ISSN No:-2456-2165

Forensic Analysis of Ransomware Infected Windows Hard Disk: A Case Study

Sangita Biswas
Assistant Central Intelligence Officer Gr-1(Documents),
Central Forensic Science Laboratory, Kolkata, India

Kananbala Jena
Director & Scientist E,
Central Forensic Science Laboratory, Kolkata, India

Abstract:- Data in digital form is considered one of the most valuable assets. Digital data may pertain to financial transactions, trade secrets and national security matters. The threat of data theft and inaccessibility of important resources has always existed. Therefore, various protections were used since earlier days of computation. The protection may be physically locking the computer room or different options available for encryption and password protection, thus restricting number of users beyond designated persons. In recent past the emphasis has been growing on connecting digital asset to various networks and internet resources for updates and quick operational requirements. Releasing certain resources for public use is unavoidable for smooth functioning of business. Emails, downloads, remote access has become a way of life. Thus, in current scenario no protection can be called full proof and attackers find one or more vulnerabilities in system. One of the most preferable methods of such cyber attack is to hold owner of digital assets as hostage using ransomware. This intrusive software can quickly make changes to the system and restrict user access so that owner of the system is unable to access the data. Warnings may be flashed on the system to demand money in exchange of renewed access. Ransomware have recently claimed a place of prominence in computer security.

Reasonable amount of literature exists on incidence response to malware attack, dynamic analysis of malware and indicators of compromise of malware. However, how one can perform such malware analysis in a forensic laboratory is not well described. In the present paper the authors describe forensic artifacts discovered on examination of a hard disk infected with 'wannacry' ransomware following static digital forensic analysis method. During forensic examination it has been observed that artifacts recovered are not an exact match with artifacts described in available literature. Moreover, some additional artifacts could be found during forensic examination. During this examination authors tried to establish a guideline in general to examine cases involving malware, so that, security of the laboratory should not be compromised and loss of valuable resources can be prevented during forensic examination.

Keywords:- *Ransomware, Wannacry, Cryptoworm, Indicators of Compromise.*

I. INTRODUCTION

Malware (short for "malicious software") refers to any intrusive software developed by cybercriminals typically delivered over a network, that infects, explores, steals data, confidential or otherwise and use such information for profit or damage of computers and computer systems[1]. Malware comes in numerous variants; there are various methods to infect computer systems. Examples of common malware[1] include viruses, worms, Trojan viruses, spyware, adware, ransomware and fileless malware. Recent malware attacks have exfiltrated data in mass amounts.

Ransomware is generally a part of phishing scam. By clicking a disguised link, the user downloads the ransomware and the attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is promised to be unlocked. Whereas some ransomware e.g., WannaCry[2] ransomware is particularly dangerous cryptoworm because it propagates through a worm by exploiting vulnerabilities in the Windows operating system and it can spread automatically without victims participation. In May 2017, this cryptoworm demanded a ransom payment in bitcoin to decrypt the files. However, even after paying, only a handful of victims received decryption keys.

Out of different types of malwares this report emphasizes on the Digital Forensic Investigation of 'wannacry' ransomware infected Windows operating system using various open-source and licensed forensic tools and techniques. In this report authors discussed about forensic analysis of ransomware in a static manner so that analysts do not have to access the files in the infected disk but ICP's (Indicators of Compromise) can be revealed by using both open-source forensic tools and licensed forensic tools.

II. BRIEF CASE HISTORY

An independent business unit which supplies Telecom and Network Services complained they are unable to access their important files and unable to run some programs critical to their business. The investigation agency seized the hard disk of particular computer and submitted for Digital Forensic examination.

ISSN No:-2456-2165

It was suspected that this is sabotage due to some malicious software installed by an insider. However, no clues or keyword were forwarded from investigation side regarding type of malicious software or what kind of indications was seen during the attack.

III. MALWARE ANALYSIS

Finding traces of malicious activity in a computer seized from scene of crime remains challenging as most of the studies are based on RAM Dumps and other live traces when incident is still happening.

Sandboxing software generally proves how activities are done after execution of software in controlled environment. However, the leftover effects of the same on a specific system can be better proved on forensic analysis when live traces are almost non-existent. Therefore, some of the well-publicized ICP may not be present or may be present in a changed form. Moreover, additional ICP's may arise from the fact that malicious software has been modified at different times to evade newer version of antimalware.

