iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.31245

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

A Review on File System-based Ransomware Detection

Srinivasa M[1], Archana Jyothi Kiran[2]
[1]*MTech Cybersecurity Student,* [2]*AssistantProfessor, Department of Computer Science and Technology*
Jain (Deemed to be University), Bangalore, India

Abstract: Over the last few years, digital revolution has absolutely changed the world. The tremendous growth of computer and technology has not only transformed the business operations but also created way for the increase in cyber-criminal activities. As per the security vendors and researcher, ransomware attack is considered as global threat and one of the dangerous attacks in the IT world. It is becoming more sophisticated attack in evading detection of defense layer and continue grow rapidly. It has become challenging task to detect this ransomware attack at early stage. In this paper, we are comparing the existing model with our proposed model which is used for ransomware detection based on file indicators of compromise (IOC).
Index terms: -ransomware, indicators of compromise, dropper, phishing, cybersecurity

I. INTRODUCTION

Over the last few years, digital revolution has absolutely changed the world. The tremendous growth of computer and technology has not only transformed the business operations but also created way for the increase in cyber-criminal activities. We are observing increase in number of cyber incidents every day and malware authors are posing serious threats to Education field, Large-scale energy generation companies, Medical fields (which includes hospitals and research laboratories). They achieve their malicious intent goals on the organization with help of different malwares.

In recent days, Ransomware attack is considered as global threat by security vendors and IT firms. According to few researchers, a new and small organizations were under ransomware attack for every 14 seconds in the year 2019. However, we may observe upswing of this attack trend by 2021. Ransomware is defined as "it is malicious software (malware) used in cyber-attacks to encrypt the user/victim's data with an encryption key which is known only to the attackers". It will disable the access to the user's system and files on the host until the ransom amount is paid to the attackers. This type of attack is increasing day to day and causing severe impact on individual and business operations.

In recent days, one of biggest IT firm was hit by Maze ransomware attack which encrypted the files present on the targeted host and demanded for the ransom amount to recover the files to its original state. It took more than a month to fully recover from this ransomware attack and spent around $ 70 million. So far victims have spent more than $150 million on these ransomware attacks in the year 2020.

In the year 2015 and 2016, we observed drastic increase in the ransomware families which was not detected by any security products and this led to series of ransomware attack in these years. As per few security vendors report, an average of 4000 ransomware attacks were observed during the first quarter of 2016, when compared to 2015 the attack ratio was increased to 300 times. Further, it continued to be more dangerous attack in 2017 and 2018 and, we saw 15% increase in ransomware attack in the year 2019.Nowadays ransomware attacks are becoming more sophisticated and evading the detection in network defense layer which is making harder cyber security professional.

In this paper, we are reviewing the existing ransomware detection model based and tools available in the market with our proposed model. Our proposed model can detect the ransomware based on file behavior indicators and alert the user at the very early stage of the infection.

II. LITERATURE REVIEW

This chapter aims to provide detailed information about different ransomware detection techniques in the recent times. This chapter includes various work and studies to support directly or indirectly helps to carry out our proposed model. Most of the researchers conducted the experiment based on network indicators, but ransomware attacks becoming more erudite and it is evading the network defense layer detection. Further, we noticed there are few ransomware detections tools available in the market however they are not that sophisticated to detect the new and recent ransomware attacks. The description of some of the previous research that propose different solutions to detect ransomware attack is described in this chapter.

A. Ransomware Detection based on Process Behavior Analysis:

Abdullahi Arabo at et,al 2019, [1] "This research paper helps in identifying the ransomware detection based on the extracted DLL files from the samples and system usage during the malicious activity. This author conducted the experiment by using 7 different

©IJRASET: All Rights are Reserved

ransomware families, 34 malware samples, and 41 benign software. Further, they created data set of these all samples and used machine learning technique to distinguish between benign and ransomware activity".
By using this method, authors were able to distinguish the ransomware activity and benign file activity based on the process behavior and warn the user at the early stage. The major benefit of this method is that we do not require any signature database, but ransomware dataset is required for the detection and classification purpose.

B. Ransomware Detection based on User's Editing Document:
Toshiki Honda at et,al 2018,[2] "This research paper proposes a detection method based on human file operating characteristics. Here, authors have evaluated the effectiveness of this detection model and consistency between displayed documents and user's editing operations". This proposed method prevented files from being encrypted by crypto ransomware by restricting file deletion and overwriting. This module can detect two different ransomware families (i.e Cerber and Jaff), However same cannot be used for new and other ransomware families for the detection and prevention.

C. Ransomware Detection based on IOC's with Machine Learning Technique:
Mayank Verma at et,al 2018, [3] In this research paper authors have extracted few indicators of compromise (IOC's) based on static analysis and implemented machine learning technique to detect and classify to its respective ransomware families. "They conducted the experiment by using 7 different ransomware families and trained 678 (labelled dataset). Further, they have extracted 11 critical IOC's based on static analysis which includes majority of network behavior and only few IOCs related file behavior and dynamic behavior. They implemented an automated system using supervised machine learning classifiers to classify the ransomware families to respective 7 classes. In the dataset, they have used 80% trained data set and 20% testing data for the analysis purpose. The experiment was conducted by using 5 different machine learning classifiers namely SVM, QDA, LDA, Complex Tree and KNN. According to the results, Complex tree give best result with the accuracy of 97.1%".

D. Network based Crypto-Ransomware Detection:
Ahmad O. Almashhadani at et.al 2018. [4] This research paper deals the ransomware detection based on network activities. Authors have conducted the experiment on specific ransomware family known as "Locky" ransomware. The proposed offers high detection accuracy, low false positive rate, valid extracted features and highly effective in tracking ransomware network activities. A total of 18 features were extracted using TCP, HTTP, DNS and NBNS traffic. These features are informative and can clearly differentiated traffic generated by compromise host. This method works on two different levels: the packet level and flow level. Experiment results shows that detection rate for each level is 97.92% and 97.08% respectively. However, this detection model will fail in detecting new generation ransomware families based on network-based behaviors.

E. CrytoDrop Anti-Ransomware Detection Tool:
"This tool was developed University of Florida and Villanova University boffins. It works by detecting suspicious activity rather than trying to inspect the malware's execution or contents, primarily through three indicators like bulk modification of data, similarity measurement and high entropy. Authors conducted experiments test of CryptoDrop against 492 real-world ransomware samples (representing 14 distinct families, the largest study of encrypting ransomware to date) and find a 100% detection rate with as few victim files lost before detection. With few files lost, the burden to pay for victims of ransomware is reduced or removed, protecting users and dismantling the economy of attackers".

III. PROPOSED METHODLOGY

In this study we have adopted different approach to detect the ransomware at the early stage of attack itself. This research work consists of following methods:

A. Collection of Ransomware Samples:
We collected few different ransomware samples for analysis which covers ransomware families from the period of 2106 to 2020. We then created sandboxed environment with available resources to conduct the analysis and to extract the features from these respective samples

B. Behavior Analysis of Ransomware Families:
In this phase, we tested different ransomware families in test bed environment and observed changes or modifications that occurs during the activity.

C. Identification of Indicators of Compromise (IOC's):
We extracted few networks based and file-based features by running the sandbox environment.

©IJRASET: All Rights are Reserved

D. Dynamic Behavioral Analysis of Specific Ransomware Families:
In this phase, we performed the behavior analysis on the specific ransomware families and gather few critical file indicators of compromise (IOC) of it.

E. Refining Critical IOC's:
In this phase, we identified and refined collected indicators of compromise (IOC's) and extracted few file-based IOCs from the observations.

F. Detection of Ransomware based on Extracted Features:
We started preparing the python scrip to detect the ransomware samples based on file behavioral indicators at the early stage of attack and to classify them to respective families.

