IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

Comprehensive Analysis and Forensic Recovery of Vipasana Ransomware

Francis Byabazaire[1*], Parag H. Rughani[2]

[1]Institue of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India
[2]Institue of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India

[*]*Corresponding Author: frankb0178@gmail.com*

Available online at: www.ijcseonline.org

Received: 16/Mar/2018, Revised: 24/Mar/2018, Accepted: 18/Apr/2018, Published: 30/Apr/2018

***Abstract*—** Ransomware is a malware that either encrypts files with specific extension on the system or locks the user out of the system demanding for the ransom in exchange of decryption key. The approach used here is to assess numerous aspects of ransomware so as to comprehend different techniques utilized by it. Ransomware has rapidly affected individuals, public and private organizations across the globe. This occurs due to system flaws and lack of recovery mechanisms. The challenging part is to recover vital data from the encrypted files. This has created severe security issues to companies of all sizes as several have lost valuable data and business proprietary information. Considering the above information, this research paper aims at examining the characteristics of a Microsoft Windows-based ransomware and potential recovery of encrypted files from the ransomware affected system. The sample was examined in an isolated environment using static and dynamic analysis techniques with open source tools. The results were encouraging as we were able to recover encrypted files with specific extensions.

***Keywords*—** Vipasana Ransomware, Ransomware Forensics, Ransomware Analysis, Offline Ransomware, Static Analysis, Dynamic Analysis.

I. INTRODUCTION

Ransomware is one of the widest spread and damaging cyber threats faced by the world today. Different types of malware were designed to achieve different objectives such as disruption, modification, data theft, deletion of files or services and terrorist attacks. In all these cases, malware writers' goal is to receive a reward in form of financial benefits or money in different forms like digital currency. Ransomware is not a new type of malware, it has been around for more than two decades, but during the last 3 years, there has been a huge increase of infections which targeted almost every system it could reach and compromise.

According to statistics, more than 140 million new malware samples were discovered in 2015 and a large portion was ransomware. Many new ransomware variants emerged in first quarter of 2017 as represented in the graph (Fig 1).

The study aims at analyzing Vipasana, the well-known Windows based Ransomware. An attempt had been made to ensemble integrative analysis of ransomware variants functionality. This research work contributes to recovery of user encrypted files using forensic methods and tools without paying the ransom to cyber criminals.

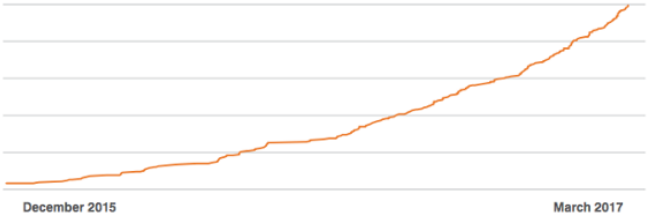

Figure 1: Growth in ransomware variants since Dec'15-Mar'17
Source: https://blog.barkly.com/ransomware-statistics-2017

This research paper aims at analysing one of the known Windows based ransomware namely Vipasana. The work carried out during the study is aimed at providing a detailed analysis of the functioning of the sample – a variant of a ransomware. This research contributes to the society by helping forensic investigators to recover important user data encrypted by Vipasana ransomware.

II. RELATED WORK

This section deals with the work carried out by researchers on different aspects of malware forensics.

The extent of the damage caused by ransomware attack is in high range at present. It is suggested that ransomware and

similar cyber-criminal activities affect end users for digital extortion at a scale never seen before [1].

As reported by Ali et al. American Bankers Association estimated $18 million loss to ransomware attacks for individuals and businesses and Cyber Threat Alliance reported that, 7.1 million attempted infections spread across the globe between 2015 to June 2016. The peak of one day of ransomware hit reached 228,496 [2].

Noted that the number of ransomware attacks were doubled in the past twelve months compared to a year earlier and predicted that it will double again the following year. The author explained that ransomware is precise in selecting targets. For example, they select florist shops before Valentine's Day because they know the heavy traffic these shops experience in that period forces them to pay the ransom [3].

Kharraz et al. conducted a study noting that ransomware attacks increased by 500% in 2013 compared to the 2012. It further gsuggested that this malware infected around 250,000 computers including a police department that ended paying a ransom to decrypt their computers and return their data [4].

Literature reports related to ransomware forensics are discussed as they worked on ransomware detection techniques and proposed some mechanisms to detect the presence of ransomware [5-8]. The work on the comparative analysis of various ransomware variants has been carried out [9-11]. As wannacry created havoc recently, substantial work is published about it by various authors [12, 13]. On the other hand, different authors worked on different ransomware variants such as cryptowall, locky, IoT based ransomware and Manamecrypt [14-17]. There is minimal research on ransomware forensics though plenty of data is published on different aspects of malware forensics [18-20].

Despite tremendous progress in research on other variants of Ransomware, the work done on Vipasana ransomware has been dealt marginally. Owing to higher rate of damage caused by Vipasana in present scenario, it might hamper the economy. Therefore the present work was conducted to elucidate the recovery of user data affected by Vipasana ransomware.

III. METHODOLOGY

III.I. TOOLS AND ENVIRONMENTAL SETUP

A physical standalone machine running Windows 10 Operating System was set up as a target machine.
The target machine was isolated to prevent the sample from infecting the entire network. Static and dynamic analysis tools were installed for the analysis of the sample.

Few files with extensions **.doc, .ppt, .jpg, .mp4, .pdf, .PNG, .txt, .xls, .zip** were stored in the C drive of the target machine to analyze complete execution and satisfy core dependency of the sample.

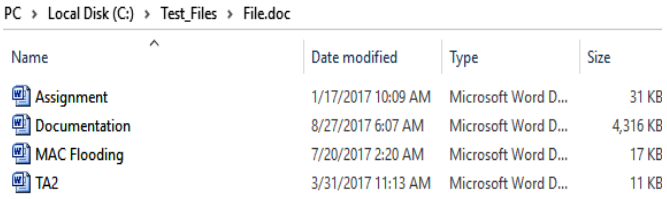

Figure 2: doc files

Figure 3: jpg files

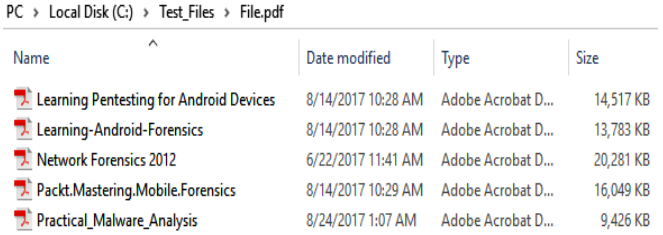

Figure 4: pdf files

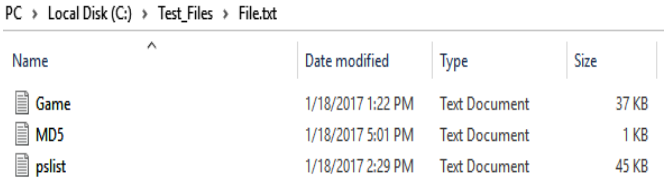

Figure 5: txt files

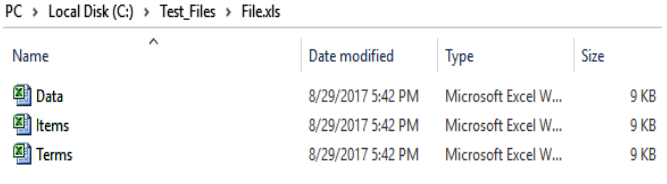

Figure 6: xls files

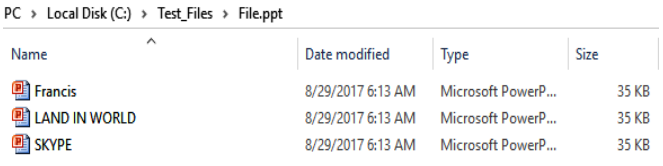

Figure 7: ppt files

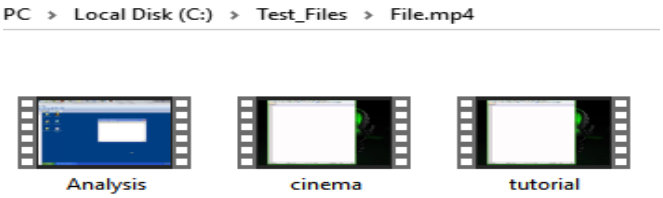

Figure 8: mp4 files

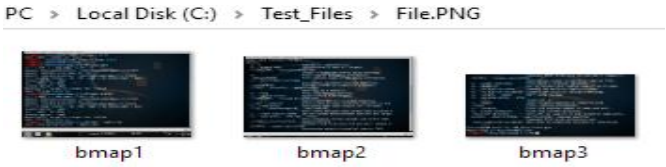

Figure 9: png files

III.II. INFECTING THE TARGET MACHINE

- The sample was copied to the target machine using a pen drive.
- Zip file containing sample was extracted on the desktop of the target machine.
- Static analysis of the sample was done**.**
- Windows security features like Windows defender, Windows firewall were disabled.
- The sample was then run by right clicking on the executable file.
- The machine was infected by the sample; files encrypted and desktop wallpaper changed with the infection details.

IV. RESULTS AND DISCUSSION

This section consists of the summary and report on the findings. It includes results of the analysis of data, presentation of findings and summary with interpretations on findings in relation to the sample.

