The Dynamic Analysis of WannaCry Ransomware

Da-Yu KAO[a], Shou-Ching HSIAO[b]

[a]Department of Information Management, Central Police University, Taoyuan City 333, Taiwan

[b]Haishan Precinct, New Taipei City Police Department, New Taipei City 220, Taiwan

[b]**Corresponding Author: oliver84312@gmail.com**

Abstract— **The global ransomware cyberattacks cripples the national hospital system across the United Kingdom, and causes waves of appointments and operations to be cancelled. Similar attacking methods have come to sweep over the world. Such trend of high-profile cyberattack sheds the lights on rapid defence through the malware information sharing platform. A complete malware analysis process is quite a time-consuming campaign. The dynamic analysis of WannaCry ransomware explores behavioural indicators and extracts important IOCs (Indicators of Compromise). Utilizing Yara tool to create customized patterns is useful for malware information sharing mechanism. Also, such mechanism help reduce time and human resource spent on detecting or finding similar malware families. We aim to generate effective cyber threat intelligence by formulating collected IOCs into structured formations. The positive effects show on immediate defensive response to security breaches, and meanwhile the integrated information security protection is consolidated.**

Keywords— **Cyber Threat Intelligence, Ransomware, Dynamic Analysis, Indicators of Compromise, Malware Information Sharing Platform**

I. Introduction

The rise of cyber threat continues to accelerate over the past decades. A surge of attacks with specific goals becomes a substantial cyber threat to individuals and enterprise alike. As organizations severely suffer from malware infection, information sharing becomes a mainstream to cooperatively combat malware. Upon facing the security breaches, first reponders need to conduct a quick analysis and take immediate response. After collecting the ransomware samples, malware analysis is not only to help giving a big picture of the attack, but also to discover the important indicators and signatures for blocking similar attack [1]. The purpose of this paper is to present a dynamic analysis approach in analyzing WannaCry ransomware and generating some actionable intelligences [13].

A. Ransomware

For the past two years, the popularity of ransomware continues to skyrocket and reaches a fever pitch ever since. Every organization may be held to ransom due to the destruction of critical information system. Instead of accessing users' personal information or stealing it, ransomware is a kind of malware that simply blocks users' access to documents or systems [8]. Ransomware is a weapon for extortion by encrypting the victim's data [7]. It is a significant issue for both individuals and enterprise to fight against ransomware.

B. Dynamic Analysis

Dynamic analysis involves running the malware and comparing the differences between infected status and the baselined environment [5]. During execution, the malware will interact with the host system in terms of four main perspectives [10]: ***processes, file system, registry, and network activity***. When an analyst attempts to grab the functionality of malware, one should prioritise the approach of performing dynamic analysis.

C. Cyber Threat Intelligence

Cyber threat intelligence is an advanced concept that enables an organization to prevent security breaches before they occur. Faced with numerous malware variants that are specifically targeting organizations, it's critical to integrate various threat intelligence gathered from community resources, past security breaches, open source intelligence, etc. The indicator of specific malware is a kind of common cyber threat intelligence. It will help identify and mitigate the potential malicious activities. The malware information sharing platform is gathering numerous sources of threat intelligence shared by different communities with a view to offering accurate and actionable intelligence. Via malware information sharing platform, we can better improve the ability to prevent and detect attacks and we are more likely to implement countermeasures to upcoming attacks

The research background is discussed in Section 2. Dynamic analysis and its environment are presented in Section 3. The dynamic analysis on WannaCry ransomware is explored in Section 4. Section 5 describes the IOCs of Wannacry execution. Our conclusions are given in Section 6.

II. Background

In pursuit of immediate financial profits, the primary goal of malware writers has shifted from stealing personal or confidential information to actively hijacking the information systems and important files. The influence on enterprise and individuals are mostly causing the loss of productivity or money. The impact range and magnitude of malware have scaled to an unprecedented level due to the infamous breakout of the ransomware WannaCry. To make matters worse, the service Ransomware-as-a-service(RaaS) have made it a new trend for people who intend to commit cybercrimes. It no longer requires programming ability and hacking techniques to implement ransomware attack, causing the wide spread of ransomware. In this paper, we address malware information sharing platform to share Wannacry YARA signatures. By exchanging threat intelligence, the range and cost of ransomware attack tends to control by zone defence.

A. Malware Information Sharing Platform

In this digital age, malware has become the major reason of information security breaches. Malicious files are interfering with the normal operation of corporation, government agencies, and the public. Malware information sharing is critical for combatting malware infection and sharing the immediate malware information. This interactive platform will synchronize the malware database and combine the functionality with cyber defence tools [3]. The malware information for sharing is the actionable result of quick analysis on newly-emerged malware. The IOCs (Indicators of Compromise) can be categorized into host-based and network-based, and their patterns are the structured-formed analysis results to share among all partners (Fig. 1) [9] [14].

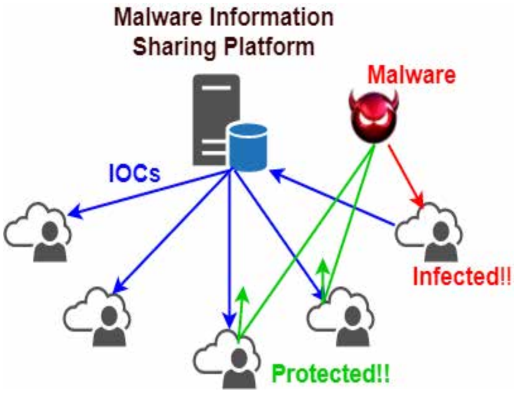


Fig. 1. The mechanism of malware information sharing

B. YARA Rules

YARA is known to be called the pattern-matching Swiss Army knife for information security. It can be implemented across multiple platform and used in command-line interface. YARA is useful for sharing the intelligence of identifying malware and building mechanisms to exploit code similarities. The combination of YARA rules and malware information sharing platform can form zone defence. With the shared synchronized database, members within the community can respond to malicious files or behaviours instantly. By utilizing YARA rules, defenders can better make use of the data captured from security incidents, which makes tracking similar threats and sharing threat information more efficiently

III. Dynamic Analysis and Its Environment

Malware analysis is one of the key strategies to cybercrime investigation, actionable threat intelligence, and information security defence. The goal of dynamic analysis in WannaCry ransomware is to figure out the timeline of security incidents and its malicious patterns. From the perspectives of process, registry, file system, and network activity, a set of IOCs can be proposed to facilitate rebuilding a secure network [9].

