DV2567

MALWARE ANALYSIS

2017-01-07

Exam rules: - PLEASE, READ THIS BEFORE YOU BEGIN WRITING

- No helping material in any form is allowed except for a paper-based English DICTIONARY.
- Write the answers in English only.
- You **must** write name, CIVIC NUMBER and course code on each sheet of paper you hand in, including this page. There is reserved space in the page header for this purpose.
- The answer of each question must be written within the given space on exam paper (*i. e.*, the empty box below the question). Note also that the number of points you get per question is in no way proportional to the amount of text you deliver.
- Be explicit in your answers. Do not leave room for the examiner to guess what you mean. Implicit answers do not warrant any points.
- If the question requires you to provide an explicit number of examples/alternatives do not provide more. If you do, each wrong example/alternative will be detracted from accumulated score in the question (however, no negative scores will be given).
- The answers that cannot be interpreted due to bad handwriting or grammar will not be awarded any points at all.
- If you wish the examiner to ignore a particular submitted solution, cross over the space allocated for the solution and write IGNORE in capital letters. If all solutions on a page must be ignored, strike the entire page and write IGNORE in capital letters at the top. Do this for every page if you want the entire exam to be ignored (you will receive grade F).
- Only whole points will be awarded for correct and complete answers. Fractional points, such as 0.5p or 0.25p, will not be used.
- The minimum passing marks are 25 points. After obtaining the minimum passing points every next grade is achieved by reaching the corresponding point range as shown in the table below:

Exam points	46–50	41–45	36–40	31–35	25–30	< 25
Grade (Swe./ECTS)	A	B	C	D	E	F

Score table (received points)

Question:	1	2	3	4	5	6	Total
Points:	2	15	9	10	10	4	50
Score:							

1. Describe the technology used by the CodeRed worm to infect victims. (2p)

2. (a) Describe a basic technique relying on compression and encryption that viruses can use to escape detection from an antivirus program. Explain the various parts of the virus code when compression and encryption are used (*e. g.*, the decompressor is one such part), and what each part is used for. (10p)

(b) Explain what is the difference between polymorphic and metamorphic viruses and highlight which parts of the virus changes appearance and when (at which stage in the propagation). (5p)

3. (a) Describe the four main parts of the memory layout for a program focusing on what is stored into each part. You can treat data/BSS as a single part. The order in which they are arranged is not important here. (4p)

(b) Explain the stack layout in memory with emphasis on how caller stack frames are ordered during a call chain. Describe what is found in a typical caller stack frame in the correct order, assuming you enumerate from a high address towards lower addresses. (5p)

4. Examine the code snippet below.

```
        mov     [ebp+var_18], 0
        jmp     short loc_401018
loc_40100F:
        mov     eax, [ebp+var_18]
        add     eax, 2
        mov     [ebp+var_18], eax
loc_401018:
        cmp     [ebp+var_18], 6
        jge     short loc_401037
        mov     ecx, [ebp+var_18]
        mov     edx, [ebp+var_18]
        mov     [ebp+ecx*2+var_14], edx
        mov     eax, [ebp+var_18]
        inc     eax
        mov     ecx, [ebp+var_18]
        mov     dword_40A000[ecx*2], eax
        jmp     short loc_40100F
```

(turn page)

(a) There are two array variables of interest, which were automatically named by IDA Pro as `var_14` and `dword_40A000` using default naming rules. What is the scope of these variables and their location (stack, data/BSS or heap) based on the assigned names? Explain your reasoning. (6p)

(b) What are the values in the arrays indicated by `var_14` and `dword_40A000` when the jump to `loc_401037` takes place? (4p)

5. Provide a short explanation of how packing and unpacking executables works. Feel free to draw some figures if it helps. Include information about modifications to PE header and entry point. Describe briefly the general work procedure to manually unpack a packed executable (as was done in Lab 1.6) including the names of the typical tools you use. Name at least 3 packers that you know of. (10p)

6. Describe the two main architectures (topologies) used by botnets and explain the advantages and disadvantages associated with. (4p)