definitive guide for preventing and detecting ransomware 2019,” https://phoenixnap.com/blog/preventing-detecting-ransomware-attacks.
[3] S. Nakamoto, Bitcoin: “A peer-to-peer electronic cash system,” 2008. https://bitcoin.org/bitcoin.pdf
[4] J. Hernandez-Castro, E. Cartwright, and A. Stepanova, “Economic Analysis of Ransomware,” 2017arXiv:1703.06660
[5] Alex Lielacher: The Most Popular Cryptocurrencies In Ransomware Attacks.https://cryptonews.com/exclusives/the-most-popular-cryptocurrencies-in-ransomware-attacks-1712.htm
[6] Benjamin Freed: “One year after atlanta's ransomware attack, the city says it's transforming its technology," 2019, https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/
[7] Doug Olenick: “Atlanta ransomware recovery cost now at $17 million, reports say” 2018. https://www.scmagazine.com/home/security-news/ransomware/atlanta-ransomware-recovery-cost-now-at-17-million-reports-say/
[8] I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-7.
[9] Thomas, Jason & Galligher, Gordon. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. Compute and Information Science. 11. 10.5539/cis.v11n1p14.
[10] Lemmou Y., Souidi E.M. (2018) Inside GandCrab Ransomware. In: Camenisch J., Papadimitratos P. (eds) Cryptology and Network Security. CANS 2018. Lecture Notes in Computer Science, vol 11124. Springer, Cham. https://doi.org/10.1007/978-3-030-00434-7_8
[11] Monika, & Zavarsky, Pavol & Lindskog, Dale. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. Procedia Computer Science. 94. 465-472. 10.1016/j.procs.2016.08.072.

[12] Craciun V.C., Mogage A., Simion E. (2019) Trends in Design of Ransomware Viruses. In: Lanet JL., Toma C. (eds) Innovative Security Solutions for Information Technology and Communications. SECITC 2018. Lecture Notes in Computer Science, vol 11359. Springer, Cham. https://doi.org/10.1007/978-3-030-12942-2_20
[13] Sittig DF, Singh H. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Appl Clin Inform. 2016;7(2):624–632. Published 2016 Jun 29. doi:10.4338/ACI-2016-04-SOA-0064.
[14] Brewer, Ross. "Ransomware attacks: detection, prevention and_cure." Network_Security 2016.9_(2016):_5-9. https://doi.org/10.1016/S1353-4858(16)30086-1
[15] Gazet, A. Comparative analysis of various ransomware virii. J_Comput_Virol 6, 77–90_(2010). https://doi.org/10.1007/s11416-008-0092-2
[16] DIMVA 2015: Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment - Volume 9148July 2015 Pages 3–24. https://doi.org/10.1007/978-3-319-20550-2_1
[17] Securonix Threat Research: GandCrab Ransomware Attack By Oleg Kolesnikov and Harshvardhan Parashar, Securonix-Threat-Research-Team. https://www.securonix.com/securonix-threat-research-gandcrab-ransomware-attack/
[18] Droppa, Martin & Matej, Boris & Harakal, Marcel. (2017). CYBER THREAT ASSESSMENT REPORT IN SELECTED ENVIRONMENT CONDUCTED BY CHOOSEN TECHNOLOGY OF FIREWALLS.
[19] Antonio Challita: "The four most popular methods hackers use_to_spread_ransomware"-2018. https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/
[20] Rizkallah, Juliette. "Securing the new wave of non-human users." Computer Fraud & Security 2019.1 (2019): 15-17. https://doi.org/10.1016/S1361-3723(19)30009-0
[21] Chen Q., Islam S.R., Haswell H., Bridges R.A. (2019) Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection. In: Liu F., Xu J., Xu S., Yung M. (eds) Science of Cyber Security. SciSec 2019. Lecture Notes in Computer Science, vol 11933. Springer, Cham. https://doi.org/10.1007/978-3-030-34637-9_15
[22] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi and R. Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence," in IEEE Transactions on Emerging Topics in Computing. https://doi.org/10.1109/TETC.2017.2756908
[23] Morato, Daniel, et al. "Ransomware early detection by the analysis of file sharing traffic." Journal of Network and Computer_Applications 124_(2018):_14-32. https://doi.org/10.1016/j.jnca.2018.09.013
[24] Narudin, F.A., Feizollah, A., Anuar, N.B. et al. Evaluation of machine learning classifiers for mobile malware detection. Soft_Comput 20, 343–357_(2016). https://doi.org/10.1007/s00500-014-1511-6
[25] Fernández Maimó, L., Huertas Celdrán, A., Gil Pérez, M. et al. Dynamic management of a deep learning-based anomaly detection system for 5G networks. J Ambient Intell Human_Comput 10, 3083–3097_(2019). https://doi.org/10.1007/s12652-018-0813-4
[26] Yasasin, Emrah, et al. "Forecasting IT security vulnerabilities–An empirical analysis." Computers & Security 88_(2020):101610. https://doi.org/10.1016/j.cose.2019.101610
[27] Figueira, Pedro Tubío, Cristina López Bravo, and José Luis Rivas López. "Improving information security risk analysis by including threat-occurrence predictive models." Computers & Security 88 (2020): 101609. 10.1016/j.cose.2019.101609
[28] Young, Adam L., and Moti Yung. "Cryptovirology: The birth, neglect, and explosion of ransomware." Communications of the ACM 60.7 (2017): 24-26. 10.1145/3097347
[29] Rhoades, Gale. "Ransomware and other malware." The Indexer: The International Journal of Indexing 34.3_(2016):126-128. https://doi.org/10.3828/indexer.2016.39
[30] Mustaca, Sorin. "Are your IT professionals prepared for the challenges to come?." Computer Fraud&Security 2014.3-(2014):18-20. https://doi.org/10.1016/S1361-3723(14)70472-5
[31] DeMuro, Paul R. "Keeping internet pirates at bay: Ransomware negotiation in the healthcare industry." Nova L. Rev. 41 (2016): 349.
[32] PATHAK, P. B., AND YESHWANT MAHAVIDYALAYA NANDED. "A DANGEROUS TREND OF CYBERCRIME: RANSOMWARE GROWING CHALLENGE." INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER ENGINEERING & TECHNOLOGY (IJARCET) 5.2 (2016): 371-373.
[33] MICROSOFT: "WINDOWS DEFENDER SMARTSCREEN" 2019. HTTPS://DOCS.MICROSOFT.COM/EN-US/WINDOWS/SECURITY/THREAT-PROTECTION/WINDOWS-DEFENDER-SMARTSCREEN/WINDOWS-DEFENDER-SMARTSCREEN-OVERVIEW
[34]"GOOGLE-SAFE-BROWSING". HTTPS://SAFEBROWSING.GOOGLE.COM/
[35] "MALWAREBYTES". HTTPS://WWW.MALWAREBYTES.COM/
[36] Savage, K., Coogan, K., & Lau, H. (2015, August 6). The evolution of ransomware. Retrieved November 28, 2017, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/theevolution-of-ransomware.pdf
[37] "Best Antivirus Software 2020, Secure your personal data." https://www.thetop10bestantivirus.com/
[38] "THE BEST ANTIVIRUS SOFTWARE FOR 2020." HTTPS://WWW.TECHRADAR.COM/BEST/BEST-ANTIVIRUS
[39] FBI, "Ransomware what it is and what to do about it?" https://www.fbi.gov/news/stories/incidents-of-ransomware-ontherise/incidents-of-ransomware-on-the-rise
[40] Gordon V. Cormack. 2008. Email Spam Filtering: A Systematic Review. Found. Trends Inf. Retr. 1, 4 (April 2008), 335–455. https://doi.org/10.1561/1500000006
[41] Mattei, Tobias A. "Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry cyberattack." World neurosurgery 104 (2017): 972-974.
[42]"No-More-Ransomware-Project," https://www.nomoreransom.org/en/about-the-project.html
[43]"FBI-Ransomware-Information," https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.
[44] "Internet Crime Complaint Center (IC3)," https://www.ic3.gov/media/2016/160915.aspx

