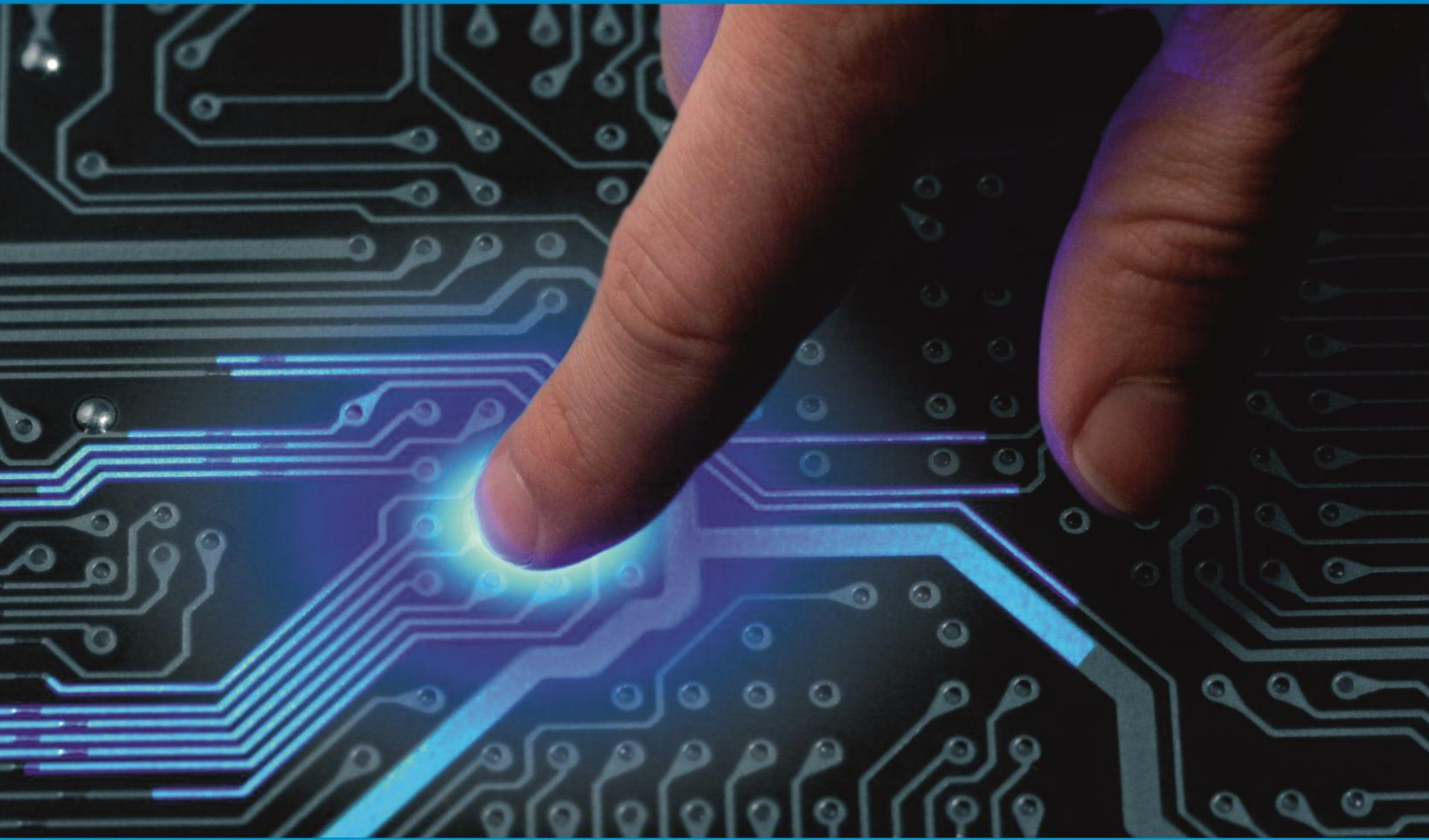
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

A Study of Ransomware Attacks and Its Behavioural Analysis

Pratik Prakash Nikam

Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce(Autonomous), Kalyan, India.

