Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Preventive Measures and Incident Response for Locky Ransomware

Kulkarni Pooja Prakash
M.Tech Scholar
Jamia Hamdard
Delhi, INDIA

Tabrez Nafis
Asst. Professor
Jamia Hamdard
Delhi, INDIA

Dr.Sidhartha Sankar Biswas
Asst.Professor
Jamia Hamdard
Delhi, INDIA

Abstract: In today's cyber world, humans connect with each other through some communication channels and digital devices. The use of Internet has been increased to such an extent that emails and online payments have become part of our life. As the increased use of Internet has spread good things, it has also spread the threat of cyber-crimes. The cyber criminals have been active finding vulnerabilities and are ever-ready to various attacks on victims. In this paper, we have tried to illuminate how a simple word document can compromise your system. It is nothing but a Ransomware. A Ransomware is the type of malware, which encrypts the data on the victim's system and then asks for the 'Ransom' in terms of money to decrypt the data to its original form. We have explicitly explained Locky Ransomware, its working methodology, encryption and prevention measures. This paper also deliberates on the computer forensics and email forensics and incident response for Locky Ransomware.

Keywords: Locky Ransomware, cyber-crime; Computer forensics; email forensics; email spoofing; bitcoin.

I. INTRODUCTION

"Every coin has two sides". In the world of cyber, we are connected everywhere through the Internet. Today infrastructures like healthcare, banking, education, energy, telecommunication, Insurance, small and large IT or non- IT businesses, etc. have become critical infrastructures for every country or nation. These infrastructures are invariably become dependent on vast use of internet, which is helpful in providing the information and for doing multiple tasks simultaneously. However, this is only one side of the coin. The other side is abuse of internet in the form of threats, frauds or we can say doing cyber-crime. Cyber-crime involves the crimes in which computers or digital devices like mobile phones, laptop, etc becomes the objects/targets using communication channel. There are different types of cyber-crimes such as forgery, email spoofing, denial-of-service, threats or malware attacks [1].

Ransomware is a type of malware which infects the target system and takes control over it and then asks for ransom, for target system data. Ransomware either locks the system or encrypt the system data and then demands through a text file or through web browser [2]. There are two types of Ransomware namely, Non-encrypting Ransomware and Encrypting ransomware. Non encrypting Ransomware threatens you with diffusion of collected personal data e.g. browsing history. In Encrypting Ransomware encrypts the user files and demands for ransom to decrypt it [3]. In this type of Ransomware, algorithms like AES-1024 bits or RSA-2048 bits are used for encryption. Cryptolocker, Torrentlocker, Cryptwall, Tesla crypt, CTB Locker, Pad crypt , Locky etc. are few known Ransomware [3]. In this paper we are going to discuss about Locky Ransomware.

II. LOCKY RANSOMWARE

A. Spoofing an email id and sending a Locky ransomware through email

Cyber criminals are very smart. They are always on duty to find vulnerabilities and make a use of these golden chances. The attacker can spoof an email-id, that is associated with any organization and then send an email to the victims. The victim thinks it as an email from a legitimate sender, so he/she may click on the document attached with the email. Just one single click and the victim's system gets infected. Fig 1 below, illustrates the methodology of the attacker. He sends the invoice word document to victim which contains malicious macros as shown in fig 2.

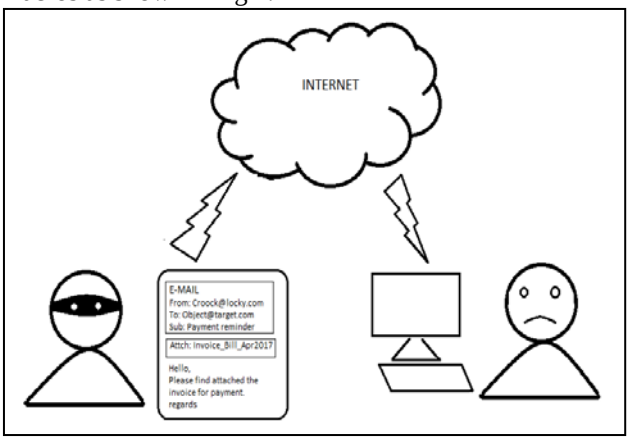

Fig 1: sending an invoice mail to victim

In the todays cyber world, we do online transactions, online shopping, makes online payments of bills and many more things are being done online. The acknowledgements of

these payments/orders are usually sent by email. The user needs to be aware whenever he/she gets an email. One should not be in hurry to click on the email because it may be a ransomware.

