Home Exam
IMT 4116
Reverse Engineering and Malware Analysis

June 1st 14:00 to June 5th 23:59

Contact: Associate Professor Geir Olav Dyrkolbotn, geir.dyrkolbotn@ntnu.no

This is part I of the exam in IMT 4116. Your home exam will be given a temporary grade, which may be adjusted up or down based upon your performance on part II, the Oral examination.

How to answer: Do not only give the final answer to the question. It should be possible to understand how you arrived at your answer for another analyst, without having to consult you. Screenshots are encouraged. As with all malware analysis, there is a balance between too many details and too few, like we practiced in the malware reports. The questions are weighted by points. Total 100 points.

You will need your analysis PC for this exam, setup as in labs. Two VM (win and remnux) is recommended as you may need remnux to provide network resources by using commands like fakedns, httpd start, ircd start etc. Also remember that different tools may provide different results. Similar tools may have different capabilities and limitations. All memory addresses given in the exam are from IDA.

You are to submit two files for the exam (NB! different deadlines):

1) **Home exam:** deadline June 5th 23:59, submit to ntnu.inspera.no
Format: pdf with answers to question 1 through 5. <your name_exam_IMT4116_S17.pdf>
Late submissions will not be accepted, but multiple improvements up to the deadline is possible (last submitted version will be graded)

2) **Oral exam:** deadline for handling in the presentation (see question 6 in this document), June 14th 12:00, email attachment to geir.dyrkolbotn@ntnu.no. The Oral examination is June 15th or June 16th. The schedule will be announced next week. Pay attention to blackboard as changes and additional information will be posted there.
Format: pdf or ppt of the presentation <your name_presentation_IMT4116_s17>

NB, caution!
You are given live malware to analyze during this exam. Use due caution regarding analysis environment and access to internet.
All malware samples are found in packed folders with the password: infected
You will need: exam_1.zip, exam_2.zip, exam_3.zip and exam_4.zip

Good luck!

1) **Basic Static Analysis (10 points) – exam_1.zip**

Use information available through basic static analysis techniques only. Describe potential indicators of compromise (IoC's) and use them to form a hypothesis about the purpose/functionality of the following samples.

a. Malware sample: exam_1a.exe

b. Malware sample: exam_1b.exe

c. Malware sample: exam_1c.exe

2) **Basic Dynamic Analysis (20 points) – exam_2.zip**

Use information available through basic dynamic analysis techniques to form a hypothesis about the purpose/functionality of the following samples, based upon IoC's in registry, file and network activity.

a. Malware sample: exam_2a

b. Malware sample: exam_2b

3) **Advanced Analysis (45 points) – exam_3.zip**

Use advanced static (e.g. IDA PRO free) and/or dynamic analysis (e.g. OllyDbg) techniques to answer the following questions:

a. Basic functionality
Malware sample: exam_3a

i. Go to address: 0x416148:
How many conditional jumps are there in sub routine sub_416148? Provide the address for each one: e.g jz at 00416xxx
ii. Go to address 0x4161DF:
What conditions is being evaluated for the jnz instruction?
iii. Go to address 0x41617D:
What conditions is being evaluated for the jle instruction?
iv. Go to address 0x416173:
What conditions is being evaluated for the jz instruction?

b. The following malware has key-logger functionality:
Malware sample: exam_3b

i. At what addresses are keys examined?

ii. Where does the polling loop start and end?

iii. How often are the keys polled?

c. We suspect the following sample to be encoded
Malware sample: exam_3c
i. What encoding technique has been used?
ii. What is the key?
iii. Decode the sample.
iv. Provide the following information about the decode file:
1. File type
2. Compilation time
3. Name of sections
4. MD5 hash value

d. During analysis you come across the following:
Malware sample: (no sample for this question)