[45] "National Cybercrime Security Center (NCSC, U.K.)," https://www.ncsc.gov.uk/guidance/protecting-your-organisationransomware.

[46] LAWRENCE ABRAMS: "THE WEEK IN RANSOMWARE - MARCH 6TH 2020 - BREACHES EVERYWHERE" HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/THE-WEEK-IN-RANSOMWARE-MARCH-6TH-2020-BREACHES-EVERYWHERE/

[47] "RECORDS REVEAL CITY OF CARTERSVILLE PAID RANSOMWARE ATTACKERS $380K" HTTP://WWW.DAILY-TRIBUNE.COM/STORIES/RECORDS-REVEAL-CITY-OF-CARTERSVILLE-PAID-RANSOMWARE-ATTACKERS-380K,24425

[48] LAWRENCE ABRAMS: "THE WEEK IN RANSOMWARE - MARCH 27TH 2020 - DON'T ATTACK HOSPITALS!" HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/THE-WEEK-IN-RANSOMWARE-MARCH-27TH-2020-DONT-ATTACK-HOSPITALS/

[49] Adel Hamdan Mohammad, Ransomware Evolution, Growth and Recommendation for Detection Vol 2014 No.3(2020). https://doi.org/10.5539/mas.v14n3p68

[50] Jimada S., Nguyen T.D.L., Sanda J., Vududala S.K. (2021) Analysis of Ransomware, Methodologies Used by Attackers and Mitigation Techniques. In: Kumar R., Quang N.H., Kumar Solanki V., Cardona M., Pattnaik P.K. (eds) Research in Intelligent and Computing in Engineering. Advances in Intelligent Systems and Computing, vol 1254. Springer, Singapore. https://doi.org/10.1007/978-981-15-7527-3_37