ABSTRACT:In the world of digitalization, where every information is stored digitally, information can be accessed anytime via internet . Our government is trying to make all theassesments online . But every pillar has two sides. The million dollar question is are we ready for it by all means? Do we have the infrastructure to fightransomware ? Is our system strong enough? Or are we ready to pay the ransom? Ransomware is a kind of malware that encrypts the essencial data on a computer and prevents the user from accessing them. The attacker then blackmails the user by requesting a ransom in exchange for the key that decrypts the files.This paper is study of ransomware attacks and its affect, ransomware families, methods for prevent such attacks and highlighted areas where the loopholes are present.

KEYWORDS: Ransomware, Cyber-attacks ,malware, safeguards.

I. INTRODUCTION

Ransomware is a familiar threat to the cyber security industry. After the second half of 2010s its families and activities were reported by various tech communities. It is a infection that if transmitted, it’s almost impossible to get out. It infects all important data and file in user’s computer . If ransomware get activated in user’s system, it encrypts files like .doc,.mp3, etc. . A ransom is amount demanded for your data and then only you will get those files. It becomes very difficult to detect that the data or files has been encrypted. At that time we have only 2 options that is Pay the ransombut it does not 100% guarantee that we will get our fileback or Format the PC and disconnect the Internet. TeslaCrypt,SimpleLocker,WannaCry,NotPetya,SamSam,Ryuk are the worst ransomware attacks in last five years. In 1989, first ransomware in history emerged that is 27 years back.

II. OBJECTIVES TO STUDY

- H1:If ransomware attacks need to be prevented then it is important to maintain updated antivirus software and backup all your critical information.
- H2:Clicking unverified links is the most popular way of ransomware infections

III. THE RATE OF RANSOMWARE INFECTIONS

We have observedsome changes in rate of ransomware infections with spikes during certain quarters over the entire period January 2018 to March 2020 according to kaspersky. 3.8% of all users that encountered malware were the users who encountered ransomware. The total number of users that encountered ransomware from 1,681,867 from January to December of 2018 to 1,554,669 from January to December of 2019 (7.6% decrease occured). The first quarter of 2020 reported the lowest number of users that encountered ransomware than any quarter of 2019 and 2018.

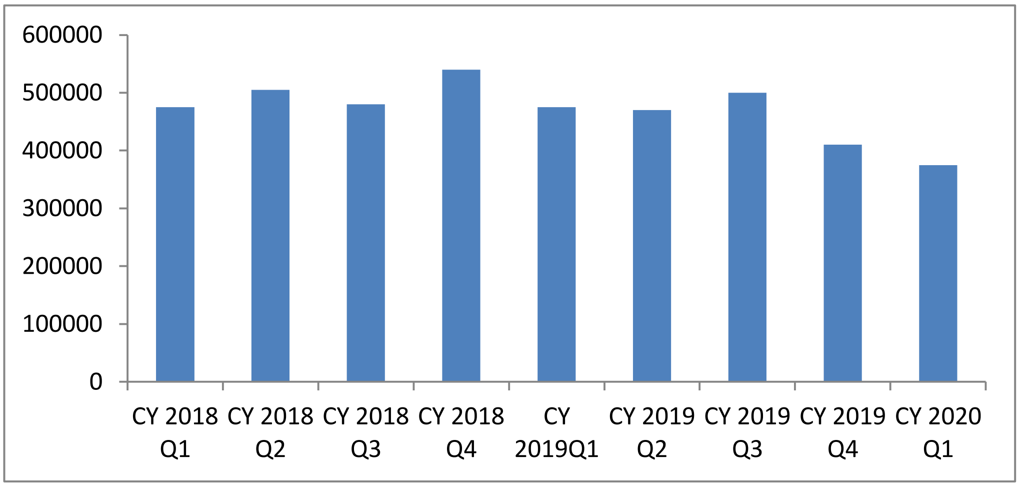


Fig.1:The number of users encountering ransomware at least once from January 2018 to March 2020

The greatest percentage of ransomware attacks observedmostly in the Middle East and Africa region. It seems like these regions are less protected against ransomware attacks, making them favourites for criminals. Both regions have complex political situations and attackers might see an opportunityto encrypt and hold for ransom politically sensitive information.For 2019 and 2018 the countries with the highest share of users attacked with ransomware were similar acccording to kaspersky. In 2019, once again Middle East and Africa were most popular areas for ransomware activity. Additionally, attackers began targeting Central Asian countries for ransomware activities. Central Asian countries may be seen as more vulnerable to ransomware because these countries are still developing and hence these countries are good target for criminals .