B. Malicious macros document

Locky is a Ransomware which spread through malicious .doc files attached to spam email messages [4]. In day-today life, we frequently use the word document for various purposes. We never think that this simple word document may be very harmful to us. The downloaded word document, for e.g. an Invoice came as an attachment with email, contains scrambled text, which appears as macros. It shows a message to enable the macros, for proper encoding to see the contents of the document, as shown in Fig. 2 below. When users enable the macros, an executable file is downloaded, which is the Locky Ransomware. This encrypts all files on the system, which will be in the form files with extensions like .aesir, .shit, .thor, .locky, .zepto etc. and it is hard to find out the original files. Files are encrypted using RSA-2048 or AES-1024 algorithms [4].

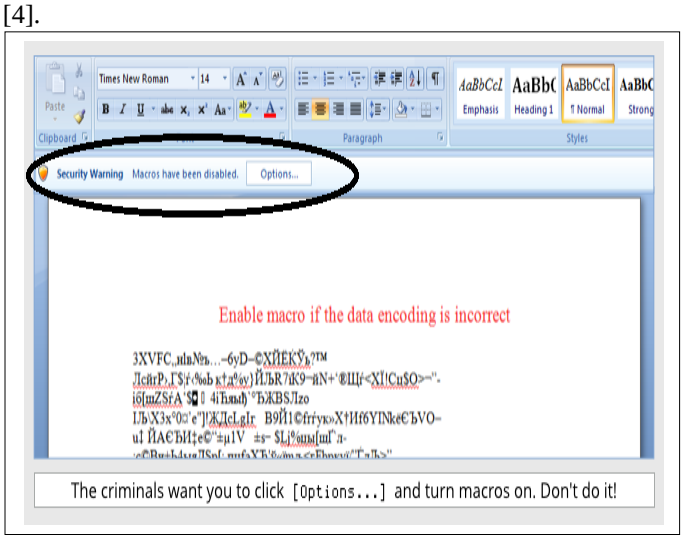

Figure 2: example of malicious macros doc file

C. Encryption in Locky Ransomaware

Locky ransomware spreads through email attachment, once the file will be downloaded then it encrypts the data files of victim system and locks it. This ransomware uses the Public key Cryptography. The data is encrypted using public key. It is decrypted using only a private key, which is only with the attacker. For decrypting these files attackers ask for ransom. After paying the ransom or money, may be in the form of Bitcoin, they will decrypt the data using private key [5].

Fig 3 below shows that the victim's system has been infected with malicious macros. It shows the message that data files are encrypted with some cryptographic algorithms. For decrypting the files we need to pay money in the form of Bitcoin. Bitcoin is a crypto-currency used in electronic payments [6]. Locky Ransomware creates an additional .txt file and _Help_instruction.html file in each folder. The ransomware also changes the desktop wallpaper to the one as shown in Fig.3 above [4].

III. HOW LOCKY RANSOMWARE WORKS

Locky Ransomware has a typical methodology of working, which has been listed below step-by-step:

- Attacker sends a spam email
- It's in the victim's Inbox
- New malicious attachment with Invoice.doc file
- Victim clicks on the .doc file
- Victim enables macros
- Creates and runs a batch file, as well as windows script
- Downloads a binary file called fail.exe
- Runs fail.exe which is a Ransomware
- Encrypts victim's data files
- Deletes shadow copies, removes local backups of files
- Displays Ransom note

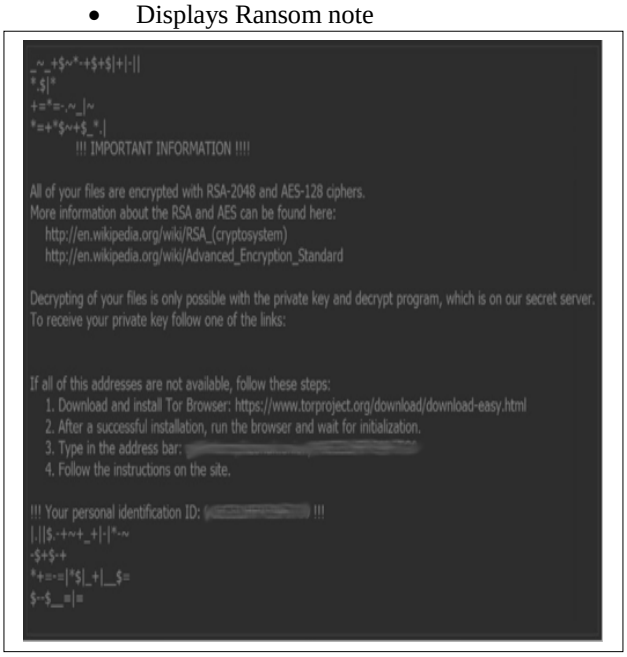

Fig 3: Encrypted Screen message of Locky Ransomware.

IV. PREVENTIVE MEASURES

- Due to human mistake, an infection begins by directly clicking on link or any email attachment and this opens the door for attackers [3]. So do not click directly without scanning the email.
- Word document can contain malicious macros, therefore it is advisable to disable macros [3].
- Disabling VSSVC.exe : It prevents from encrypting Volume Shadow copy which is the copy of the files which will be useful for recovery if any incident happens [3].
- Keep system and antivirus up to date [3].
- Restrict file permission in %TEMP% and %AppData% directories [3].
- Fragment your shares to reduce the impact of encryption [3].
- Backup your data regularly

V. INCIDENT RESPONSE AND COMPUTER FORENSIC FOR LOCKY RANSOMWARE

D. Incident Response

After the crime or incident happened there are various stages for incident response process [7].

- Preparation: We should be prepared to handle the incident right from detecting the malware to its resolution.
- Identification: Detection of the incident, its cause and type.
- Data collection and Analysis: Collecting the data for digital evidence and future use. Investigation to find the cause of the crime and the quantum of infection.
- Eradication: Removal of infection by cleanup of the system, which involves software as well as hardware cleanup.
- Recovery: Testing of the system and ensuring the service restoration.
- Resolution: Lesson learnt from the incident.
- Reporting: Making a report and case study for future use and taking preventive measures.

The incident response process for Locky Ransomware is performed with the help of computer forensics and email forensics. If system is infected by Locky Ransomware it displays the message as shown in fig 3. First, we need to disconnect the infected system from the network as well as devices which are connected to the system [3]. Second, we need to report the incident to CERT – Computer Emergency Response Team, so they can investigate the incident [3]. Third, we have to restore the files. No need to pay money for decrypting the data files because there is no guarantee of decryption even after paying the money [3].

E. Computer Forensics

If any incident is happened then it needs to be detected with proper investigation. Investigation for infected system, for finding evidence related to cyber-crime, is called as Computer Forensics. There are various tools which are used for incident response process like FTK imager, Encase, Pro-discover , etc. Forensic Toolkit Imager (FTK Imager) is one such freeware forensic tool which is used to perform computer forensic examination for reading, acquisition of physical and logical memory, decryption, analysis, and reporting of digital evidence [8]. ProDiscover is another commercial forensic tool which acquires the contents of physical memory, logical memory as well as system BIOS and also generates reports to document the digital evidence results [8]. Encase has additional search features such as EnScript commands, and string conditions which allow Encase to search data rapidly and efficiently [8].

F. Email Forensics

In Locky ransomware attacker sends email with malicious macro document attachment to victim. The attacker can spoof email-id for making trust for victim so he can easily click or download the file. Email crime investigation is nothing but Email forensics. For email forensic we can use the tool Mailxaminer [9] which is having lots of features. It scans the email and its attachment too. It can do Forensic Video analysis and examination with SHA-1 algorithm. It is purely used for email forensic. Mailxaminer [9] helps to find the email crime evidences like spoofed email id, IP address, header details, email hop view, etc. This tool is easy to handle. It is helpful in various infrastructures like small scale or large scale business, education, telecommunication, online shopping, healthcare, etc. so we can scan email and keep systems safe.

The tool has got Email view analysis and Attachment view analysis. The Email view analysis gives the properties of the email including the sender's details, sender's website, whether the message is encrypted etc. The Attachment view analysis provides the details of email attachment properties like attachment type, extension type, file name. In Attachment option, attached document is in the original form [9]. Fig.4 below shows a screen shot of the Mailxaminer tool.

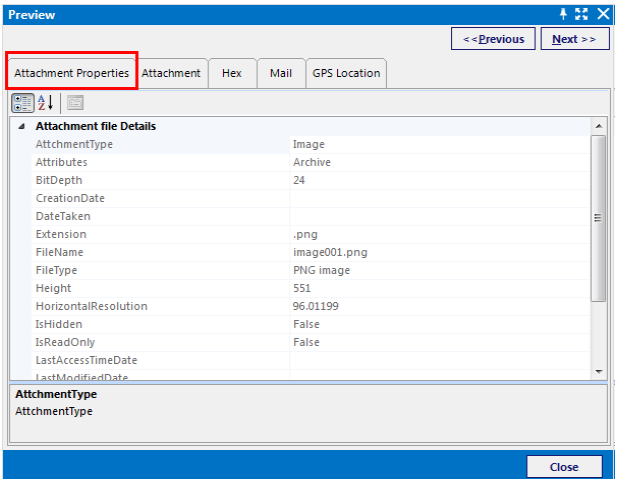

Fig 4: View analysis of attachment of email by Mailxaminer.

VI. CONCLUSION

Locky Ransomware is the malware type which easily passes through email attachment in the form of word document. Simple word document can be very dangerous which may encrypt victim's data file, locks it and ask for ransom. We have seen how Locky Ransomware works when we enable macros and what happens when the system is infected. The preventive measures discussed in this paper can be followed to keep the attacker at bay. With the help of preventive measures we can avoid this type of malware threats. Scanning of email and its attachment is the best remedy. Prevention from the Locky Ransomware is possible by using email forensic tool like Mailxaminer, which is helpful for scanning of email as well as email attachments. Incident response and computer forensics for Locky ransomware, described above, helps to recover the compromised system from the loss and preparing the organization in preventing the future attacks.

VII. REFERENCES

[1] Vinit Kumar Gunjan; Amit Kumar; Sharda Avdhanam, " A survey of cyber crime in India," 2013 15th International Conference on Advanced Computing Technologies (ICACT),2013.

[2] Dr.P.B.Pathak, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge," International Journal of

Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 Issue 2, February 2016.
[3] TLP: WHITE, Authour : CERT.be, Ransomware Whitepaper.
[4] https://www.pcrisk.com/removal-guides/9807-locky-ransomware
[5] Gagneja. Kanwalinderjit K, "Knowing the ransomware and building defense against it - specific to healthcare institutes," Third International Conference on Mobile and Secure Services (MobiSecServ),2017
[6] https://wikipedia.org/wiki/bitcoin
[7] https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103
[8] Leonardo Carvajal; Cihan Varol; Lei Chen, "Tools for collecting volatile data: A survey study," The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), IEEE Conference Publications,2013.
[9] https://www.mailxaminer.com