Journal of Theoretical and Applied Information Technology
31st July 2019. Vol.97. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DISCOVERING RANSOMWAREBEHAVIOR BY HOST-BASED APPROACH

[*]MUHAMMAD SAFWAN ROSLI, [1]RAIHANA SYAHIRAH ABDULLAH,[1]WARUSIA YASSIN, [1]FAIZAL M.A.

[*1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia

E-mail: [*]safwan.rosli92@gmail.com

ABSTRACT

Numerous researchers have discovered multiple types of ransomware that has been rampaging in cybersecurity which is the main concern for business companies where most of their data has been digitalized. However, the main problem in detecting this type of malware, where it is known as sophisticated behavior is quite challenging since it capable to do encryption in file activity system and hide its malicious activity in computer host. Nevertheless, previous researcher also has done major contribution in discovering its pattern and behavior of ransomware and provide numerous solutions in detecting this malware. This paper will be focusing on ransomware behavior during normal file activity system by using host-based approach experiment. The design of the experiment and dataset collection are one of the main important in this experiment for analyzing the ransomware behavior using available tools and software. Then, the behavior of the ransomware will be saved as log file for in-depth analysis. Finally, the results from the experiment will be tabulated and discussed further before the conclusion of the experiment.

Keywords: *Ransomware, Behavior Analysis, File Activity System, Process Explorer, Process Monitor.*

1. INTRODUCTION

The rise of ransomware as a cybersecurity threat is nothing remarkable from its introduction nearly three decades ago, to present day, where ransomware is widespread and has become a serious threat. Now, crypto-ransomware can breach victim's devices by encoding or encrypt the data and provide the decryption key after getting ransom thus, these incidents causing chaos in current trend of internet technology. Most of the cases, the attacker does not provide the key even the victim paying the ransom [19].

Trojan.Gpcoder is the first malware in crypto ransomware trend by using its own encryption techniques but, the encryption itself is weak and can be decrypted easily [14]. They also used symmetric encryption algorithms, which meant the same key was used for both encryption and decryption [14]. Since the perception of crypto-ransomware started to gain attraction [14], more ransomware has come to the surface and brings more threats in the future.

Ransomware attacker does not particularly care of their victim even the victim willing to pay the ransom for their data. For that reason, cybercriminal take this strategy to propagating the malware targeting multiple types of user with different country or region, even though the probability of the victim pays the ransom is insignificant.

In Malaysia, during May 2017, CEO of CyberSecurity Malaysia (CSM) stated that the ransomware WannaCry has breach into Malaysia using Server Message Block (SMB) to exploit security hole in Windows operating system. Furthermore, most of research regarding ransomware shows lack of analysis and most of the ransomware samples is outdated [1].

Thus, the main problems when detecting or preventing ransomware from spreading are the understanding the ransomware behavior in network traffic and file system activity. Thus, the purpose of this study is to get real-time data from the file activity system and analyze the ransomware behavior by observing the file system activity in testing environment.

1.1 Ransomware

Ransomware is a threat that acts by encrypting victim's files in filesystem then, save decryption key of the files until the ransom has been paid to ransomware attacker. Ransomware attacks are likely to attack user who are individual

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

or small business owner [5] which cyber-criminals use ransomware as good source of profits and high collateral damage [7]. Because of its pattern and behavior, it is known by IT security as one of the critical issues that need to be fear [16]. An immense research regarding ransomware attack has also been going particularly for detection and prevention process [13].

With the lack of update on most of smartphone especially android phone, android locker-ransomware has become more popular among attackers with new technique of propagation [18], since android holds the highest market share comparing to iOS and Windows phones [17]. The attackers have multiple tactics in order to lure victims to activate their ransomware such as social engineering, phishing, botnet and other exploit kits [9]. Also, current attack uses cryptographic library in operating system which difficult to crack the encrypted files [10].

There are two types of ransomware that can be identified which are, locker-ransomware and crypto-ransomware [6]. Locker-ransomware is one of two types of ransomware that is known to limit the access of victim's personal computer by acting as law enforcement authorities, forcing the user to pay fine for accessing illegal content of the website. Since ransomware infects computers through illegal websites, the possibility for the victim to pays the ransom is high to hide the embarrassment [14]. On the other hand, crypto-ransomware is a malware that employ encryption algorithm to all files that has been infected by this type of malware thus, victim cannot access the infected files. Usually, crypto-ransomware will give a warning message to pay the ransom within given time since the attacker can delete decryption key if the user exceeds the time limit [14].

Like other malwares, ransomware also have its own lifecycle that can be seen in Figure 1. Several actions are needed to make ransomware attack successful when it infects the computer [3]. The chronological attack starts with the victim download suspicious link in email attachment or accidently drive-by download from suspicious website.

This will lead into next steps which the victim execute ransomware file since typical ransomware are executable file format. When the ransomware has been executed, the malware will try to establish the connection in Command & Control (C&C) so attacker can gain encryption key of victim to bargain with the victim.

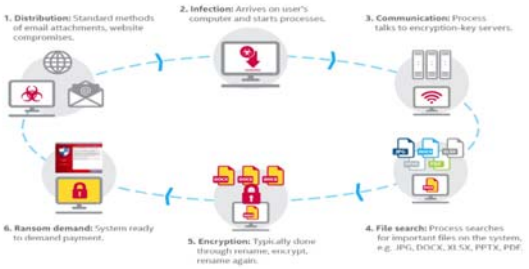

Figure 1: Ransomware Lifecycle [3]

Next, ransomware will do search related file with specific extension such as pdf, docx, xlsx, pptx, and jpg. Then, encryption will be done by renaming the file, encryption of file, then renaming it again. This step will show most of the encrypted file with unique extension based on types of ransomware. After the file in the directory has been encrypted, the ransomware will display the ransom note including the instruction and step by step to pay the ransom, mostly using Bitcoin transaction in The Onion Ring (TOR) protocol.

With the observation of ransomware lifecycle and the complexity of the encryption to crack victim files meaning the severity of the attack is high since the attack is going so fast that it capable to lock the victim's computer before it can be mitigated. It also motivates us to delve deeper into understanding ransomware behavior and conduct an experiment for analysis purpose.

2. RANSOMWARE BEHAVIOUR ANALYSIS

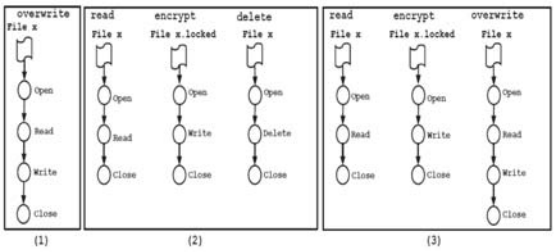

Figure 2: Ransomware Pattern [3]

Figure 2 describe search techniques such as depth-first, file size and file location in tree hierarchy are mostly being used by the ransomware to locate file-related in file directory. One of the ransomware family starts their activity by locate and encrypt the Master File Table (MFT) making the encryption process are much easier and faster rendering the drive inaccessible for victims [3].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From Figure 2, the ransomware starts with overwriting the filename, reading the file, encrypt the file then delete the file before creating a new file with encrypted file. Most original file that has been infected are likely safe or it has been deleted by the ransomware. This behavior of ransomware can lead into analysis that strive to improve the detection framework that has been made by the researcher to identify and prevent from ransomware to breach the system or filesystem. The approach divides into two types of analysis which are static analysis and dynamic analysis.

2.1 Ransomware Static Analysis

Ransomware static analysis approach extracts structural information of ransomware by examining ransomware payload that uniquely representing the ransomware itself [3]. This passive approach leads to safe analysis that provide massive data information of ransomware thus allowing prediction based on the potential execution process and path can be made by the ransomware. Ransomware static analysis also helps in terms of detection since it can detect distinct feature made by the ransomware thus, preventing the ransomware from doing its own behavior and process before encryption happens.

CryptoDrop is one of the frameworks that has been made to make early prediction using ransomware static analysis approach by monitoring the file entropy and the scoreboard, a combination of other modules to decide whether the process either malicious and consider dangerous or benign [15].

2.2 Ransomware Dynamic Analysis

Ransomware dynamic analysis approach analyses the malware at real-time environment. This approach is likely to be used in virtual environment such as sandbox with the feature to analyses the malware. The purpose of malware samples executed in controlled environment is to observe the actual behavior of the malware and the process that being interacted by the behavior and files in the directory that has been access by the malware thus, dynamic analysis is much more efficient in terms of observing the malware.

A framework based on dynamic analysis, UNVEIL, has been developed to detect both types of ransomware which are crypto ransomware and locker ransomware [11]. The purpose of the framework is to detect and observe three elements or component in computer which are I/O data buffer entropy, access pattern and filesystem activities. However, the drawback of this approach is it needs to be in safe environment and different logs with different times cause irregular in analyzing the malware.

3. METHODOLOGY

The first process of methodology is to find the information regarding ransomware, ransomware taxonomy and ransomware behavior analysis by reviewing the literature and previous research. Then, the project will perform data gathering for each types of ransomware samples thus, the project can analyses the behavior of each ransomware.

3.1 Design of Experiment

To validate and authenticate the data, the project needs to imitate the scenario of ransomware attack phase in real-time environment. By using virtual environment, we can release the ransomware in controllable manner and the network traffic will be captured to be analyzed.

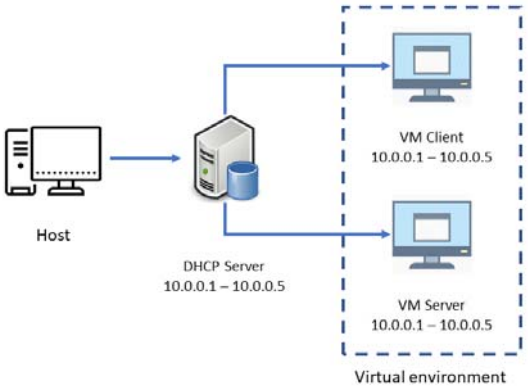

Figure 3: Testbed Environment

A desktop has been used to create a virtual environment which to capture behavior of the ransomware samples. The virtual environment has two different computers which are client and server with different range of IP addresses that has been allocated at DHCP server when creating testing environment.

Two effective network analysis tools have been selected for experiment and analysis stage where these tools are open source and has been used for multiple time for researcher to capture the data or even to analyses the data since analyzing the data are its main function. Process Monitor or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

known as ProcMon is a monitoring tools that shows a real-time environment of file system activity, registry and process activity. These logs are the arranged into several column that makes it easier to read such as process ID, the operation of process, directory path and result of the process. ProcMon also can be used to monitor and record malware activity since it provides filtering function. While, Wireshark is used to capture the flow of network traffic and analyse the packet that has been captured through network interface card. Packet that has been captured will be presented into multiple types of information such as time, source, destination, protocol, length and the info of each packet frame.

3.2 Dataset Collection

The set of data of ransomware has been download from the GitHub which is a web-based by using git command in version control. Below is the flow chart of capturing the malware sample and description of the dataset that has been used for the experiment:

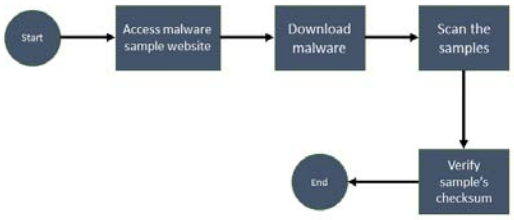

Figure 4: Flowchart of Capturing the Ransomware Samples

The process of capturing the samples starts with accessing the malware samples website which is Github. The website provides multiple samples of malware including other types of malware including virus and worm. Next, the after selecting the malware that will be used in the experiment, the malware will be downloaded in executable file format since the testbed is using windows operating system. Before the execution of the malware, the samples need to be scan using VirusTotal then verify the checksum of the samples.

Table 1: Ransomware Dataset

Ransomware	MD5	File Size	File Type
Badrabbit	fbbdc39af1139aebba4da004475e8839	431.54 KB	Win32 EXE
Cerber	8b6bc16fd137c09a08b02bbe1bb7d670	604.5 KB	Win32 EXE
GoldenEye	e3b7d39be5e821b59636d0fe7c2944cc	254.5 KB	Win32 EXE
Jigsaw	2773e3dc59472296cb0024ba7715a64e	283.5 KB	Win32 EXE
Mamba	409d80bb94645fbc4a1fa61c07806883	2.3 MB	Win32 EXE
Mischa	8a241cfcc23dc740e1fadc7f2df3965e	878.5 KB	Win32 EXE
Rensenware	60335edf459643a87168da8ed74c2b60	96.5 KB	Win32 EXE
Satana	46bfd4f1d581d7c0121d2b19a005d3df	49.67 KB	Win32 EXE
TeslaCrypt	6e080aa085293bb9fbdcc9015337d309	257.5 KB	Win32 EXE
WannaCry	84c82835a5d21bbcf75a61706d8ab549	3.35 MB	Win32 EXE

Table 1 represent ten types of ransomware samples are being used in our experiment namely, Badrabbit, Cerber, GoldenEye, Jigsaw, Mamba, Mischa, Rensenware, Satana, TeslaCyrpt and WannaCry. All ransomware samples are in Windows executable format ranging size from 49.67KB to 3.35MB based on ransomware samples.

4. RESULT, ANALYSIS AND DISCUSSION

The nature of ransomware is it need user permission in order to execute the malicious activity such as file encryption in filesystem. This requirement makes a host-based detection more popular in previous research whether anomaly detection or misuse detection. An anomaly detection can detect novel or unknown attacks that was not included in the past event during normal activity but, the risk of getting false positive is rather high. Compare to misuse detection, it can have low rate of false positive, considering it relies on signature or attack pattern of previous attacks. Since most ransomware is executable file that hides in computer host, host-based detection needs to be able to monitor file activity system so the detection can be made in early stage of attacks thus, preventing the ransomware to encrypt the files. In this experiment, the tools which are Process Explorer and Process Monitor, are used to capture the behavior of ransomware can give a hindsight of what host-based detection capable of based on the result of experiment.

Figures below describe each ransomware behavior in the file activity that has been captured using choice of tools. Since the testing environment does not connect to internet access, the packet receive at the server does not affecting the filesystem.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1 Badrabbit ransomware

BadRabbit spreads via fake Adobe Flash updates, tricking users into clicking the malware by incorrectly alerting the user that their Flash player needs an update. Once the victim's computer is infected and their information encrypted, BadRabbit reboots the system and the following message is displayed when reboot.

During the execution of the ransomware, it will try to achieve a privilege via User Access Control or UAC. Then, it will create several files under directory of "C:\Windows" and most significant files is infpub.dat file since this file is responsible for encrypting the files and modifies the boot-loader.

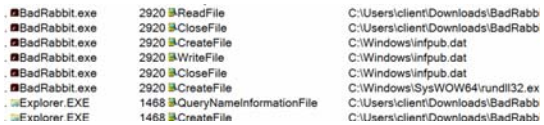

Figure 5: File written by BadRabbit

From the figure above, dispci.exe seems to be created by the process from the malware process tree in directory 'C:\Windows'. It also drops and installs other files during the process of the malware such as cscc.dat file which is legitimate disk-cryptor and need to be installed as a service

4.2 Cerber ransomware

Cerber or CRBR Encryptor is a type of ransomware that encrypts the files in the directory of the computer even the computer does not connect to the internet. Most infected file will have an extension name such as ".ba99",".98a0", ".a37b" and ".a563" depending on the variant of the ransomware. In this experiment, the file extension of the infected file is ".bdfa".

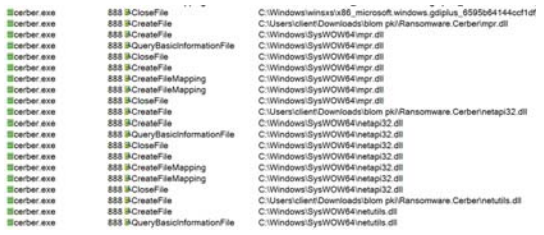

Figure 6: Creating malicious dll file

Upon execution, the Cerber malware will check to see where it is being launched from. Then, it checks whether the specific files have been as show in the figure above. If the malware does not find any specific files when it was executed, it will proceed to create these dll files in that directory.

4.3 GoldenEye ransomware

GoldenEye need to obtain administrative permission to proceed the encryption of the files. This is because one of the activities is to change the Master Boot Record (MBR) with custom boot loader. Then, the computer automatically reboot itself, showing a fake check disk and execute the encryption activity in the background process.

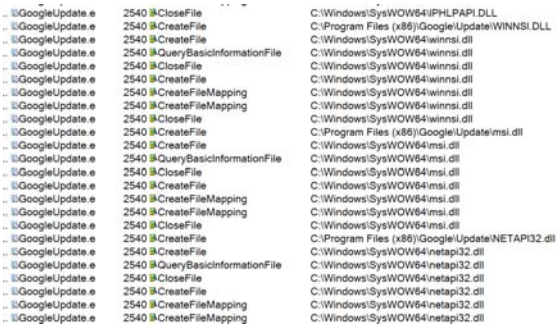

Figure 7: GoldenEye infecting GoogleUpdate.exe

Upon the execution of the malware, the malware will infect the legitimate process which is GoogleUpdate.exe. Like Cerber ransomware, it checks whether the specific files have been as show in the figure above. If the malware does not find any specific files when it was executed, it will proceed to create these dll files in that directory. After these dll has been created, the malware will start to encrypt the file while going through file directory.

4.4 Jigsaw ransomware

Jigsaw has a distinct feature where it display a ransom note featuring an image of Billy from the Saw film franchise. This ransomware encrypts the files from file directory and deletes the files permanently if the ransom has not been done in specific time given.

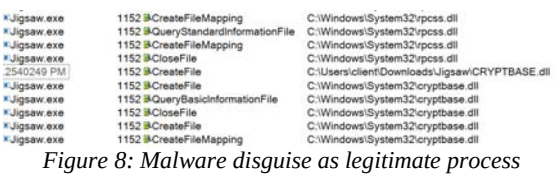

Figure 8: Malware disguise as legitimate process

During experiment, several dll has been created by the process of the ransomware which it creates in System32. However, these dll files are Trojan based malware that disguise as legitimate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process such as cryptbase.dll which is base cryptographic API from Microsoft. It also changes the name of it process into legitimate process by creating folder in file directory. After these dll has been created, the malware will start to encrypt the file while going through file directory.

4.5 Mamba ransomware

Mamba or HDDCryptor is a ransomware that encrypt the date in network sharing files such as disk drives, printers or accessing serial ports by using Server Message Block (SMB). The activity of the ransomware is mostly same with GoldenEye ransomware since these ransomwares need a permission from the administrator to make changes of Master Boot Record before displaying ransom note.

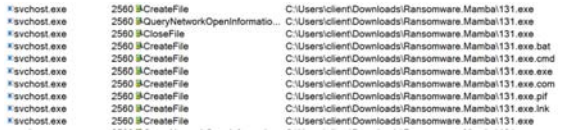

Figure 9: Several files has been created in filesystem

Although the process of file encryption does not occur during the experiment, the malware does create several files in the background process.

4.6 Mischa ransomware

Mischa ransomware is a computer virus, affectionally addressed by its creators as a “little brother” of the infamous Petya virus which recently became even more dangerous by employing a new tactic for extorting money from the infected computer users.

Unlike Petya, which needs administrative privileges to modify the master boot record (MBR), Mischa is simply installed on the computer and immediately starts scanning it for files. This virus, as well as the majority of other ransomware, targets documents, videos, images, archives but may easily infect applications, i.e. the .exe files, as well.

As soon as the users realize that they have lost access to their data, the ransomware drops documents labelled as YOUR_FILES_ARE_ENCRYPTED.HTML and YOUR_FILES_ARE_ENCRYPTED.TXT to every folder of the corrupted device.

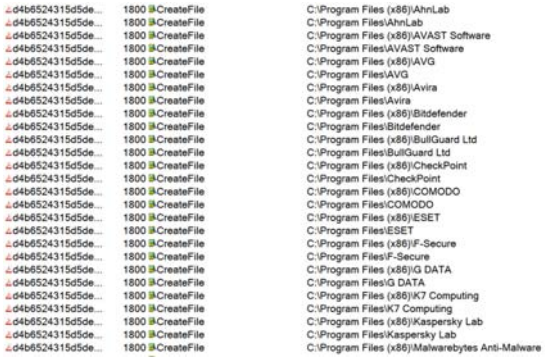

Figure 10: Scanning anti-virus software

The executable program of ransomware is packed with an icon of a PDF document. From the figure above shows the ransomware search folder names of anti-virus inside Program Files directory. Then, it will drop another malware that disguise as cryptsp.dll which is a legitimate file. After the encryption process has been done in specific directory, the malware will create two types of ransom note which are text file and HTML file.

4.7 Rensenware ransomware

Rensenware targets Windows OS and the distribution method is currently unknown. Reportedly, Rensenware was created as a "joke" by its developer and was never meant for distribution as it was designed to deliver a unique ransom demand. Victims infected by Rensenware originally needed to play a game called "TH12 ~ Undefined Fantastic Object" and reach a score above 0.2 billion in the "Lunatic" level to decrypt their files.

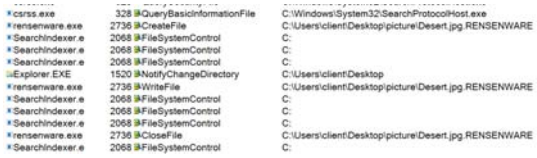

Figure 11: Rensenware file encryption

Rensenware run a scan for specific file types then start to encrypt targeted files using AES encryption method in 256-bit. Infected file will have extension file name “RENSENWARE” added after the encryption has been done. After the encryption has been done, the ransomware will display a ransom note introducing the character from the game series called Touhou Project.

4.8 Satana ransomware

Satan or Satana ransomware is a crypto-virus which operates as Ransomware-as-a-service.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It is spread via Server Message Block (SMB) exploit that was used by a scandalous Wannacry attack.

Figure 12: Create ransom note

During the malware execution, it drops several dynamic link libraries (DLL) in directory "C:\Windows\System32". Then, it create a ransom note which is "!satana!.txt" after encrypting each folder in targeted directory. Figure 13 show a pattern of encrypted file always have "<email_address>__<original_name>".

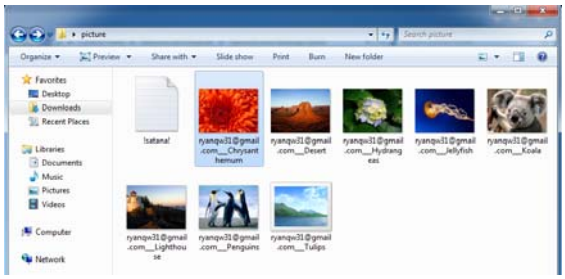

Figure 13: Modification of filename in filesystem

4.9 TeslaCrypt ransomware

TeslaCrypt pattern is the same as other typical ransomware where it creates a ransom note called "HELP_RESTORE_FILES.txt" in each directory where it encrypts the files. After the victim execute the ransomware, it will start to go through the filesystem directory then it will display the steps to send bitcoin ransom in desktop background after all the directory has been gone through.

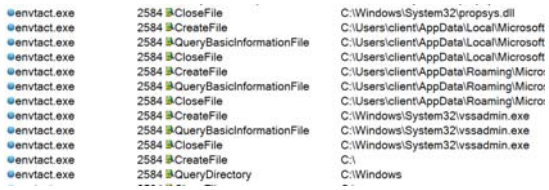

Figure 14: Create executable file

The malware will execute the file called vssadmin.exe since it able to delete all the shadow volume on the computer. As this program requires Administrative privileges to run, some ransomware will inject themselves into processes that are running as an Administrator to avoid a UAC prompt from being displayed. Then, encryption process will be done by going through each directory.

4.10 WannaCry ransomware

WannaCry start to cause uproar during May 2017 where the malware spread through network into Windows computer. The ransomware does encrypt the files, making the victim unable to access the it and it will be displaying the ransom note.

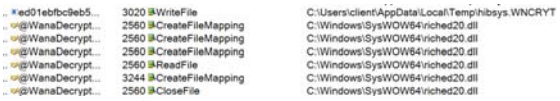

Figure 15: WannaDecryptor.exe

The function of the "@WanaDecryptor@.exe" is to show timers from the ransom note and the instruction of sending the ransom to attacker based on the language that has been setup in the operating system.

Table 2: Analysis result from ransomware behavior

Ransomware	File Open	File Create	File Executable
Badrabbit	imm32.dll	infpub.dat	rundll32.exe
	rpcss.dll	cscc.dat	schtasks.exe
	cryptbase.dll	dispci.exe	
Cerber	imm32.dll	WindowsCodecs.dll	mshta.exe
	rsaenh.dll	1dTbfrlajT.bdfa	
	cryptsp.dll	_R_E_A_D___T_H_I_S___SG08K_.txt	
Golden Eye	wow64.dll	Penguins.jpg.x4jBy3PY	InfDefaultInstall.exe
	winmm.dll	YOUR_FILES_ARE_ENCRYPTED.TXT	xwizard.exe
	imm32.dll	msimg32.dll	typeperf.exe
Jigsaw	imm32.dll	Hydrangeas.jpg.fun	drpbx.exe
	rpcss.dll	RacWmiDatabase.sdf.fun	
	cryptbase.dll	EncryptedFileList.txt	
Mamba	imm32.dll	131.exe.bat	
	sechost.dll	131.exe.cmd	
	wow6	131.exe.com	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ransomware	File Open	File Create	File Executable
	4cpu.dll		
Mischa	imm32.dll	Tulips.jpg.6NRS	
	rsaenh.dll	YOUR_FILES_ARE_ENCRYPTED.TXT	
	wsock32.dll	YOUR_FILES_ARE_ENCRYPTED.HTML	
Rensenware	imm32.dll	Tulips.jpg.RENSENWARE	dw20.exe
	rpcss.dll	Ransomware.TeslaCrypt.zip.RENSENWARE	
	rsaenh.dll	Eula.txt.RENSENWARE	
Satana	imm32.dll	desktop.ini	qxyi.exe
	rpcss.dll	!satana!.txt	VSSADMIN.EXE
	rsaenh.dll	ryanqw31@gmail.com___ps.txt	
TeslaCrypt	imm32.dll	Lighthouse.jpg.ecc	envtact.exe
	rpcss.dll	RECOVERY_KEY.TXT	
	rsaenh.dll	HELP_RESTORE_FILES.txt	
WannaCry	imm32.dll	Ransomware.WannaCry\b.wnry	taskdl.exe
	msvcrt.dll	m_bulgarian.wnry	@WanaDecryptor@.exe
	rsaenh.dll	@WanaDecryptor@.exe	taskhsvc.exe

The data from experiment were tabulated and classified in three column which are FileOpen, FileCreate and FileExecutable. FileOpen is where the ransomware samples access the DLL from the legitimate directory such as System32 or SysWOW64 as part of the process activity after the ransomware has been executed. FileCreate is where ransomware samples create the file on certain directory or create a ransomware note where the file in directory has been encrypted. FileExecutable is the name of the process that was under the ransomware process tree during the execution of the malware.

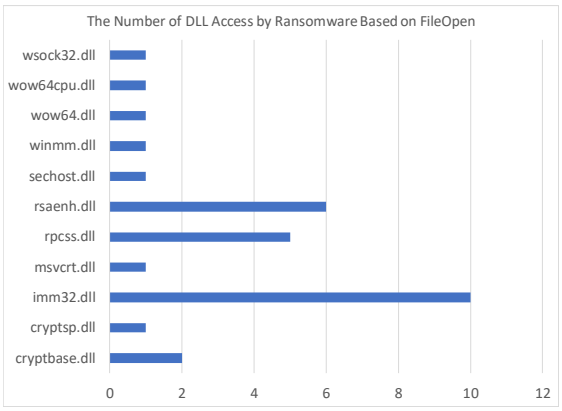

Figure 16: Clustered Bar Chart of DLL Access by Ransomware

Based on the result of experiment, there are similarity and unique behavior that has been shown by the ransomware samples during the experiment that has been conducted. In ransomware lifecycle, typical ransomware shown the process that before execution of the malware, it will be downloaded by using one of the methods which are file dropper, mail attachment, or drive-by download. Since, the ransomware samples are already downloaded before the experiment was begun, the initial action of ransomware lifecycle for this experiment can be negligible. The second phase of the lifecycle is the activity of ransomware executed in the directory of the computer system. The similarity obtained from the experiment which ransomware samples will access several dynamic link library (dll) which among dll file that being access are imm32.dll, rsaenh.dll, cryptbase.dll and cryptsp.dll. These dll files are used to perform specific process such as rsaenh.dll to perform 128-bit encryption process for file encryption. These ransomware samples also accessing legitimate process to execute other such as rundll32 to run other malicious dll file and svchost.exe to execute process such consent.exe to bypass user access control (UAC) before starting the encryption process. Other ransomware samples try to delete shadow copy by using executable program, vssadmin.exe.

Furthermore, upon execution of ransomware application, it will access the SysWOW64 and System32 directory to drop other malicious dll file. The third step in lifecycle is communication between Command & Control (C&C) server to retrieve encryption key [3]. Since the experiment are using virtual LAN network (VLAN) which is offline network, the ransomware

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sample cannot establish communication between C&C instead, it tries to send the TCP packet to another computer that have connected to VLAN.

However, all ransomware sample that send the packet does not affecting the computer except the infected computer. Next step is ransomware search file by going through all directory in computer system with specific extension file system. Most of the file extension such as pdf, xlsx, pptx, png, and docx will get search early since most of the author of the ransomware tend to set most access by the normal user. Encryption steps is the common ransomware attacks as they will rename the file, encrypt then, rename it again with the new extension of file. Most of the ransomware samples, encrypt the files only, while other sample lock the computer by reboot the system since it acquires Master Boot Record (MBR) such as BadRabbit, GoldenEye and Mischa ransomware. The last step of is to display ransom note after the encryption. All samples display the ransom note which is to notify the user to send the ransom by using Bitcoin transaction within time limit except one sample, Rensenware, which a user need to play a specific game with certain condition or requirement to unlock the file.

5. RELATED WORKS

The difference between our research and previous research is we study the relationship of multiple ransomware and analyses which files that are mostly being targeted based on our research experiment. [16] has proposed an early detection of ransomware using Windows API calls in Windows OS. The proposed framework also like our research since it uses virtual environment setup and using file type analysis as an indicator analysis. With the framework running live by using set of behavioral indicators, it will continue to extract Windows API using multiple classification factors of file type changes that specifically targets possible infected files.

When it comes to detection techniques, [12] also has done comparative analysis of ransomware detection based on previous authors from year 2016 to 2018. The authors also presented a detailed ransomware attack lifestyle and its ransomware beside existing techniques for ransomware detection.

[13] also study and predict the impact of future ransomware threats by using behavioral analysis in file system activity. The study also required to run a simulated environment to understand ransomware attack pattern with multiple analysis using Cuckoo sandbox tools. The prediction comes with available toolkits thus, they can predict the severity of ransomware attack in the future.

Another analysis done by [9] by using predictive model and human responses using quantitative research such as questionnaire and interviews with their own model called Randep, a model with multiple classifiers that capable to plot a graph model. The analysis is done by doing comparative analysis based on the results of questionnaire and Randep model.

[8] proposed a situational awareness model which consists of multiple stages in ransomware lifecycle to prevent and mitigate the attacks. They also evaluated parameters that are currently being main challenges in detecting and preventing the threats. Filesystem activity is one of the evaluated parameters.

A research focusing on WannaCry ransomware has been done in order to know its properties and propagation mechanisms. With virtual testbed has been developed, the ransomware can be dissected and further analysis such as file analysis and network analysis will be done [2].

A case study of Locky ransomware has been carried by [4]. The study analyses the ransomware using network-based ransomware detection with testbed environment for better understanding the behavior of ransomware using Locky ransomware as case study.

6. CONCLUSION AND FUTURE WORKS

The main objective of this project is to study the selected multiple set of ransomware sample in testing environment. From the multiple set of ransomware samples, ransomware behavior can be analyzed by observing the network traffic and file system activity in testing environment. All data result from the experiment have been save as file that refereeing to the tools such as PCAP file in Wireshark. Finally, the results from the experiment will be visualized into form of bar chart for comparison between each DLL access by ransomware.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The main contribution from this experiment is to propose and presenting alternative method in analyzing the data of ransomware behavior. From experiment, we also classify ransomware behavior using process monitor and Wireshark as file log and network traffic respectively.

Current limitation of this research is, it only focusing on file activity system rather than using other method to extract the data from the file. In addition, the research project using offline environment which limited of what ransomware can do to observe the malware from network traffic. Furthermore, sophisticated ransomware samples are hard to be experimented such as fast-paced ransomware that can lock the computer before data can be captured.

In future research, this research needs to have a bigger scope for future works using additional types of data from different sources such as registry, memory. Since current experiment is made in offline environment, we intend to do an online environment for more information from data packet that has been captured. The experiment also needs to have additional number of malware samples to get strong similarities in terms of ransomware behavior.

Based on overall result of an experiment in our research, we also consider expanding the research by utilizing ransomware behavior in detection scope where these results can be benefit into this area.

7. ACKNOWLEDGEMENT

This work has been supported under Universiti Teknikal Malysia Melaka research grant GLUAR/CSM/2016/FTMK-CACT/100013. The authors would like to thank to Universiti Teknikal Malaysia Melaka, Cybersecurity Malaysia and all members of CMERP INSFORNET research group for their incredible supports in this project.

REFERENCES:

[1] Adamov, A. and Carlsson, A., "The State of Ransomware . Trends and Mitigation Techniques", 2017.

[2] Akbanov, M., Vassilakis, V.G., and Logothetis, M.D., "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms", *Journal of Telecommunications and Information Technology*, (1), 2019, pp.113–124.

[3] Al-rimy, B.A.S., Maarof, M.A., and Shaid, S.Z.M., "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", *Computers and Security*, 74, 2018, pp.144–166.

[4] Almashhadani, A.O., Kaiiali, M., Sezer, S., and Okane, P., "A Multi-Classifier Network-based Crypto Ransomware Detection System: A Case study of Locky Ransomware", *IEEE Access*, PP (c), 2018, pp.1–1.

[5] Brewer, R., "Ransomware attacks: detection, prevention and cure", *Network Security*, 2016 (9), pp.5–9.

[6] Cabaj, K., Gregorczyk, M., and Mazurczyk, W., "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics", *Computers and Electrical Engineering*, 66, 2017, pp.353–368.

[7] Cohen, A. and Nissim, N., "Trusted Detection of Ransomware in a Private Cloud Using Machine Learning Methods Leveraging Meta-Features from Volatile Memory", *Expert Systems with Applications*, 102, 2018, pp.158–178.

[8] Herrera Silva, J.A., Barona López, L.I., Valdivieso Caraguay, Á.L., and Hernández-Álvarez, M., "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters", *Remote Sensing*, 11 (10), 2019, pp.1168.

[9] Hull, G., John, H., and Arief, B., "Ransomware deployment methods and analysis: views from a predictive model and human responses", *Crime Science*, 8 (1), 2019, pp.2.

[10] Irwin, A.S.M. and Dawson, C., "Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help", *Journal of Money Laundering Control*, 2019, pp.00–00.

[11] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., Mulliner, C., and Robertson, W., "UNVEIL : A Large-Scale , Automated Approach to Detecting Ransomware", 2016.

[12] Kok, S.H., Abdullah, A., Jhanjhi, N.Z., and Supramaniam, M., "Ransomware , Threat and Detection Techniques : A Review", *International Journal of Computer Science and Network Security*, 19 (2), 2019, pp.136–146.

[13] Popli, N.K. and Girdhar, A., "Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware", *Advances in Intelligent Systems and Computing*, 799, 2019, pp.65–80.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Savage, K., Coogan, P., and Lau, H., "The Evolution of Ransomware", 2015, pp.57.

[15] Scaife, N., Carter, H., Traynor, P., and Butler, K.R.B., "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", *Proceedings - International Conference on Distributed Computing Systems*, 2016-Augus, pp.303–312.

[16] Sharma, H. and Kant, S., "Early detection of ransomware by indicator analysis and WinAPI call sequence pattern", *Smart Innovation, Systems and Technologies*, 107, 2019, pp.201–211.

[17] Song, S., Kim, B., and Lee, S., "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", *Mobile Information Systems*, 2016.

[18] Su, D., Liu, J., Wang, X., and Wang, W., "Detecting Android Locker-ransomware on Chinese Social Networks", *IEEE Access*, 7, 2018, pp.20381–20393.

[19] Yalew, S.D., Jr, G.Q.M., Haridi, S., and Correia, M., n.d., "Hail to the Thief : Protecting Data from Mobile Ransomware with ransomSafeDroid".