An Analysis of WannaCry Ransomware

IT19003610 - Shiranthaka K. G. S.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe 10115, Sri Lanka
sudeepashiranthaka97@gmail.com

***Abstract* — Ransomware is a virus that spreads itself and encrypts a user's files so the attacker can hold them for ransom. These days, ransomware comes in a wide variety, with some strains aimed against individuals, others at businesses, and yet others at vital institutions like hospitals and government agencies. Today's ransomware relies on anti-recovery and infection persistence measures. Recent years have seen a rise in destructive ransomware including WannaCry, SamSam, CryptoLocker, Petya, Locky, TeslaCrypt, and Ryuk. We must comprehend the traits and habits of the variants so that we can design and enhance protective systems for them. The notorious WannaCry ransomware that caused global chaos will be the subject of this study. This implementation will be assessed for infection, persistence, and recovery prevention methods. The outcomes of this research study can be used to creation of anti-virus software, detection, and protection technologies, and other countermeasures targeting the WannaCry ransomware strain, as well as other strains exhibiting similarities to it.**

Keywords— *Ransomware, Malware analysis, Windows, WannaCry, dynamic analysis*

I. INTRODUCTION

Ransomware can categorize as a self-replicating and spreading malware type that uses cryptographic encryption mechanisms to hold the target victim's computer information until the ransom is paid. These malicious programs aim to coerce victims into paying a ransom. Shock and awe methods are used by crypto-ransomware to coerce victims into paying the demanded ransom. For example, WannaCry uses this strategy by displaying a three-day counter and threatening to erase the decryption key if the victim does not pay the ransom in time. The WannaCry ransomware attack was the largest of its kind ever recorded. Over 200 thousand machines in over 150 countries had been compromised. WannaCry has been called a network worm due to its capacity to rapidly spread to new networks. It wasn't until May 12, 2017, that the WannaCry malware was uncovered[1]. We have never seen anything like the WannaCry ransomware onslaught. There were around 200 thousand infected computers in 150 countries. WannaCry is a malicious software suite that encrypts user files and spreads itself using a worm module. WannaCry's command and control (C&C) communications occur over Tor's hidden services. WannaCry's command and control system is primarily used to verify whether or not once the victim pays the ransom, the decryption key can be released. After infection, the ransomware encrypts user files and displays instructions demanding a ransom payment of $300 or $600 in bitcoins to a predetermined location.

Various parts work together to make up the WannaCry malware. The encryption is bundled within the first dropper, along with a decryption tool called "WannaDecryptor 2.0", enclosed in a password-protected zip file are Tor and several other files that provide setup instructions and encryption keys[2].

To protect against ransomware, anti-virus software could benefit greatly from automated behavioral analysis, and many malware analysts would appreciate an automated tool or approach that would spare them the time-consuming task of manually analyzing logs collected from infected machines. Cuckoo Sandbox, a malware analysis tool, will be used to generate comprehensive WannaCry ransomware logs by inspecting the malicious file in question. It will also monitor API calls, imported procedures and libraries, file activity, and network traffic during the testing phase. The information for the analysis will come from Cuckoo[1].

The paper begins with an abstract and an introduction, both of which have been completed, and then moves on to provide background info on ransomware and the WannaCry variant, followed by the results of dynamic analysis, which examine the malware's encryption process, recovery prevention technique, methods of propagation, malicious indicators, a conclusion, and a list of sources.

II. BACKGROUND

A. Ransomware

Ransomware is a type of malicious software which encrypts or otherwise locks users out of their files, devices, or entire systems until a ransom is paid. When a computer is infected with ransomware, the user typically has only a few options, including contacting the attacker and paying the demanded ransom amount, or wiping the device's storage media and reinstalling the operating system, which will restore the device's functionality but not the user's files (even if a backup exists).

Common ransomware typically employs an encryption method that combines elements of both private key (symmetric) and public key (asymmetric) methods. If the ransomware uses public-key encryption, then the attacker's encryption keys are kept on the command and control also known as C & C server and making it nearly impossible to decrypt the files. The victims are usually given a deadline for making the ransom payment, told to purchase a certain cryptocurrency (such as Bitcoin or Ethereum), and then provide comprehensive instructions regarding the ransom payment process. The ransomware typically leads to distraction, sensitive information disclosure, command, control, etc.

