# Ransomware – A billion dollar virus

## Creation, Operation and Prevention

Pritam Padhye
Computer engineering dept.
Bharti Vidyapeeth College of Engineering
Navi Mumbai, India
Email id: pritampadhye12@gmail.com

Shurti Varade
Computer engineering dept.
Bharti Vidyapeeth College of Engineering
Navi Mumbai, India
Email id: shrutivarade27 @gmail.com

***Abstract* – In the modern world ransomware is extortion through the internet world by hijacking your system or encrypting the storage device. This accepts extortion in the form of cryptocurrency. This is in trend from not more than last few years. This paper discusses about the creation of ransomware, its operation and how it can be prevented.**

***Keywords* – *Ransomware, creation, operations, prevention, working, detection, impact analysis***

## I. INTRODUCTION

Ransomware as its name suggest that it's a combination of two words ransom that is extortion and ware is taken from malware. So basically, ransomware it's a malware that takes the unauthorized access of the victim's system and encrypt the files to make them inaccessible and now the attacker can ask for ransom in exchange of the decrypted of the system. The crytowall 3.0 made over $325 million in 2015 in US alone [1]. we will discuss about how the ransomware is created how it works and the methods we can use to prevent them. The Ransomware is a leading threat to confidential information of the countries which need to be protected. There are many methods to avoid them but very few methods to bypass the ransomware and get our data without paying ransom which will be discussed in this paper.

There are two broadly classified types of ransomware which are crypto ransomware and other is locker ransomware. The crypto ransomware is a high-level ransomware where the data of the victim's system is encrypted using AES (Advanced encryption system) or military grade encryption system. Whereas the other type uses a simple algorithm to lock the system and make it inaccessible to the victim and fetch the money in-return of the operational system [2]. The ransom is also not less in cost it can cost up to as equal as a cost of the car.

The proposed paper's authors are working to find a way on how to remove a low-level ransomware from the victim's system without paying the ransom. The authors are forward in removing a locker type ransomware from the system.

## II. LITRETURE SURVEY

Authors Savita Mohurle and Manisha Patil in their paper A brief study of Wannacry Threat: Ransomware Attack 2017 Volume 8, no. 5, May-June 2017 have stated the impact of the wannacry ransomware in the recent area but haven't touched the topic like how the ransomware works or the technicality of the working or operation which will be discussed in our paper. They also explained the critical nature of ransomware [1].

The conference paper of Automated detection analysis for android ransomware dated 30th November 2016 with authors Tianda Yang, Yu Yang have explained the problems of ransomware with the increase in smartphone and how the ransomware attacks the smartphone. They also made an application to detect the malicious entry into the smartphone. They haven't explained the effects and the working of the ransomware [2].

Authors S. Mahmudha Fasheem, P. kanimozhi, B. Akora Murthy in their paper Detection and Avoidance of Ransomware volume 5, issue 1IJEDR, ISSN: 2321-9939 have explained the working of the ransomware in detail but they haven't mention the ways to prevent the attack and also failed to give an impact analysis of the ransomware attack. Moreover, their paper seems to haven't touch the topics like features [3].

The comparative analysis of various ransomware published in the international journal DOI 10.1007/s114116-008-0092-2 have explained the communication and origins where how the ransomware origination was explained well but have lost focus when it came to working of the ransomware and gave a very good example of AIDS trojan also states scientific approach [4].

As per the News Brief in IEEE Explorer the effect of the ransomware is discussed and how the US and Some European countries took actions against the ransomware and how they made the attack a flop shows but the News Brief didn't discuss anything about the creation or prevention [5].

The authors Nolen Scaife, Henry carter, Patrick Traynor, Kevin R. B. Butler in their paper have studied and implemented the ways to stop a crypto lock type of ransomware on used data and also have stated their work in the field of the same [6].

The authors Ali Shuja Siddiqui, Chin-che Lee and Fareena Saqib of the paper titled Hardware based protection against Malware based access control mechanism have focused on the malware like ransomware and have develop a hardware based protection system to prevent the attack using PUF and access control system. But this paper hasn't explained anything about the working of the ransomware or how victim can prevent the attack using a software [7].

The proposed paper explains about the steps required to create a ransomware and how the ransomware works in reality to ask for ransom. It also states the impact analysis of the ransomware attack on the world. The proposed paper also gives ways to prevent the ransomware and criteria for detection of a malicious ransomware in the system.

## III. CREATION

The ransomware attacks generally through the internet and has different entry points such as bot injection, spam mails, or may be through a backdoor or also known as a breach. The entry from any point has a similar type of effect on the system which would result into inaccessible system or encrypted system depending on the type of ransomware which is used. The below stated figure shows the different entry point of ransomware and their later effect on the victim's system [2].

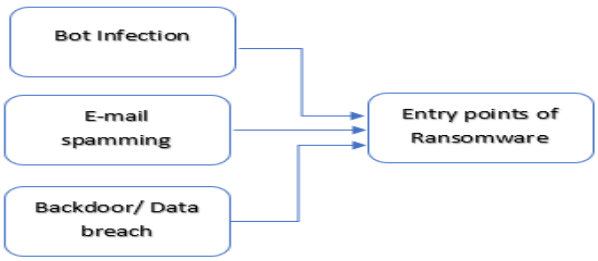


Fig 1: Entry Points of Ransomware

The ransomware is created using some malicious code that can travel through the internet without getting caught and a part of code that can infect the system [3]. There are two main modules in any ransomware one that would help to travel from system to system and another part which will actually infect the system that maybe dependent on type of ransomware. If the ransomware is crypto type then the second module is an encryption code like AES or military grade encryption and if the ransomware is of locker type then code to restrict the use of peripheral components of the system.

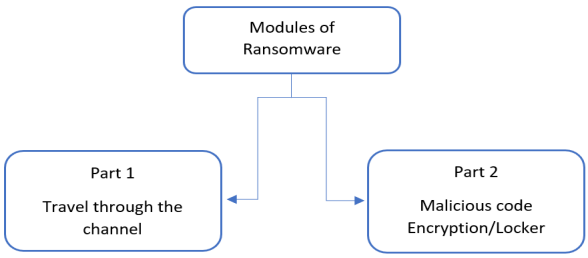


Fig 2: Parts of Ransomware Code

This was the creation part that how a ransomware is created the infection of the ransomware is the part 2 where the actual code of encryption or locking is done to attack the victim's system and ask for ransom.

## IV. WORKING

The ransomware in fact works on the policy of soft destruction which means that the infected system is not damaged it is just made unresponsive and asked for ransom which can turn into destruction if the ransom is not paid or the hacker wants to steal your data deliberately even after paying the ransom.

The general flow of the ransomware is as shown in the fig4.1 as follows. The first step is to infect the system with a malicious program that will either lock the system if it is a locker type ransomware else it will encrypt the files and folders with any of the high-grade encryption system. The next step is to provide the payment details to the user this is either done by changing the wallpaper of the system or by a dialog box that doesn't turn off. After the payment is made the system will be again be restored to the point before the attack [2].

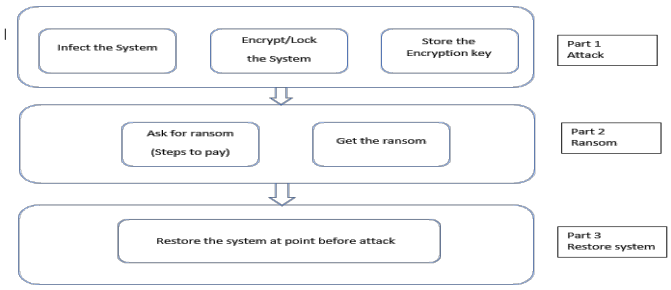


Fig 3: Working Stages of ransomware

### *A. Attack:*

The proposed paper has explained the working and the authors have divided the working into three main parts that is

the first step is attack here the infection of the system with malicious code is achieved. The system is infected from any of the infected of the entry point as discussed above. The next thing that a hacker does is the execution of the code to either lock the system or encrypt the system depending on the type of ransomware. The last thing to be done is to hide the encryption key may it be public or private key at the victim's side or hacker's side.

### *B. Ransom Collection:*

The part 2 of the working is the payment. Here the hacker explains and compels the victim to pay the ransom or else may lose his data. The payment process is explained in a dialog box or maybe by changing the wallpaper of the system. The money asked is generally or many a times 95% is in crypto-currency this means in form of bitcoins.

### *C. Restore*

The part 3 of the working is the restore point where if the ransom is paid the victim gets the encryption key or the hacker himself decrypts the files or unlocks the system to restore the attacked system to the point from where it was before the attack.

The working of ransomware has an executable code which the hacker may send using micro-joiners these joiners put the executable code in a video or audio or a text file which lures the victim open it or the malicious executable is sent deliberately through the network from one system to other. The files are sent through network in distributed type that is files are divided into small parts so as they can travel without a problem. There is a test packet to combine these files again and let them execute on the system.

## V. IMPACT ANALYSIS

### *A. Financial Profit*

The impact of ransomware getting grip on the graph after 2005 nearly from where the ransomware got into trend. The economic impact of the ransomware is just increasing day by day. The profit made by a hacker is calculated by a formula [4]. Which is as follows:

$$\Pi = \sum_i^N (p_i - c)\ li - F$$

Where N is the number of people attacked, $p_i$ is the ransom asked of a person *i*, c is the cost of dealing with any ransom money, $l_i$ is an indicator variable that takes value 1 if pi<= vi and 0 otherwise, F is the fixed cost of operating the malware.

### *B. Financial Losses:*

The impact is ever increasing and is explained pictorially as the below fig5.1 and will keep increasing if it isn't prevented or controlled in near future and would also affect the development in artificial intelligence or Internet of Things. [3] [6].

The fig 4 explains the losses the people have experienced in the course of time form a few years in India. As per statistics $5 million have been extorted from the people and around 2275 cases have been reported by cyber cell for the ransomware cases form march 2014 to march 2015 and is every increasing as the importance of data is increasing. The fig4 also says that major attacks have been taken place due to clicking phishing link or because of mail. There are as many as 230 file types that can be attacked and disrupted [6].

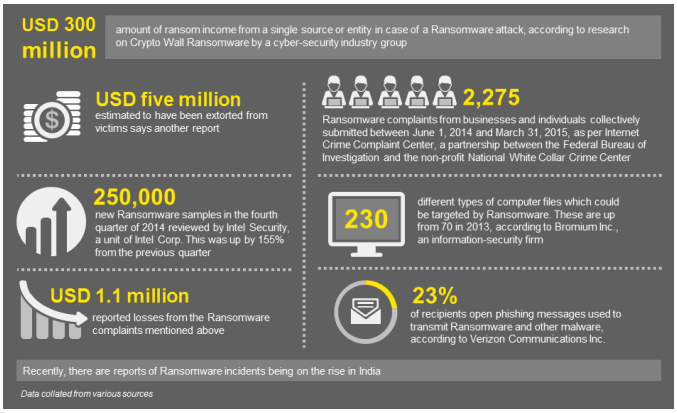


Fig 4: Ransomware Impact analysis

## VI. DETECTION

There are various ways to detect the attack of ransomware in advance to avoid the attack or take the firefighting actions to stop the ransomware. The two main types of detection systems of ransomware are hardware detection and software detection but none provide full proof security to the victim's computer.

### *A. Hardware Detection:*

The best hardware detection system is the computers Universal Extensible Firmware Interface its acts between the operating system and the hardware components One feature it provides against the bootkits is the improved security feature during the boot process but the UEFI is still not used in embedded system domain additionally UEFI can be bypassed using different software systems and exploit the target [7].

### *B. Software Detection:*

We have many third-party software that claim to detect the detection of ransomware the with the help of either the keyword detection or the use of intrusion detection system. But the intrusion detection system need some additional package to act on the ransomware.

## VII. PREVENTION

Prevention is always better than cure as preventing and taking care is rather simple then restoring the system back to normalcy as the data is like the modern-day gold for information technologist. The prevention is done using the following methods these are some of the primitive prevention techniques which will help to help to avoid the attack of ransomware.

### *A. Primitive Preventions*

1) Antivirus should always have a last update [1].
2) Spam messages should not be opened or replied [1].
3) Back up the data. To defeat, regularly updated backup [1].
4) Personalize the anti-spam settings the right way.
5) Apply patches and keep the operating system, antivirus, browsers, Adobe Flash Player, Java, and other software up-to-date [1].
6) Keep the Windows Firewall turned on and properly configured at all times [1].
7) Switch off unused wireless connections, such as Bluetooth or infrared ports [1].
8) Exercise caution before using Wi-Fi network [1].
9) Do not click on harmful links in your email and do not visit unsafe website which you think are vulnerable [1].

### *B. Technical Preventions:*

As explained in the working the ransomware is when transmitted through net there is a test packet that will reassemble the parts of the malicious code so as to execute the if this test packet is detected and denied to enter the system then ransomware fails. All the ransomware detection system acts in same way with keyword matching so as to avoid the test packet or avoid any malicious code to enter the system or cross its firewall. [2].

1) The best way is to provide security at the entry point of the system with proper password selection criteria to stop the malicious hacker to enter the system
2) The next step to prevent the malicious code from entering the organizations network is DMZ hardening
3) Ensure that the logger software send all the logs to the log server and keeps a track of the same.
4) See to it that the regular patch is maintained for the server and the systems that employees work on.
5) Avoid social engineering as long as possible.
6) The users should use two factor authentications where ever possible and note all the changes that take place in the system.
7) VLAN and subnet segmentation should be used to avoid lateral movement of malicious code inside the organizations network.
8) Backup and recovery is the last line of defense in the worst case ever happened so backing up of the data should be done regularly.
9) Home users should keep their operating systems up to date to avoid the attack
10) The system should be scanned at regular intervals of time and checked for any new unknown file extension.

