ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Analysis on Ransomwares and Prevention Approach

Chitesh Rai Tuli[1], Pankaj Sharma[2], Sakshi Malhotra[3]

B.Tech. Student (4th year), Department of Mathematics and Computing, Delhi Technological University, Delhi, India[1]

Scientist - D, CERT-In, Department of Electronics and IT, Government of India[2]

B.Tech. Student (3rd year), Department of Information Technology, Northern India Engineering College, Delhi, India[3]

ABSTRACT: Ransomware have been as globally emerging threat in the 21st century which marked their presence even before the time computer was daily need. This research paper aims to provide a Holistic study of Ransomwares from their origin back in 1989 to the current Petya attack on 27 June 2017and the necessary Preventions for the same. The working of the ransomware is demonstrated by developing through a ransomware that has been developed by us. Existence of a malware in a computer network was not something surprising until ransom notes started to appear on the computers screens. The first such attack appeared in 1989, by PC Cyborg Co-operation which demanded a huge amount to unlock the files. Back then the encryption algorithms were weak, money transfer mechanisms were futile and computers were not used by majority to store the data. However with the evolution of technology, strong non-crackable Encryption algorithms were used by the attackers to lock the files which started making the recovery of the files near to impossible without paying the ransom. To enhance the effect of Ransomwares, crypto currency and bitcoins entered the world of computer malwares. With strong algorithms like AES and RSA, Bitcoin payment system, Ransomwares such as Cryptowall, Wannacry and Petya proved to be major source of destruction earning revenue of more than $60,000 by targeting systems with centralized networks of those like hospitals and police departments etc.

KEYWORDS: Ransomware, Bitcoin, virus, Malware, Encryption, Cryptography, Ransom, File Extension, Crypto Currency, cybercrime, Wannacry.

I. INTRODUCTION

Demanding a payment for an illegal activity has been a crime prevailing since the ages of Ronald Grove and continued to the times of modern day terrorism. However, when ransom notes started to show their presence on the computer screen, a new era of cybercrime marked its presence. The definition of a typical ransomware is described as 'demanding ransom in exchange for access to the owner's file'. Technically a ransomware is seen as a malware which is introduced to a system/Network through Phishing emails, compromised web pages or even malicious Java scripts documents etc. and injects a code to the system/Network which converts the data to a format which cannot be accessed by the owner, unless he pays the ransom to purchase the unlocking key. The advanced ransomwares have claimed to be writing itself to a random character folder in 'Program Data folder with the name of 'taskche.exe [16].

Over years, with the aim to demand ransoms, ransomwares have followed different approaches to Propagate, lock/unlock files following which they have been classified broadly as

i) Encrypting ransomwares ii) Non Encrypting ransomwares / Locking Ransomwares.

A typical, Non-Encrypting/Locking ransomware locks the system and hence prevents it from further use and only restricting the capability of the system such as to pay ransom only. However due to the presence of recovery tools which brings the system back to a stage near to original, such types of ransomwares were not very successful in extorting payment from its victims as the systems were unlocked before paying ransoms by the cyber security experts.

Encrypting Ransomwares or crypto Ransomwares do not interfere with the system files or deny system access, however once when injected into a system/network they typically look for file extension (.jpeg, .pdf, .txt etc) and convert the useful data of the owner to a format which makes the data non-productive using both customized and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

advanced encryption algorithms. The Crypto Ransomwares have been typically very successful in extorting ransoms by their victims due to the presence advanced techniques like Asymmetric Encryption Algorithms, Polymorphic approach which creates a unique signature on each system and a latent time out between its installation to the system and its activation which makes the malware hide under the radar of antiviruses and hence making its detection and system recovery very difficult.

II. RELATED WORK

The existence of ransomwares has been revealed through a long time in history, which thus lead to a comprehensive research on the same. Amongst the work of the various authors mentioned in the reference section, the author of source [1] talks about the historic moves made in the history of such malwares from a simple attack to a fully fledged attack earning billions through Bitcoins. As the growth in the I.T sector proceeded, classifications of ransomwares based on the type of encryption algorithm used, the payment method etc came as suggested by the authors of source [8]. With further development, Bitcoins and cryptocurrency paved their way, which have been proposed and explained duly by the authors of sources [27] and [28].Analyzing the existing work on the subject we thus plan to propose to Brief, Analyze and Prevent Ransomwares.

III. CRYPTOCURRENCY

Today, most people are familiar with the concept of cryptocurrency. While still somehow geeky and considered esoteric by most people, banks, organizations and many companies are aware of its importance. In 2017, it is quite difficult to find a mainstream bank or a big accounting institution that didn't research cryptocurrencies or publish about it [25]. But, what is a crypto currency? As explained by Investopedia.com, "A cryptocurrency is nothing but a virtual currency that uses cryptography and its applications for security". It is difficult to counterfeit due to this unique security feature. Cryptocurrency have a salient feature, and arguably its most important, is its organic nature: the fact that they are not issued by any central agency, rendering it theoretically immune to government interference or manipulation [26].Crypto currency is an encrypted decentralized digital currency transferred between peers and confirmed in a public ledger via a process known as mining [27].There are numerous types of cryptocurrency such as Bitcoin, Ethereum, Ripple, Litecoin etc., but Bitcoin is the one most popular among firms or hackers**.**

IV. BITCOIN

In 1998, weidai introduced a concept of currency, which revolved around cryptography for its creations and transactions, rather than a central authority. Bitcoin, which is the first decentralized digital currency that marked the presence of new payment system which was completely digital, owned by none, controlled and devolved by everyone on the network. It is seen as digital cash sent across parts of the world using peer to peer network. It is an example of well executed triple entry book-keeping mechanism [28]. Bitcoins can only work properlyif there is a complete consensus amongst the community. Therefore all users and developers are required to have a strong incentive to protect and maintain this consensus. Bitcoin network is anonymous and nobody owns or controls it, which provides freedom to users to choose the software or version of their liking, but these Softwares are expected to comply with the same protocols. Bitcoins are not backed up by any bank or government and hence they do not show any physical presence in nature, however balances are maintained and kept on a public ledger in cloud along with all Bitcoin transactions which are verified with a mass amount of computing power [28].

V. STAGES OF RANSOMWARE EVOLUTION

AIDS TROJAN: Aids Trojan or PC Cyborg: During 1989, when internet and computers were just seen as fascination to majority of world population, Joseph Poph, a then scientist on AIDS distributed 20,000 floppy disks to scientists titled as 'AIDS INFORMATION-INTRODUCTION DISKETTE', claiming that the disk contains software to calculate individual's risk of acquiring AIDS. [10] However the floppy disks also contained a malicious code that would replace

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

the AUTOEXE.BAT file and waited for system to reboot 90 times after which it would lock the file names in the c drive and ask for ransoms to be paid through a post office to 'PC Cyborg Co-operation'[9].However due to simple cryptographic techniques, the decryption and recovery tools were easily available and malware was not very effective as the use of computers back then was very restricted [11].

GPCODE: Gpcode is a Trojan which encrypts the files matching with a particular set of file extensions using single key encryption algorithms. The Trojan would then drop a txt named as attention.txt in the same folder as of the encrypted files which gives the directions to pay the ransom [12].The payments were made in e-gold or via liberty reserve accounts. However Gpcode was not very successful in its attempts because the original files could be restored using the windows recovery tools and other security agencies came up with a variety of powerful tools [8].

CRYPTO LOCKER: Crypto locker is malware which marked the presence of 'Bitcoins' as a strong payment tool in the family of ransomware attacks [8].Using strong asymmetric algorithms the files with common extension were encrypted and the reverse process was only possible with the help of a unique decryption key[13]. The malware holds the capacity to encrypt the connected USB drives, network shares and even some of the cloud storage files. However the law enforcement agencies we capable in taking down the Botnet *which was spreading crypto locker [8]*.

Figure 1: Screen after CryptoLocker attack.

WANNACRY: On May 12 - 2017, the world saw its most extensive ransomware attack: WANNACRY, which attacked almost 200,000 devices in over 150 countries, occluding operations at various hospitals, network and internet providers, utility companies, and numerous businesses across the globe [20]. Wannacry is a worm that delivers a ransomware payload and has two salient components, i.e. a self-propagating worm module and a ransom module that handles the ransom extortion activities [21].The ransomware attack began on afternoon of 12th May, where it affected England's National Health Service, prompted automaker Renault to shut factories in France for days, and many others. A 22-year-old cyber security expert known as MalwareTech was able to slow the attack by registering a domain name which he discovered in the ransomwares code which also acted as a kill switch [22]. The vector that initiated the spread is still unknown, but it is believed that it started through emails and still has not been confirmed yet [21]. After the WannaCry infects a machine, the malware starts encrypting files ending with over 176 extensions [18] along with the following GUI on the desktop [22].Wannacry gave its victims 3 days to pay a ransom of $300 in bitcoins to gain access to their data, along with an option of paying twice the amount ($600) to recover the data within a week of the infection. If the user failed to pay the ransom within a week's time, the data was lost permanently.

Figure 2: Screen after CryptoLocker attack.

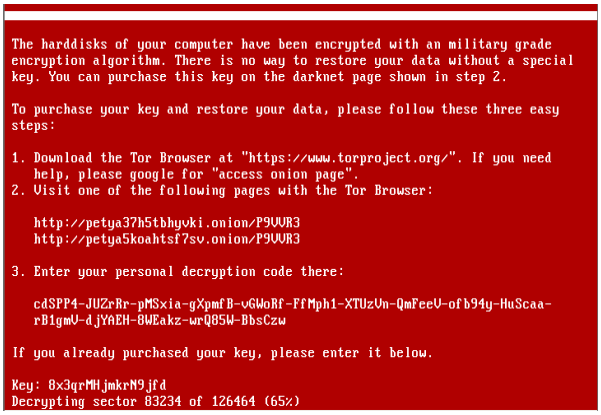


Figure 2: Screen after Petya Attack

WannaCry's ability to spread itself across an organization's network by exploiting critical vulnerabilities in Windows computers makes it is far more dangerous than other common ransomware types, the exploited vulnerabilities were patched by Microsoft in March 2017 (MS17-010). As quoted by Cnet.com, "the road to Hell is paved with good intentions" [19] The exploit, known as "EternalBlue," was first uncovered by The National Security Agency and then leaked in April in the of a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

series of leaks by a group of hackers known as the Shadow Brokers, who claimed that the group had stolen the data from the Equation cyber espionage group [18]

PETYA:A major ransomware attack that took place less than 2 months after WannaCry was Petya which took place on 27th July 2017. [7]. It hit companies in Europe, the Middle East along with the US and India, wreaking havoc for employees and customers alike, The attack prevented computers from working, instead displaying a ransom letter demanding a $300 (almost £235). The widespread attack affected numerous global and national organizations including the Ukrainian National Bank, logistics company Maersk, the advertiser WPP and the legal firm DLA Piper[31]. Like WannaCry, "Petya" spreads rapidly through networks that use Microsoft Windows, Petya also propagates through EternalBlue vulnerability.

VI. SAMPLE MODEL OF RANSOMWARE

To understand the working of Ransomware, we have created a demo Ransomware, developed in a control Environment to test the working, Analysis and thus to propose solutions to prevent further attacks from such malwares.

Understanding of the model

A certain set of files with a specified extensions have been 'Encrypted' using the Advanced Encryption Standard with a symmetric unique key password which gets stored in database, inaccessible to the users, on running of the model. The files have now been converted to a format which is not readable to the owner and can only be recovered on paying a certain amount of ransom which sets a specified column in the database of the attackers to 'PAID'. An instruction file is launched on the system which directs the victim to a website where he finds the further instructions to pay. Once is the payment is made the decryption code on running converts the effected files back to the readable mode.

V1I. THE RANSOMWARE CODE

The ransomware model searches for files in the entirety of the device. No matter how many drives are there, everything will be searched.

```
def drives():
        drives = win32api.GetLogicalDriveStrings()
         drives = drives.split('\000')[:-1]
         return str
```

The following file extensions are being targeted by the ransomware model created:

```
["*.txt","*.docx","*.jpg","*.jpeg","*.pdf","*.exe","*.mp3","*.mp4","*.avi","*.wmv","*.mov","*.csv","*.xlsx","*.pptx","
*.py","*.png","*.bmp","*.cpp","*.java","*.jar","*.xml"]
```