B. EternalBlue and SMB Vulnerabilities

The EternalBlue exploit lets a malicious actor execute arbitrary code and take complete control of the target system and any associated devices simply by sending specially crafted packets. The WannaCry virus takes advantage of a hole in the Windows implementation of the Server Message Block (SMB) protocol[3]. Sharing and Printing Network (SMB) is a Windows-specific Transport protocol for sharing and printing local files and accessing remote services[1]. The Server Message Block (SMB) protocol uses TCP ports 139 and 445. The malware spreads via TCP port 445 and the SMB v1 vulnerability. Due to this flaw, remote attackers can exploit the vulnerability and run arbitrary code on the victim's machine by sending corrupted packets.

B. Wannacry

Over 250,000 systems were infected worldwide, including multiple hospitals in the UK, and the projected global cost is around USD 4 billion. In 2017, shadow, a hacker group called "Shadow Brokers" conducted various attacks using WannaCry ransomware, and the exploit known as EternalBlue was early developed by NSA of United State. Microsoft has already provided a patch (MS17-010) for the vulnerability used by Eternal Blue, which, once applied, would make the system immune to the attack. The problem was that few people had patched their PCs with the latest updates. To be specific, these flaws are specified below in figure[4].

Common Vulnerability Enumeration	Description
CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0146	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0147	Windows SMB Information Disclosure Vulnerability
CVE-2017-0148	Windows SMB Remote Code Execution Vulnerability

Figure 1: Related vulnerabilities for WannaCry

All of the following vulnerabilities are distinct from one another, but they all affect the SMBv1 server in the same way: they allow attackers to remotely execute malicious code by sending it in specially crafted SMB packets. Except CVE-2017-0147, which has a CVSS base score in the medium range, all of the previously mentioned vulnerabilities have a high CVV Base Score of 8.1. "Wannacry" exploited vulnerabilities in SMB by delivering malicious traffic on TCP ports 139 and 445[5].

WannaCry's worm element allows it to spread and infect other machines, making it difficult to stop. This makes attacks more powerful and pervasive, necessitating defenses that can act instantly and effectively in response. WannaCry also has an encryption module based on public-key cryptography (asymmetric cryptography). The Shadow Brokers hacking group is suspected of disclosing the perpetual blue and double pulsar techniques used by WannaCry in 2017. Hackers may access and run malicious programs on compromised PCs at will thanks to DoublePulsar, a persistent backdoor. This gives the attacker the opportunity to infect the compromised system with further malware and maintain access to the system after infection. After leveraging the SMB vulnerability through active analysis of critical TCP ports like port 445 and port 139, the worm module of WannaCry begins spreading and tries to install the backdoor DoublePulsar on infected machines. This ransomware causes the infected host's starting screen to show the image below, or in some situations, the user's desktop will show the image below, and all of their data will be encrypted and inaccessible.

III. METHODOLOGY

B. Libraries and Functions

Both the worm module and the encryption module of the WannaCry binaries were subjected to dynamic analysis, and the results of that analysis are presented here.

Both modules are PE32 executables (GUI) written in Intel 80386 for Microsoft Windows.

Name	Description
b.wnry	Ransom image (BMP file)
c.wnry	Configuration file
r.wnry	Ransom note (Text)
s.wnry	Zip file containing Tor files.
t.wnry	Encryption tool with RSA keys (encrypted).
u.wnry	Decryption tool
taskdl.exe	Deletes temp files
taskse.exe	Starts decryption tool
\msg	Directory containing payment instructions in many languages (readme file)

Figure 2: Malicious files inside the malware

Using the Pestudio tool[6], we were able to determine that the WannaCry worm and encryption modules include the Dynamic-link libraries (DLLs) listed in Tables 2 and 3 below. The worm module uses a call to iphlpapi.dll to gather information about the victim's network. Kernel32.dll and msvcrt.dll are two of the most often used libraries in the encryption module. This may indicate that the sole malicious capability enabled by these two libraries is encryption. A study of library functions in use at runtime is required to verify the aforementioned observation.

Library	Imports	Description
ws2_32.dll	13	Windows Socket 2.0 32-bit DLL
iphlpapi.dll	2	IP Helper API
wininet.dll	3	Internet Extensions for Win32
kernel32.dll	32	Windows NT Base API Client DLL
advapi32.dll	11	Advanced Windows 32 Base API
msvcp60.dll	2	Windows NT C++ Runtime Library DLL
msvcrt.dll	28	Windows NT CRT DLL

Figure 3: Details of propagated Worm module DLLs

Library	Imports	Description
kernel32.dll	54	Windows NT Base API Client DLL
advapi32.dll	10	Advanced Windows 32 Base API
user32.dll	1	Multi-User Windows User API Client DLL
msvcrt.dll	49	Windows NT CRT DLL