## VIII. REMOVAL

If in any case the ransomware has passed all the security measure and has attacked the system then seeing the importance of the data the decision of paying the ransomware to be taken there are few processes to remove the malicious code from the victim's system they are full recovery of the hard disk or the force full removal of the malicious code from the disk

### *A. Hard-disk Recovery:*

The best option of backing up data is needed to recover the hard disk. The first thing is to format the whole hard disk using some third-party tool and then loading it back to the computer and installing the operating system and then transferring the backed-up data from the external storage disk and the effect of this will be a new looking hard disk without the ransomware.

### *B. Using Linux:*

Everyone knows the security advantages of the Linux operating system over its rivals like windows and mac. The process to remove the ransomware from the infected system is as follows.

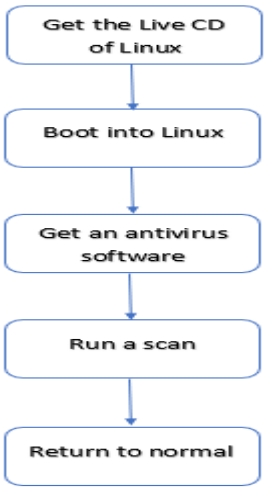


Fig 5: Removal Process using Linux

1) Get a live CD of Kali/Ubuntu Linux and go for using a live CD.

2) Boot into the Linux operating system using the live CD.
3) After booting go to application and install a Linux antivirus like Clam TK or any other Linux antivirus.
4) Run a full scan of the disk and select the drive victim want to scan victim will be able to find the malicious code and can be removed with an option of removal or quarantine.
5) Insuring the removal of malicious file victim can remove the CD and normal boot the computer.
6) The ransomware will be absent now.

This works only on some type of ransomware and authors are researching the same. The proposed steps work fine on locky type of ransomware

## CONCLUSION

The proposed paper focuses on the ransomware as a virus that can hijack a victim's system and disrupt the normal working of the system.

The proposed paper has been focusing on the life cycle of ransomware that is from creation, working, detection and prevention also. The proposed paper has also shown the different entry point for ransomware and how it travels through the network it also states the basic prevention methods, detection criteria and explained briefly about the impact of ransomware on society.

## ACKNOWLEAGEMENT

This paper was possible because of the able guidance of our professor Mrs. Sulakshana Mane and HOD Dr. D.R Ingle so we extend heartfelt acknowledge to our professor and would also like to thanks others who helped us to fulfill this paper. Would also extend our heartfelt acknowledge to our parents for encouraging us.

## REFERENCES

[1]. Savita Mohurle, Manisha Patil volume 8, No. 5, May-June 2017 International journal of advanced research in computer science, A study of Wannacry Threat: Ransomware Attack 2017.
[2]. S. mahmudha Fasheen, P. Kanimozhi, B. Akora Murthy, Volume 5, issue 1, IJDER, Detection and avoidance of Ransomware.
[3]. Alexandre Gazet, 4th july 2008, EICAR, Comparative analysis of various ransomware virii.
[4]. Julio Hernandez-Castro, Edward Cartwright, Anna Spepanova, Economic Analysis of Ransomware.
[5]. Tianda yang, Yu Yang, Kai Qian, 30th November 2015, Automated detection and analysis of android ransomware, High performance computing and communication conference.
[6]. News Brief dated july 2014
[7]. Nolen Scaife, Henry Carter, Patrck Traynor, Kevin R. B. Butler dated 2016 titled CryptoLock (and Drop it) stopping ransomware attacks on user data. 2016 IEEE 36th internation conference on distributed computing system.
[8]. Ali Shuja Siddiqui, Chia-Che Lee, Fareena Saqib tittled Hardware based protection against malware by PUF based access control mechanism.
[9]. Chris Moore dated 20th October 2016 titled – Detecting Ransomware with Honeypot technique
[10]. Aaron zimba, Zhaoshan Wang, Hongsong Chen date 18th august 2017, reasoning Crypto Ransomware Infection Vectors with Bayesian Networks.
[11]. Matiyias Wecksten, Jan Frick, Andreas Ajostrom, Eric Jarpe, dated 11th may 2017, A novel method for recovery from crypto ransomware infections.