Anaisy Garcia

5734454

Lab 12-2

Analyze the malware found in the file Lab12-02.exe.

Questions

1. What is the purpose of this program?

This program secretly launches another program.

1. How does the launcher program hide execution?

There is a process replacement to hide the execution of the other program.

1. Where is the malicious payload stored?

Within the payload stored in the malwares resource section named localization and of type Unicode.

1. How is the malicious payload protected?

It is XOR encoded which can be found in sub\_40132C. the XOR byte can be found at address 0x0040141B.

1. How are strings protected?

The strings are XOR encoded using function sub\_401000.

Lab 13-2

Analyze the malware found in the file Lab13-02.exe.

Questions

1. Using dynamic analysis, determine what this malware creates.

This program creates random files in its directory with names like “temp” and the digits for each file probably to avoid collisions.

1. Use static techniques such as an xor search, FindCrypt2, KANAL, and the IDA Entropy Plugin to look for potential encoding. What do you find?

The XOR search technique finds encoding associated functions at sub\_401570 and sub\_401739. Other techniques show nothing.

1. Based on your answer to question 1, which imported function would be a good prospect for finding the encoding functions?

Encoding functions can be found just before the call to writeFile.

1. Where is the encoding function in the disassembly?

Sub\_40181F

1. Trace from the encoding function to the source of the encoded content. What is the content?

A screen capture

1. Can you find the algorithm used for encoding? If not, how can you decode the content?

The algorithm cannot be determined. It is better to decode traffic through instrumentation.

1. Using instrumentation, can you recover the original source of one of the encoded files?

Yes. Using ImmDbg we can change the extension of a written file and change the extension to .bmp this shows the screenshot taken by the program.