Figure 4: Details of encryption DLLs

Function	Location
OpenMutexA	0xda84
GetComputerNameW	0xd8b2
CreateServiceA	0xdc2a
OpenServiceA	0xdc62
StartServiceA	0xdc52
CryptReleaseContext	0xdc14
RegCreateKeyW	0xdc04
fopen	0xdcd4
fread	0xdccc
fwrite	0xdcc2
fclose	0xdcb8
CreateFileA	0xd922
ReadFile	0xd964

Figure 5: Details of encryption module function

Function	Description
GetCurrentThread	Returns a pseudohandle for the current thread
GetStartupInfoA	Retrieves StartupInfo structure contents
StartServiceCtrDispatcherA	Connects the main thread of a service process to the service control manager
RegisterServiceCtrDispatcherA	
CreateServiceA	Creates a service object and adds it to the specified service control manager database
StartServiceA	Starts a service
CryptGenRandom	Secure pseudorandom number generator
CryptAcquireContextA	acquire a handle to a particular key container within a particular cryptographic service provider (CSP)
OpenServiceA	Opens an existing service
GetAdaptersInfo	Retrieves adapter information for the local computer
InternetOpenUrlA	Opens a resource specified by a complete FTP or HTTP URL.

Figure 6: Details of worm module function

```
pyminifakeDNS:: dom.query. 60 IN A 192.168.180.128
Respuesta: watson.microsoft.com. -> 192.168.180.128
Respuesta: teredo.ipv6.microsoft.com. -> 192.168.180.128
Respuesta: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. -> 192.168.180.128
```

After conducting a dynamic analysis, researchers discovered that the worm module uses the InternetOpenUrl function to try to establish a connection with the domain "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com."

"kill switch domain" refers to the aforementioned cyberspace location. If the malware is able to successfully connect to the domain, then the worm module will exit. When the worm module on an infected computer is unable to establish a connection to the specified domain (for example, if the domain is down), it nonetheless continues to run and, using the mssecsvs2.0 process, registers itself as the "Microsoft Security Center Service." For this reason, this kill switch domain may be taken into account during the detection phase of developing a defensive system[7].

B. Persistence Method

If the worm's executable module cannot establish a connection to the kill switch domain, it will attempt to create a "Microsoft Security Center Service" process with the name "mssecsvs2.0." WannaCry's R resource hardcoded binary is retrieved and stored in the "C:Windowsntaskche.exe" directory. An executable binary of the WannaCry encryption module can be found in the R resource. In order to spread, the worm uses the command line parameters "C:Windowsntaskche.exe/i" to run the malicious binary. Finally, to guarantee widespread infections and avoid complications with the tasksche.exe process, the malware will copy the original "C:Windowsntaskche.exe" file and rename it to "C:Windowsnqeriuwjhrf" if the former file already exists. executes every time a computer reboots, the WannaCry binary creates an entry in the Windows registry, the operating system's low-level settings database. The new entry also includes a string (like ATTWIN900) that is a randomly generated identifier for the machine. As soon as the tasksche.exe module is launched, a copy of itself is stored in a newly created directory on the compromised machine. Then, it attempts to establish memory persistence by duplicating itself in AutoRun. In conclusion, the research showed that WannaCry performs the following actions to stay on the in • Makes a note in the Windows Registry that will trigger its execution on each reboot.

- It tries to stay in your system by duplicating itself and joining Windows' autorun feature.
- The attacker uses the icacls command (which grants access to viewing and editing an ACL) to gain complete control of the system and read/write access to all files.
- Eliminates the ability to boot into safe mode by erasing all backups (shadow files) and running a long list of commands in the Windows command prompt.
- Erase all backup directories.
- Executes a large number of Windows command prompt instructions in an effort to terminate running "SQL and MS Exchange" database processes. fected system[7].

C. Encryption

Invoked by the operating system through the Task Start thread. During its operation, the cipher module verifies the presence of the following mutexes:

```
GlobalnMsWinZonesCacheCounterMutexA,
GlobalnMsWinZonesCacheCounterMutexW,
MsWinZonesCacheCounterMutexA.
```

To save time, the encryption module will abort the encryption subsystem on its own if the "MsWinZonesCacheCounterMutexA" system variable is present.

If the victim machine does not have the mutex, encryption can begin. If the mutex does not exist or cannot be made

available, encryption will begin. Once these tasks are finished, the malicious code will generate the configuration files listed in below table.

