International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Ransom Ware – A threat to secure cyber world

Navpreet Kaur[1],Dr. Yogesh[2]

[1] *Research Scholar (Computer Science), J.J.T.U Jhunjhunu Rajasthan, (India)*

[2] *Associate Professor (Computer Science), J.J.T.U Jhunjhunu Rajasthan, (India)*

ABSTRACT

As technology has become indispensible part of our life. And it is advancing more rapidly so many business organizations and even the individual are storing their important data and files electronically. Web world has become an easy ground for cyber criminals to make money. Recently ransom ware virus software hits the cyber world. Ransom ware is a malware that encrypts a user files and important data and decrypts it only if certain money called ransom generally in the form of bit coins is paid. The ransom ware new variations are growing encouraging the avoidance of numerous antivirus and interruption recognition frameworks. This paper gives an insight to understand and Preventive and security measures are discussed to eradicate this menace.

Keywords – Ransom ware, threat, wannacry, security, encrypt, decrypt etc.

I. INTRODUCTION

Today, the threat of ransom ware has become a global problem which has affected all parts of world. Ransom ware is a type of malware (malicious software). Ransom ware attempts to deny access to a user's (or organization's) data, usually by encrypting the data with a key known only to the hacker who deployed the malware. After the data is encrypted, the ransom ware directs the user to pay the ransom to the hacker (usually in a digital currency such as Bit coin) in order to decrypt its useful data. The amount of ransom is decided depending upon the importance of data and organization by the hackers.

According to Symantec's report [1] most affected countries from ransom ware are USA, Japan, UK, Canada, Germany, Italy, Australia, India, Netherland, Turkey and Brazil.

Commonly seen ransom ware categories are:

1.1 Encrypts personal files/folders – Once the files are encrypted, they are deleted from the folder and generally a text file containing instructions for payment is left behind in the same folder. This type of ransom ware is called 'file encryptor'. For example: CryptoLocker.

1.2 'Locks' the screen – It displays a full screen image that blocks all other windows and demands payment. Personal files are not encrypted. This type of ransom ware is called 'WinLocker'.

1.3 "MBR ransom ware" – An area in the computer's hard drive that permits the operating system to boot up is called the Master Boot Record (MBR). MBR ransom ware changes the computer's MBR which interferes with the ordinary boot procedure. It displays ransom demand on screen [2]

II. RANSOM WARE SO FAR

The first recognized ransom ware was the "AIDS (Aids Info Desk) Trojan" released in 1989. This was also known as "PC Cyborg Trojan". It was written by Dr. Joseph Popp. It replaced the AUTOEXEC.BAT file and it would then count the number of times the machine had booted. Once this boot count reaches 90, it would then hide directories and encrypt the names of all the files on the C: drive and make the system unusable. To have access to the data, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panamas.[3].

With the Internet making it easier to carry through Popp's ransom idea, cyber criminals began to realize that they could make a profit from ransom ware on a far wider scale. In 2006, criminal organizations began using more effective asymmetric RSA encryption. Trojans such as Archiveus, Gpcode, Krotten, MayArchive and Cryzip began utilizing more sophisticated RSA encryption schemes, with ever-increasing key-sizes [4].

III. HOW IT WORKS

Ransom ware attacks are typically carried out using a Trojan, entering a system through a downloaded file or a vulnerability in a network service [5][6].

3.1 Firstly the attacker generates keys pair and places one key in malware and place it in some email.

3.2 When a user opens the email by clicking on its attachment or link it flows into the operating system to run the ransom ware code.

3.3 Then ransom ware encrypts important files and documents of that system and demands the ransom in the form of some digital currency like bit coins.

3.4 The WannaCry ransom ware uses a window flaw to replicate itself and spread around the computer network.

IV. WannaCry Ransom Ware

WannaCry Ransom ware Attack 2017 was the worst attack that ever had before. WannaCry Ransom ware 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.

Encrypting ransom ware 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 Ransom ware attack 2017 was one of the largest attacks that were ever carried out. It grabbed the 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 ransom ware 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 organizations in UK were badly affected. Some systems were caught by malware. Lot of colleges and students computer was hit by attack in china. 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 bit coin. Otherwise gives warning that file will be deleted. Ransom ware overwrites the contents of the original file by opening the file, reading its contents, writing the encrypted contents in-place, then closing the file [7]

V. TIPS AND PREVENTIVE MEASURES TO STAY SECURE

Following are some of the preventive measure to avoid ransom ware:

- Antivirus should have latest updates.
- Avoid opening Spam messages and do not reply these.
- Use 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.).
- Always use a security suite.
- Do not enable file sharing.
- Switch off unused wireless connections, such as Bluetooth or infrared ports.
- Avoid Public 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.
- Use antivirus to block access to malicious websites and scan all downloads.
- Use advanced endpoint protection that can identify new malware types and detect malicious data.
- Contact concerned authority about suspicious pop-ups.
- Disconnect from networks instantly if you suspect infection.
- Avoid letting websites remember your password.
- Verify the authenticity of the source

A novel practice to protect against ransom ware attack is to back all files completely on another system frequently to avoid loss of data.

VI. CONCLUSION

The purpose of study in this paper is to analyze and to look at the origins, history and evolution of Ransom ware. The majority of G20 countries are hit by ransom ware. It has become a very easy tool for making money by cybercriminals. Technological advancements such as cloud computing, IoT and the growth allow cybercriminals to target new areas with ransom ware. WannaCry Ransom ware Attack 2017 was the most terrific attack. It has shown that attention to security is supreme concern for all. To fight with ransom ware we

all have to contribute The product designers has to improve security and take malicious operations and scenarios into consideration and should have the solution when such problems arise. We need to practice basic security practices to protect our data, such as avoiding clicking malicious links or attachments and patching exploitable software vulnerabilities. We should know the seriousness of ransom ware and should be prepared for minimizing hazard from ransom ware attack.

REFERENCES

[1] K. Savage, P. Coogan and H. Lau, "The evolution of ransom ware", Symantec Security Response Publications, 2015.

[2] Sophos.com, "Information on malware known as Ransom ware", 2015. [Online] Available: https://www.sophos.com/enus/ support/knowledgebase/119006.aspx.

[3]J. Bates, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0", Virus Bulletin Ltd, England. 1990.

[4]J. Leyden, "Ransom ware getting harder to break", Theregister.co.uk, 2006. [Online] Available: http://www.theregister.co.uk/2006/07/24/ransomware.

[5] Gregg Keizer, G. (2011): Ransom ware squeezes users with bogus Windows activation demand, available at http:// www. computerworld.com, accessed 18 May 2017.

[6]Robert. McMillian, R. (2010): Alleged Ransom ware Gang Investigated by Moscow Police, available at http:// www.pcworld.com/article/204577/article.html, accessed on 21 May 2017.

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