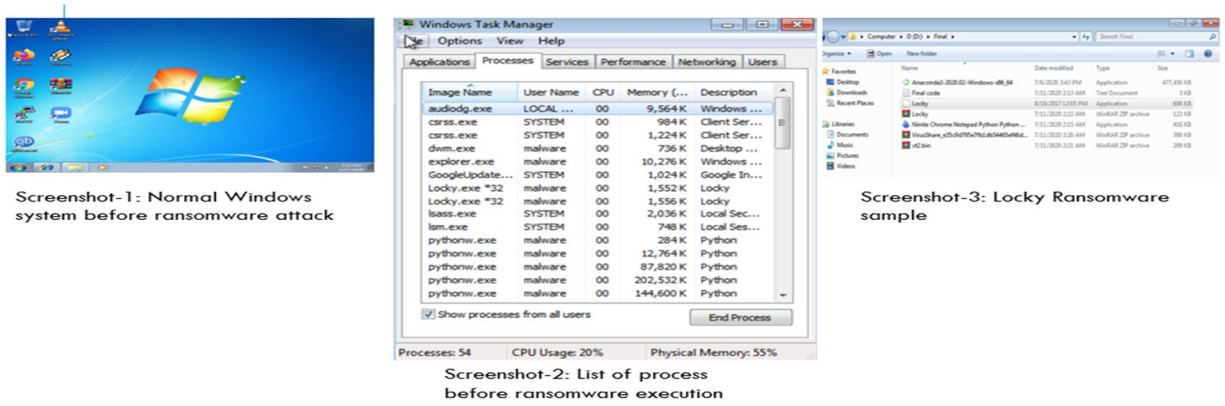
G. Detecting and classifying the Ransomware to respective Families based on File IOCs:
Based on the extracted features and some critical refined file-based IOC's were used in detecting and classifying the ransomware to its respective families.

H. Email Alert:
After detecting the ransomware sample based on the file IOC's, we will alert the user regarding the attack by triggering an email to the respective user.

IV. RESULTS AND DISUCSSION

We conducted the experiment of a specific ransomware family known as Locky ransomware to test the working of above proposed model. Further, we created python script for the ransomware detection and considered few important file IOC's to detect the ransomware activity at the very early stage. The script which we have created will keep on monitoring the system continuously. They are explained in the below phases:
Phase 1: In this phase, we considered few critical IOC's like Bypassing UAC, COM object, and execution of specific dynamic link libraries (DLL) which are related to dropper infection and this help us in detecting the privilege escalation and other suspicious activity on the host. Further we consider the system usage based on process behavior analysis which we already extracted during the ransomware family's analysis.
Phase 2: In this phase, we consider few more critical IOC's like overwriting of MBR/MFT record on the target host and DNS activity which is network related IOC's was also considered for the detection of the ransomware.
Phase 3: In this phase, we consider few file registries changes, file extension modifications and some specific files created by ransomware in specific location were consider as few critical IOC's. These features helped us in classifying the ransomware sample to its respective family.
Phase 4: In this phase, we alert the user via email and pop up message regarding the suspicious activity detected on the host.
By using the above proposed model and critical file system-based indicators of compromise (IOC's) we were able to detect the ransomware and classify it to respective family and alert the user immediately after detection at the very early stage. The below are the screenshot which represent the Locky ransomware detection less than 10 seconds of the ransom activity on the target host.

V. SCREENSHOTS



Screenshot-1: Normal Windows system before ransomware attack

Screenshot-2: List of process before ransomware execution

Screenshot-3: Locky Ransomware sample

Fig4.1: Output(a)

©IJRASET: All Rights are Reserved

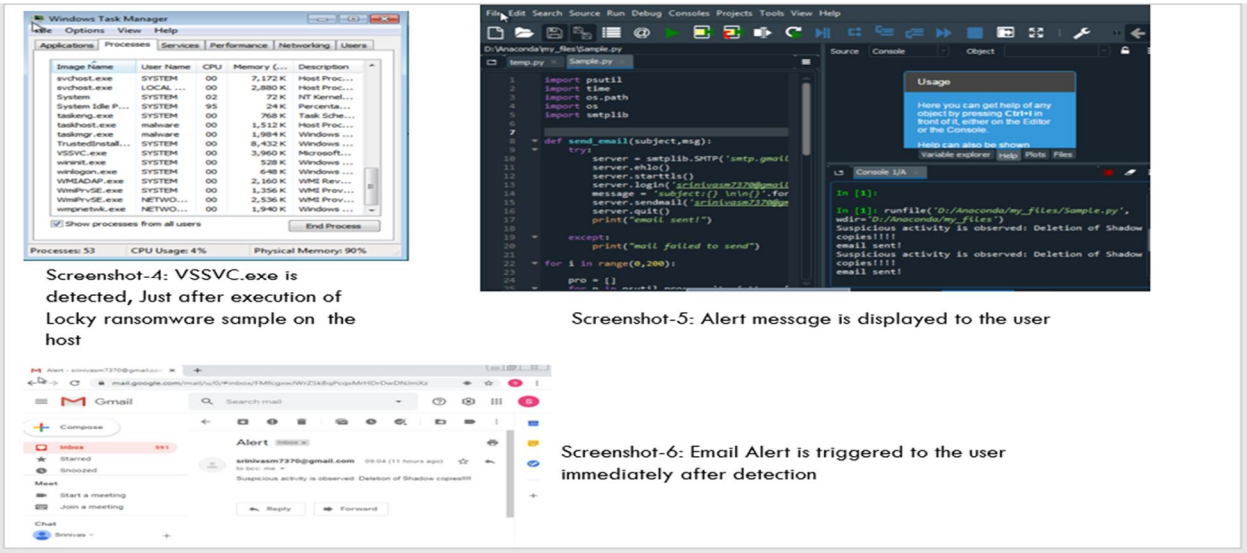


Fig4.1: Output (b)

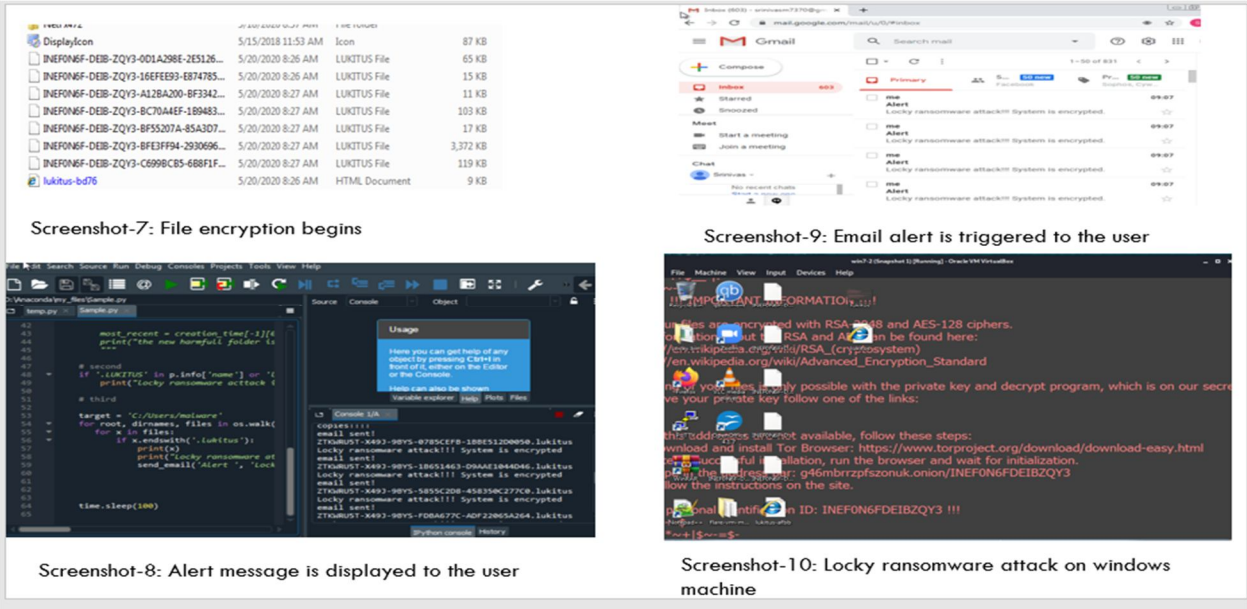


Fig4.1: Output(c)

VI. CONCLUSION

This research study proposes a method to detect ransomware based on critical file behavior indicators (IOCs). By using this method, we were able to identify and detect the ransomware family based on specific file behaviors. The experimental results show that we were able to detect the Locky ransomware in less than 10 seconds on the target host. By comparing this proposed model with other existing model, we can say that file-based ransomware detection and classification has the high detection rate.

