Detecting and Preventing LOCKY Attack by Hillstone in GFW and Emsisoft Antimalware

N. Krithika
Sri Ramakrishna Engineering College
Coimbatore, India

Abstract **- Currently, Threats and attack methods are common in the cyber security. Email is a technology for exchanging the information between people. The virus propagated into the email and causes great loss. There are various attacks in Email, Recently an attack called LOCKY emerges. This paper deal with detecting and preventing the LOCKY attack and investigate some of the removal technique.**

Index terms - CRYPTO WALL, EMSISOFT ANTIMALWARE, HILLSTONE INGFW, SHADOW COPY

I. INTRODUCTION

Email is a fast and asynchronous communication channel that is to be used for various purposes. Communication in email is of type formal and informal communication. As the technologies grow faster and faster, the same is also true for cyber crime. Email is used by criminals for illegal purposes and with intension to steal money from the user [18]. LOCKY is malware which was emerging in the year 2016 [25]. It is forwarded by the email that has an invoice which is attached to the Microsoft word document. Whenever user opens the document, it appears as garbage in that phrases pop up to the user saying that enable the macro if the data encoding is incorrect. It is one of the social engineering techniques. When the user enables the macro, macros save and run binary file that actually download the encryption Trojan which will encrypt all the files that matches the particular extensions [15]. With .LOCKY as an extension, Files names are transform to a unique 16 letters with number combinations. Message will appear to the user after encryption shows that download the Tor browser and visit the specific websites which is belong to the criminal's page.

The website contains the instructions that demand a payment of between 0.5 to 1 bit coins [25, 15]. Because criminals posses a private key and the remote private key and the remote are controlled by them. The victim can't be rectified easily if we want the decrypt the file, the user has to pay for it. These Ransom wares are distributed in the form of exploit kits, word, excel attachments with malicious macros, doc attachment and zipped js attachments. [5]The attached email looks like Dear (random name); Kindly, find the attached invoice for services in the mentioned matter hope this will be useful; sincerely; (random name title);

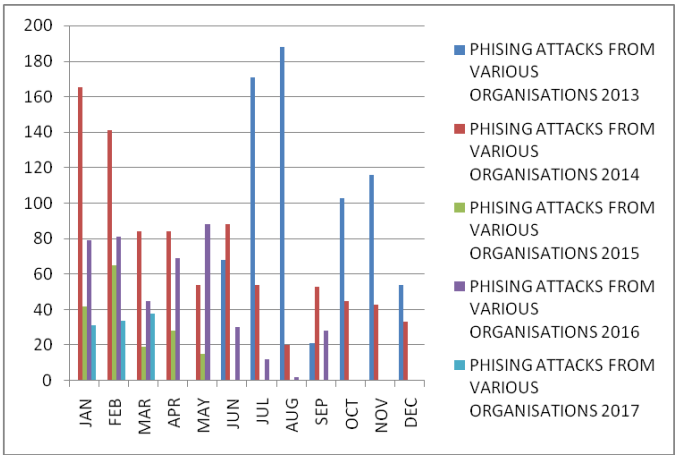

FIG 1: VARIOUS PHISHING ATTACKS FROM 2013 TO 2017

II. CURRENT LIST OF RELATED MALWARE

Identifying original file is difficult because all the files are encrypted using RSA – 2048, AES - 1024. Websites of Criminals contains step by step process [5]. To process with the payment process, Victim install Tor browser & follow the link. This virus deletes all the files shadow volume copies. Similarly to LOCKY they are various ransom ware they are [5] crypto wall, job crypt, umber crypt, Testla crypt, DMA Locker.

1. Crypto wall

It is one of the ransom ware that infects the user operating system via infected email messages & fake downloads [19]. After entered into the PC and program encrypts the files stored inside the pc and demands a payment of $500.

2. Job crypt

This malware uses the system to infect various files by using the decrypting methodology[20].The main targets of the JOB CRYPT attacks are Pc users from France where they added a.locked /.ces extension to every encrypted files. To unlock this files, users has to pay.

3. Umber crypt

It is a ransom ware that encrypt the file format such as [21] .jpeg and .doc by adding an "umber crypt-ID-your unique ID" to each affected file. After encryption, popup appears by saying users are given F2 has to buy decryption software.

4. Testla Crypt

It is malicious programs that encrypt the user file using AES encryption [23]. There are occur 40 different video

games targeted by testla which includes mine craft, star craft, Dragon Age, Steem, RPG maker.

5. DMA Locker

It is a type of side channel attack in computer security. [26] DMA locker steals the data by penetrate into the compiler of the system using ports that only permit Direct Memory Access.

III. HOW THE LOCKY RANSOM WARE ENCRYPT YOUR FILE

After which LOCKY installed on to the system, it will first check the default language in pc is Russian [8], if not it will encrypt the data. By using C&C server (command & control) that under the LOCKY criminals control and send ID associated victim infection. Thus ID contains MD5 hash which is of 16 characters GUID for storage volume. After the ID is send to the criminals website, LOCKY will reply with RSA key that mainly used for encryption process.

[8]Now LOCKY creates window registry key and scan for the local, mapped and unmapped network shares for file types that target for encryption. AES encryption key is generated after the file is encrypted. [8]Thus AES encryption key is then further encrypted by RSA key that already retrieved from C&C server. This RSA key will be now stored in the encrypted file.

The encrypted files are renamed to different formats based on the version of LOCKY. To encrypt the files LOCKY uses variant version named .OSIRIS [13]. The variant extension used by LOCKY for encrypted files is .OSIRIS [13, 11].

OPERATION

LOCKY is a virus that attach to an email with Microsoft word doc, which has a malicious code in it. The document is in the form of gibberish language that prompts the user to enable macros to view the entire document user mistakenly or without intension enable the macros and open the document. This loop hole provides the virus enter into the system memory. Once the LOCKY virus entered into the system it piles into the memory of the system and encrypts the document as hash, LOCKY files and installs .bmb files. LOCKY malware encrypted some of the network files which are of user access. After the files are encrypted [24] LOCKY create an additional .txt and -HELP- instructions. .html files in every folder that holds the encrypted files. Moreover this virus changes the desktop wallpaper. Decrypts are used by the cyber criminals to decrypt the files. For that hacker, demands the cost about .5 bit coin which is equivalent to $207.63. Only way, to avoid being payed is to restore files from backup.

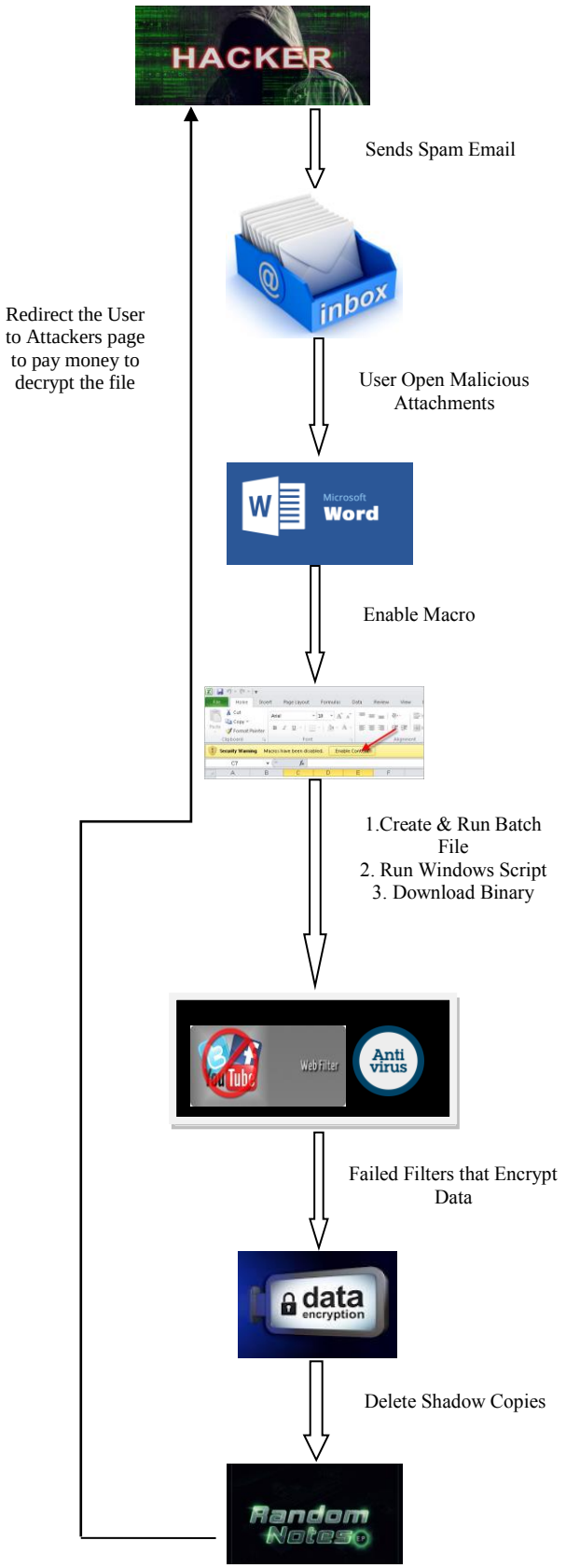

FIG 1: OPERATIONS OF LOCKY ATTACK

IV. WHAT SHOULD DO AFTER DISCOVERING THE COMPUTER WITH LOCKY VIRUS

If we see any infection in computer shut down immediately by creating a copy / image of our hard drive. If we don't plan to pay for the ransom, restore from backup then scan the pc with antimalware program or antivirus.

A. RESTORING THE FILES ENCRYPTED BY LOCKY

These are the methods to restore the files encrypted from LOCKY.

METHOD 1:
BACKUP it allows to take back up all the files which are in pc.

METHOD 2: SHADOW COPY:
It is method that is used in Microsoft windows to take the copies either in manual or automatic form even when the file is in use. There are 2 methods in shadow copy they are native window features & second method is to use a program called shadow explorer.

1) USING NATIVE WINDOW

For restoring the individual files, Right click on the file, go into the properties and select the previous versions tab. Thus a tap opens showing the list of all copies of the file that have been stored in shadow volume copy and the data the last backup are shown.

To restore the particular version of the file. Click copy and select the directory where we wish to restore the file to if we wish to restore in the existing place. Click restore button the user wish to view the contents of actual file be clicking open button to see the contents file before restoring it. If we want to restore the entire folder right click on the folder, select properties & then click previous version tabs that have a list of copies of folder that already been backup.

2) USING SHADOW EXPLORER

Start the program by clicking shadow explorer icon. This will first list all the drives and the dates that a shadow copy was created already. Select the drive and date button that we wish to restore. To restore the whole folder, right click on a folder name and select export.

B. RESTORING THE ENCRYPTED FILES ON DROP BOX FOLDERS

Restore the file can be done using login to the drop box websites first and find the way to the folder which contains the encrypted files[10].Then from the folder right tick on the encrypted files and select previous. Then select the version of the file and click restore [10]. In order to restore many folders, user can use drop box restore python script.

V. PREVENTION TECHNIQUE AND MITIGATION MEASURES

LOCKY can be prevented by using three methods namely Emsisoft Anti Malware [27], Hitmanpro: alert [28] and Malware Bytes Anti Ransomware [12] & Hitmanpro: alert programs.

A. EMSISOFT ANTIMALWARE:

[12] EAM uses the blocker that stop the behavior of certain files which has a tracking method for blocking the Ransomware, before it encrypts the data. Behavior blocker in EAM has the ability to find the malware easily

B. HITMANPRO: ALERT

It is one of the anti exploit program. It doesn't target at infections rather it provide an alert to the computers for protection against vulnerabilities [28].

C. MALWAREBYTES ANTI RANSOMWARE:

It doesn’t rely on signature/ heuristic rather by behavior. Similar to EAM configure application.

WHITELISTING:

It is a very secure method for preventing the ransom ware. This method all the executables are denied except the user permit to run. Security policy editor is necessary to run certain applications [9]. To do this, type secpol.msc in the search tab and after it opens tap on the local security policy editor. Now popup appears where we need to click on the software restrictions policy. Policy has to be created already, if the user didn’t created create a new one by right clicking on the restriction policy category and select new [9]. After creating new policy configure, the enforcement section. Now configure what file types will need to be blocked. This can be done by clicking designated file types, open the properties and click on the unknown file extensions then remove them. Now go back to restriction policy and configure the different policy that decides already created file types are automatically that decides already created file types are automatically blocked or allowed to run. To do this double on click security levels that has 3 security levels namely Disallowed, Basic user, Unrestricted. In order to select which level we need to double click on the particular level and set as default.

1. Disallowed:
Regardless of access rights of user all the programs are allowed except the certain file types.

2. Basic User:
All programs are executed as normal user rather than admin.

3. Unrestricted:

All programs run as normal. After the user select which mode wants click default and set ok. Now almost every program is blocked from executing without user permission. To check this click on the particular program in PC and run in browser. This file can't ne run because this program is blocked before group policy.

MITIGATION MEASURES

Back up regularly and keep recent backup copy offsets. [22]Don't enable the macro to document attachments that receive via email. [16] Cautions about unsolited attachments. Don't give more power for login without the user permission. Install Microsoft office viewers. Patch often and early.

REMOVING THE LOCKY

Some of steps will lead to remove LOCKY virus. Reboot the PC, Bookmark the later reference is taken as a first preference for removing the LOCKY [7]. Next way to remove LOCKY by carefully removes it or it will damage the system. This can be done by pressing [24] shift + ctrl + esc at the same time and go to the process, check what are the process causing damage. Right click on the process which are dangerous and open the location. Scan for online scanner and scan the files, if we found any infection delete it. [6]Now press start and R-COPY + Paste then click ok [17]. A new file open up that has a bunch of IP connected at the end of the word/ notepad. To know the files are being hacked, enter msconfig in search tab and press ok. Which opens an window go to that press startup and uncheck the entries that have unknown as manufacturer [2] Type regredit in search tab and click ok. Now press ctrl +F at same time to type the name of the malware and search for the virus in the registry and delete if found. Search for the files like [15]%App date%, %Local App Data%, %program Data%, %windir%, %Temp% and delete it. Now decrypt the malware files.

DETECTING THE LOCKY VIRUS WITH HILLSTONE INGFW

Detecting the LOCKY is done by using Hill stone which is one of the next generation firewall [3]. It includes the following mechanism they are Antivirus engine, Reputation engine, Domain generation Algorithm detection engine, Threat intelligence correlation module, cloud intelligent system.

ANTIVIRUS ENGINE

LOCKY email spam's are easily found out by using this method where it uses pattern match that displays the malicious attachment easily even if the files are hidden [3].

REPUTATION ENGINE

This engine has databases which are of IP and domain name reputation. [3] It has a set of known, releative malicious IP and domain names.

DOMAIN GENERATION ALGORITHM DETECTION ENGINE (DGA)

It detects DGA [3] domain names that are used as the C & C server.

THREAT INTELLIGENCE CORRELATION MODULE (TICM)

It correlates different threats events.

CLOUD INTELLIGENT SYSTEM (CIS)

It performs threat analysis/suspicious threat events.

SHOW HIDDEN FILES

IN WINDOWS 7:

Click start button, [1] type control panel in run box and select the particular files and folders then press view tab. From the advanced settings click on the show hidden folders/files.

IN WINDOWS 8/10:

Open the view tab and mark hidden items option and click apply then click ok button [1].

VI. CONCLUSION

Email threat is presently a problem in cyber security. This paper, presents the deep survey of LOCKY attack what are the root causes? How to detect and remove them in future? This paper also explains the preventive mechanism. Follow the security measures and awareness to avoid this attack in future. By creating awareness, enterprises wide and regular threat testing technique tools like Data Breach Response Toolkit (DBRT) by Global Digital Forencies (GDF) is needed to avoid the attacks in future.

REFERENCES

1) Alex Dimchev, http://bestsecuritysearch.com/thor-locky-ransomware-virus/, October 25, 2016.
2) Cammy Harbison, http://www.idigitaltimes.com/new-locky-ransomware-virus-spreading-alarming-rate-can-malware-be-removed-and-files-512956, 02/19/2016
3) Cheng,http://www.thetechrevolutionist.com/2016/05/detection-of-locky-ransomware with.html, May 04, 2016
4) Chona Esjay, https://malwarefixes.com/ remove-locky-ransomware-and-decrypt files/,August 21, 2016
5) Hasherezade, https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/, March 1, 2016.
6) Jake Doe, http://www.2spyware.com/remove-locky-virus.html, 2017-02-20
7) Lawrence Abrams, https://www.bleepingcomputer.com/virus-removal/locky ransomware-information-help, May 9, 2016
8) Lawrence Abrams, https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help#locky-encryption, May 9, 2016
9) Lawrence Abrams, https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/, May 9, 2016

10) Lawrence Abrams, https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help#dropbox-folder, May 9, 2016
11) Lawrence Abrams, https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/, December 5, 2016
12) Malwarebytes, https://www.bleepingcomputer.com/download/malwarebytes-anti-ransomware/, 09/16/16.
13) Martin Beltov, http://bestsecuritysearch.com/osiris-locky-ransomware-virus-removal-steps-protection-updates/, December 5, 2016
14) Nathan Bookshire, https://howtoremove.guide/locky-virus-ransomware-file-removal/, April 2017
15) Olivia Morelli, http://www.2spyware.com/remove-locky-ransomware.html, 2016-11-03
16) Paul Ducklin, https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/, 17 Feb 2016
17) Stelian Pilici, https://malwaretips.com/blogs/remove-zzzzz-files-encrypted/, November 24, 2016.
18) Sarwat Nizamani and Nasrullah Memon, "CEAI: CCM-based email authorship identification model", 29 October 2013.
19) Tomas Meskauskas, https://www.pcrisk.com/removal-guides/7844-cryptowall-virus,13 January 2016
20) Tomas Meskauskas, https://www.pcrisk.com/removal-guides/9796-jobcrypter-ransomware, 05 February 2017
21) Tomas Meskauskas, https://www.pcrisk.com/removal-guides/9795-umbrecrypt-ransomware, 12 February 2016
22) Threat Intelligence Team, https://blog.avast.com/a-closer-look-at-the-locky-ransomware,10 March 2016
23) Tomas Meskauskas, https://www.pcrisk.com/removal-guides/8724-teslacrypt-virus, May 19, 2016
24) Tomas Meskauskas, https://www.pcrisk.com/removal-guides/9807-locky-ransomware#a2, October 25, 2016.
25) https://en.wikipedia.org/wiki/Locky
26) https://en.wikipedia.org/wiki/DMA_attack
27) https://www.emsisoft.com/en/software/antimalware/
28) http://www.surfright.nl/en/alert
29) https://keonesoftware.com/guides/locky-virus/
30) http://myspybot.com/decrypt-locky-files/