Ransomware Evasion with its Behaviors

Ranjitha V , Tanuja G , Anughna N

***Abstract**: Ransomware is a malware, where entire system is encrypted as soon as it gets into the system. Presently it is very hot topic in the IT news as a money making scheme. Since Ransomware is evolving rapidly the studies on it becomes outdated very soon and also cybercriminals who works on Ransomware have created their own bionetwork where they always come up with new techniques like Trojans, bots, coins etc. which will penetrate inside the systems by detouring the antivirus tools. User system can free from attack either by maintaining the system with proper updates and good anti Ransomware tools like Acronics, Trend Micro and many. Companies and domestic users are the ones who are mainly affected by the Ransomware and will be under financial loss. To recognize and to get rid of Ransomware safely by making use of various countermeasures users must know the behavior and variants of Ransomware. There are various articles that gives the information about the different families of Ransomware like Crypto Ransomware, a kind of Ransomware that deletes the actual data of user and encrypts entire files present in the user's system, Wannacry is other variant that actually targets the windows operating system and encrypts the files and Cryptolocker, Locky etc. are different variants that are present which are unique in their own way. But then this article focuses on the Evasion of Ransomware with special characteristics like unbreakable encryption, giving extensions to files and its capacity lies in encrypting all kinds of data, the Evasion Method includes complete prevention of Ransomware which assists the organization and also domestic user.*

Keywords: ***Crypto Ransomware, Acronics, Trend Micro, Ransomware, Evasion, Wannacry, Cryptolocker, Locky.***

I. INTRODUCTION

Ransomware has affected various categories of industries like telecommunication, transport manufacturing, financial industries and many, only with the intention of making money; this Ransomware has become means of profit for hackers hence it is updating with respect to time. In current decade new categories of Ransomware is observed which is mentioned in the table 1.[1]

Emails, supply chains, Remote access and many are called the vectors of Ransomware where Ransomware can easily spreads, there are even the combination of Ransomware variants for encrypting the source content like notpeyta always combined with Wannacry for an attack where notpeyta cannot alone decrypt the files it takes assistance of brickware and wiperware for decrypting the files so that recovery is not possible. [2]

Tabe1: Ransomware new variants from old variants which are currently in practice from 2019 with their extension

Type	New variant	Extension
Phobos	Dever	.Dever
Dharma	RIDIK	.RIDIK
Wannacry	AWT	.AWT
Ransomware	Zeoticus	.zeoticus
Ransomware	Cohen locker	.cohen

As shown in the table 2 there are different forms of attack and such attacks even take a phases like

1) Exploration
2) Diffusion
3) Reinforcement
4) Aggression
5) Breakdown
6) Ransom

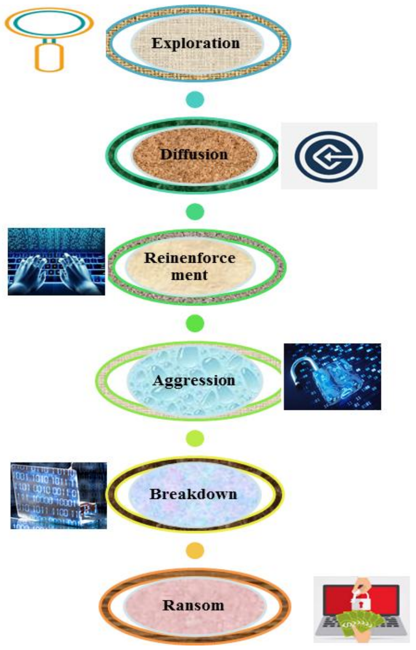

Fig 1: Various phases of Ransomware attack

Manuscript published on January 30, 2020.
* Correspondence Author

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

Tanuja G, Electronics and communication Engineering department, GITAM School of Technology, Bengaluru, India. Email: tanuja.g20@gmail.com

Anughna N, Electronics and communication Engineering department, GITAM School of Technology, Bengaluru. Email: anughna.7@gmail.com

Retrieval Number: E6605018520/2020©BEIESP
DOI:10.35940/ijrte.E6605.018520
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

1) Exploration: Gathering the data about the target and their weakness
2) Diffusion: Penetrating into the system by gaining access
3) Reinforcement: once the attackers are inside the network their chattels are protected
4) Aggression: attackers targets the sensitive information and high valued data
5) Breakdown: Attackers spoil the backups so that to the victims backups is visible but cannot recover the data
6) Ransom: This phase is for attacker to demand ransom this ransom is with time where it increases in hourly mannered. [4]

Table 2: Gives information about various types of attacks caused by different variants [3]

Variant	Name of attack	Description
cryptolocker	cryptolocker Ransomware attack	most aggressive Ransomware attack since it is with strong encryption algorithm
wannacry	wannacry Ransomware attack	other names for this is attack is wcry, wannacryptor where attackers use most widely
cerber	cerber Ransomware attack	cloud based office 365 users are targeted by phishing
cryptowall	cryptowall Ransomware attack	an advanced form of cryptolocker since cryptolocker fallen down this as come into existence
Locky	locky Ransomware attack	this actually locks the system until the suffer pays the ransom
Golden eye	Goldeneye Ransomware attack	targets mainly on human resource department where the system user downloads this infected file the macro is launched and it encrypts the files
Jigsaw	Jigsaw Ransomware Attack	most dangerous attack where it decrypts the file and mean while deletes the file in hourly manner

In this article first session is about the various attacks second session is about literature review third about characteristics of Ransomware fourth session is about different evasion methods fifth session is about the result analysis of various recognition techniques last part includes the conclusion of entire paper

II. LITERATURE REVIEW

There are works on Ransomware like life cycle of Ransomware and the types of Ransomware analysis

Table 3: Works on Ransomware in 2019

Authors	Research work	year
Maxat Akbanov , Vassilios G. Vassilakis , and Michael D. Logothetis	Work is on the variant of Ransomware that is wannacry Analysis	2019
Asibi Imaji	Work is on Ransomware Attacks: Critical Analysis, Threats, and Prevention methods	2019
Muhammad Ubale Kiru, Jantan Aman	work is on knowing the age of Ransomware with its countermeasures	2019
Juan A. Herrera Silva , Lorena Isabel Barona López , Ángel Leonardo Valdiviesо Caraguay and Myriam Hernández-Álvarez	work is on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters	2019
Camelia Simoiu, Christopher Gates Symantec Joseph Bonneau Sharad Goel	work is on the Ransomware detail study how it penetrates and behaviors of it	2019

The above works give information of Ransomware features, its lifecycle, and few measures need to be carried for avoiding the Ransomware.

Considering Ransomware statistics where Ransome paid countries

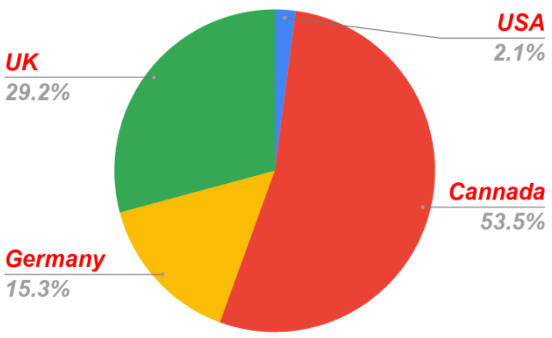

Fig 2: Shows the nations that paid High Ransom according to 2019 (source from:https://phoenixnap.com/blog/Ransomware-statistics-facts)

Table 4: 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

FEATURES OF RANSOMWARE

Users should be aware of various features that Ransomware contains so that user can have knowledge regarding Ransomware like the below table shows the variants of Ransomware and its discovered year with its features.[7][8][9]

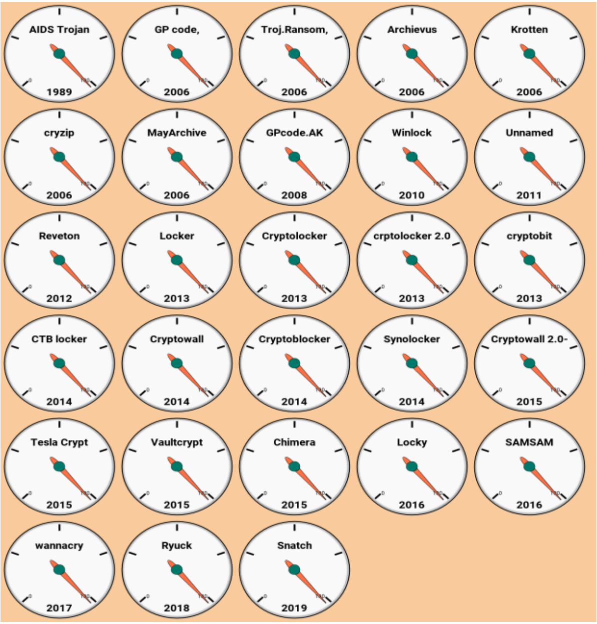

Fig 3: Shows the variants of Ransomware with years

Table 5: Different Ransomware variants and its year where it made its noise

Variant Type	Year	Descriptions
AIDS Trojan	1989	First Unknown Ransomware**AIDS**, also known as **Aids Info Disk** or **PC Cyborg Trojan**, is a trojan horse that replaces the AUTOEXEC.BAT file, It counts the number of time boot operation happens if boot count reaches 90 then it starts encrypting the files and directories
GP code,	2006	**PGPCoder** or **GPCode**. It actually encrypts the data on the infected computer
Troj.Ransom,	2006	utilizes RSA algorithm
Archievus	2006	Targets only my document folder rather than targeting other executable folders which are with extensions, in this case the user can able to access other files even Ransomware is in computer
Krotten	2006	Under Research
Cryzip	2006	Cryzip it targets the zip folder even if it is with passwords by using brute-force attack on zip folders.
MayArchive	2006	it uses Rsa algorithms with large size keys
GPcode.AK	2008	code is used to encrypt the user files and lock the files where use of a 1024-bit RSA key to lock
Winlock	2010	Primarily seen in Russia and would show porn on device screens until user pays Ransom
Unnamed Ransomware	2011	Under research
Reveton	2012	computer is used for offensive work like downloading unlicensed software or child pornography. other name is "Police Trojan".
Locker	2013	this variant will demand users to pay ransom of 150 dollars with time limit of 72 hours
Cryptolocker	2013	It mainly infects the system through infected attachments found in the emails.
crpto locker 2.0	2013	It increases anonymity Payment
Cryptobit	2013	using TOR it would encode first 1.024 bit of every file it and makes more profit
CTB locker	2014	It uses elliptical curve cryptography
Cryptowall	2014	It infects billions of files, utilizing infected emails
Cryptoblocker	2014	It does not encrypt windows files which is 100 mb and basically make use AES algorithm
Synolocker	2014	Synology encrypted Devices
Cryptowall 2.0-4.0	2015	It make use multiple attack vectors and as various versions with additional features
TeslaCrypt	2015	**TeslaCrypt** was a Ransomware trojan.basically from computer games
Vaultcrypt	2015	under Research
Chimera	2015	It is scareware Ransomware which threatens the user to pay ransom otherwise encrypted data will be published online
Locky	2016	only encrypting the user files and renames using .locky extension

SAMSAM	2016	Targets servers and proceeds to users windows system
Wannacry	2017	uses worm like infector that spreads to drives
Ryuck	2018	It disables windows system restore option, and impossible to get back encrypted files without backup
Snatch	2019	Reboots the windows in safe mode to eliminate the security

[9][10][11][12]

III. PROPOSED METHODOLOGY: EVASION METHODS

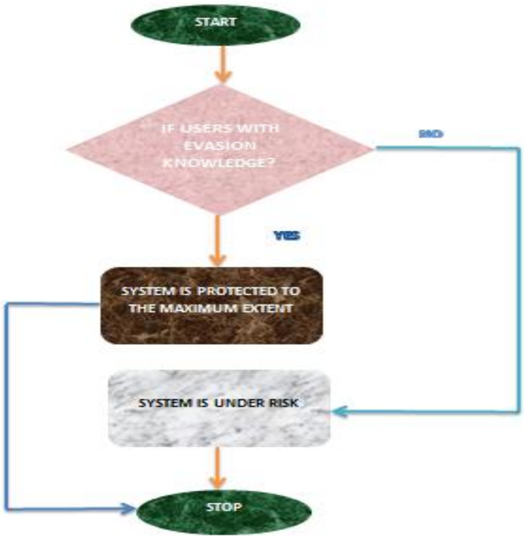
START
IF USERS WITH EVASION KNOWLEDGE?
NO
YES
SYSTEM IS PROTECTED TO THE MAXIMUM EXTENT
SYSTEM IS UNDER RISK
STOP

Fig 4: Shows the user with evasion knowledge can protect his system from risk

Algorithm

```
Step1: Start
Step2: If
User with Evasion knowledge with respect to Ransomware,
System is protected from attacks
Else
System is under risk
Step 3: Stop
```

Once the user observes the files with wrong extensions or with encrypted content then user should think that system is under risk, or user will be getting the window in demand of ransom by the attackers the symptoms that user can find once the system gets infected is

1. With Excellent Cyber hygiene: It may be with respect to company or with respect domestic user, systems should be with up to date that is hygiene with respect where many patches is covered through updating, and cautions to be taken in a timely manner, hence vulnerabilities is not known through which an attacker can get access to system through vulnerabilities .
2. Organization not only maintaining Cyber hygiene and also should have additional monitoring of data traffic and other data content by the pen testers security leaders can fix those areas before bad actors find them.
3. Single Platform or a stage to discuss about the attacks so that it gives awareness about new kind of risks to the industry people or to the domestic user so that Ransomware can be avoided
4. Basic knowledge regarding cyber security is required for both domestic and company users, so that there won't be an attack that means there is an assumption that entry point for an attack is users less knowledge regarding cyber security like phishing, smshing etc. which are under vulnerabilities
5. Not only preventing attack but also if attack taken place successfully then it should be stopped from spreading by following various measures.

IV. RESULT ANALYSIS

Users with knowledge of Ransomware and its evasion techniques the attacks are less compared to the users with no knowledge are less knowledge, here is a graph considered to depict the users with less knowledge and users with good training and knowledge and the attacks on the other side of the graph.

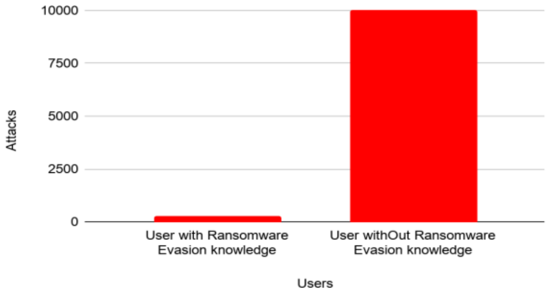

Fig 5: Shows the Result Analysis where

V. CONCLUSION

In this paper Evasion method for Ransomware is considered so that Ransomware is prevented to the maximum extent but the Cyber criminals are growing smart day by day they are with new techniques and with new variants which results in maximum financial loss and even research teams are working on the gap areas of Ransomware, but still could not avoid Ransomware infection to the maximum extent.

REFERENCES

1. EDUARDO BERRUETA1, DANIEL MORATO2, EDUARDO MAGAÑA 1,MIKEL IZAL, “A Survey on Detection Techniques for Cryptographic Ransomware” 2019
2. EST “RANSOMWARE:an enterprise perspective” 2018
3. https://enterprise.comodo.com/Ransomware-attacks.php
4. https://www.carbonite.com/blog/article/2017/08/the-6-stages-of-an-advanced-Ransomware-threat-attack
5. SH Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam “Ransomware, Threat and Detection Techniques: A Review” 2019
6. Mark Loman, Director, Engineering,” How Ransomware Attacks”, Sophos 2019
7. New York State Comptroller THOMAS P. DiNAPOLI “Local Government Management Guide Ransomware”
8. Anna Cartwright 1 and Edward Cartwright “Ransomware and Reputation” 2019

Retrieval Number: E6605018520/2020©BEIESP
DOI:10.35940/ijrte.E6605.018520
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

9. Gavin Hull1, Henna John2 and Budi Arief3* "Ransomware deployment methods and analysis: views from a predictive model and human responses" 2019
10. Samah Alsoghyer and Iman Almomani "Ransomware Detection System for Android Applications"
11. 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
12. 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.

Tanuja G, is with Electronics and communication Engineering department, GITAM University, Bangalore campus. Currently she is Assistant Professor, Her areas of interest are Digital communication, Networking, 5G Technologies. She can be reached at tanuja.g20@gmail.com

Anughna N, is with Electronics and communication Engineering department, GITAM University, Bangalore campus. Currently she is Assistant Professor, Her areas of interest are Digital communication, Networking, 5G Technologies. She can be reached at anughna.7@gmail.com