The key used for AES encryption is unique to each device and cannot be generated again, as it uses the UUID of the device, its code is:

```
def uuid():
        a = uuid.uuid4 ()
         return str(a)
```

Once the file is found and the unique key is generated, the ransomware model starts encrypting the files with the following code using AES algorithm which is not feasible to reverse via brute force:

```
        outfile.write(bytes(filesize, 'utf-8'))
        outfile.write(bytes(IV, 'utf-8'))
        while True:
        chunk = infile.read(chunksize)
        if len(chunk) == 0:
                break
         elif len(chunk) % 16 != 0:
                chunk += (' ' * (16 - (len(chunk) % 16))).encode('ascii')
         outfile.write(encryptor.encrypt(chunk))
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

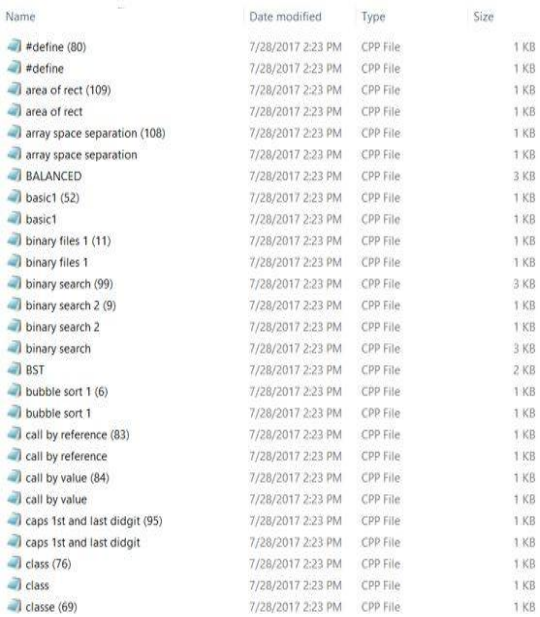
```
outfile.close()
```

A ".txt" file is generated after the code has finished executing which has the information about the ransom and the name of the files that are encrypted. The files can only be decrypted once the ransom has been paid and the attacker confirms it by changing the status of victim's device in the attacker's database. After the payment is received, the victim can run the decryption code provided at the time of the attack. The code of decryption is as follows:

```
filesize = infile.read(16)
IV = infile.read(16)
decryptor = AES.new(key, AES.MODE_CBC, IV)
with open(outfile, 'wb') as outfile:
        while True:
        chunk = infile.read(chunksize)
        if len(chunk) == 0:
                break
        outfile.write(decryptor.decrypt(chunk))
        outfile.truncate(int(filesize))
        infile.close()
        outfile.close()
```

V1I1. RESULTS AND ANALYSIS

For the sake of simplicity, the only extensions targeted were ".cpp" files as other file extensions can cause more serious damage to the working of the device. Though files like ".dll", ".exe", ".xml" were left out in this example, but they can be targeted fairly easily. As soon as the software is run, the ransomware searches for ".cpp" files on the computer system, upon finding which, it starts to encrypt them using AES algorithm. One point to ponder is that every time the software is run, a unique key is generated which makes the encryption secure as it is practically impossible to generate the same key again.



Name	Date modified	Type	Size
#define (80)	7/28/2017 2:23 PM	CPP File	1 KB
#define	7/28/2017 2:23 PM	CPP File	1 KB
area of rect (109)	7/28/2017 2:23 PM	CPP File	1 KB
area of rect	7/28/2017 2:23 PM	CPP File	1 KB
array space separation (108)	7/28/2017 2:23 PM	CPP File	1 KB
array space separation	7/28/2017 2:23 PM	CPP File	1 KB
BALANCED	7/28/2017 2:23 PM	CPP File	3 KB
basic1 (52)	7/28/2017 2:23 PM	CPP File	1 KB
basic1	7/28/2017 2:23 PM	CPP File	1 KB
binary files 1 (11)	7/28/2017 2:23 PM	CPP File	1 KB
binary files 1	7/28/2017 2:23 PM	CPP File	1 KB
binary search (99)	7/28/2017 2:23 PM	CPP File	3 KB
binary search 2 (9)	7/28/2017 2:23 PM	CPP File	1 KB
binary search 2	7/28/2017 2:23 PM	CPP File	1 KB
binary search	7/28/2017 2:23 PM	CPP File	3 KB
BST	7/28/2017 2:23 PM	CPP File	2 KB
bubble sort 1 (6)	7/28/2017 2:23 PM	CPP File	1 KB
bubble sort 1	7/28/2017 2:23 PM	CPP File	1 KB
call by reference (83)	7/28/2017 2:23 PM	CPP File	1 KB
call by reference	7/28/2017 2:23 PM	CPP File	1 KB
call by value (84)	7/28/2017 2:23 PM	CPP File	1 KB
call by value	7/28/2017 2:23 PM	CPP File	1 KB
caps 1st and last didgit (95)	7/28/2017 2:23 PM	CPP File	1 KB
caps 1st and last didgit	7/28/2017 2:23 PM	CPP File	1 KB
class (76)	7/28/2017 2:23 PM	CPP File	1 KB
class	7/28/2017 2:23 PM	CPP File	1 KB
classe (69)	7/28/2017 2:23 PM	CPP File	1 KB

Figure 3: Initial .cpp Files present in the system

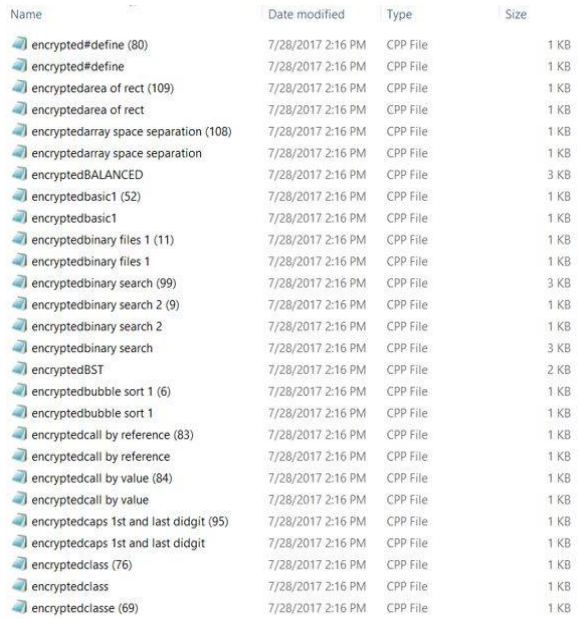
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017



Name	Date modified	Type	Size
encrypted#define (80)	7/28/2017 2:16 PM	CPP File	1 KB
encrypted#define	7/28/2017 2:16 PM	CPP File	1 KB
encryptedarea of rect (109)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedarea of rect	7/28/2017 2:16 PM	CPP File	1 KB
encryptedarray space separation (108)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedarray space separation	7/28/2017 2:16 PM	CPP File	1 KB
encryptedBALANCED	7/28/2017 2:16 PM	CPP File	3 KB
encryptedbasic1 (52)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbasic1	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbinary files 1 (11)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbinary files 1	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbinary search (99)	7/28/2017 2:16 PM	CPP File	3 KB
encryptedbinary search 2 (9)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbinary search 2	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbinary search	7/28/2017 2:16 PM	CPP File	3 KB
encryptedBST	7/28/2017 2:16 PM	CPP File	2 KB
encryptedbubble sort 1 (6)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedbubble sort 1	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcall by reference (83)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcall by reference	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcall by value (84)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcall by value	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcaps 1st and last didgit (95)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedcaps 1st and last didgit	7/28/2017 2:16 PM	CPP File	1 KB
encryptedclass (76)	7/28/2017 2:16 PM	CPP File	1 KB
encryptedclass	7/28/2017 2:16 PM	CPP File	1 KB
encryptedclasse (69)	7/28/2017 2:16 PM	CPP File	1 KB

Figure 4: Status of .cpp files after Execution of Code

As shown in the 2 figures above, there is a folder with numerous cpp files, once the ransomware is run, the files are encrypted, and in order to let the user know about the encryption, the name of the files are changed as well. The word encrypted along with the name of the file will be difficult to miss by the user and enough to startle him/her over possibility of data loss. The encryption is done through symmetric encryption which is unique to every device, so it is pointless trying to brute force the encryption. The files can only be useful to the victim once the ransom has been paid.
A ransomware has thus been created in a controlled for testing purpose to study and analyze the working of such a malware on a computer system. The malware has been analyzed on the following parameters and the results obtained are:

S.no	Parameter	Result
1.	CPU usage `before execution of code'	3%
2.	CPU usage 'After execution of code'	28%
3.	Recoverable by shadow copies(Y/N)	NO
4.	Recoverable after Paying Ransom(Y/N)	YES
5	Type of Encryption	Unique key, Symmetric Encryption

Through analysis, it can be seen that the CPU usage increased significantly after execution of the ransomware as a number of files got encrypted which the CPU was unable to access. After execution, the ransomware attacks the shadow copies of the windows device and deletes them so that the user cannot undo the effect of the attack. Moreover, the data is fully retrievable once the ransom is paid as the key is symmetric and is only stored in the attacker's database.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

IX. PROPOSED SOLUTIONS TO TACKLE RANSOMWARES

1. In the event a suspicious process is spotted on your computer, instantly turn off the Internet connection.
2. Use email filters and scan email attachments on both host and network for bad domain sources and unknown addresses**.**
3. Create regular backups for your data, both on an external hard drive and online drives like one drive etc. so that the important files always remains protected.
4. Have a defined email validation system to check email spoofing, which is a strong tactic for email phishing and spam campaigns used majorly by ransomwares for propagations.
5. Separate physical administrative network and logical business network to protect critical information and sensitive services.
6. Do not enable Marcos for documents that have been downloaded from internet, selective enablement of Marcos can done using the new tool released for office 2016.
7. Conduct regular penetration testing and risk analysis for the systems in the network containing valuable data.
8. Use strict software policy programs or similar to ensure that Softwares installed are not functioning from common ransomware targeted folders like localappdata folder.
9. Use runtime protection that detects the action of executing malware.
10. Always insist on using the most updated version for your operating system.
11. Set firewall to deny access to unknown malicious IP address.
12. Do not give more access to any user that required on a network containing useful data, set access restrictions.

X. CONCLUSION AND FUTURE WORK

In this paper we proposed a model to demonstrate the working of a ransomware, how it infects a computer once it enters it through emails, USB drives, CDs or drive by downloading. The model is written in python and encrypts the files in the device using a unique symmetric key. The scope of the project can be extended to study the exe binding to email attachments and thus develop email phishing. This shall further help us to develop tools to prevent email Phishing which is one the major source of how ransomware Propagate. The entire of objective of the paper and model was develop preventive strategies after having a rigid understanding of how ransomwares work, as such attacks have been a major sources of Devastation.

XI. ACKNOWLEDGEMENT

We wish to express sincere gratitude to the administration of CERT-In, Department of Information Technology - Government of India, Northern India Engineering College and Delhi Technological University for providing the academic environment to pursue research activities. This would not have been possible without their unending support.

REFERENCES

1. https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b
2. https://www.knowbe4.com/aids-trojan
3. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#2
4. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report
5. http://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html
6. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
7. http://indianexpress.com/article/technology/tech-news-technology/petya-ransomware-cyber-attack-india-is-worst-affected-in-asia-ukraine-on-top-globally-4727209/
8. https://www.mcafee.com/us/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf
9. https://www.knowbe4.com/aids-trojan
10. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
11. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
12. https://www.f-secure.com/v-descs/gpcode.shtml
13. https://securelist.com/gpcode-like-ransomware-is-back/29633/

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

14. https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/
15. https://nakedsecurity.sophos.com/2013/10/18/CryptoLocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
16. www.cyberswactakendra.gov.in/alerts/wannacry_ransomware.html
17. Brian Lee – " Ransomware: Unlocking the Lucrative Criminal Business Model"
18. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
19. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/
20. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#4
21. https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99
22. https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries
23. https://pastebin.com/xZKU7Ph1
24. http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html
25. https://blockgeeks.com/guides/what-is-cryptocurrency/
26. http://www.investopedia.com/terms/c/cryptocurrency.asp
27. http://cryptocurrencyfacts.com/how-does-cryptocurrency-work-2/
28. https://bitcoin.org/en/
29. Understanding the Depth of the Global Ransomware Problem - An Osterman Research Survey Report
30. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/
31. http://www.telegraph.co.uk/technology/2017/06/27/petya-cyber-attack-everything-know-global-ransomware-outbreak/