CS 458 – Computer and Network Forensics
Lab 08 Assignment
Due: 11:30 PM on Friday, 26 March 2021

Part 1: Tor Traffic Forensic Analysis

NetworkMiner

NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

Note: Network Miner (portable version) is provided along with this manual. Please download the tool and the evidence file inside the Windows VM.

Case Details: A user, let's call him "Kevin", used Tor for some dark-web activity on November 30, 2018. Kevin was using the Tor Browser on a Windows PC and RawCap was used to capture the localhost network traffic from Kevin's computer. A PCAP file with the captured packets from Kevin's PC is attached as **`TorEvidence.pcap`**.

1) Open NetworkMiner and open the evidence file in using NetworkMiner (you can drag and drop).

2) Familiarize yourself with the environment. There are several tabs such as Files, Hosts, Images, Messages, Credentials, Parameters etc.

3) Click on the parameters tab. You can list all search engine queries by looking for entries in the "Parameters" tab with parameter name "q". This technique is applicable most search engines, like Google, Bing, Yahoo! and DuckDuckGo.

4) List out the **queries** (parameter value) and their **frame numbers** in chronological order (check the timestamp column):

   i. buy fake passports 1136
   ii. qua83qGa1H1... 1165
   iii. buy guns for bitcoin 2767
   iv. buy guns for bitcoin UK 2779
   v. hG0/gPLsuw... 2787

5) Provide the domain name where all the queries were searched torproject.org

6) The **"Files"** tab in NetworkMiner contains a list of all files that have been reassembled from the analyzed PCAP file. What does the frame 1136 reveal? (Check details column)

search for buy fake passports

7) Right click on the frame **1136** and open the file. Provide a screenshot of the page. Name it as **1_frame_1136**.

8) Analyze frame **1837** and explain what does the page reveals. Also provide the title of landing page. Provide a screenshot of the page. Name it as **2_frame_1837**.

fake passport options page

9) Analyze frame **2525** and explain what does the page reveals. Also provide the title of landing page. Provide a screenshot of the page. Name it as **3_frame_2525**.

fake passport pricing

10) From the listed prices, what is the price for fake UK passport + Driving License 750euro

11) Navigate to the Images tab in NetworkMiner and scroll a bit further down, we see a picture of a weapon.

12) Analyze frames **2767, 2779, 2806, 2953** and summarize what do the pages reveal. Also provide the title of each landing page. Provide a screenshot of the pages. Name each of them as **4_frame_number**.

Frame 2767 buy guns for bitcoin results

Frame 2779 buy guns for bitcoin UK results

Frame 2896 _____

Frame 2953 UK Guns and Ammo store login

13) The credentials to login are found in the **"credentials"** tab. Provide the username and password used to login to the page displayed in frame 2953. (Hint: Look into the details and timestamps)

    i. Username: BadGuyTyrell Password: tyrellcorpFTW

14) Analyze frames **3067, 3084, 3104, 3120, 3143** and answer the following.

    i. Products in the cart 9mm Glock 19, 9mm Walther P99, 200x 9mm ammo

    ii. Bitcoin address 159BP9K8PDYnGBpdJmi6Rhyd9tgmZv50mj

Part 2: Malware Analysis Lab (Ransomware)

In this assignment you will perform reverse engineering of a Malware. Please remember that these are **live and dangerous malware**! They come encrypted and locked for a reason! **DO NOT run them unless you are absolutely sure of what you are doing**!

They are to be used **only for educational purposes** (and I mean that)!!!

I recommend running them in a VM which has **NO network connection** (uncheck the cable connected option in network settings) and **without guest additions or any equivalents**. The malwares provided are worms and will automatically try to spread out. Running them **unconstrained** means that **you will infect yourself** or others!!!

Below are some important instructions:

1) **DO NOT** download or copy the malware outside your virtual machine.
2) **DO NOT** have any shared folders between the virtual machine and your HOST machine
3) When you are executing the malware, uncheck the cable connection option in the Virtual Box (inside network options; advanced tab)
4) The malware sample provided is only for educational purpose and **should not** be used for any other purposes.

Environment details

- If the OVA file is not present in your directory, download the VM Image here.
- Refer to the "**Import__ova__Instructions"** file provided to import the ova file into the virtualbox
- The virtual machine provided hosts a 32 bit unpatched windows OS. The automatic updates of the windows are stopped on purpose. The VM contains pre-installed software and the Malware (encrypted). **It is recommended to create a snapshot before you start analyzing the malware.** As you can restore back to the original version, if you accidentally executed the malware.
- Login to the Mal-Ripper account (does not have any password)

VM security details

It is possible for WannaCry to "escape" the VM and spread to a wider network if two conditions are met:

1. The virtual machine has a network adapter that gives it access to other machines on a network, and
2. The other machines on that network are not patched against WannaCry's spreading mechanism.

For #2, this version of WannaCry uses the EternalBlue exploit to spread. Microsoft issued a patch for EternalBlue in March 2017. If you are running Windows and have installed updates since then, your machine is safe. If you are running a Mac you are safe because EternalBlue only works against Windows machines.

Important: Make sure that you take a snapshot of your Windows VM before proceeding. Having one will let you to restore your VM after WannaCry encrypts your VM. See instructions for how to create and restore a snapshot here.

Warning: If you don't create a snapshot, you'll need to download a new copy of the Windows VM after it is encrypted by WannaCry.

Overview

WannaCry. This program made international headlines in the summer of 2017 when it wreaked havoc across the world before being disabled by malware analyst Marcus Hutchins. It received the 2017 Pwnie Award for "Epic 0wnage": https://pwnies.com/winners.

WannaCry is noteworthy for several reasons:

1. It caused a huge amount of global damage. See an animated map of it spreading around the world.
2. It incorporated a zero-day exploit developed by the NSA, which was stolen and posted by the Shadow Brokers hacking group, believed to Russian operatives.
3. WannaCry put lives at risk when hospital systems in Europe were disabled and patients had to have medical procedures canceled or moved to other hospitals.
4. The rapid spread of WannaCry was stopped when then 22-year-old malware analyst Marcus Hutchins (aka MalwareTech) inadvertently found the "killswitch" for WannaCry.
5. On December 17, 2017, the White House formally attributed the WannaCry attack to North Korea. The U.K., Australia, Canada, New Zealand, and Japan, as well as Microsoft, joined the U.S. in this attribution: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

WannaCry is a ransomware that encrypts the victim's files and demands ransom in order to decrypt. **But WannaCry does not decrypt victim's files even after the ransom is paid.**

Task 1: Initial Assessment of the Malware

1) Extract the Malware (Wannacry) present on the Desktop. The password is '**infected**'.

2) Open the tool **Pestudio** (shortcut created on the Desktop). You can drag and drop the malware into the tool.

    a. What is the md5 signature of the malware

    DB349B97C37D22F5EA1D1841E3C89EB4

3) In the left pane click on the resources

    b. Provide the name of the of the file type R — 1831

    c. Provide the signature of the file type R — executable

4) Close the application

Task 2: Extracting resources

You will use another interesting tool called **resource hacker**. Open the wannacry.exe file using resource hacker (you can drag and drop the exe file on to the resource hacker icon)

1) You can observe 2 directories. Expand the directory R. Click on the file **1831:1033**.

    a. Provide the first 4 bytes of the hex code of the file — 4D 5A 90 00

2) In the left pane, right click on the file 1831:1033 and select save resource to a BIN file. Save the file as an .exe file.

3) Open the saved file in the resource hacker and identify the type of the file by looking into the header of the file. (Hint: Look into the first few HEX digits - https://en.wikipedia.org/wiki/List_of_file_signatures)

    its a zip folder.

4) Extract the contents of the saved file to a folder using 7zip.

a. Are you able to achieve? Why or why not

Yes, the file structure stays in tact when in the .bin file.

Task 3: Reverse Engineering

There are many tools to perform reverse engineering on malwares such as Ghidra (NSA's tool), IDA etc. In this assignment you will be using **x96dbg**.

1) Observe the execution flow of WannaCRY (scroll to the bottom of the document)

2) Open **x96dbg** as administrator

3) In the taskbar click on file and then click on open. In the new window navigate to the location where the malware (wannacry) is present and open the file. You should see a bunch of assembly language code. The right pane provides information about the registers in use. Get yourself familiarize with the environment.

4) Press **F9** (run) to go to the main module (**enter only once**, if you enter multiple times the malware file will be executed). You should land at the address **00409A16.** Now, decoding line by line will be a tedious process. Hence, we will look into the strings which are of our interests.

5) Right click on any instruction and select **search for → current module → string references**

6) You will land on to the references tab with assembly language code and strings associated.

7) Observe the strings and feel free to explore the strings. Most of them are Windows API calls.

8) Locate the strange string http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. This was the kill switch address for wannacry which was sink holed to hold the malicious traffic. (Check the website for yourself!)

9) **Provide a screenshot by selecting the string.**

10) Double click on the string. It will point back to the instructions.

a. Provide the address of the instruction 00408177

11) Locate the jump instruction at the address **004081A5**. Now double click on the zero flag on the right pane to toggle the value.

a. Explain what happens when the ZF is 0

when the ZF is 0, wannacry will execute the call commands activating the virus

b. Explain what happens when the ZF is 1

When ZF is 1, wannacry will jump over the commands that start the virus.

12) Minimize the **x96dbg** window

13) Now open the other extracted file using x96dbg as administrator. Since this file is a self-encrypting file, the password/key should be contained within the file. Let's find the password to decrypt the contents of the archive file.

14) Press **F9** (run) to enter to go to the main module (**enter only once**, if you enter multiple times the malware file will be executed). To find the password we need to identify the function which calls the subroutine that contains or handles resources.

15) In order to achieve that, let's examine the Intermodular calls. Right click on any instruction and select **`search for → current module → Intermodular calls.`**

16) You will land on to the references tab with assembly language code and associated intermodular calls.

17) Since we are looking for a subroutine which handles resource API calls, search for **`'resource'`** on the search bar below. The list will be populated. Double click on the **FindResource** call.

18) Identify the beginning location of the current function. (Address location: **`00401DAB`**)

19) Right click on the instruction and select **analysis → analyze module**

20) Now we have to identify the function call of the subroutine **"sub_401DAB"**. Right click on the instruction and select **xrefs**

    a. Provide the address of the function call

    00401D80

21) Observe the 2 instructions above the function call. Identify the string passed into dword.

22) **Provide a screenshot.**

23) Copy the line and use a notepad to paste. Now copy the string and use it to decrypt the extracted archive file.

24) **Provide a screen shot of the contents of the archive file**.

25) Analyze all the files using a hex editor (**HxD** shortcut on desktop).

    a. List the original file types of all the files, if the files are archive files extract and list the contents. Ignore the msg folder. (Hint: Look into the first few HEX digits - https://en.wikipedia.org/wiki/List_of_file_signatures)

    b. Rename the **6 '.wnry' files** with the original extension and open the files. **Provide screenshot of all the files opened.**

Task 4: Running the malware

1) Open Process hacker as administrator.

2) Make sure you have a good anti-virus on your host machine and is updated!

3) Now infect your VM! Right click on the wannacry.exe file and run as administrator.

4) Now connect virtual machine to the network (go to network settings of the VM and check the cable connect option).

5) Locate the process **taskche.exe** in process hacker. Right click on the process and click on properties.

    a. Provide a screenshot of the properties window

6) Locate the location of the .exe file and navigate to the location in File explorer.

a. What is the name of the directory containing the taskche.exe file

_____

b. Provide a screenshot of the files present in the location

7) In the properties window, click on the **memory tab.** In the memory tab click on **Strings** button and OK.

a. Filter the IP address used (use any regular expression filter – google it or duck duck it!) and save them to a text file.

b. Provide the **`.onion`** domains (use the filter option) which the malware is trying to connect.

The following steps must be done with precaution. Only take the risk if you are sure of what you are doing, and you have a very good antivirus installed on your host. If not, you may choose to skip.

8) Restore back the VM to the original snapshot and restart the VM with the network in the NAT Network mode (the VM should be able to access the internet).

a. Open Wireshark and start capturing packets

b. Run the wannacry executable (as admin).

c. After about 30 – 60 seconds, stop the wireshark capture and analyze.

d. Identify Host IP address to which a GET request is created. Provide the IP address. (filter by **`http.request`** and look for the strange string inside the GET requests displayed)

e. Provide a screenshot of the GET request displaying the string.

f. What is the domain of the IP address (Hint: Use **`'nslookup'`** in the cmd prompt)

g. Filter for only tcp SYN packets (**`tcp.flags.syn==1`**)

h. Observe all the syn packets and explain what do you think is happening? (Hint: Observe the port number and the IP addresses)

_____

Free Malware Sample Sources

Be careful not to infect yourself when accessing and experimenting with malicious software.

1) https://zeltser.com/malware-sample-sources/
2) https://github.com/ytisf/theZoo

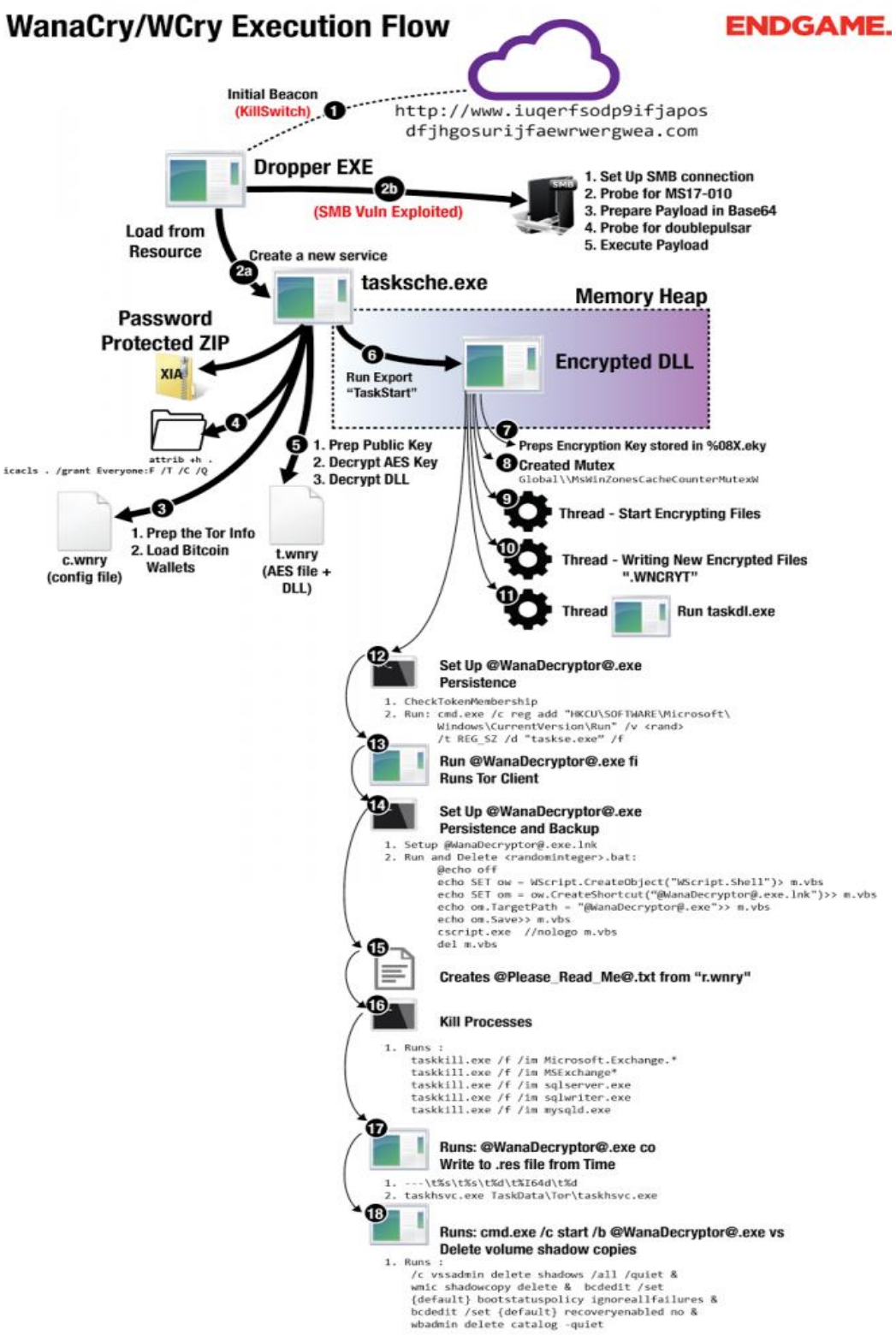
Few reverse engineering tools

1) Ghidra → https://ghidra-sre.org/
2) Valgrind → http://www.valgrind.org/
3) Fiddler → https://www.telerik.com/fiddler
4) https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools#s29

Read more

- EndGame → https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis
- FireEye → https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
- SecureWorks → https://www.secureworks.com/research/wcry-ransomware-analysis
- McAfee →https://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/

WannaCRY execution flow given in the next page



Source: https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis