RRR Concept and unknown Facts of Ransomware

Ranjitha V.

Abstract: Ransomware is the word which is very popular nowadays. Ransomware is a malicious program that infects the device once it gets into and cannot decrypt the data until the key is provided by the hacker. Ransomware not only forbids the access but also infect the network, where it is communicating with, by encrypting the content that is located on mapped and unmapped network drives where the whole organization networks falls down. In Ransomware various families exist like Cryptoworm, Raas and many. This Ransomware Target is mainly on corporates for beneficial profits. Cryptocurrency is one of the enabling factors of Ransomware. In 2019 according to research work Ransomware raised because of phishing emails and smshing to 109 percent over 2017. Ransomware detections in the first half of the year were up 77% compared to the latter half of 2018. Around 851 million Ransomware contagious activities happened in 2018. 34% of corporates came across with this malware and took months or more to recover back and to access their own data. The algorithms that are used by the Ransomware is very complex which cannot be understood by the normal users. This article is to share research findings about Ransomware, some unknown facts where exactly how Ransomware is growing, and also Restrict Recognize React concept (RRR concept) of Ransomware which is mainly for avoiding Ransomware. Restricting is the measures that as to be carried out for avoiding the Ransomware, Recognize is for identifying the Ransomware if device is infected with it, React is mainly responding to the attack to get rid of Ransomware.

Keywords : Cryptoworm, Raas, Cryptocurrency, Ransomware, phishing, smshing, RRR concept.

I. INTRODUCTION

Ransomware is combination of two words that is ransom and malware where ransom is for money and malware is for infections. For every 14 seconds there is Ransomware attack across the world which leads to the loss $11.5 billion by the termination of 2019. Symptoms that mainly victim who got infected by Ransomware will come across is

*Normal Files displays error messages like file is infected when user is trying to open and the file will be with wrong extensions.

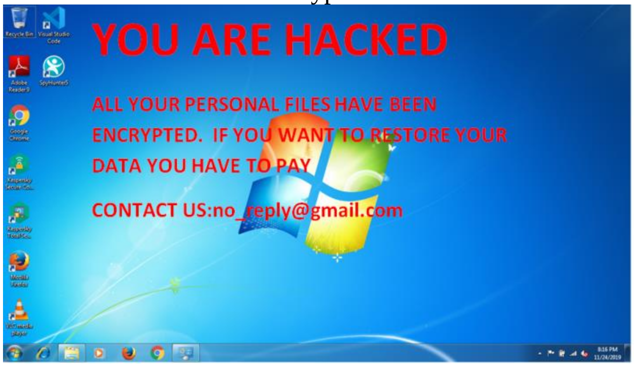
*An alert messages with alarming option is placed in desktop background with guidelines for the ransom to recover back the files

*The code is running in the background that scares the user to pay ransom within the deadline otherwise files cannot be decrypted.

*A separate window will be displayed for Ransomware code where victims cannot close it.

*Files will be in the name HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML.[1]

Figure 1: Shows a sample window how Ransomware really looks. RSA 2048 encryption is basically used by the Ransomware software to encrypt the files.



YOU ARE HACKED

ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED. IF YOU WANT TO RESTORE YOUR DATA YOU HAVE TO PAY

CONTACT US:no_reply@gmail.com

Fig 1: Sample home window with the Ransomware

To know the concept of RSA 2048 key, it is expected 6 quadrillion years to be spent by normal desktop users. For spreading Ransomware Different vectors are used like phishing, smshing, and drive by downloads, free software's and many. To recover from this Ransomware various measures as to be taken like restoring the files from the backup repositories, second is like trying to decrypt the file third is like paying ransoms.

Ransomware types

1) cryptoworm: which grows by replicating until reach the limit

2) Raas: that is Ransomware-as-a service it is a kit available in the markets and the hackers with bad intention can buy it and with less technical knowledge attackers can able to spread it to their targets.

3) Automated Active Adversary – third one where attacker will concentrate on maximum damage that is through automatic scan of internet where attacker knows about the ports which are open to do backdoor entry. [2]

This article is to share knowledge about the Ransomware and to spread knowledge about the risks that suffer will encounter. Paper is divided into the following sections:

The primary section is about background history of malware, countries affected by Ransomware from past 3 years and the recent attacks of 2019-2018 in table form.

