ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A brief study of Wannacry Threat: Ransomware Attack 2017

Savita Mohurle
Department of Computer Science
MITACSC, Alandi,
Pune, India.

Manisha Patil
Department of Computer Science
MITACSC, Alandi,
Pune, India.

***Abstract*:** Recently Ransomware virus software spread like a cyclone winds. A cyclone wind creates atmospheric instability; likewise ransomware creates computer data instability. Every user is moving towards digitization. User keep data secure in his or her computer. But what if data is hijacked. A ransomware is one of the software virus that hijack users data. A ransomware may lock the system in a way which is not for a knowledgeable person to reverse.It not only targets home computersbut business also gets affected. It encrypts data in such a way that normal person can no longer decrypt. A person has to pay ransom to decrypt it. But it does not generate that files will be released. This paper gives a brief study of WannaCry ransomware, its effect on computer world and its preventive measures to control ransomware on computer system.

***Keywords*:** Ransomware, Wannacry, encrypt, decrypt, preventive measures, threat, security.

1. INTRODUCTION

In the world of digitization, where every information is stored digitally, information can be accessed 24X7,can be accessed via internet and easily retrieved at cheaper rate. Everything is done smoothly on one click, effortlessly and efficiently maintained. Digitization has improve the life style of the computer users. But as it is said "Every pillar has two sides". Digitization has helped in decreasing crime if applied on whole, getting things done easily and has decrease documentation work. But still it creates a problem of security for personal and confidential information of an individual. Many thefts or cyber-attacks like spyware, malware, Trojan, phishing, intruders, spam, virus occurs. Ransomware is also a theft. It is a kind of infection that if transmitted, it's difficult to get out. It infects all essential data and file in user's computer system. If ransomware get activated in user's system, it encrypts file like .doc,.xls,.mp3, etc. by the public key –private key combination. A ransom is demanded pay ransom for your data and then only you will get those files. It becomes difficult to detect that the data or files has been hijacked. At that time user has only 2 options that is Pay ransom to them but it does not guarantee that we will get our file back (in decrypted format) or Format the PC and disconnect the Internet. Fig. 1.1 Ransom Attack below shows how a user computer has been locked and a user is paying ransom for his data.

Fig. 1.1 Ransom Attack

WannaCry Ransomware Attack 2017 was the worst attack that ever had before. WannaCry Ransomware is a type of malicious software that blocks user access to files or systems, holding files or entire devices hostage using encryption until the victim pays a ransom in exchange for a decryption key, which allows the user to access the files or systems encrypted by the program.It may be difficult to imagine. The first ransomware in history emerged in 1989 (that's 27 years ago). It was called **the** AIDS Trojan but, seems rudimentary nowadays. It spread via floppy disks and involved sending $189 to a post office box in Panama to pay the ransom[9].There are many types of ransomware like Reveton, CryptoLocker, CryptoLocker.F and TorrentLocker, CryptoWall, CryptoTear, Fusob and WannaCry. Ransomware Wannacry attacked many hospitals, companies, universities and government organization across at least 150 universities, havingmore than 2, 00,000 victims. It locked all computers and demanded ransom.

2. RECENT REVIEW

Many researchers by their research and research papers have published the analysis, discussions, investigations and several measures to prevent from cyber threats are being introduced by the researchers. Many automated approach is also being introduced. In 2016, Hiran V. Nath and Babu M. Mehtre in "Static Malware Analysis Using Machine Learning Methods",hascompared various machine-learning techniques used for malwares, focusing on statistical analysis [1]. Again in 2016,MattiasWeckstén, Jan Frick,Andreas Sjöström, Eric Järpe "A novel method for recovery from Crypto Ransomware infections", has analyzed the four most common Crypto Ransomwares. They identified that all infections rely on tools available on the target system to be able to prevent a simple recovery after the attack has been detected. By renaming the system tool that handles shadow copies it is possible to recover from infections from all four of the most common Crypto Ransomwares. The solution is packaged in a single, easy to use script[4]. In 2016, Pathak, P B. "Malware a Growing

Cybercrime Threat: Understanding and Combating Malvertising Attacks", has covered the essential discussion of Malware, Malvertising and the attack methods used to distribute malicious advertisements and enlists several measures to combat the problem[5]. In 2015,Amin Kharraz, William Robertson,Davide Balzarotti, Leyla Bilge and Engin Kirda in "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", has presented HELDROID, a fast, efficient and fully automated approach that recognizes known and unknown scareware and ransomware samples from goodware. It is based on detecting the "building blocks" that are typically needed to implement a mobile ransomware application [2].

3. MATERIAL

a. **Effect of Ransomware Attack 2017 :**Encrypting ransomware works by obscuring the contents of user files, through the use of strong encryption algorithms. Victims have no other alternative, than paying the attacker to reverse this process.Wannacry Ransomware attack 2017 was one of the largest attacks that were ever carried out.It grabbedthe world by storm. According to eScan antivirus reports 2017; India was one of the worst affected by cyber-attack. Interestingly, Madhya Pradesh was the worst affected region in the country with around 32.63% of total ransomware attacks detected within country followed by Maharashtra at 18.84% and Delhi at third position with 8.76% share. Companies like FedEx, Nissan, railway companies in Germany, Russian Railways, Interior ministry, telecommunication company like megaforTelefonica in spain, At least 16 NHS organisation in UK were badly effected. Some systems were caught by malware.Lot of colleges and students computer were hit by attack in china.

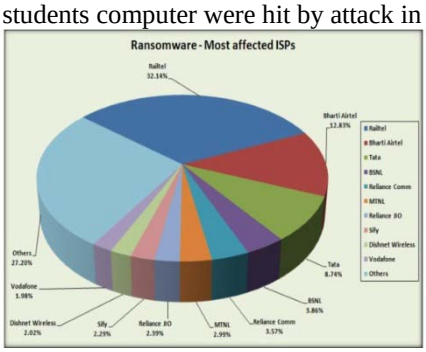

Fig.3.1 Ransomware affected ISP's

Fig. 3.1 above shows that companies like RailTel to Vodafone who are the well-known ISP's were affected the most.

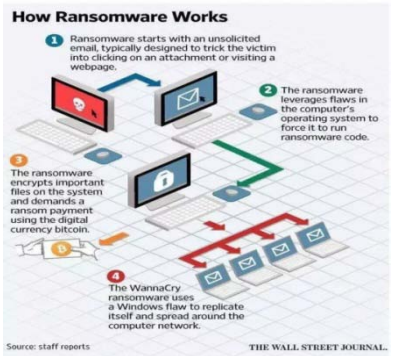

Fig.3.2. Working of Ransomware[9].

Fig. 3.2.above shows working of Ramsomware WannaCry Attack. WannaCry locks all the data on a computer system of user and leaves only two files for user instructing, what user should do next and decrypt program. Hackers demand payment in bitcoin. Otherwise gives warning that file will be deleted.ransomware overwrites the contents of the original file by opening the file, reading its contents, writing the encrypted contents in-place, then closing the file[6].

b. Preventive Measures: Prevention is essential in keeping computer safe. Its a recommendation for users to keep their operating system and software updated. Make use of multilayers protection security solutions that is reliable. Back up all important and valuable data offline regularly.
Ransomware can be sent through various sources like Emails, Advertisement, by creating websites and many more things that can share the ransomware to the computer users. Ransomware restricts the use of the system in various ways after intruding the system. It is mainly classified into the following three types: Scareware, Lock-Screen, and Encrypting [8][9]. WannaCryransomware virus attacked the whole world and no one knows how to decrypt these files. Ransomware is a type of Malicious software designed to block access to computer system until some of money is paid. Following are some of the preventive measure to avoid ransomware:

- Antivirus should always have a last update.
- Spam messages should not be opened or replied.
- Back up the data. To defeat, regularly updated backup
- Personalize the anti-spam settings the right way.
- Apply patches and keep the operating system, antivirus, browsers, Adobe Flash Player, Java, and other software up-to-date.
- Keep the Windows Firewall turned on and properly configured at all times.
- Enhance the security of your Microsoft Office components (Word, Excel, PowerPoint, Access, etc.).
- Think of disabling remote services.
- . Filter EXEs in email.
- Use a reputable security suite.
- Use System Restore to get back to a known-clean state.
- Use System Restore to get back to a known-clean state.
- Sure to disable file sharing.
- Switch off unused wireless connections, such as Bluetooth or infrared ports.
- Exercise caution before using Wi-Fi network.
- Do not click on harmful links in your email.
- Do not visit unsafe and unreliable websites.
- Rather than clicking any web links, type out web address on address bar.
  A novel practise to protect against ransomware attack is to back all files completely on another system frequently to avoid loss of data.

4. CONCLUSION

The purpose of study in this paper is to analyze and to make aware of what is ransomware, its effect and some of the preventives measures. We come to the conclusion that WannaCry Ransomware Attack 2017 wars the most terrific attack. The most important source of ransomware virus via phishing emails andvisiting a website that contains a

malicious program. So, it's essential for computer users to keep back of data regularly.

5. REFERENCES

[1]. Hiran V. Nath and Babu M. Mehtre, "Static Malware Analysis Using Machine Learning Methods",International Conference on Security in Computer Networks and Distributed Systems, 2014.

[2]. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. , "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks"". In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, vol 9148. Springer, Cham, 2015.

[3]. Nikolai Hampton, Zubair A. Baig, "Ransomware: Emergence of the cyber-extortion menace",The Proceedings of [the] 13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia.

.[4]. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, "A novel method for recovery from Crypto Ransomware infections", Computer and Communications (ICCC), 2016 2nd IEEE International Conference.

[5]. Pathak, P B**."**Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks",2016, International Journal of Advanced Research in Computer Science.

[6]. Nolen Scaife , Henry Carter, Patrick Traynor , Kevin R.B. Butler." CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data",2016, IEEE 36th International Conference on Distributed Computing Systems

[7]**.** Sanggeun Song, Bongjoon Kim, and Sangjun Lee. "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2946735, 9 pages.

[8]. N. Andronio, S. Zanero, and F. Maggi, "HelDroid: dissecting and detecting mobile ransomware," 2015, in Research in Attacks, Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer.

[9]. The wall street Journal, America.www.wsj.com