

**Reverse Enginnering Malware**

Year 2 (2019/20), Semester 3

## School of InfoComm Technology

Diploma in Cybersecurity and Digital Forencis

**On-line Test 1**

Date: 02 July 2020 (Thursday)

Time: 4.30pm – 5.30pm

INSTRUCTIONS TO CANDIDATES:

1. There are THREE questions. Answer ALL questions .
2. This is on-line open book test (you can refer to any printed materials or pre-

downloaded materials) but you cannot access Internet Browser and Visual

Studio during the test.

1. Rename the file to your student ID (SXXXXXXX.docx) and submit the anwers

using the same document through the link provided in MeL.

1. This paper consists of **5** pages including this cover page.

There are THREE questions. Answer **ALL** questions.

**QUESTION 1** (15 marks)

(a) For each of the following marked entries, show the values of the destination operand and the Sign, Zero, and Carry flags:

mov ax,00FFh

add ax,1h ; AX=0100h SF=0 ZF=0 CF=0

sub ax,1h ; AX=00FFh SF=0 ZF=0 CF=0

add al,1h ; AL=00h SF=0 ZF=1 CF=1

mov bh,6Ch

add bh,95h ; BH=01h SF=0 ZF=0 CF=1

mov al,2h

sub al,3h ; AL=FFh SF=1 ZF=1 CF=1

(10 marks)

(b) Given the following data definitions:

.data

myBytes BYTE 10h,20h,30h,40h

myWords WORD 3 DUP(?),2000h

myString BYTE "School of ICT"

What will be the value of EAX after the execution of each of the following instructions?

1. mov eax,TYPE myBytes 1
2. mov eax,LENGTHOF myBytes 4
3. mov eax,SIZEOF myBytes 4
4. mov eax,TYPE myWords 2
5. mov eax,SIZEOF myString 13

(5 marks)

**QUESTION 2** (15 marks)

(a) In the following instruction sequence, show the values of the Carry, Zero, and Sign flags where indicated:

mov al,00001111b

test al,00000010b ; a. CF=0 ZF=0 SF=0

mov al,00000110b

cmp al,00000101b ; b. CF= 1 ZF=0 SF=0

mov al,00000101b

cmp al,00000111b ; c. CF=0 ZF= 1 SF= 0

(6 marks)

(b) Answer the following questions based on the code listing in Figure 2b below:

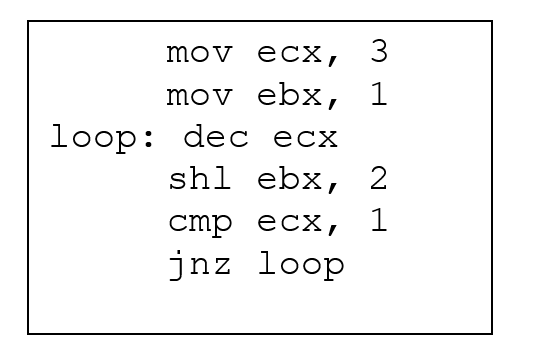


Figure 2b: Code Listing

1. How many times will the loop repeat itself? 2

(2 mark)

1. What is the value of ecx when the loop ends? 1

(3 marks)

1. What is the value of ebx and ZF when the loop ends? Ebx=16 ZF=0

(4 marks)

**QUESTION 3** (20 marks)

A malware analyst is analysing a newly found malware, Destroyer.exe.

1. An extract of the start of *main* function is shown below in Figure 3a.

**.text:00401440 \_main proc near ; CODE XREF: start+DEp**

**.text:00401440**

**.text:00401440 var\_4 = dword ptr -4**

**.text:00401440 argc = dword ptr 4**

**.text:00401440 argv = dword ptr 8**

**.text:00401440**

**.text:00401440 mov eax, [esp+argc]**

**.text:00401444 sub esp, 44h**

**.text:00401447 cmp eax, 2**

**.text:0040144A push ebx**

**.text:0040144B push ebp**

**.text:0040144C push esi**

**.text:0040144D push edi**

**.text:0040144E jnz loc\_401813 ; program exits at loc\_401813**

**.text:00401454 mov eax, [esp+54h+argv]**

**.text:00401458 mov esi, offset aPwd ; "abc120"**

**.text:0040145D mov eax, [eax+4]**

**.text:00401460**

**.text:00401460 loc\_401460: ; CODE XREF: \_main+42j**

**.text:00401460 mov dl, [eax]**

**.text:00401462 mov bl, [esi]**

**.text:00401464 mov cl, dl**

**.text:00401466 cmp dl, bl**

**.text:00401468 jnz loc\_401488 ; program exits at loc\_401488**

**.text:0040146A test cl, cl ; test is cl is 0**

**.text:0040146C jz short loc\_401484**

**.text:0040146E mov dl, [eax+1]**

**.text:00401471 mov bl, [esi+1]**

**.text:00401474 mov cl, dl**

**.text:00401476 cmp dl, bl**

**.text:00401478 jnz loc\_401488 ; program exits at loc\_401488**

**.text:0040147A add eax, 2**

**.text:0040147D add esi, 2**

**.text:00401480 test cl, cl ; test is cl is 0**

**.text:00401482 jnz short loc\_401460**

Figure 3a: Extract of the start of main function

1. How many arguments does the main function take? 4

(1 mark)

1. How many local variables does the main function declare? 4

(1 mark)

**QUESTION 3** (cont.)

1. Explain when is the jump to loc\_401813 taken at address 0x40144E and if the jump is taken what happens?

The jump will happen when eax is equel to 0 or 2 and when it happen, it will exit the application.

(4 marks)

1. There is a loop structure in in figure 3a. Identify the code block (start address & end address) of the loop structure.

The loop start at loc\_00401460 and end at loc\_00401482

**.text:00401460 loc\_401460: ; CODE XREF: \_main+42j**

**.text:00401460 mov dl, [eax]**

**.text:00401462 mov bl, [esi]**

**.text:00401464 mov cl, dl**

**.text:00401466 cmp dl, bl**

**.text:00401468 jnz loc\_401488 ; program exits at loc\_401488**

**.text:0040146A test cl, cl ; test is cl is 0**

**.text:0040146C jz short loc\_401484**

**.text:0040146E mov dl, [eax+1]**

**.text:00401471 mov bl, [esi+1]**

**.text:00401474 mov cl, dl**

**.text:00401476 cmp dl, bl**

**.text:00401478 jnz loc\_401488 ; program exits at loc\_401488**

**.text:0040147A add eax, 2**

**.text:0040147D add esi, 2**

**.text:00401480 test cl, cl ; test is cl is 0**

**.text:00401482 jnz short loc\_401460**

(4 marks)

1. What is the purpose of the loop structure identified in 3(a)(iv)?

(4 marks)

It is a loop that add 2 to eax and esi everytime when it never meet the condiation of loc\_**00401468, loc\_0040146A and loc\_00401478**

1. What are the two conditions that must be met before the malware can be executed?

(6 marks)

The condition is eax must not be equel to 2 or 0 and the test for cl is 0.

**\*\* END OF PAPER \*\***