The secondary section is workflow of malware exactly how it acts with the victim.

*The third portion demonstrates the various steps genuinely worried in Ransomware after downloading the Ransomware with RRR concept of Ransomware.

*The closing segment suggests the belief information of the Ransomware. [3]

II. LITERATURE REVIEW

System files or system where accessed by hacker or attacker via downloading the malicious software called Ransomware from malicious websites by user which later blocks user from accessing his/her own system.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author

Ranjitha V.*, department of Computer Science and Engineering, GITAM School of Technology, Bengaluru, India.
E-mail: ranjithapriu@gmail.com

Entire devices are encoded with attacker’s extensions it cannot be decoded until ransom amount is paid. This malware first came into existence in the year 1989 with the “AIDS TROZAN”.

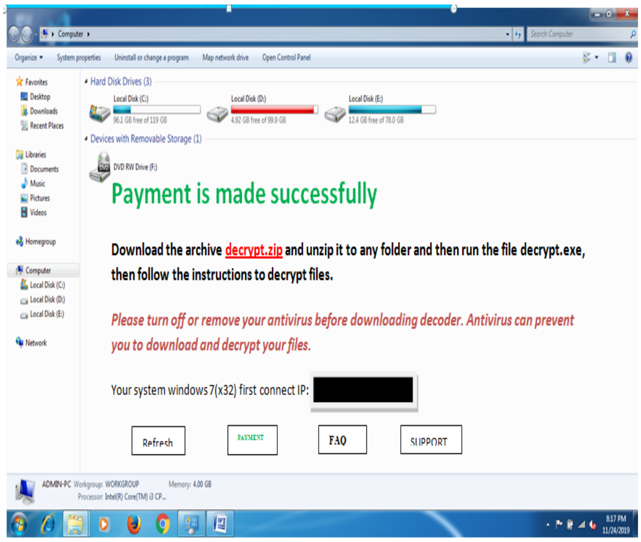
Ransomware is popular name from decades where various fields are continuously on research work to completely eradicate Ransomware.

*In 1996 data hijacking was hosted by making use of public key cryptography which was introduced by Adam L. Young and Moti Yung.

The Ransomware actually as various categories like
*Encrypted Ransomware,
*Non-encrypted Ransomware,
*Dox ware,
*Mobile Ransomware.

Each and every category of Ransomware has its speciality and damaging standard in its own way. There are even families of Ransomware like ”ACCDFISA, Amnesia, Annabelle, BadRabbit, Bart, Cerber, Cryptolocker, GandCrab, Globe, GlobeImposter, Hermes, HiddenTear, LeChiffre, LockCrypt, Magniber, Nemucod, NotPetya OpenToYou, PCLock, Petya, Rapid, SamSam, Satan, Scarab, SynAck, TeslaCrypt, Troldesh, UIWIX, WannaCry, Xmas, Xoris”

The attackers who constantly involved in this activity are mainly for gaining beneficial profits. It mainly focus on Encrypting the files, spreading around, but nowadays it is with predefined infrastrures that is non-encrypted malware which mainly infects overall and ensures reverse-engineering is hectic. Explanation given by Ryan Francis managing editor of CSO and Network World “New-age Ransomware involves a combination of advanced distribution efforts such as pre-built infrastructures used to easily and widely distribute new varieties as well as advanced development techniques such as using crypters to ensure reverse-engineering is extremely difficult.”[4]



Payment is made successfully

Download the archive decrypt.zip and unzip it to any folder and then run the file decrypt.exe, then follow the instructions to decrypt files.

Please turn off or remove your antivirus before downloading decoder. Antivirus can prevent you to download and decrypt your files.

Your system windows 7(x32) first connect IP: [redacted]

Fig 2: Pattern window of a hit price that is successful payment

Ransomware as global impact that is there are many countries which is facing huge financial loss and where most of the Ransomware affected region are Soudi Arabia, Turkey, china spain south africa and many according to cyber edge shown in the graph.

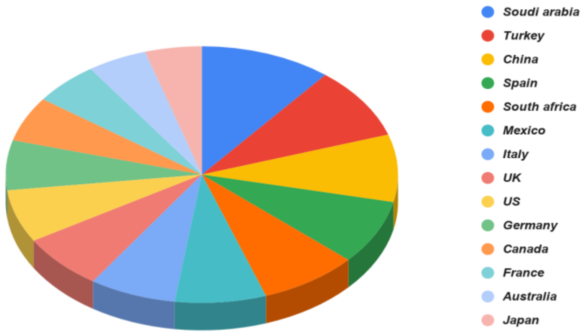


Fig 3: Source from cyber edge which suggests numerous regions suffering from Ransomware in 2018-2019

From the above graph it is virtually recognized that numerous countries are affected by Ransomware and nevertheless they're paying ransoms which is cutting-edge records of November 2018.

But in the year 2017 it's far determined that Spain and China changed into in first location and 2d area and plenty of different countries.

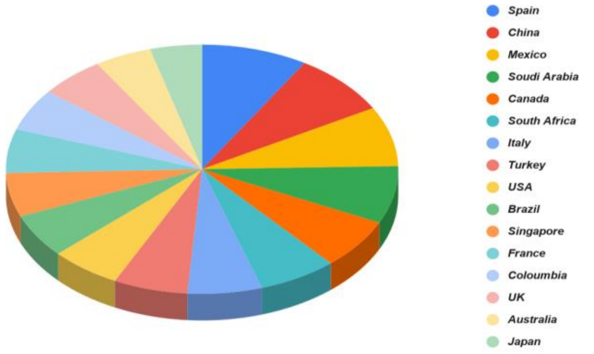


Fig 4: Various regions laid low with Ransomware in 2017-2018 (source from cyberedge 2018)

From the above graph it is clearly known that various countries are affected by Ransomware and still they are paying ransoms which are latest statistics of November 2018.

Ransomware attack if we are considering in the year 2016-2017 according to the survey by the cyberedge it is found that various countries had exaggerated are clearly shown fig 5.[5]

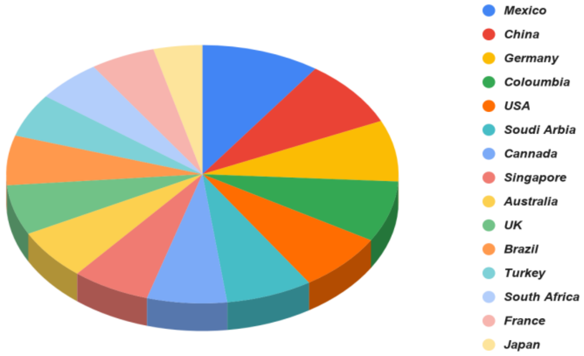


Fig 5: shows the diverse international locations subjected to the Ransomware assault in the year 2016-2017(source from cyberedge 2017)

Table1:

Details of the Ransomware attack and the form of Ransomware worried in the attack and the targeted countries with year [6]

TYPE	YEAR	TARGETED	RANSOM
A kind of Ransomware	Dec 2019	New Orleans	Not disclosed yet
MAZE	Dec 2019	Pensacola	Asked to pay $2.3 million
Ryuk	Oct 2019	DCH Health System, a regional health care system	Not disclosed
RobbinHood	May 2019	city of Baltimore in maryland	Asked for approximately $76,200
Malware from Email	May 2019	Riviera Beach	paid $600,000
A kind of Ransomware	March 2019	Jackson County	Paid $400,000
SamSam	April 2018	city of Atlanta	Done Ransom of $2.6 millions

III. PROPOSED METHODOLOGY: RANSOMWARE FLOW

Fig 6: RRR concept blocks

Restrict, Recognize, React or RRR concept(R3 concept)

Restrict,Recognize,React or R3 concept: It is better to follow R cube procedure to avoid the Ransomware the first letter R is for Restrict that is restring or preventing the Ransomware attack, second R is for Recognize, if system is affected with Ransomware the steps that need to be carried out to analyse what kind of Ransomware got downloaded in the system and the status of the system. Third R for the react that is after recognizing the Ransomware what steps need to be performed to overcome out of it

Process workflow of Ransomware with flow diagrams can be shown in Fig 7. Through using RRR concept the flow has been considered.

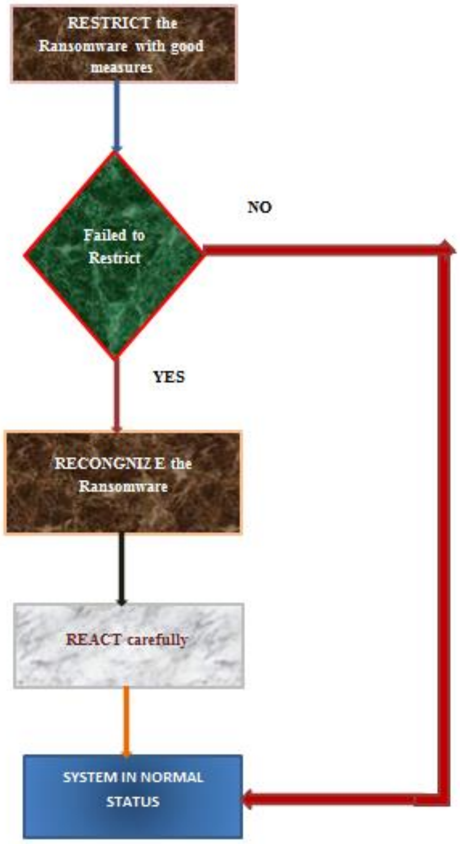

RESTRICT the Ransomware with good measures
Failed to Restrict
NO
YES
RECONGNIZ E the Ransomware
REACT carefully
SYSTEM IN NORMAL STATUS

Fig 7: Ransomware Workflow

```
ALGORITHM
STEP1: START
STEP2: RESTRICT THE RANSOMWARE WITH CORRECT MEASURES
STEP3: IF (RESTRICTION FAILED) GO TO STEP 4
STEP4: RECOGNIZE THE RANSOMWARE AND THE STATUS OF THE RANSOMWARE, GO TO STEP 5
STEP5: REACT CAREFULLY
STEP6: ELSE SYSTEM IS NORMAL
STEP 7: STOP
```

The workflow of Ransomware actually redirects based on victims actions

1. Users system somehow comes in touch with Ransomware either through phishing activity or in other ways like outdated issues
2. Entire system files is completely encrypted as shown in fig 1
3. After getting infected sufferers will get ransom note for paying the ransom in this step it can be like victim can either pay ransom or not
4. There is a minimum amount of time for paying ransom depending on the attacker. If that deadline exceeds then ransom will be increased in fact it is multiplied.
5. If user pays ransom then decryption key is provided or else functionality of system is lost.
6. If backups are there then sufferers does not pay ransom [7]

IV. STEPS TO AVOID RANSOMWARE

RRR concept or (R3 concept)

RESTRICT

To avoid Ransomware attack or any other forms of attack several steps need to be followed which mainly comes under first R that is Restricting Ransomware through following steps

*Avoid opening untrusted website link which usually mislead to an attack where system user he/ she himself will give an authority to the hacker.

*Always system as to be up to date. Any applications and the operating system present in the system should be in current version.

*Always downloads should be from trusty websites where securely downloads should happen that is it should not be from the unreliable links that is like http which is not secured compare to https so always users should go for trusty websites

* Leaking individual's data via untrusted phonecalls, replying to the untrusted mails or through some other means leads to the attack that is either by phishing, smshing, vishing, or through any other social media which mainly contains our activities details leads to the Ransomware attack.

*Careful with emails and messages before opening: Before opening the mail or messages makes sure it is from genuine persons, any case of suspect avoids the mails and messages from opening.

*Content scanning and filtering is a way to avoid mostly the Ransomware where it scans for malware anomalies like Ransomware.

*Before plugging in the other external device to the system scan for virus.

*File integrity monitoring or file internal monitoring this procedure helps in monitoring the files if any changes in the files happen then alert messages is given to system admin.

*System as to be with regular backup in order to safeguard the data.

*System as to be with strong passwords.

*Virtual private networks help primarily in using public wi-fi and that avoids Ransomware.

*Most of the times antivirus software, firewall and the Internet security even avoids the Ransomware.

*Traffic monitoring that takes place on a daily basis need to be monitored only to avoid or block the initial attack.

*By monitoring log user can identify the traces of attacker if attacker is targeting the system for Ransomware attack.

*Create Restore points and recovering points from system control panel settings which mainly assists in recovery.

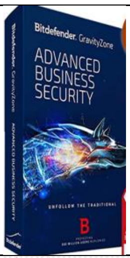
*Network segmentation (private networks) to avoid infected shares or critical computers and to protect genuine data present in the system.

*Users who are using the system should not be given with admin rights when they are not required.

*Creating awareness by educating employees, family friends about the Ransomware attack and the consequences of it.

There are even tools that restrict Ransomware from the attack this tools as various layers of security in 2019 this are tools which are making sounds in the society.[8]

Table 2: TOOLS of 2019 that are restricting Ransomware to maximum extent.

SL. NO.	LOGO	FULL FORM	GOAL
1	Acronis	Acronis Ransomware Protection	Acts upon type of Ransomware like wannacry, petya, Osiris, 5GB of data can be protected
2	avast	Avast Free Antivirus	Avast can remove the threats to maximum extent. Six layers of security to catch Ransomware
3		Bitdefender GravityZone	End points Security for threat avoidance
4	Check Point SandBlast AGENT	**Check Point SandBlast Agent**	Protecting from Ransomware attack by sidestepping the convolution network making organization isolated.
5	CISCO	**Cisco Ransomware Defense**	Protecting from DNS to email to End point where Ransomware attack is more.
6	COMMVAULT	**Commvault Ransomware Protection**	This protection can give alerts to the company when Ransomware attacks happen so that company can react faster for it.

7		**Kaspersky Anti-Ransomware Tool**	Scanning cloud to block the Ransomware immediately and gives the protection from WannaCry, Petya, Bad Rabbit, Locky and TeslaCrypt.
8		**Malwarebytes Premium**	It provides protection for the operating systems like MAC, ANDROID etc., It also warns the user when user accidentally visits the website
9	Symantec. Endpoint Protection	**Symantec Endpoint Protection**	It detects the Ransomware malware and also it searches for the other threats with the assistance of machine learning
10	TREND MICRO AntiRansomware	**Trend Micro Anti-Ransomware Tools**	It is an intelligent technology that generally applies the required methodology at the right time.

RECOGNIZE

If System is affected with Ransomware because of system Admin who failed to avoid the attack the following **symptoms** as to be observed by the sufferers to know that they under attack, Indications like

1) ENCRYPTION,
2) RENAME of files,
3) WINDOWS wallpaper display,
4) Multithreaded tasks and many.

The kind of Ransomware that hit the system can be of various variants of Ransomware which as its own specialty of spreading.[9]

Table 3:

There are few Ransomware kinds which are very lively in 2019[2]

Sl.No.	Type	FUNCTIONALITY
1	STOP(DJVU)	It locks the system content and main targets are the home users when they download unsecure files from torrents
2	DHARMA	Instructions will be provided in order to contact hacker to pay ransom by locking the system
3	PHOBOS	Spreads from unsecure remote Desktop protocol ports same as Dharma gives guidelines to contact hacker
4	GLOBELMPOSTER	Its next variant of above type, make use AES 256 to encrypt files
5	REVIL	First discovered in 2019 also called as sodinokibi and uses very advanced technique to escape from the software
6	GANDCRAB	It infects and encrypts all files within the system and also it is from various exploit kits.
7	MAGNIBER	Encryption of file happens where each file is encrypted with a different key, And files are with different cipher text
8	SCARAB	It makes use of emails to get into system as a group of malware.
9	RAPID	Once system gets infected the malware tries to remove windows copy volume and also stops database. It encrypts all files and issues ransom bill
10	TROLDESH	Other name is shade account spreads through zip files which is Javascript encrypt the files
11	WANNACRY	Main target is the systems with windows 7 operating system

