iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.39758

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: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

Ransomware Attacks in History of Cyber World

Fizza Zafri
Department of Forensic Science, Chandigarh University, Chandigarh, Punjab, INDIA

Abstract: ***Technology advancement since last few decades creates cyber attack a critical issue. Cyber security has become an important part today. It has also become an important and crucial subject in the field of forensic science. Increased in the growth of internet technology and internet devices have increased the risk of cyber attack. Almost every organization today are depends on the internet and devices. There are many types of cyber attack. This paper is the detailed review about Ransomware attack. This paper is consisted about vast of the information about What is Ransomware Attack, how does it work, how ransomware attack emerged. After reading this paper you will learn about the ransomware attacks in history of cyber world. This will help you to learn and understand about ransomware attack, how to prevent yourself from ransomware attack. As a forensic science student, it is always important to be aware about the attacks that have happened in the history of cyber world. Before writing this paper, I have read and analyze many research paper and internet articles, so that I can write a detailed review paper which can help students and for the forensic awareness.***

Keywords: Cyberattack, Hacking, Ransomware, cyberworld, cyber security, ransomware, forensic, network security

I. INTRODUCTION

A. What is Malware?

Any Software which is developed by the hacker to damage, destroy or block the data is known as malware. These software's are consist of scripts which are written using programming languages. Some commonly known malwares are viruses, spyware, adware, Ransomware, fileless malware.

B. What is Ransomware?

Ransome is a malware software which is used to retrieve sensitive data from a system. Using this malware practice all the storage, files and even the device is encrypted. This can only be solve using the decryption. In such cases hacker demands to pay some amount in the exchange of decryption key. The first case of ransomware was introduced in 1989, today ransomware have several varieties. Ransomware varieties are increasing rapidly, which has advanced capability of spreading. Latest ransomware has advanced spreading and development technique. They can develop themselves using crypters and apply reverse engineering which make it very complicated to understanding and decrypt. Now a days, the use of offline encryption has increased, which make ransomware one of the most dangerous malwares and a serious concern for the business and online system. Those attack are advanced and more complicated and becoming more challenging day by day.

II. HOW RANSOMWARE ATTACK WORKS

Ransomware is nothing but a program, which is need to inject to a device. The main purpose of ransomware is to block the system access from the admin or the owner of that system. The name "Ransomware" itself define its agenda. This attack is used to stop a business from financial gain. These Ransomware programs are injected using email, fake website or using pendrive or other external devices. That virus software shares biological illness which harm the device and gain access of entry points which is termed as "vectors".

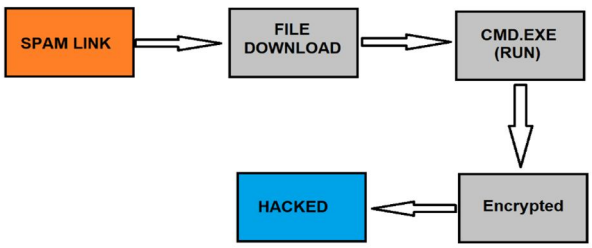


Figure 1:- Diagram show how Ransomware works

Some examples of Ransomware vectors are mentioned below.

1) *Email Attachments:* Sending ransomware using an email is a common method. If you check your spam/junk folder there are plenty of junk emails. Email which asks you to click on link or want some details. If you click on those links, it may be the entry point of Ransomware.