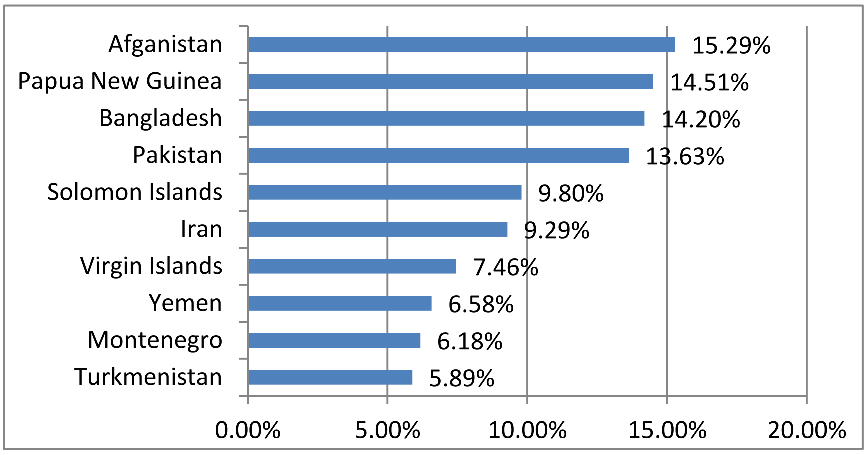


Fig.2:Countries with biggest share of user attacked with ransomware attacked in 2019

Once again, despite a moderate decline in numbers, we can observe high levels of activity in the Middle East region. The biggest takeaway from this is that ransomware is a ubiquitous and everyone should continue to trackthe activity of even those types of malware that seems to be disappeared.

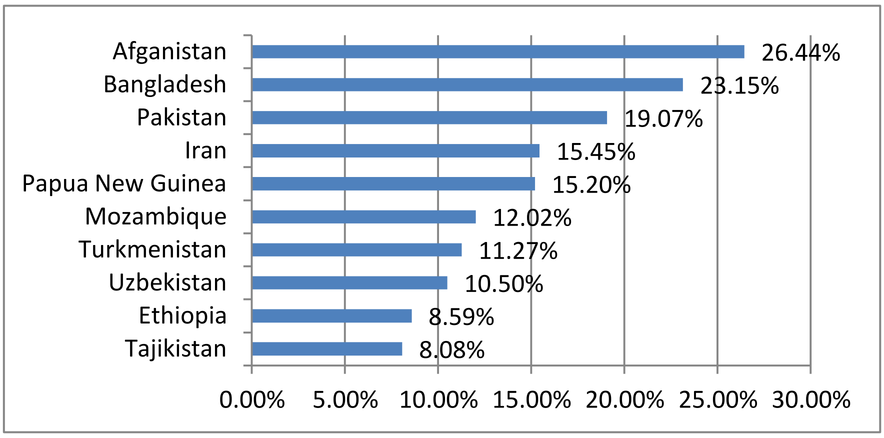


Fig.3:Countries with biggest share of user attacked with ransomware in 2020 Q1

IV. THE MOST ACTIVE RANSOMWARE FAMILIES IN 2018-2020

Crypto-ransomware is a type of ransomware that encrypts users files until a demanded ransom is paid makes up a significant portion of the total number of ransomware infections: 48% percent for period from January 2018 to March 2020: 46% in 2018, 49% in 2019, and 47% in 2020 Q1.For 2018, WannaCry is the infamous encryptor that swept devices around the world in 2017 and it is still active affecting 34% of all users that encountered crypto-ransomware attacks. One new ransomware family also registered named as GandCrab. This encryptor follows the ransomware-as-a-service model in which the criminals sell their technologies to the other broader community. Other older ransomware families are also active: Cerber, Shade and Cryakl.

In 2019, WannaCry infected the highest number of users but only the percentage reduced to 21%; it attacked 164,433 users out of the 767,907 users that were attacked by encryptors. Shade and GandCrab remained active, but less so, and a new family entered the scene called as Stop. This malware is spread through malicious installer bundles imitating software usually searched by users.

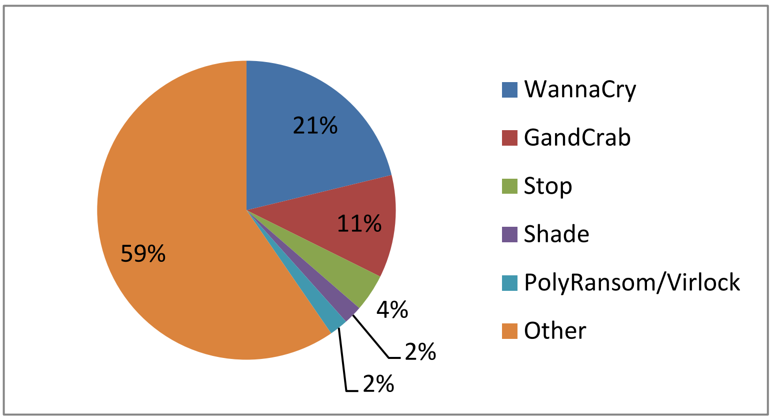


Fig.4:Distribution of users attacked with different ransomwares in 2019

WannaCry ,GandCrab and stop attacks continued in 2020. The past years demonstrate a trend that was first noticed back in early 2018: the ransomware landscape has continued to merge with only a few families maintaining a presence.

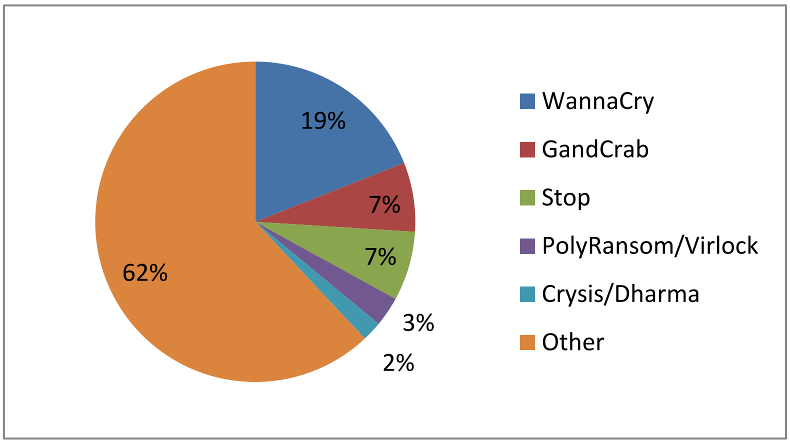


Fig.5:Distribution of users attacked with different ransomwares in 2020

V. INDUSTRIES TARGETED BY RANSOMWARE

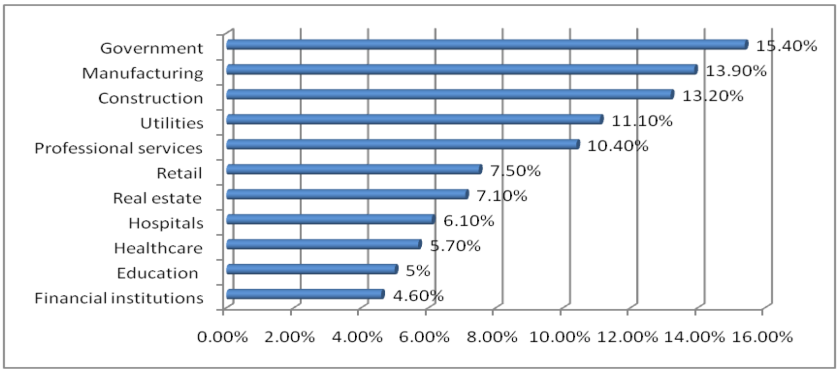


Fig.6:Industries in North America reporting ransomware attacks in 2019

VI. RANSOMWARE ATTACKS PREVENTION

1) Never click on any malicious link.Downloading gets started when you click on malicious link.It is a way that your computer gets infected
2) Never try to open untrusted email attachments.Never open attachments that ask your permission to enable macros to view them
3) Download from trusted and verified sites.Do not download anything from unknown websites
4) Use updated software and operating system.It will protect you from malware
5) Always keep backup of your data.Additionally, you can also use cloud storage

VII. LITERATURE REVIEW

In a study published by Richardson ,et al.[1] in 2017, It involved history of ransomware,the arguments for and against paying the ransom,best practices to prevent an infection and to recover from an infection.All approaches mentionedfor preventing ransomware are quite expensive.

In a study published by Yaqoob ,et al.[2]in 2017 , A detailed study of ransomware attacks and security concerns in internet of things.The threats of data perception were at the device level where IOT devices are prime targetsforthe attackers.

