AUM AMRITESWARYAI NAMAHA

Enrollment Number _____

Amrita Vishwa Vidyapeetham
Amrita School of Engineering, Amritapuri
Amrita Center for Cybersecurity Systems and Networks
Third semester MTech CSN

16SN708 – Malware Analysis
First Periodical, August 2017

Duration: 2 Hours Max. Marks: 15

Note
There are 3 questions in total and 2 pages. Please ensure you have all questions and all pages of the question paper before starting. All regular examination rules apply. Do not copy and do not use internet during exam: a score of 0 will be awarded. You can refer to assembly programs discussed during the lectures. Good luck!

SECTION A
(*Each question carries 2 marks*)

1. Use the sample provided along with questions to answer the following questions.
   a) The sample is obfuscated or packed using some technique. Identify which obfuscation or packing technique has been applied to the sample and describe how you discovered the technique used. Also, deobfuscate/unpack the sample for answering the remaining questions. 1 mark
   b) The malware sample infects a specific desktop application. See if you can identify the target application of the malware by analysing the sample. Justify your answer with evidence/information obtained from the analysis. 1 mark
   c) The sample possibly stores some data in a database on the infected machine. Can you identify which database application/engine is used to store the data? Justify your answer with evidence/information obtained by analysing the malware. 1 mark
   d) Other analysts feel that the malware sends out HTTP requests and receives HTTP responses from a remote server. Identify the Windows API functions imported by the sample that support this hypothesis. 1 mark
   e) A user agent string is a string included in request headers by HTTP clients(eg: web browsers) to identify the software being used by the client. The provided sample uses a specific browser user agent string to possibly masquerade as a web browser. Identify which browser agent string used by the sample. 1 mark
   f) During dynamic analysis, you will observe outgoing data from the malware exchanged over the network. Since the sample possibly sends out HTTP requests, can you identify 1 URL, to which the sample probably sends requests, which should be monitored. 1 mark

2. Write an assembly program that accepts N integers from the command line and prints out the maximum among them. You can assume that at least two integers will be provided and they will fit within 32 bits. Use of standard C library functions is permitted. You cannot invoke any additional code besides the assembly code you write

and the standard C library functions. Submit the source file of the assembly code you wrote.(Hint: Use the atoi function) 4 marks

Sample output

```
$ ./find-max.out 70 43 91 58 18 10 51 45 47 81
91
```

We will compile and execute your code using the following commands.

```
$ nasm -f elf find-max.asm
$ gcc -m32 find-max.o -o find-max.out
$ ./find-max.out <list of numbers>
```

3. Write an assembly program to calculate the Nth fibonacci number and print it's value to stdout. If no fibonacci number exists, print -1. Multiple Ns will be passed as command line arguments. See sample output for examples. Submit the source file of the assembly code you wrote. 5 marks

Sample session

```
$ ./get-fib.out 1 2 3 4 5
0
1
1
2
3
$ ./get-fib.out 10
34
$ ./get-fib.out -12
-1
$ ./get-fib.out 53
32951280099
```

We will compile and execute your code using the following commands.

```
$ nasm -f elf get-fib.asm
$ gcc -m32 get-fib.o -o get-fib.out
$ ./get-fib .out <list of Ns>
```