Name	Description
00000000.res	Tor info
00000000.pky	Public key (RSA)
00000000.eky	Private key (Encrypted - RSA)

Figure 7: WannaCry Configuration files

After these settings files are created, the encryption module can begin protecting critical system data. It does this by spawning a large number of threads. The "CryptGenRandom" method is used to generate an AES key of 128 bits for each file. After the file has been encrypted using this key and it's encrypted using victim's public key which is on RSA format and combined with the header of the file. After a file has been encrypted, the .wncry extension is added to the end of the filename.

D. Propagation

The WannaCry worm module is responsible for the majority of the malware's dissemination and exploitation, specifically the EternalBlue exploit and the DoublePulsar backdoor used to exploit the SMB vulnerability. After confirming communication with the kill switch domain, the worm will begin operating, at which point it will launch the mssecsvs2.0 service and install the ransomware. Using the SMB exploit, this service intends to distribute the malicious payload to all vulnerable devices on the internal and external networks. WannaCry accomplishes this by spawning two separate threads within the affected machine that replicate the worm's payload simultaneously across all affected networks. Calling the "GetAdaptersInfo" function on the internal network, the malware obtains IP addresses of local network interfaces and learns about any existing subnetworks before beginning its propagation phase. Now that it's finished, the worm module will try to connect to all of the IP addresses it found on port 445, the default SMB port in IP. If that succeeds and connections are established to port 443, the worm will try to use those vulnerabilities to compromise the SMB service[8].

E. Recovery

After the successful execution and when encryption process is completed, there are several recovery steps can be followed. These steps are executed by WannaCry to prevent data recovery[7]:

- All backup copies of shadow volumes are deleted using the "wmic shadowcopy delete" command.
- Make use of the "vssadmin" command to get rid of shadows (replicas). All shadow volumes in the system will be deleted without warning. The information on these disks is a backup in case something goes wrong with the system.
- We may now guarantee that the machine boots up by issuing the command "bcdedit/set default bootstatuspolicy ignoreallfailures," which will simply ignore any faults that may occur during the boot process.
- If you want to prevent Windows from using its recovery partition, you can do so with the "bcdedit/set default recovery enabled no" command. In doing so, we block victims' access to earlier states of consciousness.
- When a system is compromised, all backup files stored on the Windows Server will be useless to the intruder unless they run the "wbadmin delete catalog" command.

F. Indicators of compromise

Several of the more alarmingly harmful behaviors exhibited by this strain of the WannaCry ransomware are described below.

- At least one antivirus system has detected malicious code in the sample.
- Several antivirus programs have detected the binary as malicious.
- Efforts to prevent and conceal boot failures
- Memory allocation for a remote process
- Sends information to a distant program
- Protocols in the network using non-standard ports
- Identical YARA signature
- Catalog of backups is removed
- Gets rid of backups of the volume
- File ACLs are updated to reflect the changes.
- Initiates a chain reaction of events.

F. C & C communication

During the malware's installation, it also tries to make contact with the C&C (Command & Control) servers. Next, the s.wnry file is unzipped, and the contents, including the Tor executable, are copied to the installation folder. Malware typically starts listening on localhost at port 9050 before unpacking (127.0.0.1:9050). The Tor browser application is typically configured via the localhost address on ports 9050 or 9001. If the files in the s.wnry zip file cannot be used, WannaCry will try to download the Tor executable from a URL that is hardcoded to the malicious binary code (are corrupted). A copy of "TaskDataTortor.exe" will be made in "TaskDataTortaskhsvc.exe" once the Tor executable is ready for usage. Malware then reads the following ".onion" addresses and the tor client configuration files from the c.wnry file:

- https://dist.torporject.org/torbrowser/6.5.1/tor
- -win32-0.2.9.10.zip
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion
- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion

Following this, the ransomware sends first 8 bytes of the .res file will be send to command and control center. The compromised computer's username and the hostname are stored in these eight bytes. During encryption, a.res file is generated containing 88 bytes of information such as timestamps, flags, and counters.

IV. WANNACRY ANALYSIS

A. Static Analysis

Static analysis is the process of analyzing the malware binary without executing it and observe the malware executable functions and code. Initial process of static analysis is staring with generate and compare the hash value for malware binary.

