



PROFESSIONAL TRAINING REPORT

at

**Sathyabama Institute of Science and Technology
(Deemed to be University)**

Submitted in partial fulfillment of the requirements for the award of Bachelor
of Engineering Degree in Information Technology

By,

**Lakku Snehalatha Reddy
Reg.No:39120115**



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU**

NOVEMBER 2021

SATHYABAMA



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI

CHENNAI- 600119

www.sathyabama.ac.in



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of Lakku Snehalatha Reddy (**Reg. No: 39120115**) who carried out the project entitled "**WannaCry Ransomware attack**" under my supervision from June 2021 to November 2021.

Internal Guide:

Dr.Mary Gladence.L, M.E.,Ph.D.,

Head of the Department

Dr.R SUBHASHINI,M.E.,Ph.D.,

Submitted for Viva voce Examination held on _____

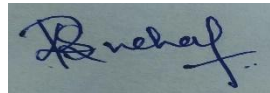
Internal Examiner

External Examiner

DECLARATION

I, **Lakku Snehalatha Reddy** hereby declare that the project report entitled **WannaCry Ransomware attack** done by me under the guidance of **Dr. Mary Gladence.L ,M.E.,Ph.D.**, is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology.

DATE:

A handwritten signature in blue ink, appearing to read 'Snehalatha Reddy', is written on a light blue rectangular background.

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to the Board **of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D**, Dean, School of Computing, **Dr. R. Subhashini, M.E., Ph.D. Head of the Department of Information Technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Mary Gladence.L M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved the way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



CERTIFICATE OF COMPLETION

CSW-I-13-081121 is given to

**LAKKU SNEHALATHA
REDDY**

*For completing the Cyber Security training that includes
basics of Cyber Security, Pentesting, Networking, and
WebApp.*

Aaron V Sandeen

AARON SANDEEN
CEO - CSW

N. Vengatesh

VENGATESH NAGARAJAN
MENTOR



Abstract

Security was a big deal for a long time. With viruses, malware and ransomware are other problems seen by the practitioner. This paper shows the working of ransomware with its evolution and general characteristics of few popular ransomware. In the evolution part, the paper provides a study from first ransomware to current days. The study shows the light on various kinds of infection performed by ransomware including data infection and infected machines. Different attackers made choices to target various attacks; the paper provides a sight on various target types of the ransomware. This paper is trying to demonstrate a few ransomware attacks case studies to show the problem created by various ransomware as an example. After an attack, what a victim should do after infection is also discussed at the end of the paper. How people can save their system and what are the safety measures to save the system from ransomware, are also discussed by the researcher. At the end of the paper, the researcher points out a few steps to save systems and data.

TABLE OF CONTENTS		
CHAPTER	TITLE	PAGE NO
	CERTIFICATE	v
	ABSTRACT	vi
1	INTRODUCTION	01
2	EVOLUTION OF RANSOMWARE	02
	2.1 BEFORE RANSOM AS A SERVICE	02
	2.2 AFTER RANSOM AS A SERVICE	03
3	INFECTION BY RANSOMWARE	04
	3.1 DATA ON INFECTION	04
	3.2 AN INFECTED MACHINE	04
4	TARGETS FOR RANSOMWARE	05
	4.1 USER WISE	05
	4.2 SYSTEM WISE	05
5	SAFETY METHOD	07
6	CONCLUSION	09
	REFERENCES	10
	APPENDIX A: SNAP SHOTS	10

Fig No	Figure Number	Page No.
1	1.1	01
2	2.1.1	02
3	2.2.1	03
4	4.1	06
5	5.1	07

CHAPTER 1

INTRODUCTION

Cybersecurity was always a challenging issue since it arose from computers. It has been increased with the internet improvement of internet facilities. Many kinds of cyberattacks are currently performed by cybercriminals. Apart from the other threat issues, spreading ransomware is an illegal business. It has been in flow for the network since 2005 but for personal computers started from the year 2015[1]. Crypto ransomware is the category of malware that is able to encrypt data of victim machines whereas locker ransomware locks the machine, thus in the second kind user is not able to use their own machine. Both ransoms can be understood just as first one is like a lock that applies on the home of victim's goods by which he can enter the home but cannot use the items of their own whereas the second case is that someone locks gate of home of victim by their unknown lock in this case victim is not able to enter in their own house. Paper represents threats of ransomware in terms of IoT infrastructure. Few famous cases are enlisted here as:

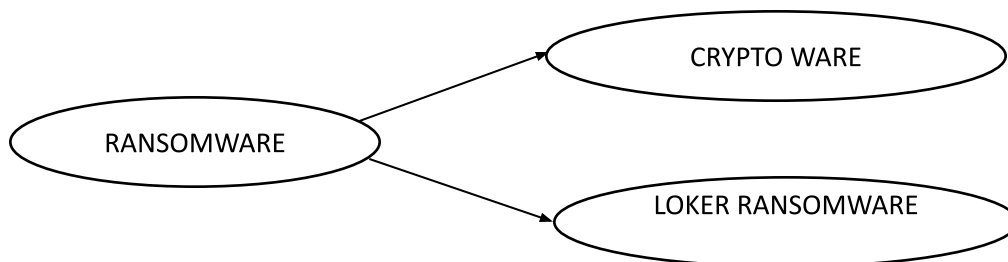


Figure 1.1: Classification and few examples

Attackers have developed a way to monetize files already on a victim's computer. They accomplish this through encrypting select files and then charging for access to the key. This type of malware has spawned a new classification, crypto-ransomware, but is more commonly known by the name of the most prevalent version, CryptoLocker, or its variants TeslaCrypt and Cryptowall.

- **Famous Cases:**

- In August 2016, Bournemouth University was successfully attacked and corrupted files by ransomware 21 times during the previous 12 months.
- In April 2016, A Network Hospital of MedStar Health in Maryland, was attacked and blocked working by the Samsa ransomware.
- In February 2016, Hollywood Presbyterian Medical Center was attacked by Locky ransomware and disrupted working for two weeks until they paid 40 Bitcoin (about \$17,000) to recover its files.

Study of famous cases shows that ransomware attackers target a system of professional bodies. After seeing the importance of the awareness about ransomware the study on ransomware was started. Evolution of ransomware has shown in Chapter II with its division before ransomware as a service and after ransomware as a service. These Chapters indicate basic characteristics of ransomware and indicate a light on new ransomware introduced in 2017. Chapter III, showing various kinds of infections performed by ransomware after an attack. After this, chapter IV classifies various targets for a ransomware attack; it also shows the situation of a machine after an attack. At the end of the paper Chapter V explains the safety measures for ransomware while the paper concludes in Chapter IV.

CHAPTER 2

EVOLUTION OF RANSOMWARE

From 1989 attacks of ransomware were started and got typical to crack with the expansion of type. Ransomware's attack became very common after including it as a service in the form of ransomware-as-a-service. As per Ronny and Max, we have classified evolution in two parts.

2.1 BEFORE RANSOM AS A SERVICE:

A ransomware with the name AIDS Trojan had come into existence in 1989 that was also famous as a PC cyborg. This virus was created by Joseph L. Popp and distributed through a floppy disk.

YEAR NAME	DESCRIPTION
1989, AIDS Trojan (PC cyborg)	♣ Symmetric cryptography based ♣ Distributed at WHO international AIDS conference by floppy drive
2005, Trojan.Gpccoder	♣ Custom symmetric cryptography ♣ Via spam email to claim a job application.
2006, Trojan.Cryzip	♣ Deleted files. ♣ Create password protected file after duplicity.
2006, Trojan.Archives	♣ like Trojan.Cryzip ♣ Demanded order id of purchase medication of specific pharmacy for password.
Starting of Locker ransomware, 2007	
2008, GPcode.AK	♣ 1024-bit RSA key ♣ asked for payment of \$100 to \$200
2012, Lyposit	♣ Opened as pop-up to say machine involved in illegal activity ♣ Shows locked by the FBI/ Judiciary
Trojan.Randso.C	♣ Displayed self as a Windows Security Centre message. ♣ Asked to reactivate their Windows license.
2013 CryptoLocker	♣ encrypted about 67 file types, including MS Office data files. ♣ provide thee day to pay. ♣ if not paid within the time limit than demands higher to retrieve files.
December,2013 CryptoLocker 2.0	♣ written in a different language than CryptoLocker. ♣ As per Symantec, the number of attacks grew from 100,000 in January to 600,000 in December. ♣ They estimated that 3% percent of infected users paid ransom.
2014	♣ Two vendors, FireEye and Fox-IT, found the database of decryption keys and released CryptoDefense.
2015, CryptoWall	♣ CryptoWall passed Cryptolocker as the leading version of ransomware.

Table 2.1.1: Evolution of ransomware before Ransomware-as- a-service Year

The year 2011 was very tough for internet users because of the attack by bulk ransomware. In this year more than 30,000 samples were found in two starting quarters while 60000 ransomware samples attacked in the third. The year 2015 was found as a golden year for ransomware criminals. In this year a new kind of cryptolocker was introduced while a TOR website started using ransomware as a service. This website provided ransomware on the commission of 20%.

2.2 AFTER RANSOM AS A SERVICE:

After providing ransomware on rent or commission, a frequency of ransomware attack has been increased, that is why researchers classify the evolution into two parts as before and as after ransomware.

YEAR NAME	DESCRIPTION
May 2015, ransomware-as-a service	♣ Using a TOR website, attackers could create ransomware for free. ♣ The site handles payment and takes a 20 percent cut of the ransom.
2015, Tor sites	♣ As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications.
September, 2015,LockerPin	♣ It infects Android systems and changes the PIN.
Nov,2015 Linus.Encoder.1	♣ In was discovered by Dr.Web, a Russian computer security firm.
November, fourth iteration of CryptoWall	♣ It includes a modified protocol to help avoid detection. ♣ Additionally, it alters the file names when it encrypts files, making it harder to determine what files were actually encrypted.
January, 2016. JavaScript-only	♣ It is a ransomware-as-a-service. ♣ multi-platform attack, including Linus and MacOS X.
April, Petya	♣ Makes the whole hard disk inaccessible until the ransom is paid. ♣ It does this by overwriting the master boot record (MBR) of the infected computer. ♣ Without the MBR, the operating system cannot reconstruct the unencrypted files.
KeRanger, Jan, 2016	♣ KeRanger is the first ransomware attack targeting the Apple system. ♣ It takes three days to activate and is designed to encrypt more than 300 file types
Xbot, feb 2016	♣ To target Android devices in Australia and Russia. ♣ Tries to steal online banking details.
Jigsaw, 2016	♣ Embeds an image of the clown from the Saw movies into a spam email. ransom payment of \$150, according to Webroot
Locky, July 2016	♣ added a failsfe mechanism that begins encrypting files even if the ransomware cannot request a unique encryption key from the criminals' servers due to the target computer either being offline or blocking the communications (Constantin, 2016c).
NotPetya, 2017	♣ It comes with a fake software update, harms systems of more than 100 countries
Jeff, 2017	♣ It attacked in May 2017 with spam mail and collected money in form of bitcoin

Table 2.2.1: Evolution of ransomware after Ransom-as-a-service

CHAPTER 3

INFECTION BY RANSOMWARE

Once infected, a user has four options:

- Pay the ransom
- Restore from backup
- Lose the files
- Brute force the key

To brute force, the key would require factoring 617-digit numbers, which would take about 6.4 quadrillion years on a standard desktop computer.

3.1 Data on Infection

Symantec uses telemetry data to track ransomware infections by country. The rankings are shown in table 1 below. For the most part, criminals are targeting large or affluent countries.

In the initial days ransomware was attacked on Windows platform but in these days, it is able to infect Apple and Android systems, even few are also in the air to infect Smart watches that come into the category of IoT devices. Now ransomware is moving to IoT, as services are moving from the Internet to the world. From 2016, SVG (scalable vector graphics) is a new method of a cyberattack. SVG files are a file that allows system code, such as JavaScript, to be embedded in the graphic. This code can be run through a browser. Few codes and techniques also in the air to decrypt the files of the victim such as Popcorn Time allows a free decryption to files of victims if infected.

3.2 An Infected Machine

Dealing with ransomware is a costly job even if it is backed up and not going to pay; because correction of a system can take days to weeks. So, after infection, a machine has limited options to operate. Ransomware does not destroy data. Rather, it locks up the data until a ransom is paid. Antivirus company AVG recommends the following steps:

Step 1: Run a full scan to find out the ransomware used.

Step 2: Copy the encrypted files to a USB drive so they can be decrypted on an uninfected computer.

Step 3: Use a tool to decrypt the files on the USB drive. AVG provides free tools for decrypting six Ransomware strains: Apocalypse, BadBlock, Crypt888, Legion, SZFLocker, and TeslaCrypt.

When files are recovered ok in any way ransomware must be removed.

CHAPTER 4

TARGETS FOR RANSOMWARE

4.1 User wise:

The Average User:

All age groups are considered as a target to get ransom, but its people who are not a technical person pressurize easily. Attackers sometimes increase pressure by including a timer with the increment ransom amount. A solution of ransomware like TeslaCrypt is coming in the form of TeslaDecoder but if people do not use it with the decoding of the encrypted file, then ransomware can do their job even if it is easily decodable. Individual users are targeted because they pay ransom due to the fear of corrupted files and not having a backup for valuable data. On the other hand, organizational members due to business secrecy sometimes pay due to not having cybersecurity personnel. As per Symantec 25% home users do not have a backup, 55 % backup some files and only 25 % have regular backups in a week. The rest only made backups sometimes.

Businesses:

Businesses are on priority for ransomware because their systems are the house of valuable databases with sensitive data, important documents, and other information; in the meantime, they have the general system updated and tried to secure it. Crypto ransomware focuses on targeting the corporate network or individual systems to be spread in the whole network.

Emergency Services:

Ransomware targets these organizations also due to Multi-State Information Sharing and its importance by which it can pay the cost of delay in terms of lives. Most vulnerable emergency services are law enforcement, fire departments, and hospital chains. On the other hand, the healthcare sector is not a traditional target for a few years; these were also targeted, including the example of Hollywood Presbyterian Hospital Medical Center which was infected with the Locky. ransomware.

Financial Institutions: The banking and finance sector is the frequent target of ransomware schemes including botnet like problems. Dyre, Dridex, and Ramnit are botnets included especially for the banking sectors. Educational Institutions and religious organizations are also the favorite target of ransomware criminals due to these having all the costly data with least security mechanism.

4.2 System wise:

All kind of system is valuable to the user and also might be a target for ransomware due to the profitability target system including:

Personal computers (PC): PCs are the current primary target of ransomware due to easy compromise.

These systems generally used un-updated OS and software. Ransomware variants are designed to target various OS but windows systems are soft targets generally.

Mobile devices: Ransomware currently active in the air for smartphones also.

Servers: An organization's servers and databases store all of their critical information. Within a server are an organization's documents, databases, intellectual property, personnel files, client list, and other intangible resources. The compromise of one essential server can hobble an organization. Despite their value, organizations regularly fail to secure, update, and patch the systems. This makes servers susceptible to lateral movement and attack. When a server is compromised, the organization goes into a panic. Even if the attack is a ransomware attack, there is a concern for reputational harm due to the perception of lost customer data.

Even if the organization has a business continuity plan or disaster recovery plan, the amount of time necessary to revert to a redundancy system may be unacceptable.

PAYMENT METHODS:

Bitcoins are the first choice for criminals but in general we can say digital payment mechanism is the choice of criminals.

Bitcoins:

Bitcoin is a kind of cryptocurrency that can be assumed as an electronic coin. It allows people to transfer digital payment from one end to another. It is an easy system of payment due to not involving any financial institution in the process for any kind of activity as a mediator. To find out a payment a ransomware instructs to victims as:



Fig.4.1.Ransomware attack

CHAPTER 5

SAFETY METHOD

Mobile phones are also found to be attacked by ransomware as other machines, while data recovery from a ransomware affected system can be done by a forensic tool as described by PH Rughani [9], who tested the practical over android phone and found better success rate on SD card than phone.

To deal with ransomware experts given few suggestions to use before and after infection as:

Step 1: Back Up

Step 2: Avoid all spam links if unknown. Use Ad blockers can protect against malvertising. Turning off Java and JavaScript.

Step 3: Patch and Block All the OS, browsers, and security systems should always be kept patched and up-to-date including third-party plug-ins, like Java and Flash.

Step 4: Drop-and-Roll If a machine found the sign of infection, then to minimize the infection infected machine should immediately turn off, the network also should be turned off if this machine is on the network. On the basis of case studies, to deal with ransomware, few suggestions are as:

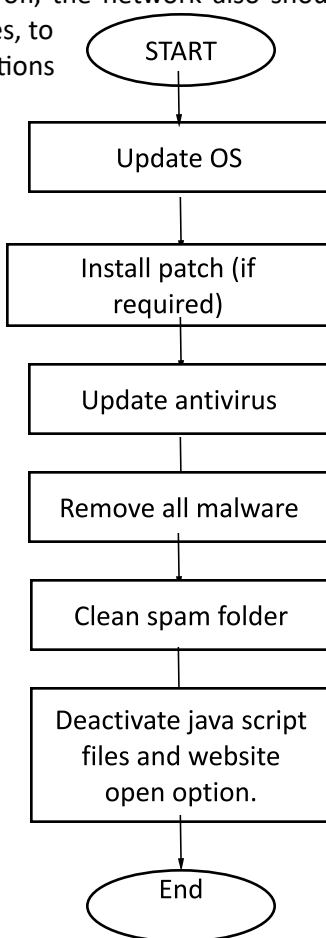


Fig.5.1

1. To save a system from ransomware attack is the first step to update the operating system, sometimes it requires the patches thus installation of patches is the next step.
2. Do not use an Operating System that is not supported.
3. Tasks of step 1 are meaningless if the system does not have any updated antivirus, so it is a suggestion that the system must have a good quality antivirus.
4. Cleaning of spam folders must be the next step after a removal of all malware/spyware.
5. JavaScript files and website open option is risky so deactivate it at the end of all precautions.

CHAPTER 6

CONCLUSION

- WannaCry is undoubtedly one of the most destructive malware ever used by cyberattacks. The first malicious campaign utilizing this dangerous virus had a truly unprecedented scale.
- Due to Cybersecurity professionals, the attack was contained in just a few days by finding an effective kill switch and patching the vulnerability in the Microsoft operating systems that the ransomware was targeting. However, even despite such quick reaction times made by cybersecurity professionals all around the world, billions of dollars were lost by victims all across the world.
- To prevent devastating cyber attacks such as the one performed using the WCry virus, researchers should learn as much as possible about the existing malware samples and analyze their code. This task is greatly simplified with the use of interactive sandboxes like [ANY.RUN](#), which allows users to influence the simulation in real-time in order to get the best results.

REFERENCES:

- [1]. R. Richardson and M. Nort, "Ransomware: Evolution, Mitigation and Prevention", International Management Review, Vol. 13, No. 1 2017.
- [2]. An Osterman Research, "Best Practices for Dealing With Phishing and Ransomware SPON", White Paper Published September 2016.
- [3]. C.Beek and A. Furtak, "Targeted ransomware No Longer a Future Threat: Analysis of a targeted and manual ransomware campaign", Advanced Threat Research, Intel security, feb2016.
- [4]. J. Wyke and A. Ajjan, "The Current State of Ransomware", A SophosLabs technical paper December 2015.
- [5]. WannaCry Response, Metasys, Johnson Control, June 2017.
- [6]. WannaCry Ransomware Analysis, White paper, May 2017, Stream scan.
- [7]. B. N. Giri, N. Jyoti, Mc. A. AVERT, AVAR 2006, Auckland.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.5881&rep=rep1&type=pdf>
- [8]. P. Bihola, R. Sheth, "Emerging Threats of 2017: Ransomware, IOC's", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2 | Issue 6, pp.-996-1003.
- [9]. P.H. Rughani, Data recovery from ransomware affected android phone using forensic tools, vo.-5, issue-8, International Journal of Computer science and Engineering, pp. 67-70

APPENDIX A: SNAP SHOTS

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy