International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Ransomware: An Illustration of Malicious Cryptography

Jagsir Singh, Jaswinder Singh

Abstract: ***Malware are the serious threat to the computer systems. Malware are written for many reasons: for stealing confidential data, for financial gain or to affect the working of the computer system. Ransomware is the most disastrous kind of malware which encrypts the user's whole data and demands ransom (money) to decrypt the data. The user has to pay ransom for getting the decryption key. This becomes the nuisance of encryption algorithms which are used in ransomware attacks. In this paper, a study of ransomware malware is done with the perspective of encryption algorithms.***

Index Terms: Bitcoins, Encryption, Malware, Ransomware.

I. INTRODUCTION

Malware are the malignant software which harms the computer resources. Ransomware is the most harmful malware. It is a combination of the two words ransom and software. Ransom means demanding the bribe. Ransomware encrypts the user's data and asks for the ransom to the user for decrypting the data [1, 2]. When the user system is attacked through ransomware then it shows the message on the computer screen like as shown in figure 1. It is amazing that the user's data is encrypted so efficiently then it becomes impossible for the user to recover the encrypted data.

Generally, the user encrypts his data for the security reason that no one can read their data. Also, the organizations keep their data in an encrypted form for the security reason. Other main uses of the encryption algorithms are in transmitting the data over the network especially over the public insecure Internet. However, the attacker started using encryption algorithms to attack the user or organization by making their data unavailable [4,9] and creating complex malware (polymorphic, metamorphic) by using obfuscation techniques to evade the malware detection systems [29].

Nowadays ransomware has become the biggest threat for everyone because computer systems are used almost everywhere suchlike at home, in the organizations and educational institution as well. As in last few years, many ransomware attacks have happened which did great loss in form of money and data.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

Jagsir Singh*, Ph.D. Research Scholar in the Department of Computer Science and Engineering, Punjabi University Patiala.

Dr. Jaswinder Singh, Associate Professor in the Department of Computer Science and Engineering, Punjabi University, Patiala.

Wannacry was the one of the most distributed ransomware. Wannacry affected the millions of PCs across the world.

Therefore all the major defending organization has been working hard to provide the protection from the ransomware attack such as TrendMicro [10], McAfee [22], Kaspersky [7], Malwarebytes[18], Sophos [28] etc.

A. Execution Cycle of Ransomware

Step 1. The payload is drooped into the systems in many ways like the drive-by download, attachment in Gmail, by exploiting the system vulnerability to enter into the system or spread through USB drive.

Step 2. After the payload dropping then payload starts to connect with command and control server.

Step 3. Generate cryptographic credential (encryption and decryption keys).

Step 4. Encrypt the user data and decryption key with the public key of command and control server.

Step 5. Take the full control of the system and render a display screen with the message as shown in figure 1 and specify instructions to pay the ransom for getting the decryption key.

Step 6. If the user pays the ransom by following the mentioned instructions in their bitcoin account then a user might get the decryption key or might be further asked to pay more ransom. If a user gets the correct key only then user can decrypt data properly.

Figure.1 Victim computer shows the message of Ransomware attack [12].

B. Bitcoins: Bitcoin is an electronic currency.

The concept of bitcoins was given by Satoshi Nakamoto [8]. He wrote a paper in 2008 on electronic currency in which he explained the idea how to convert the physically currently of world into a single digital currency. The exchange between the users can be done directly without the intervention of any other person or province, the state even the country. Every person will have a secure unique account and will not provide them with any information about the user. It is just a unique id to exchange the money in form of bitcoins. A bitcoin can be divided up to 8 decimal places. A 0.00000001 bitcoin is one Satoshi. From this, it can be understood how Satoshi was aware of its popularity and the acceptance of this currency system in all across the world. When it came into the market it was less worthy than $1 (one dollar) but now its value is so high more $12000. The limit of bitcoins is 21 million which was fixed and still, these are mined. Mining will be stopped when it will reach the fixed limit. At present 16.7 millions bitcoins are mined and only 4.7 millions remained which will be mined very soon as the coin miners are increasing day by day.

Since attackers exploit the anonymity of bitcoin account. They encrypt the user's data and demand the ransom from a victim for decrypting the data [3, 4]. An attacker uses the multiple bitcoins. They use some public bitcoins accounts to receive the ransom from victims and then transfer the money in their other accounts [5]. The victims who send the money cannot see the other addresses owned by the attackers. Additionally, nothing is identifiable from the bitcoins address itself. For ensuring the anonymity the attacker uses the long chains of bitcoin addresses. Therefore the nature of bitcoins is also helpful for the attacker to hide their identity for receiving money from the victims.

C. Encryption Algorithms

Encryption is the process of scrambling the original data which can't be read by other users. Primarily, the encryption algorithms are used for securing the data from unauthorized access or transmitting the data securely over the public unsecured network from one system to another. Various symmetric and asymmetric algorithms are used for encrypting data through ransomware [3]. When these algorithms were designed nobody ever thought that these algorithms would be used for attacking the computer systems. The magnificence of these algorithms is that these are secure which can't be cracked. Now a day the attacker tends to start using cryptographic algorithms for encrypting the user's data or organizational data without their concern. In simple terms, the attacker attacks the system for encrypting the user data and compelling him to pay money for getting data back [11].

In most ransomware attacks the symmetric algorithms AES, DES are used to encrypt the user data and the asymmetric algorithms RSA, ECC are used to encrypt the encryption key which is used by the symmetric algorithm [13, 14]. In the next section, many ransomware are discussed which provides the better understanding of the use of encryption algorithms.

II. Chronological Study of the Evolution of Ransomware

In 1989, Joseph Popp has written the 'AIDS Trojan' in which symmetric key cryptography was used. Young and Young described the failure of 'AIDS Trojan' malware that decryption key (private symmetric key) could be extracted from the malware.

The original concept of malicious cryptography was implemented by Young and Young (1996) [3]. They presented a paper at the IEEE conference in which they explained the life cycle of malicious cryptography. They explained how the electronic money can be extorted using the malicious cryptography in which both asymmetric and symmetric will be used. Point in time they implemented this idea and provide the proof how the malicious cryptography would be a big problem for computer security. And after a couple of years, in 2005 a new ransomware Gpcode was reported in which 660 bit RSA public key was used to encrypt the data [6]. Users were supposed to request to decrypt the files only after giving a ransom of $100-200 [5]. Again in 2010, the new version of Gpcode was released with high complexity in which RSA-1024 bit and an AES-256 key were used to encrypt the data [7].

For the time being the usage malicious cryptography was slow down. In late 2013, again the ransomware returned back when nations around the world started using the digital Bitcoins cryptocurrency. This is one of the main reasons of increasing ransomware because the bitcoin account of the attacker does not reveal any information about the identity of an attacker. The ransomware attacker uses the many different bitcoin accounts to maintain the privacy and also uses the onion router (TOR) to avoid the IP logs. In 2013 CryptoLocker ransomware attack happened [25]. This ransomware was implemented using 2048-bit RSA key pairs with AES 256-CBC. In 2014 again the new variants of CryptoLocker ransomware: Cryptolocker.F and Torrentlocker were developed with more complex structure [23]. After that Crytowall (2014), Fusob (from April 2015 to March 2016), Spora (2014) new ransomware were designed by exploiting systems vulnerabilities [19, 24, 29]. Fusob ransomware demanded the $100 to $200 from the victim for sending the private key for decrypting their data. In the year 2016, the growth of ransomware was increased. Some most destructive ransomware like Emper (Jan 2016), Locky (RSA+AES-128 CTR, Feb 2016), Patya (March 2016), CryBee(July 2016), Telecrypt (Nov 2016) and Cerber (RSA+RC4-256, 2016) were discovered especially Locky, Patya and Cerber ransomware compromised the computer system all around the world [10, 22, 25]. Not only the computer ransomware are developed, the mobile ransomware are also developed. On 30th May 2017 the Judy android ransomware was discovered which was present since April 2016. It was hidden on the play store which was downloaded by million users.

The day we all remember 12th May 2017 when a severe ransomware attack happened which actually made the world cry that was WannaCry ransomware [[12]. It affected the more than 300000 computer across the 150 countries. It demanded the $300 in form of bitcoins from the victims. This ransomware exploited the vulnerability of Windows 7 operating to drop the payload. Windows 7 operating system was the reason behind its spreadness. This operating system is used worldwide. In this RSA-2048 bit encryption algorithm was used to encrypt the secret key which was used to encrypt the user's data. A few months later again in 2017 the new variant of Patya (2016) ransomware Not Patya was developed. This time different key algorithms were used to make the encryption process difficult.

After the wannacry attack, people not only from computer/IT background stated to know but also the almost every computer user became aware of ransomware attacks. Various other ransomware such as Samsam(2016), Not Petya(2017), BadRabbit (2017) and Ryuk(2018) etc which did the good business in millions.

III. How to prevent Ransomware Attack

Ransomware attacks are more severe attacks which can jeopardize the working of any organization, individuals business or even the nation as well. Paying ransom does provide a guarantee that the attacker will send the original decrypting key. In some cases user paid the ransom and attacker again demanded the more ransom. As per US-CERT [29] paying ransom is not a solution as some user who paid the ransom and got the wrong decryption key. When ransomware encrypts the user's data then there remains only two ways for the user either pay the ransom or to loss the data permanently. To handle this problem the user should follow the prevention mechanism [15, 17, 28]. The main challenge is how to prevent the ransomware attacks. Because, it is clear that encryption algorithms can't be cracked to compute the decryption key without paying ransom. Essentially, there are some steps which must be considered to forbid the severe malware attacks especially in the case of ransomware.

i. Patch the vulnerability. The initial phase of the attack is to exploit the vulnerability either present in the operating system or in the installed application. To fix them update the system regularly. Also, try to avoid the third party software tools which are mostly exploited by the malware developer to enter into the system then escalate the administrator privileges
ii. Disable the Remote Access of the system. Like in Windows Operating System disables the RDP (Remote Desktop Protocol).
iii. Use anti-malware software. It must be licensed and update it regularly.
iv. Try to use Internet surfing in the guest mode not in administrator mode to avoid automatically running files.
v. Keep the backup of data at the isolated place from the network like external Hard Drive.
vi. Additionally, the updated and licensed versions of the software should be installed on the system.
vii. Don't connect the flash drive to the computer system if the system does not have any malware detection software or not outdated.

viii. Don't click on the attachment in the email before the proper verification and scanned by antivirus.
ix. Disconnect the system to the network when no need of it.
x. Keep the backup of data at more than one place like in the Hard Drive or on the cloud.
xi. Precaution is the best solution to handle the ransomware attacks. Always, surf the Internet carefully. Because the internet is the main media through which attackers reach your computer easily. Never click on pop-ups, open secure website links. Most essential, try to avoid the use of third-party free software which are the main sources for the attacker to exploit them for dropping malware payloads into your system.

As we believe that malware doesn't affect the system ignorance does". Yes, it's true. Therefore to handle such types of severe attacks we need to update the system regularly and need to develop a psychological attitude for that.

IV. CONCLUSION

Ransomware are the most catastrophic type of malware which totally take the control of whole data. Other malware may delete the data, steal the data, slow down the system or in most rare case crash the system. Even though there would have some probability to recover the data. After the ransomware attack, to decrypt the encrypted data is almost impossible because during encryption those encryption algorithms are used which are not cracked yet. Therefore, the best way to avoid ransomware attack to follow the certain the prevention mechanism strictly such as patch the vulnerability, update the system regularly and keep the backup of data regularly.

