ARL-TR-8627 ● JAN 2019

US Army Research Laboratory

Hands-on Cybersecurity Studies: Multi-Perspective Analysis of the WannaCry Ransomware

by Jaime C Acosta, Adriana Escobar de la Torre, and Salamah Salamah

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when no longer needed. Do not return to the originator.

ARL-TR-8627 ● JAN 2019

US Army Research Laboratory

Hands-on Cybersecurity Studies: Multi-Perspective Analysis of the WannaCry Ransomware

by Jaime C Acosta
Computational and Information Sciences Directorate, ARL

Adriana Escobar de la Torre and Salamah Salamah
University of Texas at El Paso, El Paso, TX

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
January 2019	Technical Report	January 2018–January 2019

4. TITLE AND SUBTITLE
Hands-on Cybersecurity Studies: Multi-Perspective Analysis of the WannaCry Ransomware

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jaime C Acosta, Adriana Escobar de la Torre, Salamah Salamah

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
ATTN: RDRL-CIN-D
White Sands Missile Range, NM 88002-5501

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-8627

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
When the WannaCry ransomware was first launched in May 2007, it led to devastating impacts due to the continued use of unpatched and vulnerable software. In this technical report, we describe one of the earlier versions of the ransomware and then provide a series of steps, in the form of an educational exercise, to set up and analyze the malware. We include a multi-perspective analysis of the malware using system observation, network packet analysis, and reverse engineering. In the final steps of the exercise, we describe near-term fixes to stop the malware spread (by implementing a kill switch, which is uncovered through the exercise) and also longer-term mitigations and best practices to protect against similar malware in the future.

15. SUBJECT TERMS
forensics, malware, hands-on cybersecurity, CyberRIG, WannaCry

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jaime C Acosta
Unclassified	Unclassified	Unclassified	UU	23	19b. TELEPHONE NUMBER (Include area code) (575) 993-2375

Contents

List of Figures

1. Introduction

Ransomware is malware that essentially obstructs a user from accessing digital assets through various mechanisms. These assets are held hostage and inaccessible until a user pays a ransom. In most cases, this is accomplished using encryption; where, once the malicious program executes, it will target and encrypt certain files and will release the decryption key at the time of payment. Some ransomware instances target only certain common user-generated files such as media and documents. In this case, system files and others required for the operating system to function correctly (user authentication, process execution, etc.) are unaffected. Others encrypt much more and seek to lock out entire systems.

The spread of ransomware is accomplished through various channels including business applications, USB drives, websites, and email. Email, however, is the most prevalent[1] through the use of phishing campaigns. To this end, from 2016–2018, the number of emails carrying ransomware increased by 6,000%.

WannaCry is ransomware that was originally released in May 2017. WannaCry demanded ransoms be paid in the form of bitcoin, in attempts to preserve anonymity. Although different for variants of WannaCry, the initial amount started at $300 worth of bitcoin and increased to $600 after 72 h. After 7 days, the files were permanently inaccessible. A few months later, in August 2017, the WannaCry operator(s) converted the collected bitcoins to Monero, which is claimed to be more anonymous due to its use of distributed consensus through ring signatures.[2]

While the WannaCry binary file can be spread through email—in which case, a user downloads and executes the file—it can also spread without human intervention. This is because it takes advantage of unpatched Windows Operating Systems that have the Server Message Block version 1 (SMBv1) service enabled (typically used for file sharing). More information about this vulnerability and the associated proof of concept can be found in the Microsoft Security Bulletin.[3] Certain variants of WannaCry would test, before spreading, whether a Domain Name Server (DNS) entry to a specific URL could be resolved. If resolved, then the malware would halt; otherwise, it would spread. This was known as the WannaCry kill switch and was identified a few days after its launch, which helped to slow the spread of the malware. However, hours later, other variants, with the removed kill switch, were released and continued to spread and infect victim machines.

In this report, we describe a multi-perspective analysis of the WannaCry ransomware in the form of a cybersecurity exercise. We start by documenting the

setup, including the software and network configurations. Next, we provide the annotated exercise document, and then conclude with a summary of learning objectives and mitigations.

2. Setup and Configuration

We based our setup, configuration, and analysis on Colin Hardy's walkthrough[4] of identifying different ways of finding the malware's kill switch (that is, the mechanism that makes the ransomware stop spreading). We set up a sandbox environment to run and investigate the WannaCry ransomware sample. Specifically, the setup consisted of the following:

- Ubuntu 16 LTS laptop with 7th generation i7 processor and 16 GB RAM
- VirtualBox 5.2.6
- Two Windows 7 Professional 64-bit Virtual Machines
- IDA Pro Free (version 5.0)
- Wireshark (version 2.6.6)
- WannaCry malware variant with MD5 Hash: db349b97c37d22f5ea1d1841e3c89eb4

We used VirtualBox to create a virtual machine with an unpatched version of Windows 7 (containing MS17-010 [ms17-010]), called *victim*. We copied the WannaCry malware onto the desktop and also created a text file named TextFile.txt on the desktop that contained the following string: "This is just some random text. Nothing encrypted". A cloned copy of this machine was created and called *clean.* We then installed the Internet Information Services (IIS) web server that comes with Windows 7 Professional and applied the patch for MS17-010 on *clean*. Both virtual machines were configured to use a single common VirtualBox internal network named *intnet_WannaCry*. This allowed the virtual machines to communicate only with each other and not with any outside devices.

As part of WannaCry's kill switch validation logic, when it is first instantiated, it will attempt to query a DNS address only if the machine has an active network interface card with an IP address. Since network analysis is one perspective of the exercise, we set up IP addresses on both the victim and clean machines (11.0.0.100 and 11.0.0.101, respectively).

As the final setup step, we captured a snapshot of both of the virtual machines. This exercise can be completed in one of three ways. First, it can be downloaded and

executed from the packaged virtual machines, as exported from the VirtualBox software. Alternatively, the emulation sandbox software EmuBox[5] can be used to access the machines using a Remote Desktop Client (e.g., MS-RDP)[6] or by configuring a custom virtual machine and connecting into the US Army Research Laboratory South Cyber Rapid Innovation Group (CyberRIG) Collaborative Innovation Testbed (CIT).

3. Learning Objectives

The exercise described in the next section demonstrates the potential dangers and impacts of WannaCry. The exercise was developed with a learning aspect in mind—both for high-level cybersecurity awareness and technical analysis. The following are the targeted cybersecurity awareness learning objectives:

- Keep systems patched and disable any unused services. WannaCry spreads by taking advantage of a vulnerability in the SMBv1 service. This service is known to be vulnerable and should be disabled and replaced with a more recent version.[7]
- Only use administrator privileges when needed; constantly monitor and maintain the list of administrator users on a system. Executing WannaCry without administrator privileges greatly decreases its impacts.
- Practice defense-in-depth. Even if WannaCry infects a machine, its spread can be minimized if multiple layers of defense are in place. For example, firewall rules should restrict SMB traffic on networks that do not require this service. Network and host-based intrusion detection systems can be used to monitor systems and issue alerts for anomalous behaviors.

The following are the targeted technical analysis learning objectives:

- Basic malware analysis using an isolated, sandbox environment. This was done using VirtualBox, but can also be accomplished using physical systems that are physically segregated from outside networks and devices. Although not the case for WannaCry, some malware is able to detect when it is being run in a sandbox environment or in a software debugger and modify its behavior accordingly.[8]
- Basic understanding of black-box network analysis. The Wireshark tool is used to observe traffic that is generated when executing WannaCry. This exercise provides a simple understanding of the Wireshark graphical user interface (GUI) and basic capabilities.

- Basic understanding of the IDA Pro tool for analyzing a compiled binary. IDA Pro is used to open a binary and understand the basic flow of program logic using the graphical interface.
- Basic understanding of a DNS query. The Wireshark tool is used to dissect and view bidirectional DNS packets from a client and server machine.

4. Exercise

The exercise is separated into two main activities. In the first, the ransomware is executed and analyzed from different perspectives in order to identify the kill switch. In the second activity, the kill switch must be implemented and tested. In total, the exercise requires roughly 1–1.5 h to complete.

4.1 Activity 1: Analysis

Wireshark is a free and open source network packet analyzer. Wireshark captures network packets and displays the packet data as detailed as possible. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

The following are the steps for Activity 1, including annotations:

1) Open the remote desktop connection called …Victim….rdp.
2) Locate Wireshark  on the desktop and double click on the icon to open the program.
3) Click on *Local Area Connection.*
4) Start Wireshark (*Click on the shark fin*) as shown in Fig. 1.

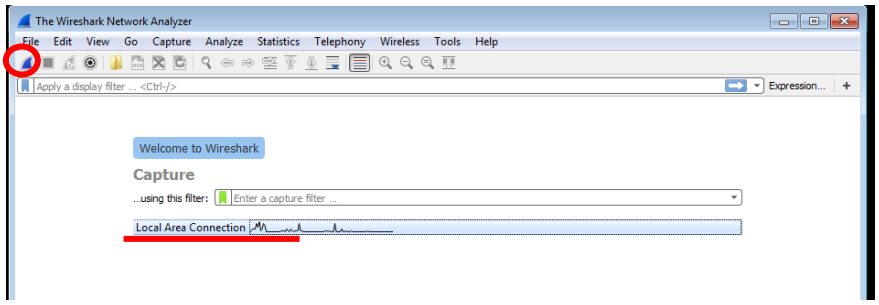


Fig. 1 Wireshark startup screen

Leave Wireshark running throughout the remainder of the exercise.

5) Run WannaCry (it is on your desktop) without administrator privileges as shown in Fig. 2 (you are using a sandbox environment):

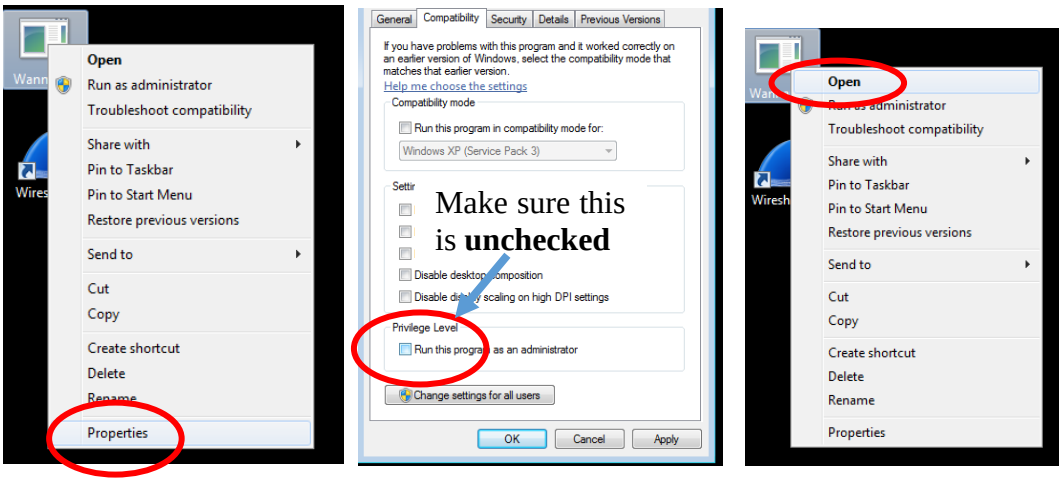


Fig. 2 Executing WannaCry as non-admin

If the following prompt appears (Fig. 3), click on "This Program works correctly":

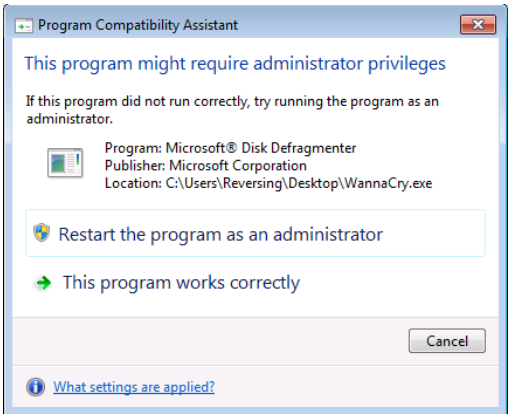


Fig. 3 Compatibility popup

Note that this will not infect your machine, but you can still observe it trying to communicate with other devices through Wireshark.

DNS packets are used to query a server to obtain the mapping between names (e.g., google.com) to addresses (e.g., 72.14.207.99). These packets may be a good way to identify malware communication channels.

6) In Wireshark, click on the Filter Toolbar, type DNS, and then press enter to show only DNS packets (see Figs. 4 and 5).

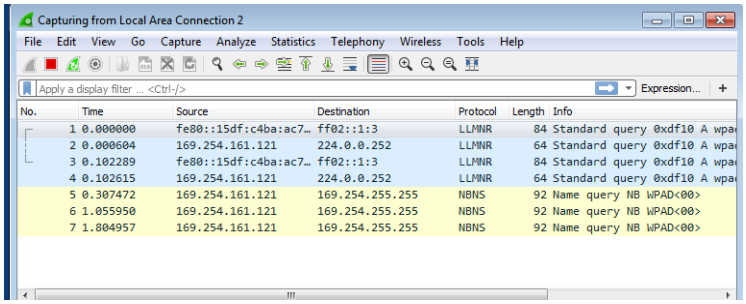


Fig. 4 Wireshark packet View A

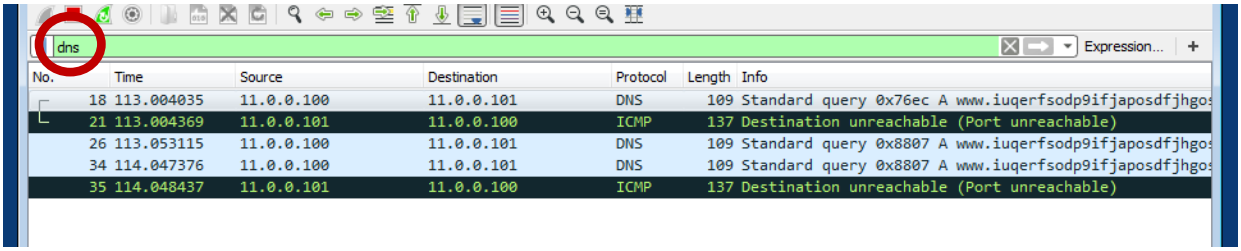


Fig. 5 Wireshark packet View B

7) Click through each DNS packet while observing the packet's details (lower window). You should find at least one packet with a suspicious domain that is requested (hint: it starts with www.). Write it here:

www._____

8) Now run WannaCry with administrator privileges. Right click on the WannaCry icon and select "Run as administrator". When prompted, press the Yes button as shown in Fig. 6.

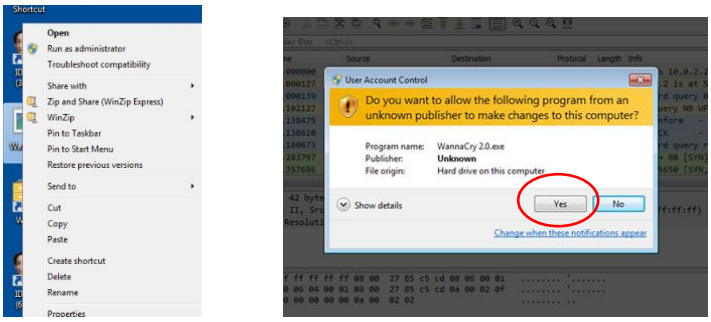


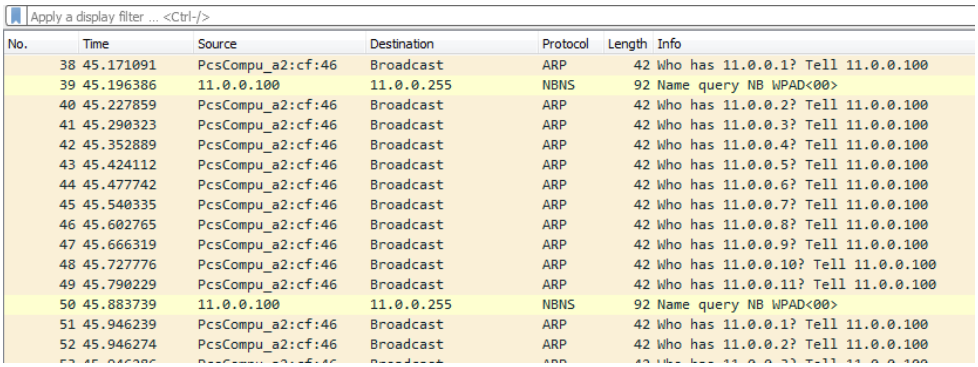
Fig. 6 Executing WannaCry run as admin

9) After a short while, you will notice that a file on the desktop has been encrypted (this may take up to 5 min). Write down the name of this file:

_____

Before two devices can communicate, similar to sending a letter through the mail, they must know the other's physical address. This is accomplished by sending data in the form of address resolution protocol (ARP) packets.

10) In Wireshark, clear out the existing filter and then apply a filter to view only ARP packets (use ARP as your filter string as shown in Fig. 7).


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
38	45.171091	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.1? Tell 11.0.0.100
39	45.196386	11.0.0.100	11.0.0.255	NBNS	92	Name query NB WPAD<00>
40	45.227859	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.2? Tell 11.0.0.100
41	45.290323	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.3? Tell 11.0.0.100
42	45.352889	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.4? Tell 11.0.0.100
43	45.424112	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.5? Tell 11.0.0.100
44	45.477742	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.6? Tell 11.0.0.100
45	45.540335	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.7? Tell 11.0.0.100
46	45.602765	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.8? Tell 11.0.0.100
47	45.666319	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.9? Tell 11.0.0.100
48	45.727776	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.10? Tell 11.0.0.100
49	45.790229	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.11? Tell 11.0.0.100
50	45.883739	11.0.0.100	11.0.0.255	NBNS	92	Name query NB WPAD<00>
51	45.946239	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.1? Tell 11.0.0.100
52	45.946274	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.2? Tell 11.0.0.100

Fig. 7 ARP packets in Wireshark

11) Based on your observations (look at the ***Info*** column in Wireshark), in your own words, do your best to briefly describe what you think the malware is trying to do:

_____

The Server Message Block (SMB) protocol is a protocol that lets devices share files over a network. It was originally specified by Microsoft, IBM, and Intel.

12) Clear the current filter and apply a filter to show only SMB packets.

Wireshark provides packet symbols to identify packets that are related. Click on a line of the "Packet List" pane to show the packet symbol.

First packet in a conversation.
Part of the selected conversation.
Not part of the selected conversation.
Last packet in a conversation.
Request.
Response.
The selected packet acknowledges this packet.
The selected packet is a duplicate acknowledgment of this packet.
The selected packet is related to this packet in some other way, e.g. as part of reassembly.

13) Look at the SMB traffic flow as shown in Fig. 8 and do your best to give a high-level explanation of what the malware is trying to do.

Hint: Look into the Info column of each packet.

ne	Source	Destination	Protocol	Length	Info
.804998	11.0.0.100	11.0.0.255	BROWSER	251	Domain/Workgroup Announcement WORKGROUP, NT Workstation,
3.453567	11.0.0.100	11.0.0.101	SMB	142	Negotiate Protocol Request
4.185232	11.0.0.101	11.0.0.100	SMB	185	Negotiate Protocol Response
4.185609	11.0.0.100	11.0.0.101	SMB	157	Session Setup AndX Request, User: .\
4.261511	11.0.0.101	11.0.0.100	SMB	175	Session Setup AndX Response
4.261929	11.0.0.100	11.0.0.101	SMB	126	Tree Connect AndX Request, Path: \\11.0.0.101\IPC$
4.262656	11.0.0.101	11.0.0.100	SMB	93	Tree Connect AndX Response, Error: Non specific error co

Fig. 8 SMB packets in Wireshark

14) Wait until the window shown in Fig. 9 appears. (This may take up to 5 min.)

Fig. 9 WannaCry infection notice window

15) Open Windows Explorer and list a few file types that are encrypted and some that are not encrypted. The system will be slow… keep in mind that malware is running.

16) What is the malware using to decide which files to encrypt?

Congratulations! You have completed Activity 1.

4.2 Activity 2: Implementing the Kill Switch

Part 1: Binary analysis using IDA Pro.

IDA Pro is a combination of dissembler and debugger. It facilitates both static and dynamic analysis. It is a powerful tool commonly used by professionals to perform malware analysis.

Minimize ***(do not close!)*** the *victim* machine (…Victim….rdp) and open the remote desktop connection called …Clean….rdp.

The following are the steps for Activity 2, including annotations:

1) Locate IDA Pro  and drag the binary named *WannaCry* onto the IDA Pro icon. Click *OK* on the two popout windows (as shown in Fig. 10) and *Close* in Help.

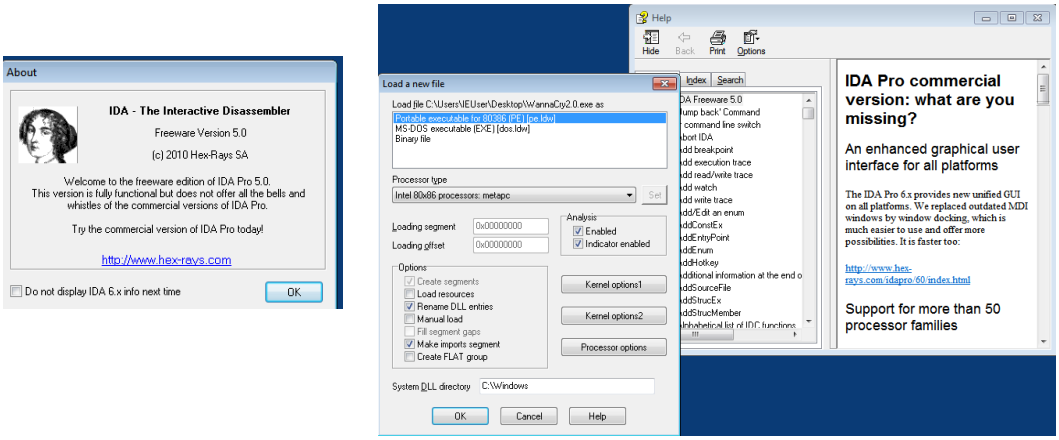


Fig. 10 IDA Pro startup windows

2) Click on the tab named ***IDA View-A***, as shown in Fig. 11.

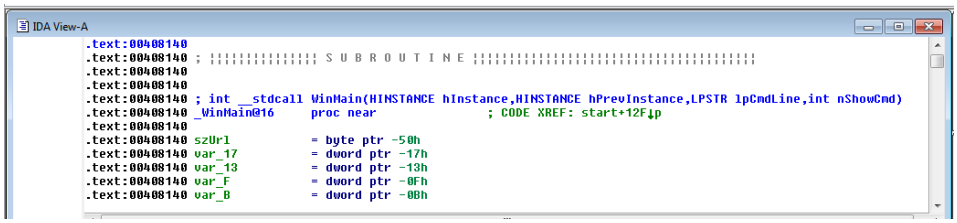


Fig. 11 IDA Pro text view

A *kill switch* is a mechanism used to shut down or disable machinery of a device or program. The importance of finding a ransomware's kill switch is to prevent it from spreading. Keep in mind that not every malware has a kill switch.

3) Scroll down until you find the domain name (the "www…" string that you found in Activity 1, Step 7) as shown in Fig. 12.

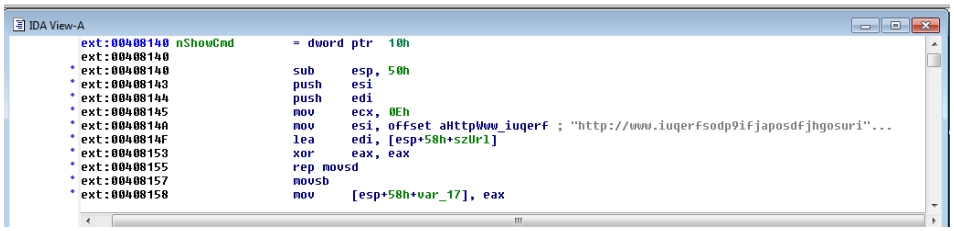


Fig. 12 Kill switch URL in IDA Pro

In the low level (or assembly) code, the following imports (names written in pink) are used to interact with the Internet. The Windows Internet (WinINet) Application Programming Interface (API) enables applications to interact with File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP) to access Internet resources. These are some of the functions that make up the API:

- **InternetOpen** function initializes an application's use of the WinINet functions.
- **InternetOpenUrlA** function opens a resource specified by a complete FTP or HTTP URL.
- **InternetCloseHandle** function closes a single Internet handle. Returns TRUE if the handle is successfully closed, or FALSE otherwise.

4) Scroll down to find the functions that access the network in the code (see Fig. 13).

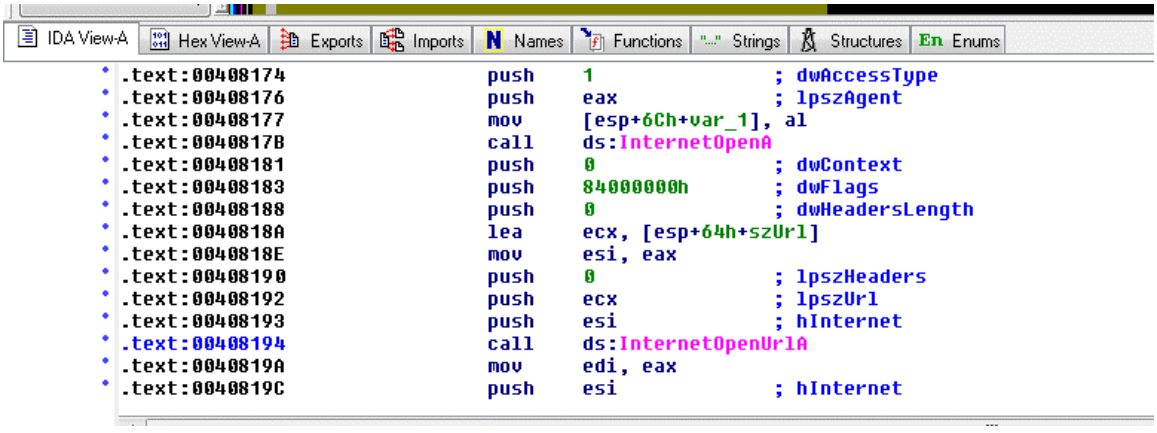


Fig. 13 Network functions in IDA Pro

Another way to find these functions is to view the Imports tab and look for the names of the functions and then right-click and select “jump to xref”. This will list all places in the code that reference the function.

5) Right click on the IDA View-A window and click on graph view as shown in Fig. 14.

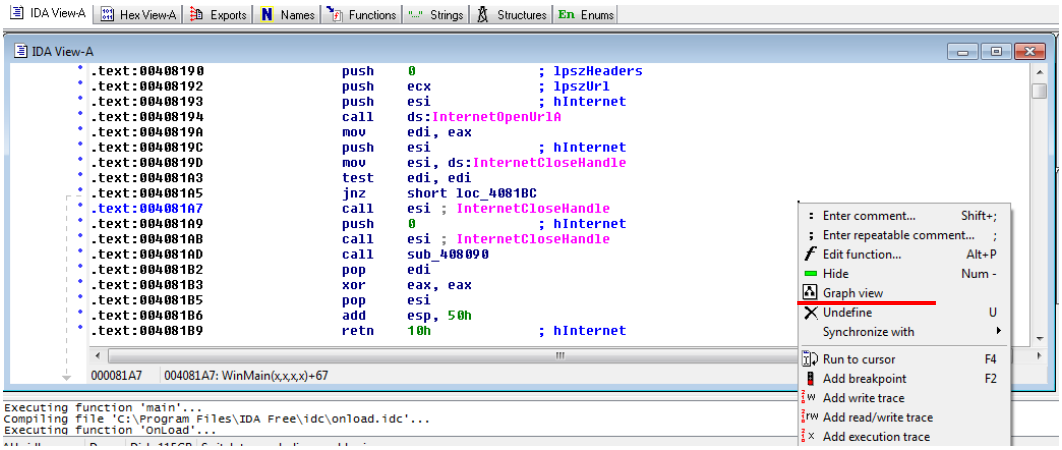


Fig. 14 Switch to graph view in IDA Pro

Some common instructions found in assembly are the following:

- ***call*** jumps to another block of code; when execution of that block is complete, the program execution will return.
- ***jmp*** jumps to another block of code; when execution of that block is complete, the program execution does not need to return.
- ***test*** executes a logical AND (typically used for value comparisons).
- ***jnz*** jumps to another block of code if a condition is met: result of the previous instruction is not zero.
- ***mov*** instruction moves data from one location to another.
- **PUSH** adds values to the top of the stack.
- pop removes a value from the top of the stack into a register or memory address.

Focus on ***call*** instructions and the ***pink function names*** and then do your best to generally explain what is happening in the code.

6) Look at the subroutines after the conditional jump (follow the two arrows to below the jnz instruction as shown in Fig. 15). Which subroutine (or **block**) is the one that continues with the encryption and which one stops before encryption occurs? Explain why.

Hint: See the code within functions by double-clicking on the function names. You can go back by pressing ESC or the back arrow.

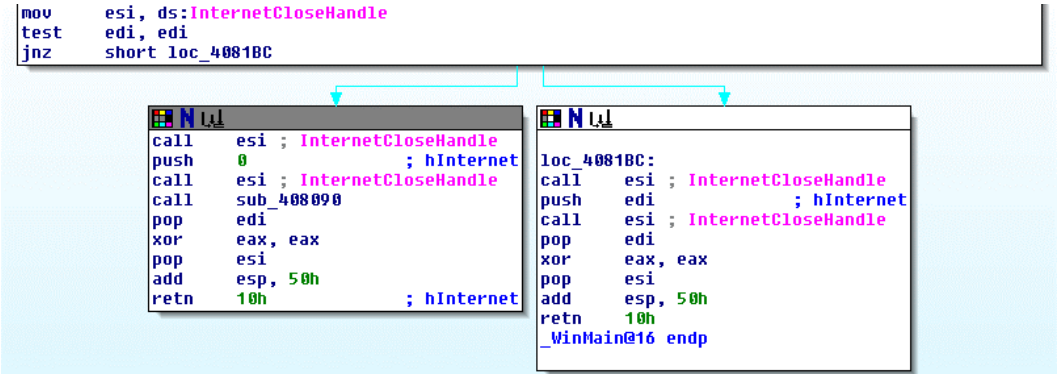


Fig. 15 Conditional branch in IDA Pro

7) Based on what you observed so far, do your best to guess what would prevent the encryption; that is, what should we do to reach the **block** that **stops** the malware; what is ***the kill switch***? (*Remember, you can always ask one of the coordinators to help.*)

Part 2: Set up the kill switch.

There is a file named *hosts* on Windows systems. This is a text file that contains mappings from hostnames to IP addresses (think of it as a stored copy of a DNS that maps google.com -> 72.14.207.99).

8) Add a mapping as shown in the following:

   a) Open File Explorer  .

   b) Navigate to the folder with the *hosts* file by entering **%WINDIR%/system32/drivers/etc** into the navigation bar, as shown in Fig. 16.

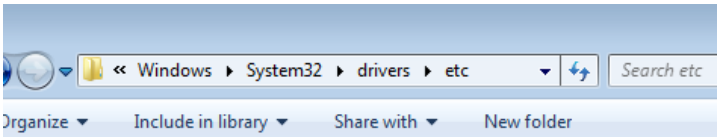


Fig. 16 Navigation bar

   c) Edit the *hosts* file by right clicking and selecting ***notepad++*** as shown in Fig. 17.

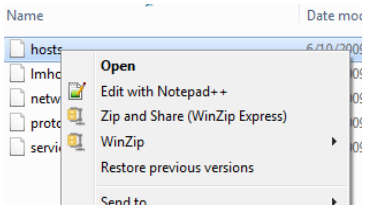


Fig. 17 Notepad++ in context window

d) Add a mapping between google.com and the loopback address: **127.0.0.1**, as shown in Fig. 18. This is a special address used to communicate within your own machine.

```
18
19  # localhost name resolution is handled within DNS itself.
20  #    127.0.0.1       localhost
21  #    ::1             localhost
22  127.0.0.1 google.com
23  127.0.0.1 www.google.com
24
```

Fig. 18 Windows hosts file

e) Save the *hosts* file. If you received a ***Save failed*** prompt, press the Yes button, as shown in Fig. 19.

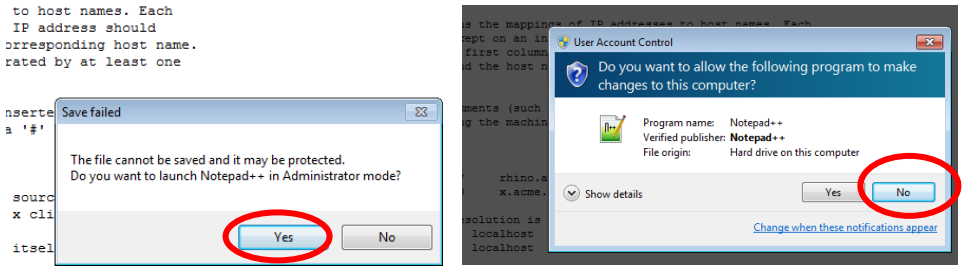


Fig. 19 Hosts file save windows

f) Navigate to google.com (this may take 1–2 min). You will see the page returned from your own machine's web server as shown in Fig. 20 (note that this is ***not*** Google's web server).

Fig. 20 Default IIS7 web page

9) Now, set up the kill switch by adding a mapping to the address you found in Activity 1, Step 7, using the *hosts* file.

10) After you set up the kill switch, run the malware as an administrator.

Hint: Before running the malware make sure the domain works. Go to the site and check that it accesses the local host.

If done correctly, your system will not be encrypted.

Uber Question: Why do you think this ransomware has a kill switch?

Congratulations! You have completed Activity 2.

5. Conclusion

In this document we described the WannaCry ransomware and some of its behavior. We provided a hands-on exercise that demonstrates a multi-perspective analysis of the malware using several techniques and tools that are available to the general public. Additionally, we documented our setup and configuration for the exercise. Similar analyses may be applied to other types of malware, their function, and ways to mitigate their impact.

In the future, we will use this exercise not only for training and awareness, but to also uncover research questions that can be addressed collaboratively by security professionals, students, and faculty.

6. References

1. Challita A. The four most popular methods hackers use to spread ransomware. 2018 Aug 9 [accessed 2019 Jan 15]. https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware.

2. Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: International conference on the theory and application of cryptology and information security. Berlin (Germany): Springer; 2001 Dec 9. p. 552–565.

3. Microsoft Security Bulletin. Security update for Microsoft Windows SMB server (4013389). 2017 [accessed 2019 Jan 15]. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

4. Hardy C. WannaCry 2.0 – Three ways to find the Kill Switch. 2017 [accessed 2019 Jan 15]. https://youtu.be/d56g3wahBck.

5. Acosta JC, McKee J, Fielder A, Salamah S. A platform for evaluator-centric cybersecurity training and data acquisition. Proceedings of the Military Communications Conference (MILCOM); 2017 Oct 23; Baltimore, MD. MILCOM 2017 - 2017 IEEE. IEEE; 2017. p. 394–399.

6. Microsoft Windows IT Pro Center. Getting started with remote desktop on Windows. 2018 [accessed 2019 Jan 15]. https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/windows.

7. Microsoft Windows Support. How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server. 2018 [accessed 2019 Jan 15]. https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smb.

8. Sikorski M, Honig A. Practical malware analysis: The hands-on guide to dissecting malicious software. San Francisco (CA): No Starch Press Inc.; 2012.

List of Symbols, Abbreviations, and Acronyms

API	application programming interface
ARP	address resolution protocol
CyberRIG	Cyber Rapid Innovation Group
CIT	Collaborative Innovation Testbed
DNS	Domain Name Server
FTP	File Transfer Protocol
GUI	graphical user interface
HTTP	Hypertext Transfer Protocol
IIS	Internet Information Services
IP	Internet Protocol
SMB	Server Message Block
SMBv1	Server Message Block version 1
URL	Uniform Resource Locator
USB	Universal Serial Bus
WinINet	Windows Internet

1 (PDF) DEFENSE TECHNICAL INFORMATION CTR DTIC OCA

2 (PDF) DIR ARL
IMAL HRA
RECORDS MGMT
RDRL DCL
TECH LIB

1 (PDF) GOVT PRINTG OFC
A MALHOTRA

2 (PDF) ARL
RDRL CIN D
J CLARKE
RDRL CIN D
J ACOSTA