A. Perspectives in Dynamic Analysis

1) ***Process:*** Process is the direct indicator of running malware. The observation of process includes the spawning process tree, the parameters, image path, and loaded DLLs.
2) ***Registry:*** In malware analysis, utilizing registry offers valuable information to help understand the followings: changes by specific programs, signs of the infected computer, and artefact of persistence mechanisms.
3) ***File System:*** The increase or decrease of files indicates that the malware may drop malware-related files, modify specific files, or delete the malware-generated artefacts to hide itself. For example, encrypting users' files will lead to frequent file system I/O operations.
4) ***Network Activity:*** Network activity is an important part in malware lifecycle. It is necessary to implement network function for domain name checking, worm propagation, or Command and Control (C&C) server. Upon conducting network analysis, a general observation of network connecting status should be examined at the very beginning. Then the follow-up packet analysis can be utilized to figure out the packet payloads of network activities.

B. The Baseline of Analysis Environment

In order to analyse WannaCry ransomware without actual damage, the malware analysis environment is necessarily isolated from real host and network. At the point of performing behavioural analysis, this paper adopts VMware Workstation to build two host-only machines and configures them in the same LAN (Fig. 2). The baseline of analysis environment and analysis tools are shown below:

- Virtual Machine: VMWare Workstation Pro
- OS: Windows 7 x64 SP1
- Analysis Tools: Process Explorer, Autoruns, Regedit, Process Monitor, Process Hacker, and Wireshark

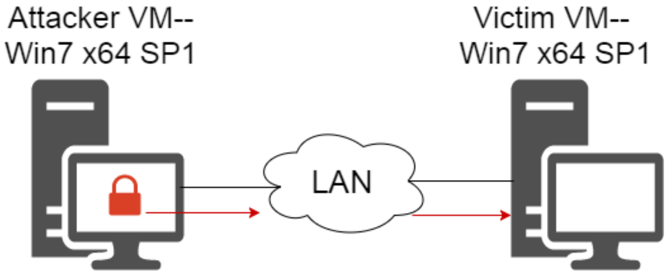


Fig. 2. The baseline of analysis environment

The WannaCry has many kinds of variants from version one to version three. Some of the unprecedented ransomware features in version one or two are not completely developed. Malware authors will keep going on changing the code and start it repeatedly. Some of these different variants just updates the domain name or even disable the initial kill-switch domain check [12]. The propagation code using Eternalblue to exploit MS17-010 vulnerability is uncompleted until the version two variant is released. This paper uses one of the variants as sample: SHA256 hash value is "24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea0 4703480b1022c".

IV. Dynamic Analysis Of WannaCry Ransomware

A typical approach to observe the behaviour of WannaCry is to track system modifications [4]. The changes include what kinds of processes systems have initialized, how many files have been dropped by the malware, the modification of registry key, and the network traffic pattern. This section uses Sysinternals suites and Wireshark to conduct behavioural and network analysis.

A. Process in Process Explorer

This ransomware is a multi-stage campaign. The initial mssecsvc.exe will load the main ransomware tasksche.exe, and launch the following three processes: @WanaDecryptor@.exe, taskdl.exe, and taskse.exe (Fig. 3).

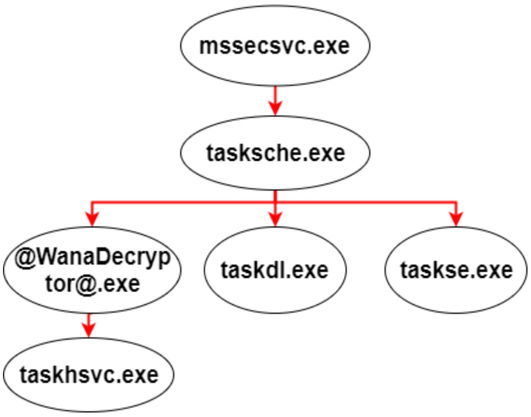


Fig. 3. The relationship of each process

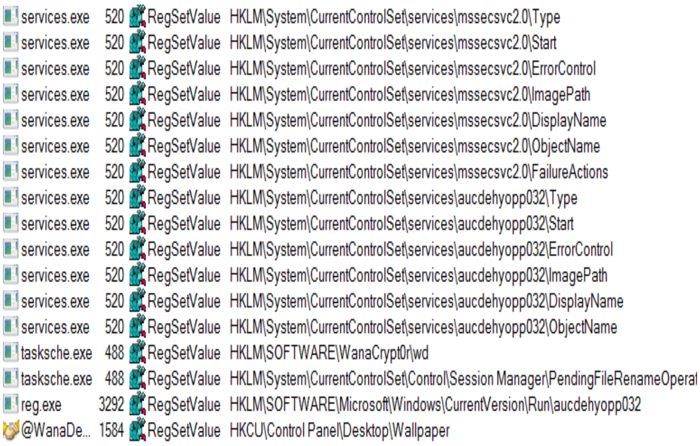
This section uses the Process Explorer of analysis tools to monitor the pop-up processes. Several processes have defined its command parameters to realize different features. The main running processes and their features are listed in Table 1.

TABLE 1. Main Processes and their Features

Process Name	Features	
	parameters	*descriptions*
mssecsvc	N/A	In the beginning of infection, the payload delivered to the infected machine launches mssecsvc within the lsass process without any parameters. 1.Install mssecsvc2.0 service for prpagation. 2.Load resources into the tasksche.exe.
	m security	The "-m security" parameter symbolizes the service mode of mssecsvc called mssecsvc2.0 with "Microsoft Security Service (2.0)" description. This service scans specifically for devices both locally and on the Internet, exposes port 445, exploits the MS17-010 vulnerability, and installs the Doublepulsar backdoor.
tasksche	N/A	The operations are listed as follows: 1. Create the registry: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\aucdehyopp032 2. Release XIA resource 3. Get TOR configuration from c.wnry used in the follow-up onion server connection by @WanaDecryptor@.exe 4. Run command "attrib +h" 5. Run command "icacls . /grant Everyone:F /T /C /Q" 6. Decrypt t.wnry
	i	The parameter "i" implies the installation mode of tasksche. It will first create a working directory C:\Windows\ProgamData\<randomized_id>\tasksche.exe to store its released binaries. Other released binary will be stored in the above directory. After installation, the tasksche will then be executed without parameters.
@WanaDecryptor@	N/A	Present the ransomware user interface.
	fi	Attempt to connect to the onion server (C&C) in the dark web and send the user name, host name, and some information about the infected system. The response may include an updated bitcoin address in c.wnry.
	co	Launch "taskhsvc" as sub-process to do the communication with onion server (C&C) and send some information about encrypting the users' files from 00000000.res, including end time of encryption, the amount, the size of encryption
	vs	Delete volume shadow copies utilizing the Windows built-in vssadmin utility. It will launch the following command as sub-process "vssadmin.exe delete shadows /all /quiet" to implement the shadow deleting utililty.
taskhsvc	N/A	Connect to onion server (C&C). This is the same binary as the "tor.exe" but renamed by the Wannacry to evade detection of dark web communication.
taskdl	N/A	SQL Client Configuration Utility, which also impersonates as the Microsoft Corporation process.
taskse	N/A	Utility used to launch @WanaDecryptor@.exe

B. Registry in Process Monitor and Autoruns

This paper uses Autoruns and Process Monitor tools to monitor the added registry value by WannaCry (Fig. 4). Different registry key represents different functionality in the system. Some of the keys are for autoruns, and others are supporting the ransomware operations.



```
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\Type
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\Start
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\ErrorControl
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\ImagePath
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\DisplayName
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\ObjectName
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\mssecsvc2.0\FailureActions
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\Type
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\Start
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\ErrorControl
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\ImagePath
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\DisplayName
services.exe   520  RegSetValue  HKLM\System\CurrentControlSet\services\aucdehyopp032\ObjectName
tasksche.exe   488  RegSetValue  HKLM\SOFTWARE\WanaCrypt0r\wd
tasksche.exe   488  RegSetValue  HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperat
reg.exe       3292  RegSetValue  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\aucdehyopp032
@WanaDe...    1584  RegSetValue  HKCU\Control Panel\Desktop\Wallpaper
```

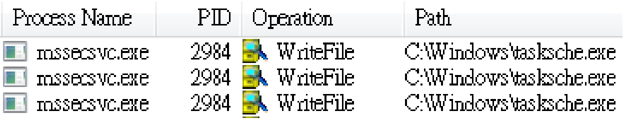
Fig. 4. HKEY_CURRENT_USER\Software\WanaCrypt0r\wd

C. File System in Process Monitor

While observing effect on file system, we mainly focus on newly added files and deleted files. In the case of Wannacry, it generally adds two types of files on the infected system: Wannacry-related binaries and victim encrypted files.

The mssecsvc.exe will first create tasksche.exe in directory 'C:\WINDOWS\', rename it to "qeriuwjhrf", and prepares to load resource into tasksche. The purpose of this behaviour is to prevent users from defending the real "tasksche.exe" of WannaCry by using disguised "tasksche.exe" in Process Monitor (Fig. 5).

- C:\WINDOWS\tasksche
- C:\WINDOWS\qeriuwjhrf



```
Process Name   PID   Operation   Path
mssecsvc.exe   2984  WriteFile   C:\Windows\tasksche.exe
mssecsvc.exe   2984  WriteFile   C:\Windows\tasksche.exe
mssecsvc.exe   2984  WriteFile   C:\Windows\tasksche.exe
```

Fig. 5. "tasksche.exe" is created by mssecsvc.exe

The tasksche.exe run with "/i" parameters will unzip resource XIA with password "WNCry@2ol7" in its .rsrc section, and drop the following folders and files to C:\ProgramData\kzvuujeikxgdr888\:

- C:\ProgramData\kzvuujeikxgdr888\msg (the folder that contains message in different languages)
- C:\ProgramData\kzvuujeikxgdr888\@Please_Read_me@.txt
- C:\ProgramData\kzvuujeikxgdr888\b.wnry
- C:\ProgramData\kzvuujeikxgdr888\c.wnry
- C:\ProgramData\kzvuujeikxgdr888\r.wnry
- C:\ProgramData\kzvuujeikxgdr888\s.wnry
- C:\ProgramData\kzvuujeikxgdr888\t.wnry
- C:\ProgramData\kzvuujeikxgdr888\u.wnry
- C:\ProgramData\kzvuujeikxgdr888\tasksche
- C:\ProgramData\kzvuujeikxgdr888\taskdl
- C:\ProgramData\kzvuujeikxgdr888\taskse
- C:\ProgramData\kzvuujeikxgdr888\@WanaDecryptor@.exe
- C:\ProgramData\kzvuujeikxgdr888\00000000.eky
- C:\ProgramData\kzvuujeikxgdr888\00000000.pky
- C:\ProgramData\kzvuujeikxgdr888\00000000.res