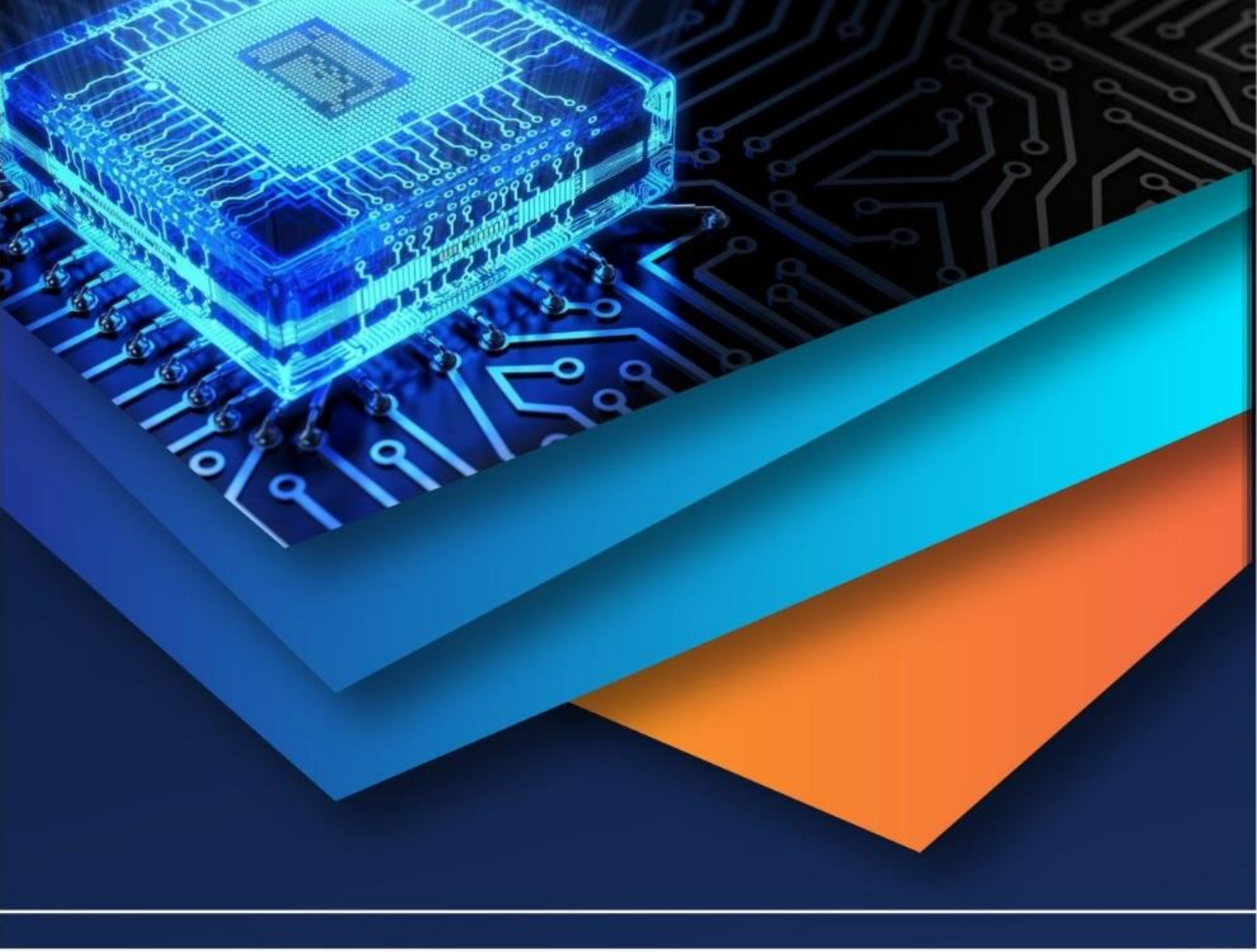
REFERENCES

[1] A. Arabo, R. Dijoux and T. Poulain, "Detecting ransomware using process behavior analysis", *ELSEVIER*, 2019. [Accessed 29 August 2020].
[2] T. Honda, K. Mukaiyama, T. Shirai, T. Ohki and M. Nishigaki, "Ransomware detection considering User's document editing", *International Conference on Advanced Information Networking and Applications 2018.*, 2018. [Accessed 29 August 2020].
[3] M. verma, D. Kumarguru, S. Deb and A. Gupta, "Analysing indicator of compromise for ransomware:Leveraging IOCs with Machine learning technique", 2018. [Accessed 29 August 2020].
[4] A. Almashhadani, M. Kaiiali, S. Sezer and P. O'Kane, "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware", *IEEE Access*, vol. 7, pp. 47053-47067, 2019. Available: 10.1109/access.2019.2907485

©IJRASET: All Rights are Reserved

[5] E. Montalbano, "ISS World Hit with Malware Attack that Shuts Down Global Computer Network", *Threatpost.com*, 2020. [Online]. Available: https://threatpost.com/iss-world-hit-with-malware-attack-that-shuts-down-global-computer-network/153109/. [Accessed: 29- Aug- 2020].
[6] A. Scroxton, "Facilities firm ISS World crippled by ransomware attack", *ComputerWeekly.com*, 2020. [Online]. Available: https://www.computerweekly.com/news/252478890/Facilities-firm-ISS-World-crippled-by-ransomware-attack. [Accessed: 29- Aug- 2020].
[7] "2019 Baltimore ransomware attack", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack. [Accessed: 29- Aug- 2020].