12	SAMSAM	Single threaded it decrypts at most one document at a time came in to existence in 2015 most overwhelming
13	BITPAYMER	Single threaded, Knows to abuse alternate data streams
14	RYUK	Multithreaded at a time many files are encrypted even network drives
15	LOCKERGOGA	Which reduces the antimalware detection system efficiency, single threaded does not encrypt network drives
16	MEGACORTEX	Renames the document before encrypting the file, it as a dynamic link library of 32 bit, single threaded
17	ROBBINHOOD	It make use Sample SHA-256
18	SODINOKIBI	Distribution is Through malspam that is malware zip is from emails to systems

All listed Ransomware make use of SHA-256 with various indications like

- WannaCry ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
- GandCrab 6FBA19BF0CC1BB764E063C1DE51CAF0CF0A6CC90FA76B592BCDE28CEEE161BDC
- SamSam 8C0425ECA81E1EEAF8043764EB38A2BC103598163D3307E583F4E5AD7EB0E708
- Dharma B8D32ED92E3227836054ED6BB4E53AD2E0ABE4617F1215D5E81162F9F5513EC2
- BitPaymer 655C44BEBB2A642E665316236A082C94F88A028721C19BD28B5F25E1C40A13B8
- Ryuk 830F83578F3A5593B103EA4A682788DC376E96247CD790417F2630884D686E9F
- LockerGoga 2CE4984A74A36DCDC380C435C9495241DB4CA7E107FC2BA50D2FE775FB6B73CE
- MegaCortex F5D39E20D406C846041343FE8FBD30069FD50886D7D3D0CCE07C44008925D434
- RobbinHood 3BC78141FF3F742C5E942993ADFBEF39C2127F9682A303B5E786ED7F9A8D184B
- Sodinokibi 06B323E0B626DC4F051596A39F52C46B35F88EA6F85A56DE0FD76EC73C7F3851[3][14-15]

REACT

Once sufferers found that he has been infected by the Ransomware the steps that victim should follow which comes under Reacting process are

1) FREE EVERYTHING

*As soon as recognizing the attack makes sure that the system is isolated from the network.

*off the all wireless functionalities which are running in the background like Wi-Fi, Bluetooth etc.

*SEPTICITY RANGE AS TO BE IDENTIFIED

Checking whether the devices like USB drives, files, and folders have been encrypted or not only to know that to what extent has the infection been spread.

*RECOGNIZE

Identifying which type of Ransomware has been affected to the system eg:DHARMA which is listed in the recognizing procedure[10]

REACT

1) BRING BACK FROM THE BACKUP

If person as good backup of data then not to worry documents that person wanted, can get back from cloud garage,

Second manner of reacting is

2) TRYING TO DECRYPT THE ENCRYPTED FILE

Applying all sense of decryption intelligence and getting back the content material is very difficult due to complex algorithms that are used for encryption.

2) DO ZERO

Instead of doing many complicated tasks to get information back and knowing which could be very hard to do, sufferers no need to do anything no longer to pay even Ransom additionally.

3) PAYING RANSOM

Next method is paying ransom where either with the aid of negotiation or via paying entire ransom as soon as sufferers pay fig 2 sample is displayed

4) PROTECTING FROM FUTURE

Protecting the device completely from the Ransomware and every other attack with the help of safety stuff which are referred to within the Restrict procedure [11-13]

Third manner is

Contact cyber security professionals, who can help in deciding the best manner to continue and may be Capable of lend free technical information important to analyze and clear up the annoyance. A few Corporations that inspect and offer this steering include: Center for Internet Security's (CIS) Multi-State Information Sharing & Analysis Center [14-15]

V. RESULT ANALYSIS

As according to the RRR concept awareness among the users reduces the total number of attacks here is sample window shown in the graph where Y axis is with attacks taken in thousands and X axis is with RRR and without RRR concept, so with RRR concept less number of attacks is seen.

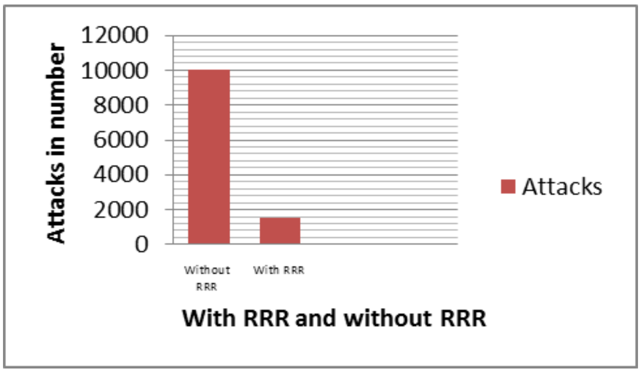


Fig 8: Result analysis of RRR concept

VI. CONCLUSION

This paper gives idea regarding many unknown factors of Ransomware where it created its footprints in many regions of the continent and they are financially affected, the process flow of the Ransomware program and various paths that victims takes based on the criteria they have, and the steps that mostly avoids the Ransomware like RRR acronym, that provides the knowledge like always system as to be up to date, Scan before plugging in the other external device to the system, and backup for data and many.

LIMITATION AND FUTURE WORK

There are few strategies to stop this Ransomware like predictive models and collecting human responses but it could do approximately, however there are gap environs in completely abolishing this Ransomware.

REFERENCES

1. 2019 State of Malware-Malwarebyte resources page no.20-22
2. McAfee Labs Threats Report August 2019 given by MCAFEE labs.
3. RANSOMWARE Hostage Rescue Manual 2019-hubspot
4. Muhammad Ubale Kiru,Aman B. Jantan"The Age of Ransomware: Understanding Ransomware and Its Countermeasures".
5. Gavin Hull1, Henna John2 and Budi Arief3"Ransomware deployment methods and analysis: views from a predictive model and human responses".
6. Ransomware on the Rise But with OneXafe Never Pay the Ransom 2019
7. Nihad A. Hassan"Ransomware Revealed A Beginner's Guide to Protecting and Recovering from Ransomware Attacks"
8. Mihail Anghel, Andrei Racautanu "A note on different types of Ransomware attacks" page no. 3
9. Mark Loman, Director, Engineering," How Ransomware Attacks", Sophos 2019
10. New York State Comptroller THOMAS P. DiNAPOLI "Local Government Management Guide Ransomware"
11. Kruse, Clemens Scott* | Frederick, Benjamin | Jacobson, Taylor | Monticone, D. kyle,"Cybersecurity in healthcare: A systematic review of modern threats and trends",Technology and Health Care, vol. 25, no. 1, pp. 1-10, 201, page no.5-6
12. Volume 14, 2017 Accepting Editor: Eli Cohen │ Received: November 29, 2016 │ Revised: January 18, March 2, 2017 │ Accept-ed: March 28, 2017. Cite as: Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware.
13. "I was told to buy a software or lose my computer. I ignored it": A study of Ransomware Camelia Simoiu Stanford University Christopher Gates Symantec Joseph Bonneau New York University Sharad Goel Stanford University
14. From the internet cyber edge source https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf,https://cyber-edge.com/wp-content/uploads/2017/03/CyberEdge-2017-CDR-report.pdf
15. A note on different types of Ransomware attacks Mihail Anghel, Andrei Racautanu, email: racautanu.andrei.nicolae@info.uaic.ro Computer Science Faculty, "Al. I. Cuza" University, Iasi, Romania. (Internet sources)

https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_Ransomware_Enterprise.pdf
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-Ransomware-behavior-report.pdf
https://www.kaspersky.co.in/resource-center/threats/how-to-prevent-Ransomware
https://phoenixnap.com/blog/preventing-detecting-Ransomware-attacks
https://www.csoonline.com/article/3287099/10-ways-to-prevent-detect-and-recover-from-Ransomware-and-zeroday-threats.html
https://www.backblaze.com/blog/complete-guide-Ransomware/
https://enterprise.comodo.com/different-types-of-Ransomware.php

AUTHORS PROFILE

Ranjitha V., is with Computer Science and Engineering department, GITAM University, Bangalore campus. Currently she is Assistant Professor, Her areas of interest are Cyber Security, IOT, Machine learning, Big data, Networking, 5G Technologies. She can be reached at ranjithapriu@gmail.com