The WannaCry will put the ransom bitmap in current user desktop for wallpaper substitution:

- C:\Users\<Current_User>\Desktop\@WanaDecryptor@.bmp

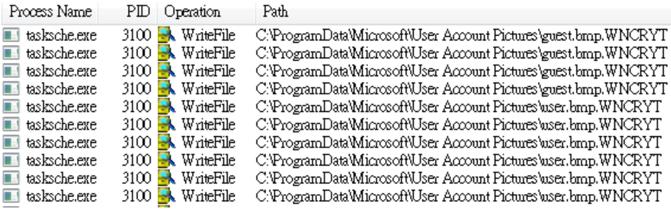
During the encryption routine, the ransomware will put two ransom-related files in each folder:

- <Encrypted_Folder>\@WanaDecryptor@.exe
- <Encrypted_Folder>\@Please_Read_me@.txt

TABLE 2. REGISTRY MODIFICATION TABLE

Process (set by)	**Descriptions**		
	key	***data***	***features***
services.exe	HKLM\System\CurrentControlSet\Services \mssecsvc2.0	ImagePath: cmd.exe /c "C:\ProgramData\aucdehyopp032\tasksche.exe" DisplayName: aucdehyopp032	Autorun
	HKLM\System\CurrentControlSet\Services \aucdehyopp032	ImagePath: C:\Users\S\Desktop\mssecsvc.exe -m security DisplayName: Microsoft Security Center (2.0) Service	Autorun
reg.exe	HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run	aucdehyopp032: "C:\ProgramData\aucdehyopp032\tasksche.exe"	Autorun
tasksche.exe	HKLM\Software\WanaCrypt0r	wd: C:\ProgramData\aucdehyopp032	Prevent accidentally encrypting itself.
	HKLM\System\CurrentControlSet\Control\ Session Manager	PendingFileRenameOperations	Original file name is preserved in this key for deletion after encryption.
@WanaDecryptor@.exe	HKCU\Control Panel\Desktop	Wallpaper: C:\Users\S\Desktop\@WanaDecryptor@.bmp	Present the ransom declaration on the desktop.

The WannaCry will copy the file contents from the original files into memory and append the ".WNCRYT" extension to store the encrypted files (Fig. 6). The original files are deleted after encryption.

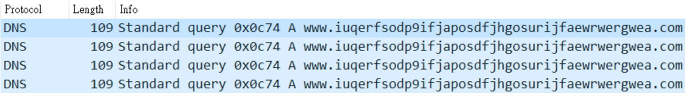


```
Process Name   PID   Operation   Path
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\guest.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\guest.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\guest.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\guest.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
taksche.exe    3100  WriteFile   C:\ProgramData\Microsoft\User Account Pictures\user.bmp.WNCRYT
```

Fig. 6. Writing "WNCRYT" files

D. Network Activity in Process Hacker and Wireshark

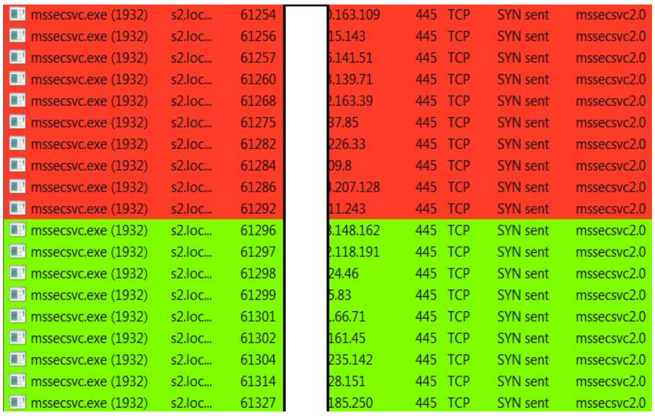
In network perspective, the Process Hacker of analysis tools is used to view the rough network connection, while Wireshark is adopted to capture, filter, and inspect details on packets. Malware behaviour focuses on the Command-and-control network, the worm propagation activities, and the TOR communication network flow. This executable sends a request to the domain "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" for connection (Fig. 7). Once the website responds normally, then the binary exists.



```
Protocol  Length  Info
DNS          109  Standard query 0x0c74 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
DNS          109  Standard query 0x0c74 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
DNS          109  Standard query 0x0c74 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
DNS          109  Standard query 0x0c74 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
```

Fig. 7. Kill-switch domain query

After the domain check, the mssecsvc.exe will register the mssecsvc2.0 service and enter the service mode for propagation. The mssecsvc2.0 will repeatedly send TCP SYN packets to port 445 of both LAN and randomly IP in WAN to attemp propagation (Fig. 8). The malware evidently escalates the scale of spreading in other devices, and leverages the NetBIOS packets that are not blocked from outside to spread across the Internet. This stands for the widespread infection at first outbreak and the reason that makes it difficult to judge the initial vector malware may emanate from.



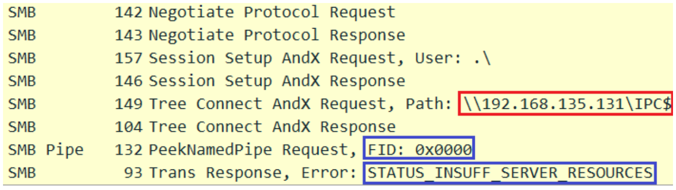
```
mssecsvc.exe (1932)  s2.loc...  61254  [redacted]  .163.109  445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61256  [redacted]  15.143    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61257  [redacted]  .141.51   445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61260  [redacted]  .139.71   445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61268  [redacted]  .163.39   445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61275  [redacted]  37.85     445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61282  [redacted]  226.33    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61284  [redacted]  09.8      445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61286  [redacted]  .207.128  445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61292  [redacted]  11.243    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61296  [redacted]  .148.162  445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61297  [redacted]  .118.191  445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61298  [redacted]  24.46     445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61299  [redacted]  5.83      445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61301  [redacted]  .66.71    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61302  [redacted]  161.45    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61304  [redacted]  235.142   445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61314  [redacted]  28.151    445  TCP  SYN sent  mssecsvc2.0
mssecsvc.exe (1932)  s2.loc...  61327  [redacted]  185.250   445  TCP  SYN sent  mssecsvc2.0
```

Fig. 8. The network propagation of mssecsvc.exe

Once a machine with an open NetBIOS port is found, the WannaCry will gain TCP socket for port 445, connect to SMB socket, and get SMB tree id for later use. Another characteristic is that the malware will send three NetBIOS session setup packets to it. One has the proper IP address (192.168.135.131) of the machine being exploited. Others contain two IP addresses (192.168.56.20 and 172.16.99.5) in the malware body. The phenomenon and characteristic of the exact host IP address is for the MS17-010 SMB RCE detection [11].

1) MS17-010 SMB RCE Detection

The detection method is to use information disclosure to determine if MS17-010 has been patched [11]. WannaCry connects to the IPC$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", it indicates that the machine does not have the MS17-010 patch (Fig. 9).

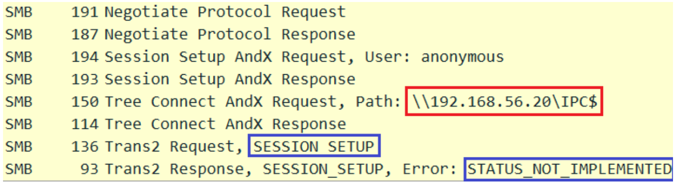


```
SMB        142 Negotiate Protocol Request
SMB        143 Negotiate Protocol Response
SMB        157 Session Setup AndX Request, User: .\
SMB        146 Session Setup AndX Response
SMB        149 Tree Connect AndX Request, Path: \\192.168.135.131\IPC$
SMB        104 Tree Connect AndX Response
SMB Pipe   132 PeekNamedPipe Request, FID: 0x0000
SMB         93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

Fig. 9. The detecting packets by Wireshark

2) SMB Doublepulsar Probe

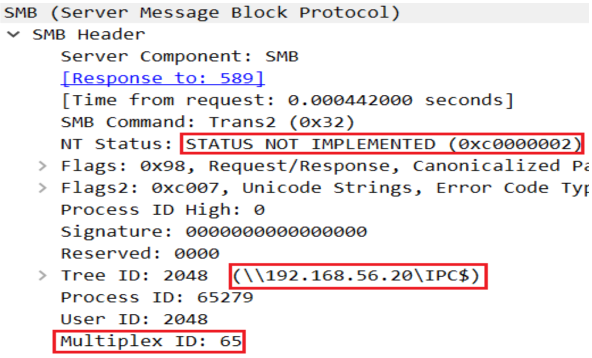
The intent of the SESSION SETUP Trans2 Request is to check if the system is already compromised with the Doublepulsar backdoor (Fig. 10).



```
SMB   191 Negotiate Protocol Request
SMB   187 Negotiate Protocol Response
SMB   194 Session Setup AndX Request, User: anonymous
SMB   193 Session Setup AndX Response
SMB   150 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB   114 Tree Connect AndX Response
SMB   136 Trans2 Request, SESSION_SETUP
SMB    93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
```

Fig. 10. The probing packets by Wireshark

If the field "Multiplex ID" is equal to 65(0x41), it indicates the current system is normal systems (Fig. 11). Otherwise, "Multiplex ID" is equal to 81(0x51). It means the system has already been infected with Doublepulsar backdoor.

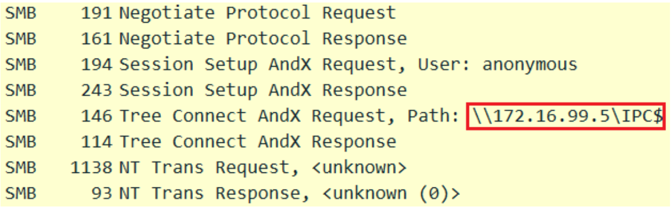


```
SMB (Server Message Block Protocol)
  v SMB Header
        Server Component: SMB
        [Response to: 589]
        [Time from request: 0.000442000 seconds]
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
      > Flags: 0x98, Request/Response, Canonicalized Pa
      > Flags2: 0xc007, Unicode Strings, Error Code Typ
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
      > Tree ID: 2048  (\\192.168.56.20\IPC$)
        Process ID: 65279
        User ID: 2048
        Multiplex ID: 65
```

Fig. 11. The SMB Header of Trans2 Response

3) *Triggering the Vulnerability*

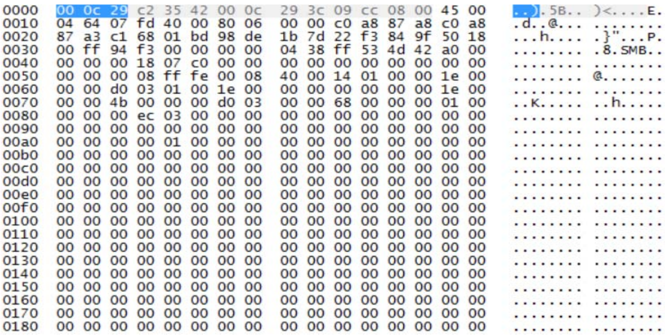
If the detection result shows that the target contains MS17-010 vulnerability and yet not infected with Doublepulsar backdoor, it will proceed to install Doublepulsar backdoor through Eternalblue exploit (Fig. 12).



```
SMB     191 Negotiate Protocol Request
SMB     161 Negotiate Protocol Response
SMB     194 Session Setup AndX Request, User: anonymous
SMB     243 Session Setup AndX Response
SMB     146 Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
SMB     114 Tree Connect AndX Response
SMB    1138 NT Trans Request, <unknown>
SMB      93 NT Trans Response, <unknown (0)>
```

Fig. 12. The vulnerability triggering packets by Wireshark

An initial NT Trans request comprises a sequence of NOPs. This is intended to look for where the vulnerability exists in the compromised devices. The attacker can leverage a specialized-crafted packet to exploit targets' SMB protocol (Fig. 13). The large NT Trans request causes multiple Secondary Trans Requests and serves as indicators for attackers to trigger the vulnerability.



```
0000  00 0c 29 c2 35 42 00 0c  29 3c 09 cc 08 00 45 00   ..).5B.. )<....E.
0010  04 64 07 fd 40 00 80 06  00 00 c0 a8 87 a8 c0 a8   .d..@... ........
0020  87 a3 c1 68 01 bd 98 de  1b 7d 22 f3 84 9f 50 18   ...h.... .}"...P.
0030  00 ff 94 f3 00 00 00 00  04 38 ff 53 4d 42 a0 00   ........ .8.SMB..
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 08 ff fe 00 08  40 00 14 01 00 00 1e 00   ........ @.......
0060  00 00 d0 03 01 00 1e 00  00 00 00 00 00 00 1e 00   ........ ........
0070  00 00 4b 00 00 00 d0 03  00 00 68 00 00 00 01 00   ..K..... ..h.....
0080  00 00 00 ec 03 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 01 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Fig. 13. The large sequence of NOPs

4) *Doublepulsar Instrcution*

After the completion of Eternalblue attack, the control transfers to the doubepulsar backdoor. A series of SMB packets are sent between the WannaCry propagating machine and the targeted victim with the Doublepulsar instructions in specific hidden fields (Fig. 14).

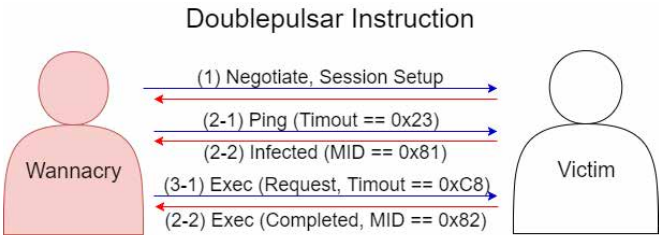
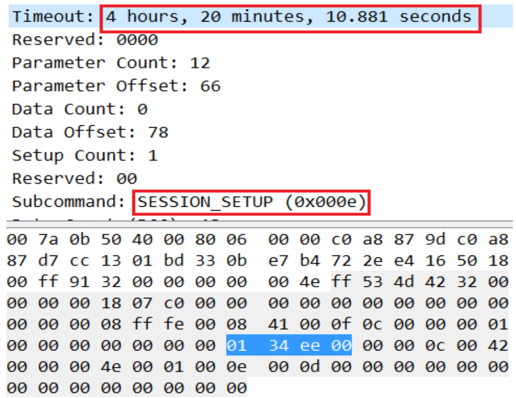

Doublepulsar Instruction
Wannacry
Victim
(1) Negotiate, Session Setup
(2-1) Ping (Timout == 0x23)
(2-2) Infected (MID == 0x81)
(3-1) Exec (Request, Timout == 0xC8)
(2-2) Exec (Completed, MID == 0x82)

Fig. 14. Doublepulsar instruction

a. *Ping Request*

After the initial negotiate and session setup, the WannaCry will send a ping request to the target by sending multiple ping packets to the compromised device. The purpose of ping request is to check if the hook of Doublepulsar is installed successfully. The "ping" instruction is hidden in the "Timeout" field, which is originally the amount of time the client waits for the server to respond to an outstanding request (Fig. 15). According to the Microsoft Open Specifications, the default value of Timeout field is set to 45 seconds. In the experiment, the Timeout field is set to 4 hours 20 minutes 10.881 seconds (0x00ee3401). This abnormal Timeout value is actually not referring to the time out set, but implying the Doublepulsar instruction opcode. The algorithm of calculating this opcode is adding each byte and removing the overflow as result. The intent of the ping command is to check if the Doublepulsar backdoor has successfully installed on the infected system.



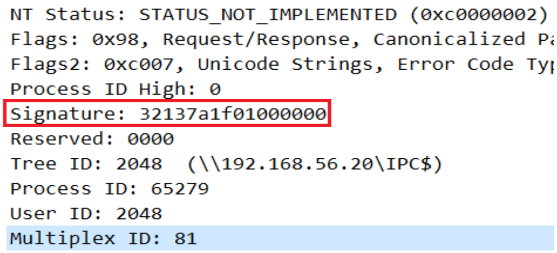
```
Timeout: 4 hours, 20 minutes, 10.881 seconds
Reserved: 0000
Parameter Count: 12
Parameter Offset: 66
Data Count: 0
Data Offset: 78
Setup Count: 1
Reserved: 00
Subcommand: SESSION_SETUP (0x000e)

00 7a 0b 50 40 00 80 06  00 00 c0 a8 87 9d c0 a8
87 d7 cc 13 01 bd 33 0b  e7 b4 72 2e e4 16 50 18
00 ff 91 32 00 00 00 00  00 4e ff 53 4d 42 32 00
00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00
00 00 00 08 ff fe 00 08  41 00 0f 0c 00 00 00 01
00 00 00 00 00 00 00 01  34 ee 00 00 00 0c 00 42
00 00 00 4e 00 01 00 0e  00 0d 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Fig. 15. "Ping" command in hidden Timeout field

b. *Ping Response: Infected*

While the Doublepulsar backdoor responds to the "ping" command with the field "Multiple ID (MID)" set to 0x81, it implies the presence of itself. This packet has another implication using the "Signature" field (Fig. 16). The signature field is set to value 0x011f7a1332. The first byte(0x01) means the machine is the x64 platform. As for the rest four bytes (0x1f7a1332) is the encrypted XOR key, which will use for the packet payload encryption afterwards.

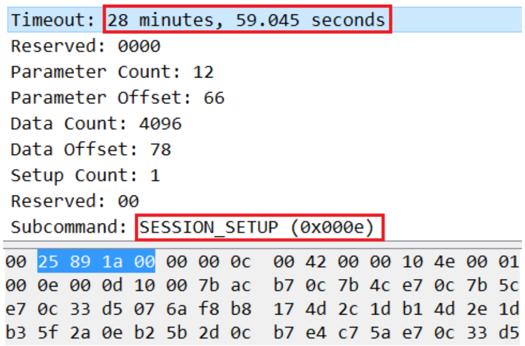


```
NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
Flags: 0x98, Request/Response, Canonicalized Pa
Flags2: 0xc007, Unicode Strings, Error Code Typ
Process ID High: 0
Signature: 32137a1f01000000
Reserved: 0000
Tree ID: 2048  (\\192.168.56.20\IPC$)
Process ID: 65279
User ID: 2048
Multiplex ID: 81
```

Fig. 16. Hidden Response in MID field with Signature field set to contain XOR key

c. *Exec Request*

After the confirmation of backdoor presence, the WannaCry will resume sending the "exec" Doublepulsar command to the target and order the backdoor on the target to start the injection of the ransomware into lsass process. As indicated in the "ping" command, the packet sets the "Timeout" field to an abnormal value. In the "exec" command, the value will once again set the "Timeout" field to the value 0x001a8925 (Fig. 17).



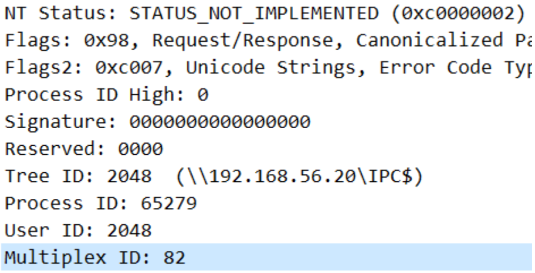
```
Timeout: 28 minutes, 59.045 seconds
Reserved: 0000
Parameter Count: 12
Parameter Offset: 66
Data Count: 4096
Data Offset: 78
Setup Count: 1
Reserved: 00
Subcommand: SESSION_SETUP (0x000e)

00 25 89 1a 00 00 00 0c  00 42 00 00 10 4e 00 01
00 0e 00 0d 10 00 7b ac  b7 0c 7b 4c e7 0c 7b 5c
e7 0c 33 d5 07 6a f8 b8  17 4d 2c 1d b1 4d 2e 1d
b3 5f 2a 0e b2 5b 2d 0c  b7 e4 c7 5a e7 0c 33 d5
```

Fig. 17. "Exec" command hidden in Timeout field

d. *Exec Response: Completed*

As the shellcode completed, the Doublepulsar backdoor will send a packet with the field MID set to 0x82, meaning that the task is completed (Fig. 18).



```
NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
Flags: 0x98, Request/Response, Canonicalized Pa
Flags2: 0xc007, Unicode Strings, Error Code Typ
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
Tree ID: 2048  (\\192.168.56.20\IPC$)
Process ID: 65279
User ID: 2048
Multiplex ID: 82
```

Fig. 18. Task completed

V. Shareable Malware Information: IOCs

Yara offers the opportunity to create customized rules for binary signature and promotes the detection rate of newly-discovered malware. By analyzing the malicious code, we are able to find specific patterns for malware. In our condition, we apply the patterns of WannaCry to YARA rules, and members among the malware information sharing platform mechanism can benefit from collected intelligence. The following YARA rules match the dropped resource binaries and SMB exploit.

A. *Rule WannaCry: Resource Binary*

In the file system analysis part, many unique resource binaries are found. These binaries are used as patterns in a representative form of YARA rules as shown below:

```
rule WannaCry: Resource Binary{
        meta:
          description = "Detect resource binaries "
          resource = "XIA"

        strings:
           $binary 1 = "taskdl.exe"
           $binary 2 = "taskse.exe"

           $wnry 1 = "b.wnry"
           $wnry 2 = "c.wnry"
           $wnry 3 = "r.wnry"
           $wnry 4 = "s.wnry"
           $wnry 5 = "t.wnry"
           $wnry 6 = "u.wnry"

           $key 1 = "00000000.eky "
           $key 2 = "00000000.pky "

        condition:
           all of ($binary*) and 3 of ($wnry*) and all of ($key*)
}
```

B. *Rule WannaCry:_SMB_ms17010*

WannaCry will do the SMB tree connection, which has the SMB header of "SMBr" (0x534D4272), "SMBs" (0x534D42 73), "SMBu" (0x534D4275), and "SMB2" (0x534D4232) respectively. In addition, two hardcoded IP addresses are used to do the null connection for detecting the exploit. Therefore, we use the unique patterns of the packets content throughout the tree connection, and these patterns can be matched in the following rule:

```
rule WannaCry:_SMB_ms17010 {
    meta:
      description = "Detect WannaCrypt0r propagation"
      hash1                                          =
  "24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614e
  a04703480b1022c"
    strings:
      $op1 = {53 4D 42 72 00 00 00 00 18 53 C0 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 FF FE 00 00 40 00  00 62 00
  02 50 43 20 4E 45 54 57 4F 52 4B 20 50  52 4F 47 52 41
  4D 20 31 2E 30 00 02 4C 41 4E 4D  41 4E 31 2E 30 00 02
  57 69 6E 64 6F 77 73 20 66 6F 72 20 57 6F 72 6B 67 72 6F}
      $op2 = {53 4D 42 73 00 00 00 00 18 07 C0 00 00 00 00
  00 00 00 00  00 00 00 00 00 00 FF FE 00 00 40 00 0D FF
  00 88  00 04 11 0A 00 00 00 00 00 00 00 01 00 00 00 00
  00 00 00 D4 00 00 00 4B 00 00 00 00 00 00 57 00  69 00
  6E 00 64 00 6F 00 77 00 73 00 20 00 32 00  30 00 30 00 }
      $op3 = {53 4D 42 75 00 00 00 00 18 07 C0 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 FF FE 00 08 40 00 04 FF 00
  5C 00 08 00 01 00 31 00 00 5C 00 5C 00 31 00 39 00 32 00
  2E 00 31 00 36 00 38 00 2E 00 35 00 36 00  2E 00 32 00
  30 00 5C 00 49 00 50 00 43 00 24 00  00 00 3F 3F 3F 3F
  3F 00 00 00 00 4E FF }
      $op4 = {53 4D 42 32 00 00 00 00 18 07 C0 00 00 00 00
  00 00 00 00 00 00 00 00 00 08 FF FE 00 08 41 00 0F 0C 00
  00 00 01 00 00 00 00 00 00 00 01 34 EE 00 00 00 0C 00 42
  00 00 00 4E 00 01 00 0E 00 0D}

      $s1 = "\\\\192.168.56.20\\IPC$" fullword wide
      $s2 = "\\\\172.16.99.5\\IPC$" fullword wide


    condition:
          uint16(0) == 0x5a4d and all of ($s*) and 2 of ($op*)
  and        pe.imports("ws2_32.dll",       "connect")       and
  pe.imports("ws2_32.dll",                 "send")           and
  pe.imports("ws2_32.dll", "recv") and
```

```
    pe.imports("ws2_32.dll", "socket")
}
```

VI. Conclusions

The outbreak of WannaCry inaugurates a new era of ransomware attack. The shutdown of critical information system casts a huge gloom over the society. The imagination of cyber criminals taking over traffic control system or medical health care system is terrifying no less than bombs or missiles attack. This paper conducts dynamic analysis to understand process, registry, file system, and network activities. This interactive behavioral analysis aids the integration of cyber defense, accumulates substantial amounts of malware indicators, and strengthens the malware information sharing mechanism. Multidimensional cooperation to connect threat information is imperative to defeat advanced malware attacks. The application of synchronization of malware database gives protection against the continuous growth of ransomware threats.

Acknowledgment

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-107) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 106-2221-E-015-002-.

References

[1] Awad, R. A. and Sayre, K. D., “Automatic Clustering of Malware Variants,” 2016 IEEE Conference on Intelligence and Security Informatics (ISI 2016), pp. 298–303, 2016.

[2] Ceron, J. M., Margi, C. B., and Granville, L. Z., “MARS: An SDN-based Malware Analysis Solution,” in 2016 IEEE Symposium on Computers and Communication (ISCC), pp. 525–530, June 2016.

[3] Friedman, J. and Bouchard, M., *Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks*, Cyberedge Press, pp. 1-60, 2015.

[4] Fujino, A., Murakami, J., and Mori, T., “Discovering Similar Malware Samples Using API Call Topics,” in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pp. 140–147, Jan 2015.

[5] Hansen, S. S., Larsen, T. M. T., Stevanovic, M., and Pedersen, J. M., “An Approach for Detection and Family Classification of Malware Based on Behavioral Analysis,” in 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1–5, Feb 2016.

[6] Islam, A., Oppenheim, N., and Thomas, W., “SMB Exploited: WannaCry Use of Eternalblue.” [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-Eternalblue.html

[7] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., and Kirda, E., “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware,” in 25th USENIX Security Symposium (USENIX Security 16), pp. 757–772, USENIX Association, 2016.

[8] Liska, A. and Gallo, T., *Ransomware: Defending Against Digital Extortion*, 1st Edition, O’Reilly Media Inc., pp. 1-22, 2016.

[9] Lock, H. Y., 'Using IOC (Indicators of Compromise) in Malware Forensics,' SANS Institute, pp. 2-11, 2013.

[10] Malin, C. H., Casey, E., Aquilina, J. M., and Rose, C. W., *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field*, Elsevier Inc., pp. 363-400, 2012.

[11] Microsoft, “Microsoft Security Bulletin MS17-010 - Critical: Security Update for Microsoft Windows SMB Server (4013389).” [Online]. Available: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[12] Mosli, R., Li, R., Yuan, B., and Pan, Y., “Automated Malware Detection Using Artifacts in Forensic Memory Images,” in 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1–6, May 2016.

[13] Rousseau, A., “WCry/WanaCry Ransomware Technical Analysis.” [Online]. Available: https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis

[14] Rudman, L. and Irwin, B., “Dridex: Analysis of the Traffic and Automatic Generation of IOCs,” in 2016 Information Security for South Africa (ISSA), pp. 77–84, Aug 2016.

Da-Yu Kao is an Associate Professor at Department of Information Management, Central Police University, Taiwan. With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.

Shou-Ching Hsiao is an information lieutenant at Haishan Precinct, New Taipei City Police Department, Taiwan. She is responsible for information system management, information security, and real-time video for security control. She can be reached at oliver84312@gmail.com.