[8] B. Sussman, "Baltimore, $18 Million Later: 'This Is Why We Didn't Pay the Ransom'", *Secureworldexpo.com*, 2020. [Online]. Available: https://www.secureworldexpo.com/industry-news/baltimore-ransomware-attack-2019. [Accessed: 29- Aug- 2020].
[9] A. VILLAS_BOAS, "A Florida city was forced to use pen and paper and pay a $500,000 ransom after hackers took control of its computers", *Business Insider*, 2020. [Online]. Available: https://www.businessinsider.in/small-business/tech/a-florida-city-was-forced-to-use-pen-and-paper-and-pay-a-500000-ransom-after-hackers-took-control-of-its-computers/articleshow/69978391.cms. [Accessed: 29- Aug- 2020].
[10] "2nd Florida city in just a week to pay hackers big ransom for seized computer systems", *Cbsnews.com*, 2020. [Online]. Available: https://www.cbsnews.com/news/ransomware-attack-lake-city-florida-pay-hackers-ransom-computer-systems-after-riviera-beach/. [Accessed: 29- Aug- 2020].
[11] A. Ivanyuk, "Ransomware Attack Costs $1.5 Million in Riviera Beach, FL", *Acronis.com*, 2020. [Online]. Available: https://www.acronis.com/en-us/blog/posts/ransomware-attack-costs-15-million-riviera-beach-fl. [Accessed: 29- Aug- 2020].
[12] "SonicWall 2019 Mid-Year Threat Report Shows Worldwide Malware Decrease of 20%, Rise in Ransomware-as-a-Service, IoT Attacks and Cryptojacking - SonicWall", *SonicWall*, 2020. [Online]. Available: https://www.sonicwall.com/news/sonicwall-2019-mid-year-threat-report/#:~:text=In%20the%20first%20half%20of%202019%2C%20SonicWall%20observed%20a%2055,quarters%20of%20the%20previous%20year.&text=Cryptojacking%20volume%20hit%2052.7%20million,

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)