REFERENCES

1. Jack Schofield, "How can I remove a ransomware infection?"The Guardian, July 2016.
2. Michael Mimoso (28 March 2016). "Petya Ransomware Master File Table Encryption". Retrieved 28 July 2016.
3. Young, A.; M. Yung, "Cryptovirology: extortion-based security threats and countermeasures", IEEE Symposium on Security and Privacy. Pp no.129-140, 1996.
4. Justin Luna (September 21, 2016). "Mamba ransomware encrypts your hard drive, manipulates the boot process"NeowinRetrieved 5 November 2016.
5. https://bitcoin.org/en
6. Eran Tromer. "Cryptanalysis of the Gpcode.ak ransomware virus", 2008.
7. Kaspersky Labs, "GpCode-like Ransomware Is Back". 2010.
8. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System".
9. Allisy-Roberts, P., Ambrosi, P., Bartlett, D. T., Coursey, B. M., DeWerd, L. A., Fantuzzi, E., & McDonald, J. C. Executive Summary. Journal of the ICRU, Vol: 6(2), pp no.7–8, 2006.
10. TrendLabs. Ransomware. (2017).
11. Advanced, H., "An Introduction to Advanced Malware and How It Avoids Detection, 2017
12. Adylkuzz, T., May, A. N., Pdt, A. M., Roessler, B., Images, G., Wannacry, T., Adylkuzz, O. Botnet using NSA ' s exploits could grow bigger than WannaCry, 2017
13. Kolodenker, E., Koch, W., Stringhini, G., Egele, M. "Defense Against Cryptographic Ransomware", 2017.
14. Ponemon Institute Research Report "The Rise of Ransomware Sponsored by Carbonite". 2017.
15. Loman, M. "How ransomware works Recent poll on ransomware in the UK", 2016.
16. Technology, I. National Cyber Security Policy , 2013.
17. Song, S., Kim, B., & Lee, S. (2016). The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform, 2016.
18. 18. Malwarebytes. (2017). Cybercrime Tactics and Techniques Q1 2017. Malwarebytes Labs, 1–26.
19. Aziz, S. M. (2016). Ransomware in High-Risk Environments IT-792 , Independent Research Project December 2016 Advisor .
20. Security, I. T., Systems, C., & October, E. Advanced Malware Protection Against ransomware, 2016.
21. Carter, H., Traynor, P., Butler, K. R. B., "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", 2016.
22. McAfee Labs, "Report on Threats Predictions", 2017.
23. S., Francesco., "Analysis of a Cryptolocker" , IISFA, 2015.
24. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E., "Cutting the Gordian Knot : A Look Under the Hood of Ransomware Attacks", pp no. 1–20, 2013
25. Labs, M., Advisories, T., Advisory, T. T., Advisory, T., Labs, M., McAfee Labs Threat Advisory, 2016.
26. Findings, K. E. Y. , Special Report : "Ransomware and Businesses", 2016.
27. Singh, J., Singh, J., "Challenges of Malware Analysis: Obfuscation Techniques", International Journal Of Information Security Science", Vol.7, No. 3 pp no. 100-110,
28. MacAfee White Paper, "Understanding Ransomware and Strategies to Defeat it", 2016.
29. Wyke, J., A. , Anand, "The Current State of Ransomware", A SophosLabs technical paper, 2015.

AUTHORS PROFILE

Jagsir Singh is currently a Ph.D. Research Scholar in the Department of Computer Science and Engineering, Punjabi University Patiala. He received his B.Tech degree from Punjabi University, Patiala in 2014. He did his Master of Engineering degree from Panjab University, Chandigarh in 2016. His area of interest includes: Computer and Information Security, Mobile, Machine Learning.

Dr. Jaswinder Singh is presently working as Associate Professor in the Department of Computer Science and Engineering, Punjabi University, Patiala. He did Ph.D. in Computer Engineering. He has more than 14 years experience in field of Computer Science & Engineering. His area of interest includes: Computer and Network Security, Mobile Ad-Hoc Networks, Internet of Things, Machine Learning.