Lab 5-1

March 23, 2020

Contents

1 Question 1

`0x1000D02E`

2 Question 2

`0x100163CC`

3 Question 3

`5`

4 Question 4

`pics.practicalmalwareanalysis.com`

5 Question 5

`20`

6 Question 6

`1`

7 Question 7

`10095B34`

8 Question 8

A command is appended and then it is executed.

9 Question 9

It is set by the return value of `sub_10003695`

10 Question 10

`sub_100052A2` is called.

11 Question 11

Firstly, a subroutine calls that makes sure the OS platform ID is Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000, and the major version is 5. Otherwise, `PSLIST` is not run.

Depending on the parameter to the function, a list of running processes is either written to `xinstall.dll` or sent over the passed network socket. If a non empty string is passed to the function, the specific function is opened and some additional information is logged or sent over the socket.

12 Question 12

Based on the systemcalls, it probably formats and sends a message over a socket:

- `GetSystemDefaultLangID`
- `malloc/free`
- `sprintf`
- `send`
- `strlen`

13 Question 13

It calls 4 API functions at a depth of 1, and ~31 with a depth of 2.

14 Question 14

EAX is loaded with the string "[This is CTI]30", then 13 is added, bringing the string to "30". Then atoi is called which converts the string into a number, and it is multiplied by 1000. Thus, the program will sleep for 30 seconds.

15 Question 15

- af = 2
- type = 1
- protocol = 6

16 Question 16

- af = AF_INET
- type = SOCK_STREAM
- protocol = IPPROTO_TCP

17 Question 17

Yes. We find one occurrence at 0x100061DB. We see a number 0x564D5868 used with the instruction, which corresponds to ASCII "VMXh".

Following the XREFs back to the Install* functions, there appears to also be another VM detection function at loc_10006119.

18 Question 18

We find a strange sequence of bytes that seems to be printable. It could be an encrypted or ciphered string of some sort.

19 Question 19

The script decrypts the string.

20 Question 20

By pressing the `A` key.

21 Question 21

The script XORs each byte with `0x55`, decrypting the string.