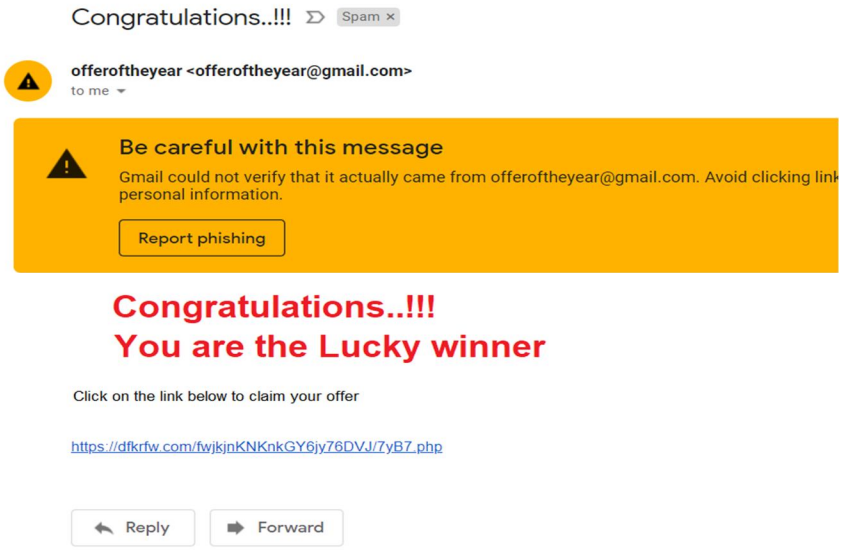


Figure 2:- An example of spam link shared on E-mail for the Ransomware Attack

2) *Messages:* Yes, you see it right, injecting ransomware in your system is that easy. The codes can be share in your message inbox. Even using facebook messager. The attacker create account with some random name or with the name of 'friends. Using that account the attacker will share that malware program.
3) *Pop-ups:* These days pop-ups are used to show advertisement. But very few know those pop-ups are used in most of the hacking practice. Because it was a creative practice to share forcefully any data.
4) *By Downloading File from Unknown Source:* If you search for free movie download or song download, you can see thousands of website. By downloading unknown file or file from unknown source you can welcome ransomware in your system.

III. EVOLUTION OF RANSOMWARE ATTACK

1) *1989:* The first ransomware attack happens in 1989 which is the famous attack of the cyber world known as "AIDS Trojan". This attack was done by Joseph Popp who was a PhD researcher on AIDS. He distributed 20,000 floppy disks to other AIDS researchers all around the world. He tell them that the disk contains a program that analyze the risk of AIDS on human being. But the disk also has his created malware program which will only activate after power on the computer 90 times.

Figure 3:- One of the disk used in AIDS Trojan attack(first Ransomware attack).

After 90 times turning on the system the program run automatically and display a message "user's license to use a certain piece of software had expired" and ask to pay an amount of $189 to an account register with the name of PC CYBORG CORPORATION. Later Popp was declared mentally unfit, and he promised to donate the amount in AIDS research fund. However, It was not required to pay because in this attack only file name was encrypted. This was the first register case of ransomware attack in the cyber world. After this the ransomware attack highlighted.

2) *1996:* In 1996 another ransomware attack was introduced. This time the attacker used RSA (Rivest-Shamir-Adleman) and TSA (Tiny Encryption Algorithm) which encrypt the victim's data. This virus contains the encrypted key which block the access of files and the required decrypted key (which decrypt the virus and allow all access to the user) was keep private to the user. Such type of attacks were commonly used in cyber world till the mid-2000s, where new different variant was used for the attack based on the same scenario.
3) *2010:* In august 2010, a non-encrypting ransomware was found, when Russia arrested few people who build a ransomware trojan "Winlock". This ransomware doesn't have any decryption code. User need to pay around $10 to receive a SMS code that is need to enter to unlock the system. This non-encrypting ransomware hit thousand of people across Russia and many other countries. According to a report earning of this group was around $16 million. In 2011 a similar case was reported where hacker asks for 6-digit code to unlock the system.
4) *2013:* In 2013 a new evolution gets started, where a 21-year-old man was a victim from Virginia. The victim was blackmailed by showing him his private communication. This is the time when first ransomware case where they use FBI logo was introduced. This virus was known as FBI MoneyPak Ransomware. FBI published an advice to not to pay the money and it was not from official FBI. Some other attackers are using their logo and asking people for money.

Figure 4:- FBI logo used in ransomware

A. Mobile Ransomware

With the increase in the number of devices platform get increased. Today the number of smartphone devices are increasing very rapidly, and thus mobile ransomware get introduced. Mobile ransomware is a type of ransomware used to block the access or forcefully do a task using mobile phone. This mobile ransomware is majorly used to target Android smartphones. With the evolution of mobile and technology ransomware is getting advanced. It is always recommended not to download APK file for android from unknown source. Because such files are used to target ransomware attacks. There are many application reported which are installed from third party source and they try to block their SMS, notification and sometimes even lock the device. Here a new term introduced which is "Clickjacking". In clickjacking it forcefully asks for all the device administrator permission even gallery, camera and microphone. Not only this happens with android smartphone but also for iOS. As per a report Apple detect a serious bug on iOS 10.3 that was explored by many ransomware activity. In today's world ransomware are targeting IoT devices (Internet of Things) and DSLR. Digital cameras like DSLR use PTP (Picture Transfer Protocol). In research it was found that this protocol was also hit by Ransomware attack.