Two basic techniques may be used for forensic analysis[3]:

- **Static Analysis**: In this method forensic analysis of malware binary is done without actually executing or downloading the files. This is a process of determining the origin of malicious files and by understanding the behavior of malware by analyzing the extracted indicators.
- **Dynamic Analysis**: In this method malware detection and analysis is done in a controlled environment[4] so that it doesn't affect other systems. This process uses behavior-based approach to determine the functionality of the malware by actually executing the malware in a controlled and isolated environment.

This report is based on static analysis method of malware detection and analysis.

IV. METHODOLOGY

- *Software and Hardware Used:*

Falcon Imager, Encase Version 8, Internet Evidence Finder Version 6, Regripper Software and Workstation.

- *Collection of Digital Evidence:*

Bit stream image of the hard disk is prepared using Falcon hardware Imager (fig.1) in E01 format. The image was duly verified by matching the acquisition MD5 hash value.

Fig 1:- FALCON Imager used for preparing bit stream image of infected hard disk

- *Analysis of Collected Digital Evidence:*

Bit stream image of the hard disk was loaded in licensed ENCASE software (ver. 8). Files in accordance with the date of complaint were previewed (fig.2).

Name	File Ext	Last Accessed	Entry Modified	File Created	Last Written
b.wnry	wnry	11/05/17 20:13:20	18/05/17 17:33:48	11/05/17 20:13:20	11/05/17 20:13:20
r.wnry	wnry	11/05/17 15:59:14	19/05/17 13:44:26	11/05/17 15:59:14	19/05/17 13:44:26
t.wnry	wnry	12/05/17 02:22:56	19/05/17 13:44:26	12/05/17 02:22:56	19/05/17 13:44:26
f.wnry	wnry	17/05/17 14:08:46	18/05/17 17:33:48	17/05/17 14:08:46	17/05/17 14:11:51
s.wnry	wnry	09/05/17 16:58:44	18/05/17 17:33:48	09/05/17 16:58:44	09/05/17 16:58:44
m_chinese (simplified).wnry	wnry	20/11/10 04:16:58	19/05/17 13:44:35	20/11/10 04:16:58	19/05/17 13:44:35
m_chinese (traditional).wnry	wnry	20/11/10 04:16:58	19/05/17 13:44:34	20/11/10 04:16:58	19/05/17 13:44:34
m_croatian.wnry	wnry	20/11/10 04:16:58	19/05/17 13:44:34	20/11/10 04:16:58	19/05/17 13:44:34
m_czech.wnry	wnry	20/11/10 04:16:58	19/05/17 13:44:34	20/11/10 04:16:58	19/05/17 13:44:34
m_danish.wnry	wnry	20/11/10 04:16:58	19/05/17 13:44:33	20/11/10 04:16:58	19/05/17 13:44:33

Fig 2:- Files present in the hard disk with 'wnry' extension around the date of complaint.

- *Techniques Used:*
- *Timeline Analysis:*

After filtering all the files around date of complaint numerous files with extensions 'wncry' were found. This 'wncry' extension followed another text in the filename which appeared as another extension recognisable by commonly used applications in Windows operating system such as 'jpg', 'xlsx', 'txt', 'doc' etc. (fig.3). Change of extension appeared to be immediate cause of files not opening using their familiar extension. However, the files could not be opened by changing extension to original one.

Name	File Ext	Last Accessed	Entry Modified	File Created	Last Written
linkfilter.png.WNCRY	WNCRY	24/06/16 13:52:01	17/05/17 14:34:14	24/06/16 13:52:01	07/03/14 14:31:26
linkfilter.png.WNCRY	WNCRY	07/03/14 14:31:26	17/05/17 14:34:22	07/03/14 14:31:26	07/03/14 14:31:26
link_join_text.jpg.WNCRY	WNCRY	21/07/15 11:46:21	17/05/17 14:33:30	21/07/15 11:46:21	11/02/15 20:15:02
COMPINST.DBF.WNCRY	WNCRY	27/03/14 12:09:32	17/05/17 14:16:23	27/03/14 12:09:32	01/01/02 00:30:02
COMPINST.DBF.WNCRY	WNCRY	27/03/14 11:59:40	17/05/17 14:27:08	27/03/14 11:59:40	01/01/02 00:30:02
COMPINST.DBF.WNCRY	WNCRY	25/03/14 17:25:33	17/05/17 14:33:32	23/12/13 13:08:27	26/03/14 16:53:24
line.jpg.WNCRY	WNCRY	10/07/15 12:27:25	17/05/17 14:37:26	10/07/15 12:27:25	28/02/14 16:33:52
line.jpg.WNCRY	WNCRY	21/07/15 11:46:20	17/05/17 14:37:27	21/07/15 11:46:20	28/02/14 16:33:52
Lighthouse.jpg.WNCRY	WNCRY	14/07/09 10:22:25	17/05/17 14:33:31	14/07/09 10:22:31	14/07/09 10:22:25
LIFE CERTIFICATE.pdf.WNCRY	WNCRY	13/04/17 15:00:24	17/05/17 14:26:10	13/04/17 15:00:24	13/04/17 14:59:50
Please find the enclose.docx.WNCRY	WNCRY	24/10/16 17:16:53	17/05/17 14:26:08	17/10/16 14:07:12	17/10/16 14:13:57

Fig 3:- Files with commonly recognisable extensions 'jpg', 'pdf', 'xlsx' etc. followed by 'wncry' extension modified on 17.05.2017

- *Analysis by Extensions:*

All the extension starting from 'wnry' was enlisted. It is found that extensions 'wnry', 'wncry', 'wncryt' are available around the suspected timeline.

Some files with 'exe' extension were also found with name 'WanaDecryptor@.exe' and was executed several times between 17.05.2017 to 20.05.2017 fig.4.

Fig 4:- Execution of 'WanaDecryptor@.exe' within suspected timeline.

- *Litreature Review:*

On the basis of above observations, we followed some literature and articles which indicated a ransomware called 'wannacry' is available and attack on various system were worldwide reported during the same timeline[5]. Indicators of compromise were also reported in various attacks.

- *Registry Forensics:*

NTUSER.DAT is a file that is available in Windows operating system and it stores the information of the user account settings and customizations. Each user has their own NTUSER.DAT[6] file in their user's profile in hidden form in the path '*C:\Users\Username'*. This file ensures that any changes made in user account are saved. This DAT file was extracted from the E01 image loaded in Encase and analysed using Regripper (open-source) forensic registry analysis software.

V. OBSERVATIONS

- Files named 'b.wnry', 'c.wnry', 'r.wnry', 's.wnry', 't.wnry', 'u.wnry', 'f.wnry', 'taskdl.exe', 'taskse.exe' and 'tasksche.exe' could be found which are also available in literature**[7, 8].**
- Hash values of the files may differ from one instance to other as observed from literature. In this case also some of the hash values were different and others matched with some of the reported cases.
- The hash values of b.wnry, s.wnry, could be verified as malicious by virustotal[9], however, other hash values could not be verified as malicious. Details of MD5 hash values as found in this case are provided in the following table:

Files	MD5 HASH VALUES found in case
b.wnry	c17170262312f3be7027bc2ca825bf0c
c.wnry	b07a3e01839b404dbe662c485141b0b2
r.wnry	225081d5de690310a3c7211e2fd96dac
s.wnry	ad4c9de7c8c40813f200ba1c2fa33083
t.wnry	1bab8430e6f4e77e37f2e98a9f5fa5e5
u.wnry	d6483ec79f21a1d18b21fec56bfd0000
f.wnry	4c994cef144c85fe1a0abd77f065e430
taskdl.exe	e0077f9ee92e888868a9d2298e1c6a4f
taskse.exe	662b2256d873d03d4a4324878f4b6c6c
tasksche.exe	edf044c89c50c514f2fcfc12db355327

Table 1:- Details of MD5 Hash Values as Found in Case

- Few bmp files namely '@WanaDecryptor@.bmp' with warning message could be found (fig.5).

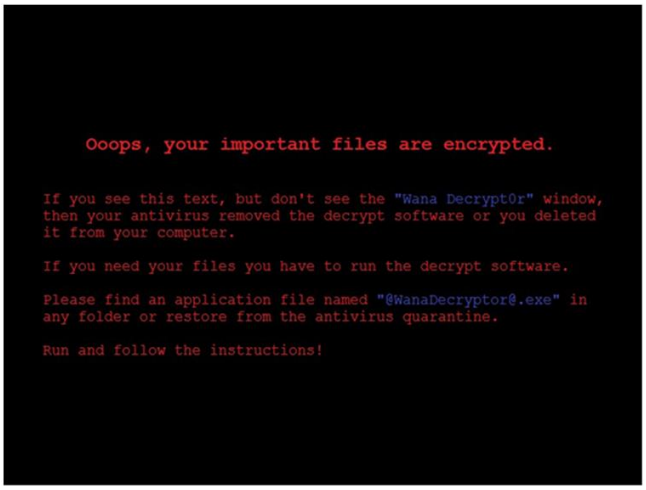

Fig 5:- Warning message for files being encrypted

- Files '@Please_Read_Me@.txt' found which contains instruction to decrypt files on paying ransom (fig.6).

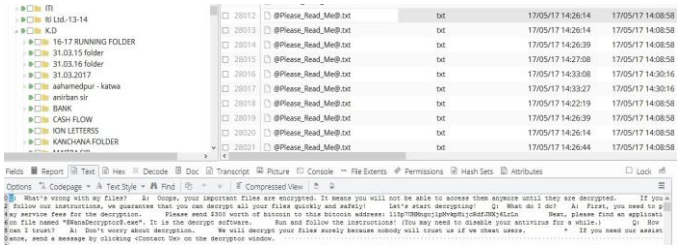

Fig 6:- Files containing instruction for paying ransom

- Registry analysis indicates 'WanaCrypt0r' is among the software key with last write time '2017-05-17 09:38:55' (fig.7). The traces of execution of '@WanaDecryptor@.exe' were also found in several occasions in registry hive which certainly establish execution of malicious file to infect the operating system.

```
----------------------------------------
listsoft v.20200517
(NTUSER.DAT) Lists contents of user's Software key

List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

2017-05-20 07:29:27Z   Chromium
2017-05-20 07:29:26Z   Noflat
2017-05-20 06:39:04Z   Microsoft
2017-05-17 09:38:55Z   WanaCrypt0r
2017-05-15 10:15:03Z   WinRAR
2017-05-11 10:10:46Z   InstallCore
2017-05-09 11:59:14Z   AlphaGo
2017-05-09 09:11:25Z   heheelibom
```

Fig 7:- Registry analysis confirms presence of software key 'WanaCrypt0r'

- Internet cookies around same timeline included url 'heheelibom.com' and 'brobgser.com'. These urls reported as malicious when checked on 'virustotal' website. However, malware detection facility in the 'IEF 6' does not report 'wannacry' malware.

ISSN No:-2456-2165

VI. RESULTS AND DISCUSSIONS

- During forensic examination it is observed that malwares can be present in any media brought in for analysis unknown to the laboratory. Extracting data from the devices and opening files during analysis being routine process in forensic examination can affect examination workstation and malicious software can spread to other connected resources in the process. Therefore, forensic laboratories should follow some guidelines to prevent malwares from affecting laboratory resources.

Guidelines to be followed during forensic examination:

- Keep a copy of local machine for reinstallation if required
- Nothing (i.e., any files or folders) to be extracted and saved in local machine.
- Use tools/ options within the tools which do not copy anything as a part of report.
- Do not archive under any condition which can contaminate.
- Use well understood tools/ options within tools to ensure no remnants.
- The workstation used for analysis should not be in a networked environment,
- No USB devices should be used to transfer data.

- Though past experience of researchers found in literatures is great resource, malicious software always change strategy. Therefore, the codes may be changed and modified uniquely within system which is infected. Certain changes beyond available literature are possible. All such variations should be documented for quick detection of the variants.

REFERENCES

[1]. Lutkevich, B. *malware*. https://www.techtarget.com/searchsecurity/definition/malware.
[2]. Alex Berry, J.H., Randi Eitzman. *WannaCry Malware Profile*. https://www.mandiant.com/resources/blog/wannacry-malware-profile.
[3]. Khillar, S. *Difference Between Static Malware Analysis and Dynamic Malware Analysis*. 2022.http://www.differencebetween.net/technology/difference-between-static-malware-analysis-and-dynamic-malware-analysis/
[4]. Diana Rathod, D.P.S., *DIGITAL FORENSIC ANALYSIS OF RANSOMWARE INFECTED WINDOWS SYSTEM*. JETIR, 2019. **6**(5).
[5]. McDonald, G., et al., *Ransomware: Analysing the Impact on Windows Active Directory Domain Services.* Sensors, 2022. **22**(3): p. 953.
[6]. Lo, V., *Windows shellbag forensics in depth.* SANS Institute. Retrieved from, 2014.
[7]. Erika Noerenberg, A.C., Nathanial Quist. *A Technical Analysis of WannaCry Ransomware*. https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/.
[8]. Team, C.T.U.R. *WCry Ransomware Analysis*. https://www.secureworks.com/research/wcry-ransomware-analysis.
[9]. YusirwanS, S., Y. Prayudi, and I. Riadi, *Implementation of malware analysis using static and dynamic analysis method.* International Journal of Computer Applications, 2015. **117**(6): p. 11-15.