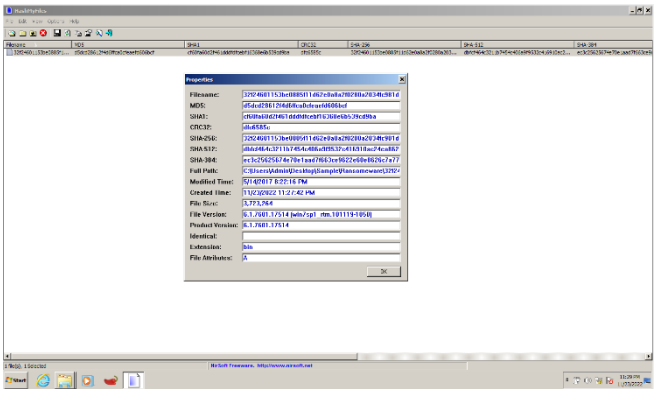

Figure 8: Generated hash values

After obtained the malware we can search various online malware identifying tools for detecting malware as following.

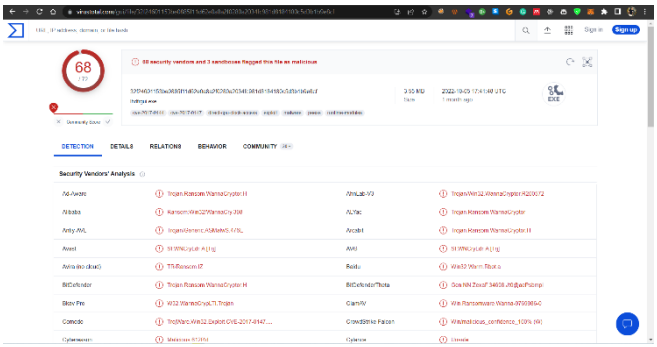

Figure 9: Result of Virus Total

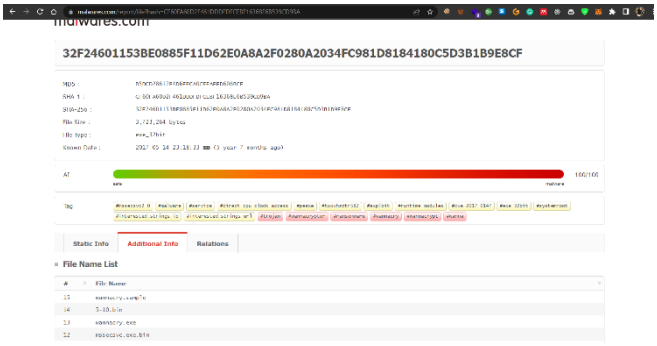

Figure 10: Result of Malwares.com

By observing those results we can ensure that the malware is WannaCry ransomware and next we can conduct the string analysis to identifying any of human readable words, strings inside the malware code. This well helps to identifying malware name, author information, interesting hosts, or URLs etc. The following figure illustrates the results of bintext viewer tool.

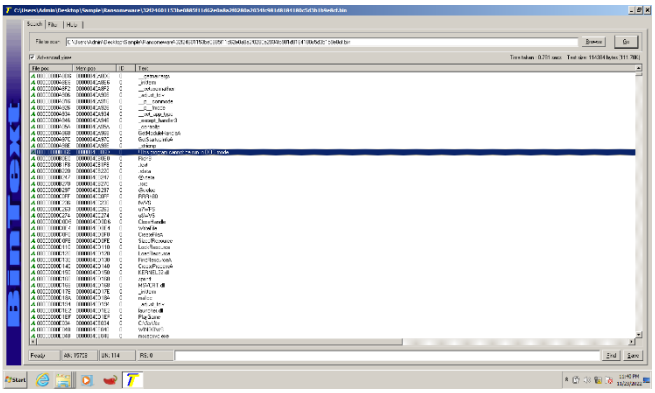

Figure 11: Results of string analysis

By analyzing the strings, we can observer there are some functions to create, delete or modify the files.
Next, we can use hiew32demo tool for analyze the PE header and following figure shows the results.

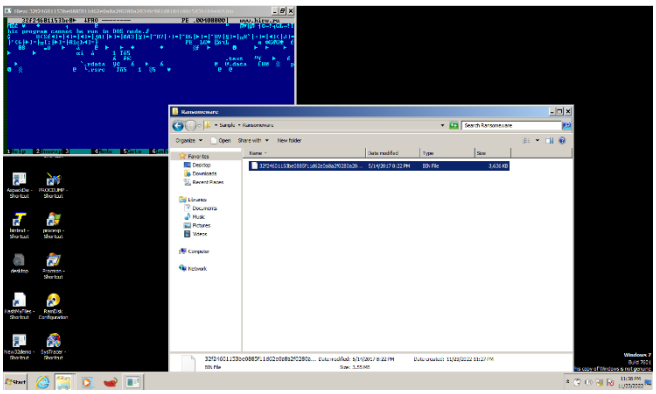

Figure 12: PE header information

Another important part of the static analysis is to identifying import and export table information. For that we can use tool like CFF Explorer to analysis and finding artifacts.

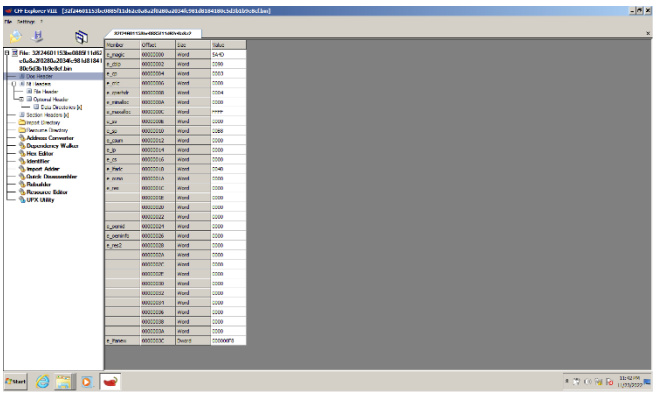

Figure 13: DOS header information

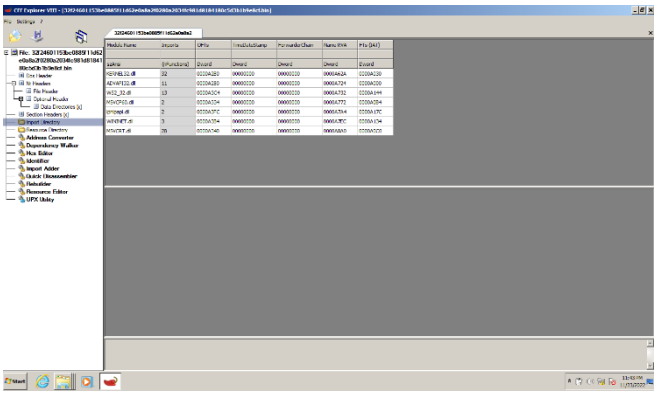

Figure 14: Imports directory

A. Dynamic Analysis

Dynamic analysis is the process of executing malware and closely monitoring the behavior of the malware. First, we are using any run online sandbox for dynamic analysis.

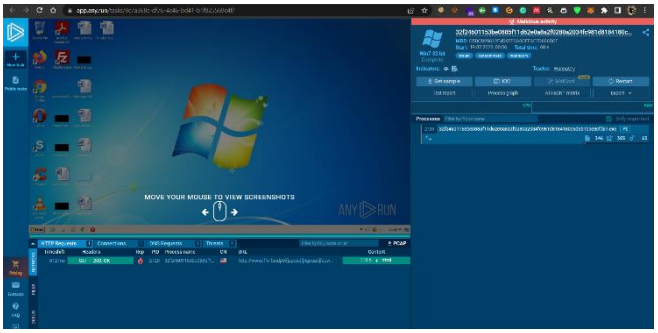

Figure 15: Executing the malware on any. Run

As we can see on the following figure, there are some new files added, deleted from the system when after the execution of malware.

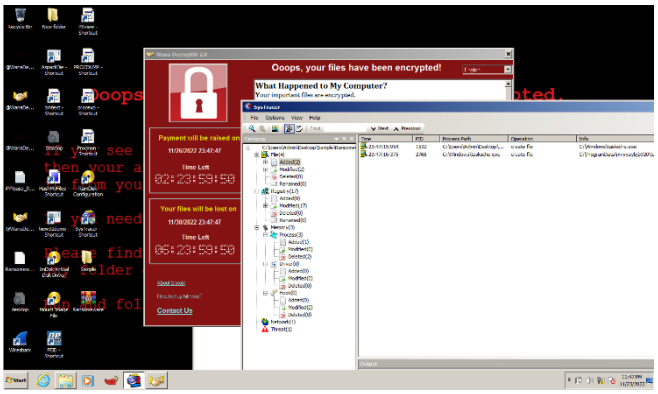

Figure 16: Added files after execution

Figure 17 illustrates, how the malware relates to the command-and-control center by using malicious URL.

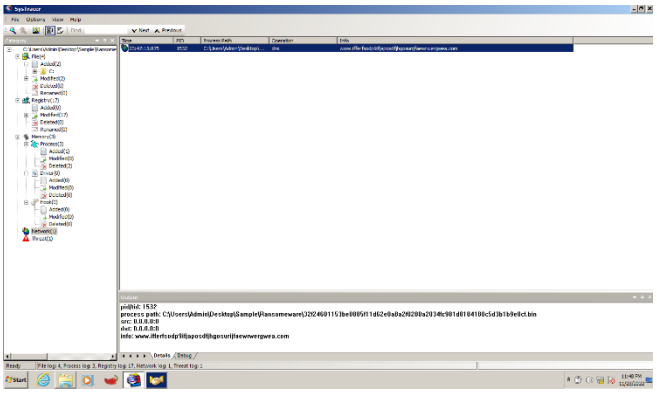

Figure 17: Command and control to the malicious host

Next, we analysis the running processes when the malware is executing. We can observe following suspicious processes created and running as following figure 18.

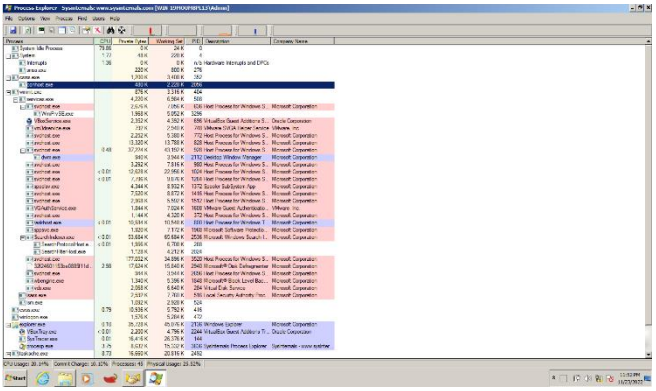

Figure 18: Results of Process explorer

After execution of the malware registry entries had been changed as following.

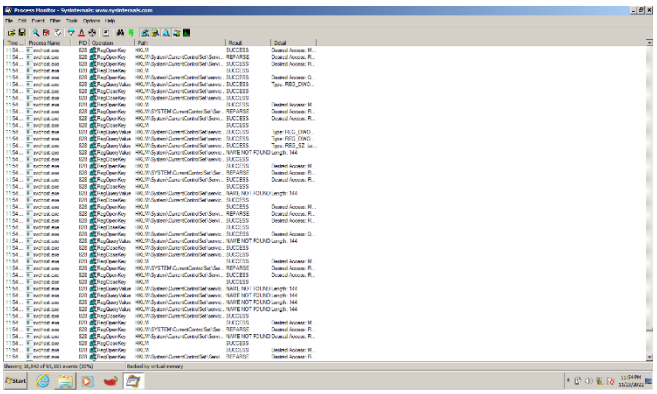

Figure 19: Results of registry changes

Figure 20: Ransom banner after compromised victim's host

We can use the fake net connection to illustrate as malware behaviors on the real network environment and following figure 21 and figure 22 related to the network anomaly detection and analysis for the malware execution. There are lot of malicious packets are created and malware was communicated with different type of malicious hosts.

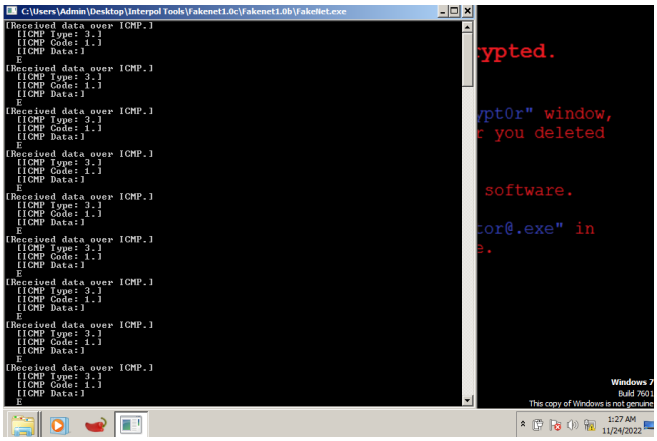

Figure 21: Fake net connection

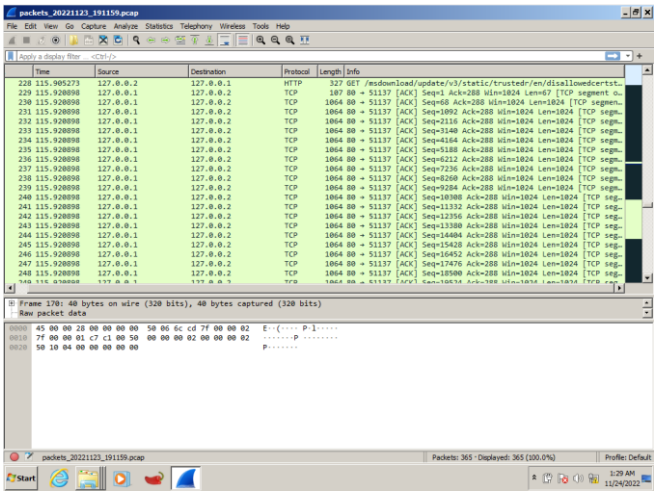

Figure 22: Captured malicious traffic using Wireshark

V. CONCLUSION

The most notorious type of WannaCry ransomware that caused devastation worldwide in 2017 was the subject of in-depth study. Analysis of the malware showed that it is made up of two separate parts. A worm-like module and an encryption module work together to encrypt all of the data on the victim's system after the system has been compromised by the worm-like module. In this study, we examined both units separately. Methods of persistence, encryption, preventing recovery, spreading, communicating with C&C (Command & Control) servers, and initial malware exchanges are the primary areas of study. Crucial characteristics and actions of the malware in action were uncovered by the investigation. Communication between C&C nodes was uncovered to take place over Tor. There were traces of TCP and DNS traffic, SMB querying, and malware that remained persistent. The malicious worm component can exploit and spread via the Microsoft SMB vulnerability on infected devices by sending SMB sample inquiries to the affected devices on port 445. Researchers found that the RSA key was encoded in the WannaCry binary, which allowed them to decrypt the malicious DLL that makes up the encryption module. Upon discovery, it was found that the worm module generates an initial IP address list before scanning both internal and external networks for vulnerable Microsoft SMB workstations. Using the generated host list, the worm sends out SMB packets to port 445 in an attempt to communicate with the hosts. The timing of the execution of the malware payload was also observed to be A binary program verifies its link to the kill switch server. In addition, two IP addresses were found to be hard coded within the SMB packets that were transmitted during SMB enquiry, which was also uncovered by the research. In addition to connecting with the embedded .onion addresses via the insecure port 443 (https port), the virus could also connect via the more commonly used 9001 and 9050 Tor ports to download the installation software for the Tor browser. This is conditional on the contents of the binary's s.wnry dump file. The results of this study can be used to effectively counter WannaCry and other ransomware variants with similar behavior.

VI. ACKNOWLEDGMENT

The author myself wishes to express my gratitude to Mr. Lakmal Rupasinghe, the lecturer in charge of the Information warfare module, for providing guidance and encouragement from the start of this project. I will take my steps to express my gratitude to Mr. Lakmal Rupasinghe, the lecturer on the Information Warfare module for conducting all the lectures for the Module. Additionally, I like to express my gratitude to Ms. Ayesha Wijesooriya and Mr. Binura Ganegoda, who provided a great deal of assistance with conducting lab sessions for the module. Finally, I would like to express my gratitude to everyone who contributed resources and ideas to assist in the completion of this project.

VII. REFERENCES

[1] W. Alraddadi and H. Sarvotham, "A Comprehensive Analysis of WannaCry : Technical Analysis, Reverse Engineering, and Motivation," 2017.

[2] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of wannacry ransomware," *Proc. - 16th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2017*, vol. 2017-Decem, pp. 454–460, 2017, doi: 10.1109/ICMLA.2017.0-119.

[3] "A Vulnerability in Microsoft Windows SMB Server Could Allow for Remote Code Execution (CVE-2020-0796)." https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution-cve-2020-0796_2020-036/ (accessed Jun. 01, 2021).

[4] W. Matsuda, T. Mitsunaga, and M. Fujimoto "Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log," *2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019*, pp. 42–47, 2019, doi: 10.1109/AINS47559.2019.8968703.

[5] "Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs." https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (accessed May 14, 2021).

[6] "PeStudio - Download." https://pestudio.en.lo4d.com/windows (accessed Nov. 21, 2022).

[7] V. G. Vassilakis, and M. D. Logothetis and M. Akbanov "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *J. Telecommun. Inf. Technol.*, no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[8] "Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Player 3 Has Entered the Game: Say Hello to 'WannaCry.'" https://blog.talosintelligence.com/2017/05/wannacry.html (accessed May 25, 2021).

VIII. AUTHOR PROFILE

Shiranthaka K. G. S.

4th year 2nd semester Undergraduate in BSc in Information Technology specialized in Cyber security.
Sri Lanka Institute of Information Technology (Malabe, Sri Lanka)