Some famous Ransomware Attacks which occur in recent years are as follows

1) Atlanta cyber attack (2018)
2) Baltimore ransomware attack (2019)
3) Luas cyberattack, Ireland (2021)
4) Health Service Executive cyberattack (2021)
5) Colonial pipeline cyberattacks (2021)
6) JDBS cyberattack (2021)
7) Steamship authority cyberattack (2021)
8) Kaseya VSA ransomware attack (2021)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

IV. NEW RANSOMWARE THREATS

To protect yourself from ransomware it was always recommend to change your codes and update your system. Developer keep developing new solution to protect you. But in my research I have found few new ransomware threats which I am sharing here for your awareness.

1) *DLL side Loading:* In this thread malware script and software hide itself from getting detected.
2) *Web Servers as Targets:* If you are using a shared hosting for your important files, than it can be dangerous because if that specific hosting server get affected you will also be the victim.
3) *Spear-phishing is Preferred over Standard Phishing:* Attackers try to target a potential system but not to a large target audience.
4) *Raas (Ransomware as a Service):* With the introduction of RaaS ransomware attack have increased rapidy.

V. THE BUSINESS IMPACT FROM RANSOMWARE

Today most of the business are depend on data. If we take example of hospital management, banks, airlines and any big organization. These are totally depended on Internet network and a server to store data. If these businesses get effected by ransomware attack, it can not even imagine how much loss these big corporation have and people have. Attack majorly tries to attack those business from where they get revenue or they can break a business. In the history of ransomware attack, it can be seen clearly that the attack happens for the revenue or for personal benefit.

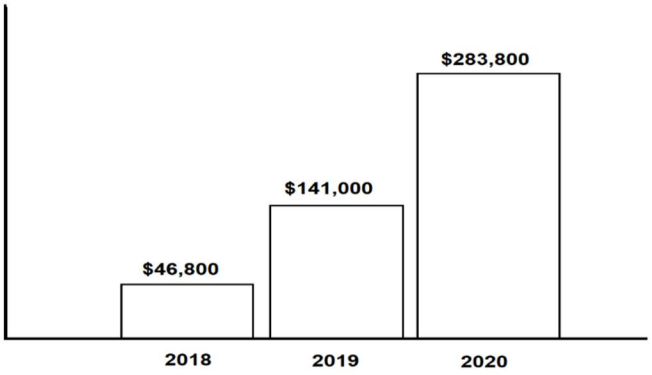


Figure 5:- The Average cost of Ransomware caused downtime per incident

Ransomware can stop a productivity, reduce efficiency, it is always important to be aware about cyber-attack and especially for ransomware.

VI. FUTURE OF RANSOMWARE

As looking in the history of ransomware, it can be clearly found. After every attack ransomware become more dangerous. While some victims have broke attackers plan, this is because of their awareness about this attack. Below I have mentioned few points on how to prevent ransomware attacks.

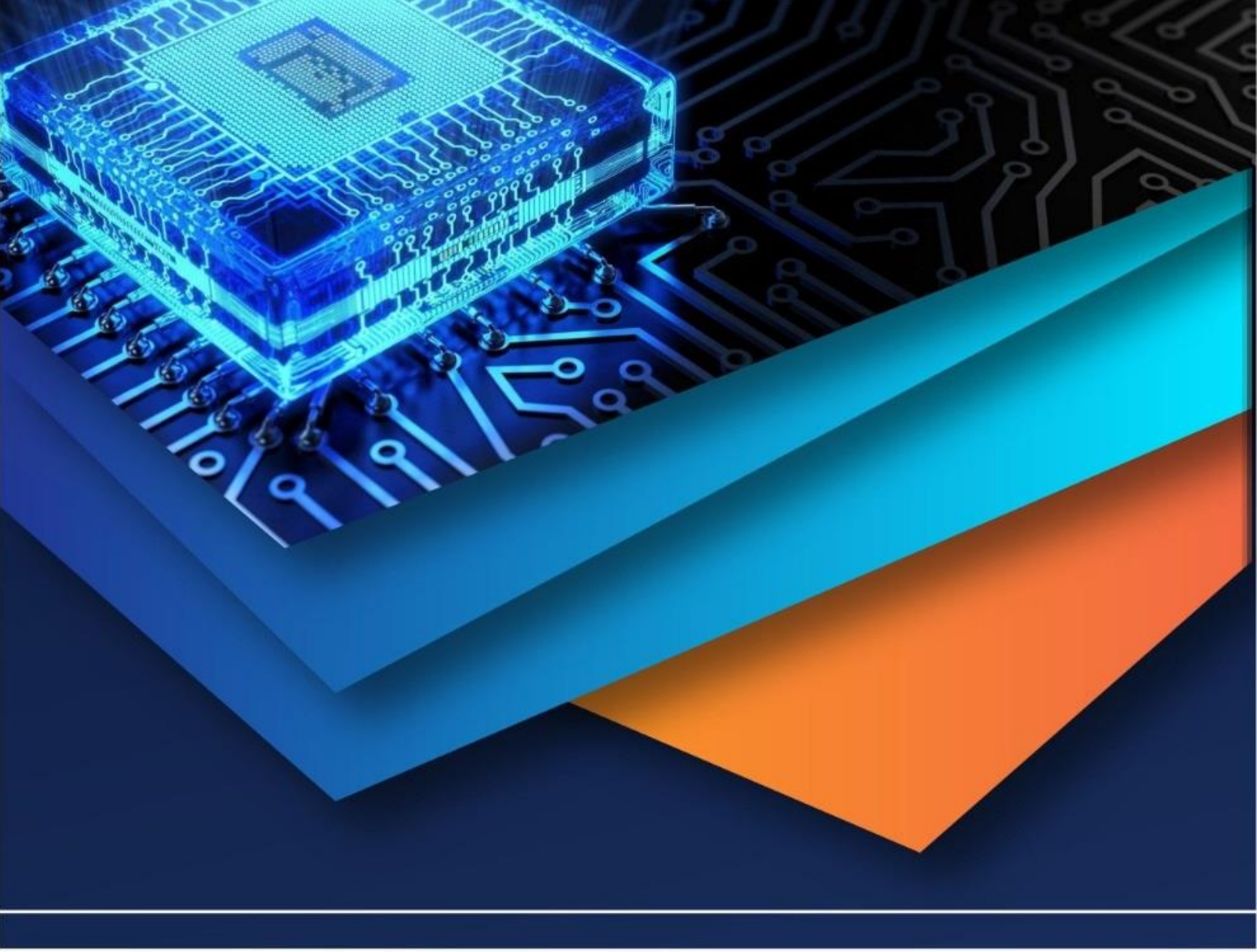
A. Use Antivirus in your system to protect yourself from ransomware attacks.
B. Keep your system update, so that all bug will get automatically fixed.
C. Do not download apps from unknown source or do not click on spam links.
D. Never share your information on unknown website source
E. Backup your data not only on same system but on a different system.
F. Apply application whitelisting and greylisting

VII. CONCLUSION

It can be clearly stated that no cybercrime occurs without a loophole. It you keep yourself with latest updates and aware yourself about the network and security you can protect yourself. From the first case to latest case the ransomware was injected into a system using an unknown source. Before writing this paper, I have analyzed and study many research papers, internet articles and take expert advice. It is always important to know your work and motive this will keep you protect and your device. Never forget to backup your data, if you become a ransomware victim than you can backup your files and defeat the attack this was the best solution in such cases. Always keep update your device, software.

REFERENCES

[1] A study on Ransomware and its Effect on India and Rest of the world – Naveen Kumar C.G, Dr, Sanjay Pande M.B (IJERT)
[2] Ransomware Threats – Nagarajan Seshadri (IJERT)
[3] Ransomware Evolution, Target and safety measures 2018 – researchgate.net
[4] A history of Ransomware Attacks – Digitalguardian.com
[5] Ransomware, List of cyberattacks – en.wikepedia.org
[6] What is Ransomware – Proofpoint.com
[7] What is Malware – cisco.com
[8] Ransomware: A Research and a personal case study of dealing with this nasty malware – Azad Ali (IISIT.org)
[9] Ransomware Evolution, Target and Safety Measures – Researchgate.net
[10] An empirical study of ransomware attacks on organizations by Lena Yuryna Connolly, David S Wall, Michael Lang, Bruce Oddson – academic.oup.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY