Practical Assignment 3

ACCDFISA File Crypter Malware Analysis

You are given a directory on your Windows Desktop named *ACCDFISA File Crypter* containing a file named *sys100s.exe_*. This can be renamed to be executed by double-clicking.

You have until Wednesday 9 April at 11:55 PM to complete your assignment and turn in your report via Sakai.

I suggest you reserve three or four hour blocks for analysis of this malware and release your reservation (pressing the *I'm Done* button as soon as you are finished). Take screen shots, make good notes, record everything necessary for either your report or continued analysis in a later netlab session.

I strongly suggest you make a task list identifying all the steps you plan to take in your analysis in the order in which you take them.

Your report should take the following form:

1. Report Title Block

The report title block should include

a) Report title

b) Date of preparation

c) Your name

d) Your email address

e) Assignment and Class

2. Executive Summary

Briefly describe the purpose and behavior of this software providing a recap of all results noted below.

3. Basic Static Analysis

Check at least the following for the packed executable:

a) Report the MD5 hash of this and any other relevant files that may be created dynamically by the malware. Inspect these hashes externally through the web to see what you can find out.
(A list of possible MD5 hashes is separately supplied for your convenience.)

b) Is the program packed?

c) Identify the compilation date of the program.

d) Identify any functions imported by the program.

e) Identify any relevant strings (ip addresses, registry keys, urls, etc.).

f) Identify the program sections and their possible contents.

g) Use ResourceHacker to investigate resources (if any).

4. Basic Dynamic Analysis

Check at least the following:

a) Run the software and determine what it does. There are several phases to its execution. Identify what the malware does both before and after reboot. Describe the behavior in a concise yet complete manner.

b) Identify any files the malware creates and explain their use. Some may be executable while others may just contain data.

c) Identify any Registry Keys created/modified by the malware. What is the significance of any such changes?

d) What network connections does this malware attempt to make?

5. Further Static and Dynamic Analysis

a) Try to identify any special key values that might need to be employed to remediate the effects of this malware.

b) Use both IDA and Olly to analyze this program. Answer the following questions:

1. What does the function sub_4057D6 do?
2. What arguments is sub_4057D6 called with?
3. From what locations is function sub_4057D6 called?
4. Discuss any other interesting functions you find.

6. Indicators

Identify any host-based indicators of infection and network behavior indicators that could be used by an IPS.