IV.I. STATIC ANALYSIS

1) FileAlyzer tool

Using FileAlyzer, brief details about the sample were obtained as shown below:

MD5 : **2AEA3B217E6A3D08EF684594192CAFC8**
Size : **379392 bytes**
File Name : **1.exe**
File Type : **Portable Executable**
Last Write : **Thursday, February 18, 2016 2:44:22 AM**

Proof of concept:

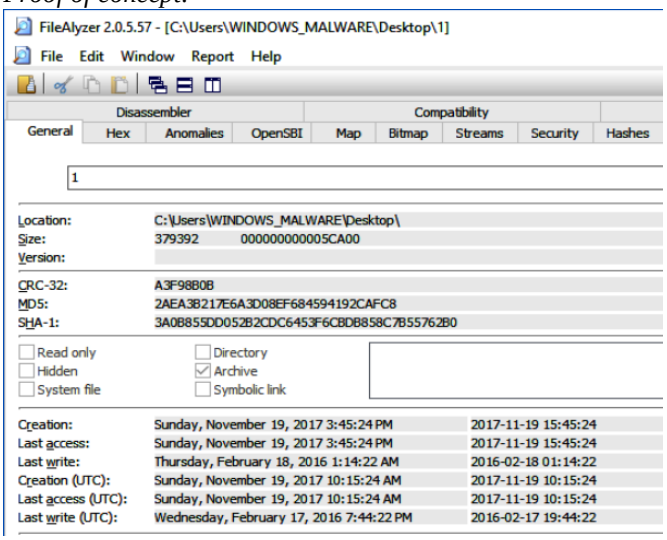

Figure 10: FileAlyzer

2) Dependency walker tool

List of DLLs imported: Details of Dynamic Link Libraries from where the sample imported functions were discovered.

Proof of concept:

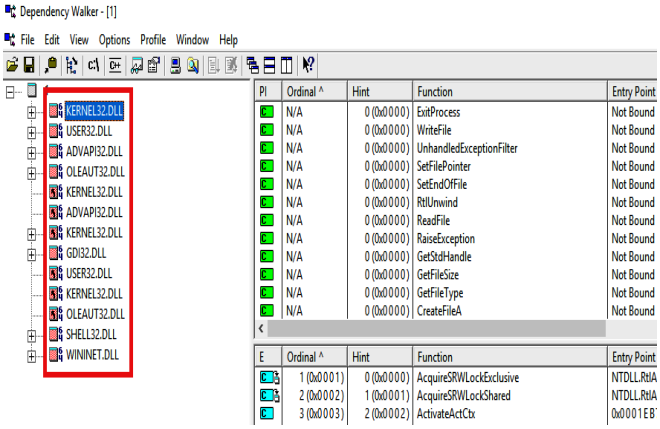

Figure 11: Dependency Walker - Imported DLLs

Some of the important function calls related to the sample being ransomware were observed as shown below:

a. GetLocalTime function

Contains ability to query machine time, this seems to be used by the sample to start the timer for the duration by which victim needs to pay the money or ransom.

Proof of concept:

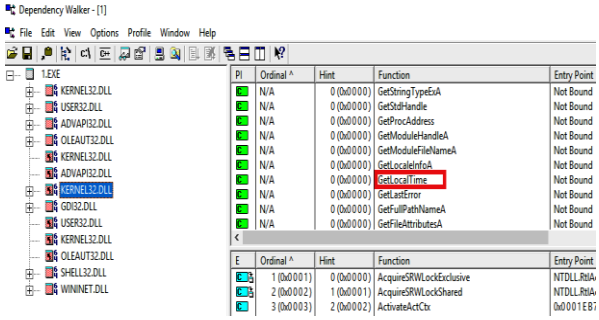

Figure 12: Dependency Walker-GetLocalTime

b. GetVersionExA function

The sample contains ability to query the machine version which is a basic requirement for any malware. Sample retrieves information about which version of Windows is currently running on victim machine; this can be used as part of a victim's machine survey.

Proof of concept:

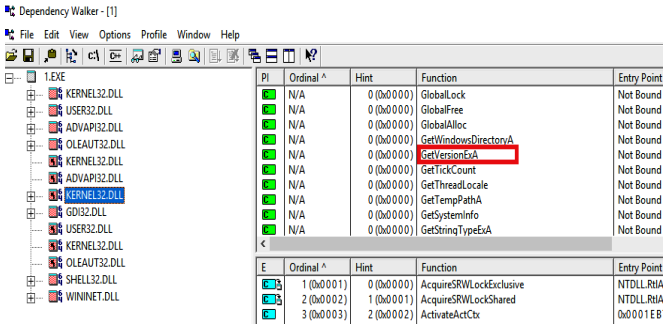

Figure 13: Dependency Walker-GetVersionExA

c. GetDiskFreeSpaceA function

The sample contains ability to query volume size of the victim's machine.

Proof of concept:

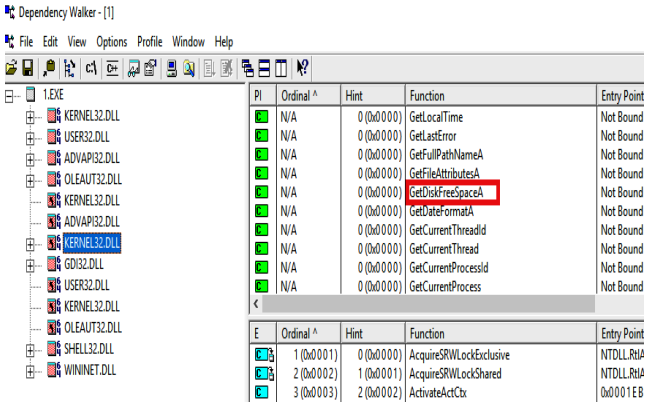

Figure 14: Dependency Walker-GetDiskFreeSpaceA

d. WININET.DLL

Contains ability to read and download files from the Internet**.** The sample possibly once connected to internet communicates with command and control server for key exchange.

Proof of concept:

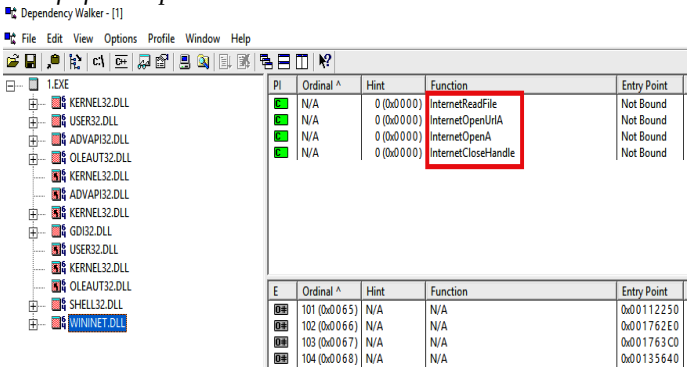

Figure 15: Dependency Walker-WININET

3) Virus Total tool

The sample was then uploaded to Virus Total and was identified as malicious by a large number of antivirus engines. The antivirus engines identified the sample as Vipasana.

Proof of concept:

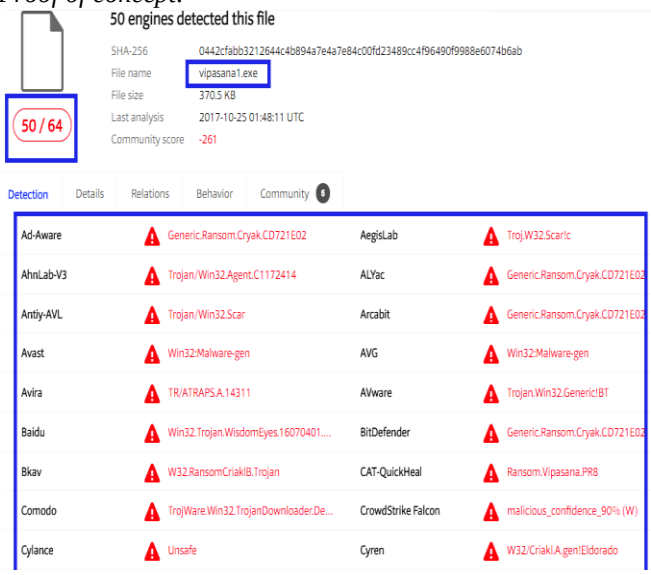

Figure 16: Virus Total

4) Resource Hacker tool

Resource hacker clearly displayed desktop wallpaper image with a ransom note suspected to appear after target machine gets infected.

Proof of concept:

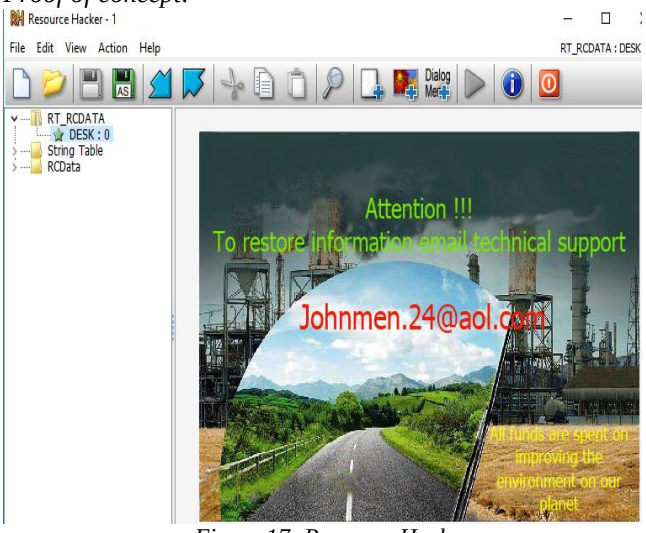

Figure 17: Resource Hacker

IV.II. Dynamic Analysis

Static analysis of the sample discovered many important details and evidences of the sample being a ransomware, but the dynamic analysis is required to get more concrete information on the same. On the other hand as the paper aims at recovery using forensic techniques, the sample needs to be executed. In this part of the experiment, the sample was executed in an isolated machine as mentioned earlier and observations were made.

1. Process Monitor

The sample, upon execution copied itself in the Program Files directory of the target machine.

Proof of concept:

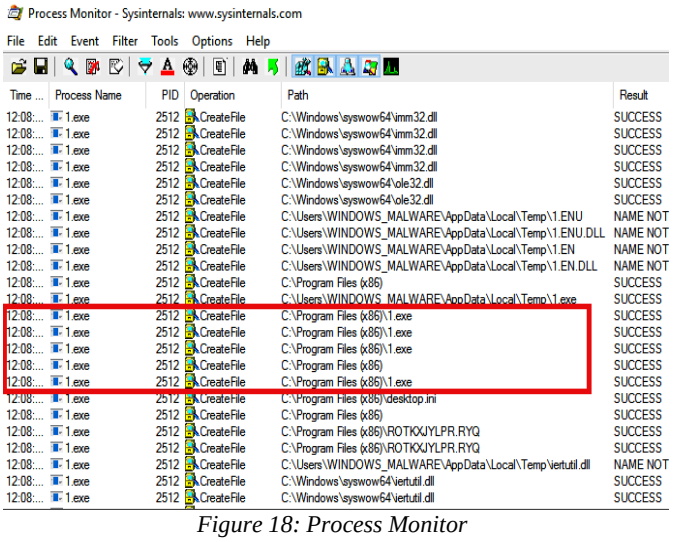

Figure 18: Process Monitor

2. Reshot tool

The first shot was taken before running the sample on the target machine and the second shot was taken after the sample was executed. The result showed that a malicious Run key to the registry was added by the sample.

Proof of concept:

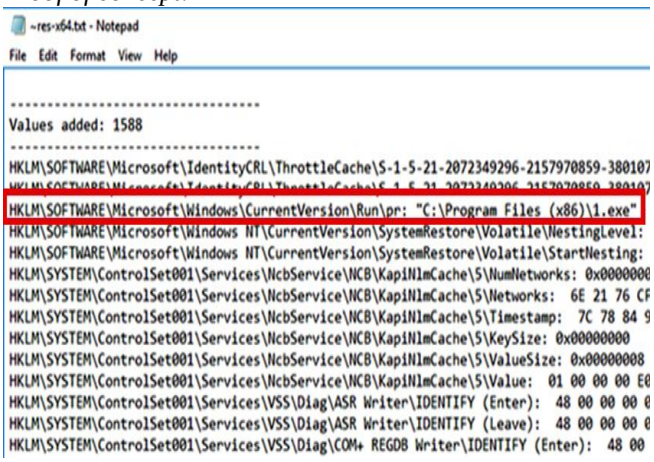

Figure 19: RegShot

3. ApateDNS tool

The sample made no relevant DNS request. Implying that it is an **offline** Ransomware; sample does not require internet in order to carry out its malicious activities on the victim's machine.

Proof of concept:

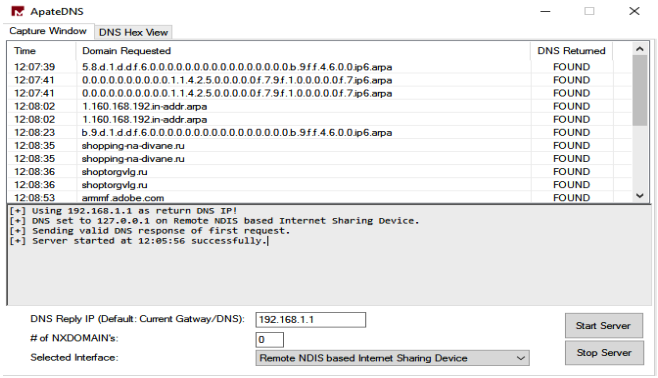

Figure 20: ApateDNS

4. WireShark tool

No relevant hosts were contacted; no relevant HTTP requests were made. No communication between the sample and any external server like command & control were requested. This further confirms that the sample is an offline Ransomware and does not get the keys from any Command and Control server.

Proof of concept:

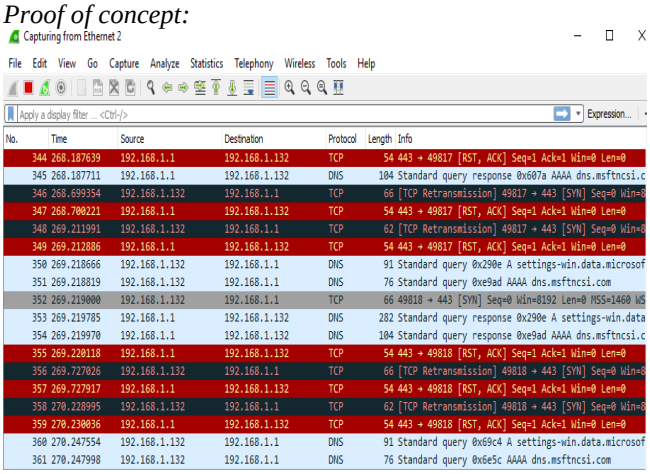

Figure 21: WireShark

Status of Desktop after infection of the machine

Figure 22: Desktop status before infection

Status of Desktop after infection of the machine

After the sample was executed on the target machine, the desktop wallpaper was changed with a ransom message on it.

Proof of concept:

Figure 23: Desktop status after infection

As mentioned earlier, the test data used in this research was encrypted by the sample as shown in screenshots below.

Proof of concept:

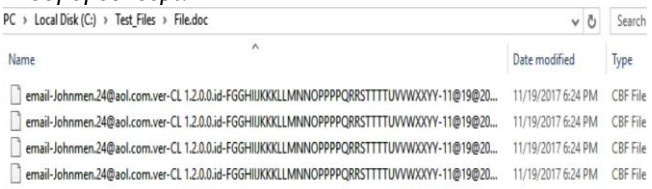

Figure 24: Encrypted doc files

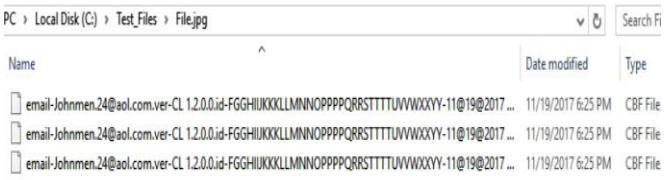

Figure 25: Encrypted jpg files

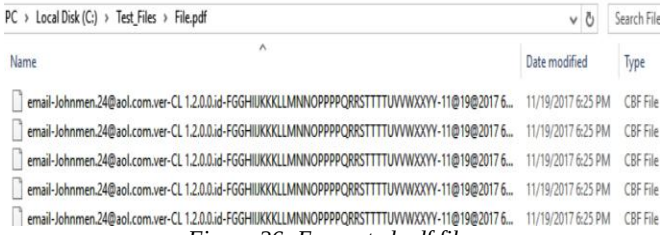

Figure 26: Encrypted pdf files

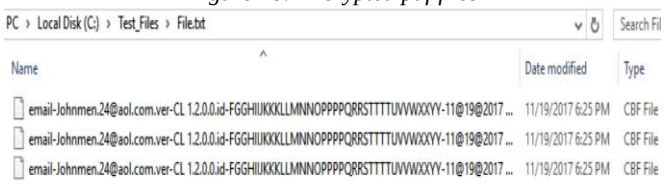

Figure 27: Encrypted txt files

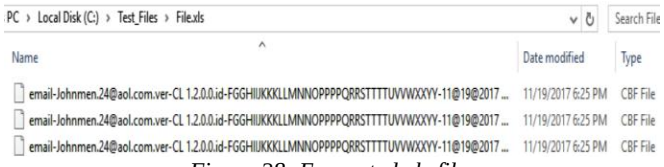

Figure 28: Encrypted xls files

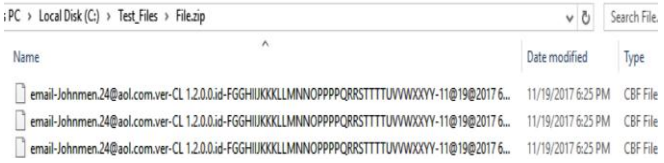

Figure 29: Encrypted zip files

IV. FORENSIC RECOVERY

The hard disk image of the infected machine was acquired using Forensic Falcon. Then Sleuthkit Autopsy was used to analyze the image. Following are a couple of important

reasons behind selecting autopsy for analysis compared to other tools:

1. EnCase does not allow loading evidences having malicious files.
2. Autopsy is Open Source and the latest version of it is equally powerful and user-friendly.

Proof of concept:

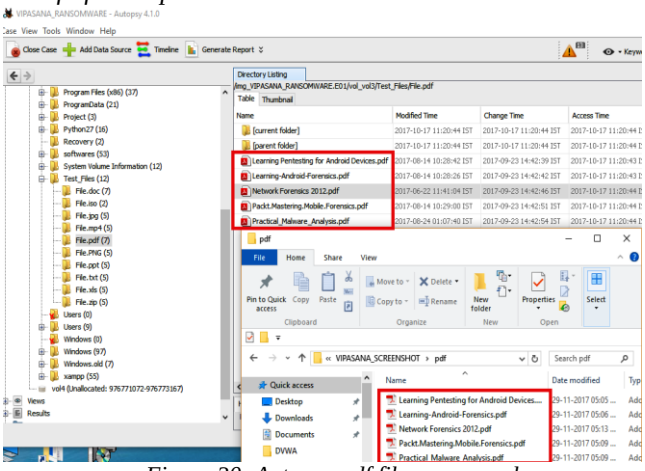

Figure 30: Autopsy-pdf files recovered

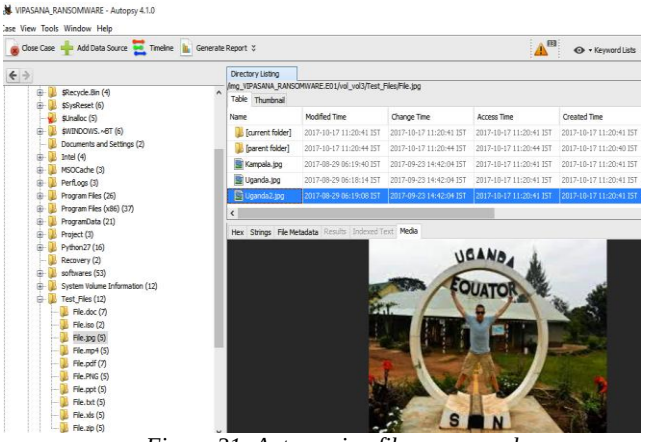

Figure 31: Autopsy-jpg files recovered

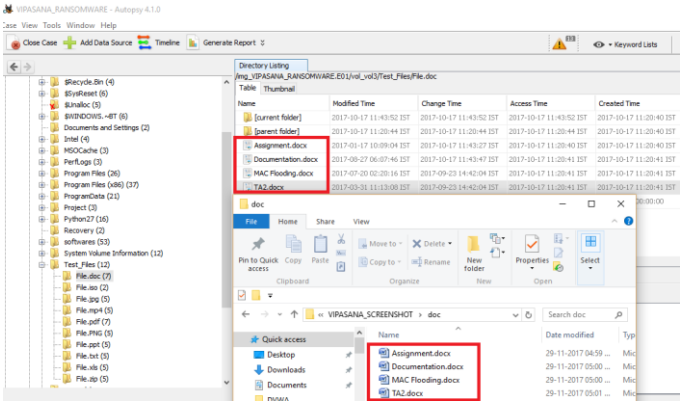

Figure 32: Autopsy-doc files recovered

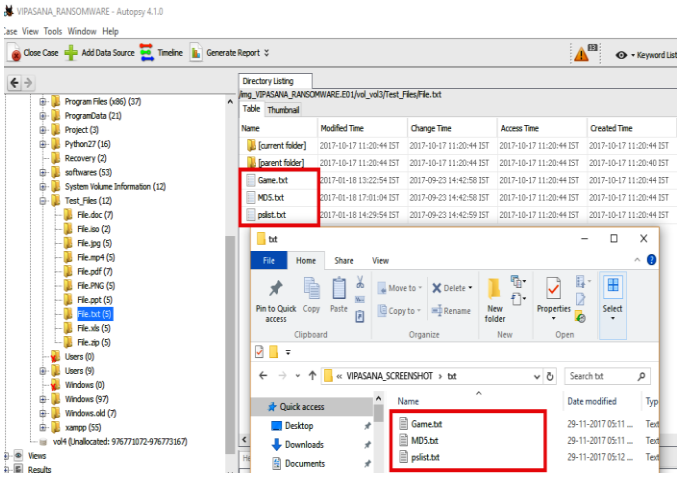

Figure 33: Autopsy-txt files recovered

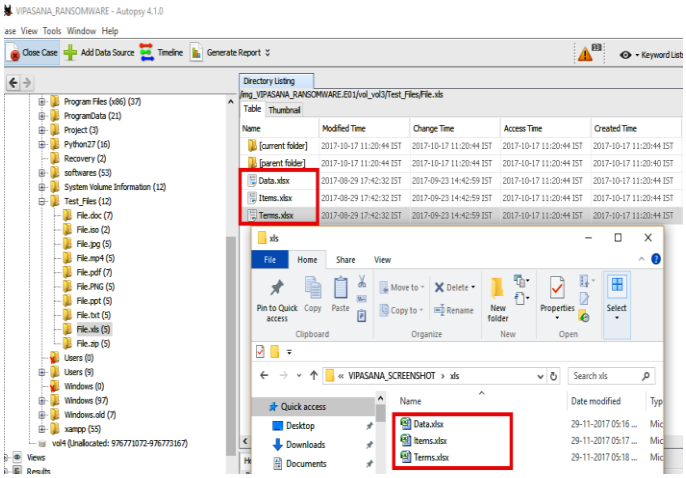

Figure 34: Autopsy-xls files recovered

In brief, during the analysis it was observed that the files encrypted by sample with extension **.doc, .ppt, .jpg, .pdf, .txt, .xls** were successfully recovered by autopsy. This was a big achievement as victims can rely on this uncommon technique to recover important documents without paying ransom to cyber criminals.

V. CONCLUSION AND FUTURE SCOPE

In conclusion, recovering files encrypted by the Ransomware is a great challenge to the Malware Analyst especially when the decryption key is not possible or difficult to identify. So, the present study demonstrated that digital forensic tools such as Autopsy can be used to recover user important files without paying a ransom.

On this basis, further studies can be implemented as: Reverse engineering the samples in order to obtain the decryption key, Analysis of the sample images using more Digital Forensics tools, Cuckoo Sandbox analysis technique,

Comprehensive RAM forensics analysis, Analysis and comparison of samples in bulk.

ACKNOWLEDGMENT

The authors are grateful to Dr. M.S. Dahiya, Director, Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, for providing the infrastructure and the facilities for the completion of the project.

REFERENCES

[1] A. Bhardwaj, V. Avasthi, H. Sastry, G. V. B. Subrahmanyam, "*Ransomware Digital Extortion: A Rising New Age Threat*", Indian Journal of Science and Technology, Vol.9, Issue.14, 2016.

[2] A. Ali, "*Ransomware: a research and a personal case study of dealing with this nasty malware",* Issues in Informing Science and Information Technology, Vol.14, pp.087-099, 2017.

[3] C. Everett, "*Ransomware: to Pay or Not to Pay?*" Computer Fraud & Security, Vol.2016, Issue.4, pp.8–12, 2016.

[4] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, "*Cutting the gordian knot: A look under the hood of ransomware attacks",* In: M. Almgren, V. Gulisano, F. Maggi (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, Springer, Cham, Vol.9148, pp. 3-24, 2015.

[5] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, "*Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence*", IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2017.

[6] E. Kirda, "*UNVEIL: a large-scale, automated approach to detecting ransomware (keynote)",* In Software Analysis, Evolution and Reengineering (SANER-2017) IEEE 24th International Conference, pp.1-1, 2017.

[7] K. Cabaj, M. Gregorczyk, W. Mazurczyk, "*Software-Defined Networking-Based Crypto Ransomware Detection Using HTTP Traffic Characteristics*", Computers & Electrical Engineering, Vol.66, pp.353–368, 2018.

[8] J. K. Lee, S. Y. Moon, J. H. Park, "*CloudRPS: a Cloud Analysis Based Enhanced Ransomware Prevention System*", The Journal of Supercomputing, Vol.73, Issue.7, pp.3065–3084, 2017.

[9] A. Gazet, "*Comparative Analysis of Various Ransomware Virii*", Journal in Computer Virology, Vol.6,Issue.1,pp.77–90, 2010.

[10] V. U. Bala, B.D.C.N.Prasad "*A Study on- Identifying and Evading Ransomware (Ransomware)*", SSRG International Journal of Computer Science and Engineering (SSRG - IJCSE), Vol.5, Issue.2,pp.9-13, 2018

[11] S. Mohurle, M. Patil, "*A brief study of wannacry threat: Ransomware attack 2017*", International Journal, Vol.8, Issue.5, pp.1938-1940, 2017.

[12] "*North Korea Blamed for WannaCry, PoS Attacks and Bitcoin Phishing*", Network Security, Vol.2018, Issue.1, pp.1-2, 2018.

[13] J. MacRae, V.N.L. Franqueira, "*On Locky Ransomware, Al Capone and Brexit,"* In: P. Matoušek, M. Schmiedecker (eds) Digital Forensics and Cyber Crime (ICDF2C 2017) Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Cham, Vol.216, pp.33-45, 2017.

[14] P. P. Kulkarni, T. Nafis, S.S. Biswas, "*Preventive Measures and Incident Response for Locky Ransomware*", International Journal of Advanced Research in Computer Science, Vol.8, Issue.5, 2017.

[15] A. Zahra, M.A. Shah "*IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting*", In proceeding of 23rd International Conference on Automation and Computing (ICAC- 2017), pp.1-6, 2017.

[16] S. Berkenkopf, "*Manamecrypt–a ransomware that takes a different route*", 2016. https://www.gdatasoftware.com/blog/2016/04/28234-manamecrypt-a-ransomware-that-takes-a-different-route.

[17] J. Li, D. Gu, Y. Luo, "*Android malware forensics: Reconstruction of malicious events",* In proceeding of 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW-2012), IEEE, pp.552-558, 2012.

[18] M. Brand, C. Valli, A. Woodward, "*Malware Forensics: Discovery of the Intent of Deception*", The Journal of Digital Forensics, Security and Law, Vol.5, Issue.4, pp.31, 2010.

[19] B. Ruttenberg, C. Miles, L. Kellogg, V. Notani, M. Howard, C. LeDoux, A. Lakhotia, Pfeffer, "*Identifying Shared Software Components to Support Malware Forensics*", In: S. Dietrich (eds) Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA-2014), Lecture Notes in Computer Science, Springer, Cham, Vol.8550 , pp.21–40, 2014.

[20] Z. Deng, D. Xu, X. Zhang, X. Jiang, "*Introlib: Efficient and transparent library call introspection for malware forensics*", Digital Investigation, Vol.9, pp.S13-S23, 2012.

Authors Profile

Mr. Francis Byabazaire pursed Bachelor of Science from Kyambogo University, Uganda. He is currently pursuing Msc. Digital Forensics and Information Security from Gujarat Forensic Sciences University, Gandhinagar, India. His research area of interest are Malware Analysis, Digital Forensics, Cyber Forensic Analysis, Vulnerability Assessment and Penetration Testing.

Dr. Parag H. Rughani completed his Ph. D. in computer science from Saurashtra University. He is currently working as an associate professor in Digital Forensics and Information Security at Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar since November, 2014. He has 12 years of teaching experience and has published more than 10 research papers in reputed international journals. His area of expertise include Digital Forensics, Memory Forensics, Android Forensics, Malware Analysis and IoT Security and Forensics.