Q29uZ3JhdHVsYXRpb25zLCB5b3Ugc3VjY2Vzc2Z1bGx5IGRlY29kZWQgdG
hpcyBtZXNzYWdlLCB5b3UgbWF5IHByb2NlZWQh

i. What encoding technique is this?
ii. Decode and provide the result

e. We suspect this malware to connect to a C2 server:
Malware sample: exam_3e

i. What is the IP address of the server?
ii. What protocol is used for this connection?
iii. What API call is used to get the handle necessary to read data from the open connection? Include the memory address of both the API call providing the handle and the API call reading data
iv. Identify the commands supported by the channel

f. We suspect this malware to use anti-debug techniques
Malware sample: exam_3f

i. At what address does this code check for the presence of Virtualbox?
ii. What other analysis tools are checked for?
iii. What do you think is the purpose of the subroutine at 408C47?
iv. From which address is the subroutine 408C47 called?
v. Explain the conditional branch directly after this (at address: 408CCA)

g. We suspect this sample to use mutex (also known as mutant)
Malware sample: exam_3g

i. What is the most likely purpose of using mutex/mutant?
ii. What is the mutex/mutant for this sample? Provide its name and the way you found this name (Hint! Look for handles in Process Hacker)
iii. Identify the address where the mutex is created. Provide a screenshot of the surrounding code.
iv. The subroutine creating the mutex takes certain inputs. What are they and how are they provided to the subroutine?
v. One of these inputs depends on a specific system parameter that will make the mutex unique for each system. In what subroutine do you find this system parameter and what is its name?

4) **Combined analysis (20 points) – exam_4.zip**
You are give the following files
Malware sample: exam_4a and exam_4b
Answer/perform the following and document the results:

a. Basic static analysis
b. Basic dynamic analysis, normal execution (not admin privileges) of the sample
    i. Look at files, registries and network traffic as usual.
c. Basic dynamic analysis, sample executed with administrator privileges
    i. Look at files, registry and network traffic again. Do you detect any differences?
d. Provide necessary network resources so that you are able to detect the nickname and channel name used. Describe what you do and what the nickname and channel name is.
e. Exam_4a is looking for one particular filename in one particular folder. Rename the file exam_4b to the filename that exam_4a asks for and place it in the correct folder.
    i. What is different about the network traffic from exam_4a now that this particular file is available?
f. Address 40141D pushes strings on the stack then calls sub_4012C6 each time. What is the purpose of this subroutine? Provide two of the values returned by the subroutine.
g. Make sure exam_4b is available with correct name in the correct folder. exam_4b is encoded, but exam_4a will decode it. Use OllyDbg (or equivalent).
    i. Find the location in exam_4a that opens exam_4b (different name in the code), hint "fopen" (first instance).
    ii. Then locate a call to subroutine 405366, set breakpoint, so that you can read what sub routine 405366 returns. Document the 10 first return values.
h. Based on what you have now (no additional analysis required) write an executive summary of you findings.

5) **Open source (5 points)**
The head of the IT department calls you. They are concerned with the outbreak of WannaCry. They want to know what to do. Explain to the IT department:
a. What is the purpose of WannaCry?
b. How does is spread?
c. How can they detect if their system is infected?
d. What should they do to prevent the attack?

NB! This is not an analysis task, but to see if you are able to find and understand others analysis results and communicate that to your IT department.

6) **Oral exam preparation (not part of the home exam, but may be smart to think about already)**

The oral examination will start with a presentation from you, lasting 10-15 minutes. You should focus on what you did to get the results. Include what you think you did well and what you think you didn't do well (self assessment). The goal is to convince me that you really know what you are doing, that this is your work and to what extent you are aware of your own strengths and weaknesses. You do not have to cover everything, but try to cover all sections of the exam and include the topics, basic static and basic dynamic analysis and advanced analysis using of IDA and/or OllyDbg.

We will of course ask follow up questions.

You need to provide the presentation you will use (e.g. powerpoint or pdf) ahead of time. **Deadline: June 14th at 12:00.**