In a study published by Bansal ,et al.[3]in 2020 ,This paper presented the study to find insights about ransomware attacks using web search logs.Inefficientmethod because after minor increase inqueries, the query volume continued to decline.

In a study published by Kharraz,et al.[4]in 2017,It contained information about REDEMPTION which is a novel defense that makes theoperating system more resilient to ransomware attacks.Defended against ransomware on the end-host only.

In a study published by Huang,et al.[5]in 2018,This paper represented creation of measurement framework to perform large scaleend to end measurement of ransomware payments,victims and operators .Transactionfiltering methods were not effective for some ransomwarefamiliesthat had a dynamic pricing structure orfor which we did not know the demanded ransom amount .

In a study published by Hampton,et al.[6] in 2018,The paper presented analysis of 14 strains of ransomware that infected windows platforms over the years.Identified only windows API calls that differs.

In a study published by Kirda ,et al.[7] in 2017 ,It contained a novel dynamic analysis system called as UNVEIL that is specifically designed to detect ransomare attacks.Unawareness of any systems that aimed to detect ransomware in the wild.

In a study published by Chen,et al.[8] in 2017,This paper contained a method to identify and rank the most discriminating ransomware features from a set of ambient system logs and log stream containing ambient and ransomware behaviour.False indicators of methodby non malware features occurring in the malware document malware could arise by this.

In a study published by Hernandez-Castro,et al.[9]in 2017,This paper represented economic analysis of ransomware withrelevant data from cryptolocker,cryptowall,tellacrypt and other major strands.With rudimentary analysis of this data criminals could almost certainly obtain higher profits.

In a study published by Cabaj,et al.[10]in 2016,This paper presented software defined networking which can be utilized to improve ransomware mitigation.Besides the presented approaches other SDN based method can also be envisioned which could further improve the detection and the countering of ransomware.

In a study published by Zhang,et al.[11]in 2019,This paper proposed an approach based on static analysis to classifying ransomware sequences and samples which are transformed into N-gram sequences.Approaches based on dynamic analysis could not deal with ransomware that can fingerprint the environment.

In a study published by Chen ,et al..[12]in2019,It involved details about automated ransomware pattern-extraction and early detectiontool that extracts the sequence of events induced by seven ransomware attacks, identifies the most discriminating features using three machine learning methods, and creates graphs tofacilitate forensic efforts by visualizing features andtheir correlations.Discriminating features were automatically promoted by thismethod that malware analysis reports failed to identify.

In a study published by Genç,et al.[13]in 2020,This paper presented benefits and limits of using cyber-intelligence and counter-intelligence strategies that could be usedagainst ransomware attacks.Didn't backed their speculations with fieldstudies or interviews.

In a study published by Scaife,et al.[14]in2016,It stated that careful analysis of ransomware behavior can produce an effective detection system that significantly mitigates the amount of data lost by ransomware attacks. CryptoDrop was unable to determine the intent of the changes it inspects. It couldn't distinguish whether the user or ransomware is encrypting a set of documents

In a study published by Herrera Silva,et al.[15]in 2019, This paper provided classification of ransomware articles based on detection and prevention approaches.It provided few parameters that are monitored and analyzed in order to prevent these kinds of attacks at an early stage and there is no complete list of them

In a study published by Nyikes,et al..[16]in 2019,This paper presented prevention of ransomware attacks by increasing security awareness among internet users.More prevention measures could be included.

In a study published by Ali,et al.[17]in 2017, This paper shared research finding about ransomware, depict the ransomware work in a format that commonly used by researchers and practitioners and illustrate personal case experience in dealing with ransomware attacks.Expected more effective awareness about this malware.

In a study published by Luo,et al.[18]in 2007,This paper showed us how important awareness is to prevent ransomware.Very less information was given about awareness.

In a study published by Hull,et al.[19]in 2019,This paper included investigation on 18 families of ransomware, leading to a model for categorising ransomware behavioural characteristics, which can then be used to improve detection and handling of ransomware infections.This paper also presented a user study into ransomware deployment through questionnaire and in-depth interviews by involving universities and stakeholders.

In a study published by Pandey,et al.[20]in 2020,This paper presented difficulties and components that the users have to contend with on the internet. It also investigated ongoing malware attacks. It explained the significance of the research, malware investigation, social engineering, and user awareness in the field of malware attacks.Researchers should dedicated their efforts to the in-depth identification and mitigation of security issues emerging due to malware.

In a study published by Monika,et al.[21]in 2016, This paper provided insights on how ransomware have evolved from its starting till March 2016 by analyzing samples of selected ransomware variants from existing ransomware families in Windows and Android platforms.

In a study published by Joseph,et al.[22]in 2020,This paper included insight on importance of memory forensics and provides widespread analysis on working of ransomware, recognizes the workflow, provides the ways to overcome this attack.This paper also implemented user defined rules by integrating into powerful search tools known as YARA to detect and prevent the ransomware attacks.Included too much complicated stuff.

In a study published by Paquet-Clouston,et al.[23]in 2019,This paper presented data-driven method for identifying and gathering information on Bitcoin transactions related to illicit activity based on footprints left on the public Bitcoin blockchain.Analysis should extended to additional ransomware families.

In a study published by Kakavand,et al.[24]in 2020,This paper included Analytical research on a distinct form of malware known as crypto-ransomware.Computing cost was elevated because execution and assembly are time consuming.

In a study published by Dhawan,et al..[25]in 2020,This paper presented various aspects of ransomware, its emergence, historical insights, and various routes that may be adopted by ransomware practitioners. There is a strict need to develop advance preventive technique to make sure that horrifying incidents never turn into a reality.

VIII. METHODOLOGY

A survey was taken to check people's awareness about ransomware attacks The survey was taken with the help of Google forms .A total of 55 participants were were involved in this survey(35 males ,20 females).70% the population responding to this survey were students.The survey was conducted within the city limit of Mumbai.A Google form was circulated using simple random sampling.the Google form was circulated for 10 days.

IX. EXPERIMENT

The questions appropriate for our study was taken from survey which may affect our hypothesis.Chi-square test with 95% confidence level is performed.A gender parameter was a distinguishing factor.A calculated value was compared with tabulated value by considering degree of freedom as 5% according to which the rejection of null hypothesis could be impacted which is inversely proportional to alternate hypothesis.The two questions were:Do you keep backup of all your critical information? Have you ever visited any malicious link? The first question provided calculated value of 0.7558 and the other question provided calculate value of 1.8546.These values were checked with tabulated value of 3.84 with confidence level of 95%.

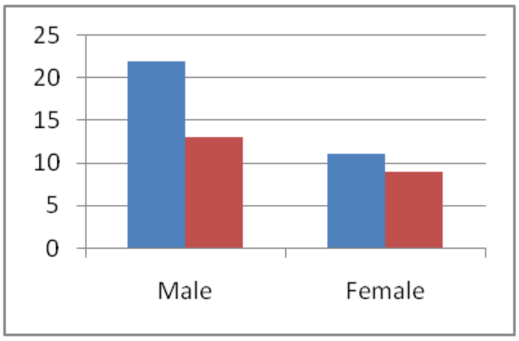


Fig.7:Question 1

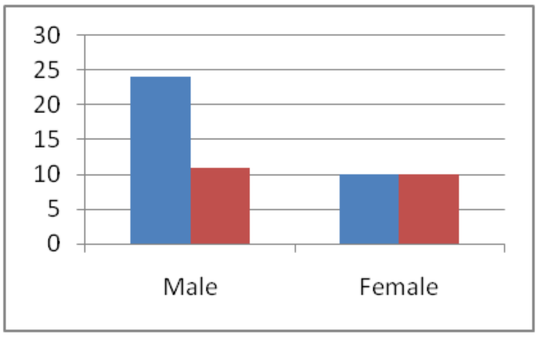


Fig.8: Question 2

X. RESULT

We performed chi square test by collecting data from survey.So according to the experiment H1 is accepted :If ransomware attacks need to be prevented then it is important to maintain updated antivirus software and backup all your critical information.

XI. CONCLUSION

Actors behind ransomware attacks are targeting users worldwide, hitting even the smallest countries and most remote regions. This will most likely not to change, meaning that all areas need to adopt appropriate security measures against ransomware attacks .In this work, we did the study to find insights about ransomware attacks. We analyzed its behaviour and found that early recognition and prevention of risk factor can significantly improve data protection for both individuals and companies.

ACKNOWLEDGEMENT

Sincere thanks and gratitude to Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce(autonomous), Kalyan for providing needful guidance for this paper.

GLOSSARY

1. IOT:Internet of things
2. SDN:Software defined network
3. YARA:The tool which is used for malware research and detection
4. Chi-square test:Non parametric test of independence used for comparison with categorical and associated variables

REFERENCES

[1] Richardson, Ronny and North, Max M., "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276.https://digitalcommons.kennesaw.edu/facpubs/4276

[2] Yaqoob, I., Ahmed, E., Rehman, M. H. . u. r., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

[3] Bansal, C., Deligiannis, P., Maddila, C., & Rao, N. (2020). Studying Ransomware Attacks Using Web Search Logs. Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. https://doi.org/10.1145/3397271.3401189

[4] Kharraz, A., & Kirda, E. (2017). Redemption: Real-Time Protection Against Ransomware at End-Hosts. Research in Attacks, Intrusions, and Defenses, 98–119. https://doi.org/10.1007/978-3-319-66332-6_5

[5] Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., & McCoy, D. (2018). Tracking Ransomware End-to-end. 2018 IEEE Symposium on Security and Privacy (SP), 1–14. https://doi.org/10.1109/sp.2018.00047

[6] Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. Journal of Information Security and Applications, 40, 44–51. https://doi.org/10.1016/j.jisa.2018.02.008

[7] Kirda, E. (2017). UNVEIL: A large-scale, automated approach to detecting ransomware (keynote). 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). https://doi.org/10.1109/saner.2017.7884603

[8] Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). https://doi.org/10.1109/icmla.2017.0-119

[9] Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic Analysis of Ransomware. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2937641

[10] Cabaj, K., & Mazurczyk, W. (2016). Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall. IEEE Network, 30(6), 14–20. https://doi.org/10.1109/mnet.2016.1600110nm

[11] Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., & Sangaiah, A. K. (2019). Classification of ransomware families with machine learning based on N-gram of opcodes. Future Generation Computer Systems, 90, 211–221. https://doi.org/10.1016/j.future.2018.07.052

[12] Chen, Q., Islam, S. R., Haswell, H., & Bridges, R. A. (2019). Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection. Science of Cyber Security, 199–214. https://doi.org/10.1007/978-3-030-34637-9_15

[13] Genç, Z., & Lenzini, G. (2020). Dual-use Research in Ransomware Attacks: A Discussion on Ransomware Defence Intelligence. Proceedings of the 6th International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0009000505850592

[14] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 1063–6927. https://doi.org/10.1109/icdcs.2016.46

[15] Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 11(10), 1168. https://doi.org/10.3390/rs11101168

[16] Nyikes, Z., & Szűcs, E. (2019). Prevention of Ransomware Attacks by Increasing Security Awareness. Műszaki Tudományos Közlemények, 11(1), 149–152. https://doi.org/10.33894/mtk-2019.11.33

[17] Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. Issues in Informing Science and Information Technology Education, 14, 87-99. Retrieved from http://www.informingscience.org/Publications/3707

[18] Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. Information Systems Security, 16(4), 195–202. https://doi.org/10.1080/10658980701576412

[19] Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, 8(1), 1186. https://doi.org/10.1186/s40163-019-0097-9

[20] Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Trends in Malware Attacks. Advances in Digital Crime, Forensics, and Cyber Terrorism, 47–60. https://doi.org/10.4018/978-1-7998-1558-7.ch004

[21] Monika, Zavarsky, P., & Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. Procedia Computer Science, 94, 465–472. https://doi.org/10.1016/j.procs.2016.08.072

[22] Joseph, P., & Norman, J. (2020). Systematic Memory Forensic Analysis of Ransomware using Digital Forensic Tools. International Journal of Natural Computing Research, 9(2), 61–81. https://doi.org/10.4018/ijncr.2020040105

[23] Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. Journal of Cybersecurity, 5(1), 1–11. https://doi.org/10.1093/cybsec/tyz003

[24] Kakavand, M., Arulsamy, L., Mustapha, A., & Dabbagh, M. (2020). A Novel Crypto-Ransomware Family Classification Based on Horizontal Feature Simplification. Advances in Computer, Communication and Computational Sciences, 3–14. https://doi.org/10.1007/978-981-15-4409-5_1

[25] Dhawan, S., & Narwal, B. (2018). Unfolding the Mystery of Ransomware. International Conference on Innovative Computing and Communications, 25–32. https://doi.org/10.1007/978-981-13-2324-9_4

[26] Kapersky's ransomware report

[27] Internet security threat report(ISTR)

[28] https://en.wikipedia.org

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details