Homework 5: Basic Malware Analysis

See Webcourses and the syllabus for due dates.

What to turn in

For the problems in this homework, you will upload a word document or a PDF file.

General Directions

This homework is intended for individuals, but may benefit from working in groups as well. If you work in a group, be sure to follow the course grading policy, especially the cooperation section of the course grading policy, so that you properly certify that everyone in the group understands and participates in the solutions.

What to Read

Read chapters 1-3 of the book *Practical Malware Analysis* [SH12]. Chapter 2 gives information about setting up a virtual machine. You should try some of the exercises at the end of chapters 1 and 3. See also the course's analysis tools page.

Problems

Warning: be sure to work in a virtual machine or some other safe environment! See Chapter 2 of the book *Practical Malware Analysis* [SH12] and the course's analysis tools page for how to do this.
Also, when visiting unknown websites it may be wise to browse with JavaScript disabled (e.g., using firefox's no-script extension). We cannot guarantee whether the websites referred to here are safe (except for the course website, which is safe).

1. [Validate] Run flawfinder on the code from exam 2, which includes the files `query.c` and `prompt.c` (and `prompt.h`) in this homework's zip file. Then answer these questions:
   (a) (10 points) Are there any false positives found?
   (b) (5 points) Are there any problems missing (false negatives)?
   (c) (5 points) Overall, how well does flawfinder do at finding all the problems in the code?
2. [Reversing] Download the "WinMD5.exe" from the page http://winmd5.com/.
   (a) (5 points) Does the program use any DLLs in ways that one should be concerned about?
   (b) (5 points) What do virus scanners say about the file?
   (c) (5 points) Is the file packed? (Give a brief justification.)
   (d) (10 points) What does the file do when you run it (carefully, in a VM)?
   (e) (10 points) Summarize whether you think the file is malware or not and briefly justify your decision. This should be written as an "executive summary," without rehashing all the details, but getting at the most relevant information you uncovered.
3. [Reversing] Take the file `ClashBot.bin` from this homework's zip file, and change its file extension to exe, so that the file is renamed `ClashBot.exe`.
   (a) (5 points) What is the MD5 code of this program?
   (b) (5 points) Does the program use any DLLs in ways that one should be concerned about?

(c) (5 points) What do virus scanners say about the file?

(d) (5 points) Is the file packed? (Give a brief justification.)

(e) (5 points) What does the file do when you run it (carefully, in a VM)? (Note that you may need to use the properties to make it run in XP compatability mode.)

(f) (5 points) Summarize whether you think the file is malware or not and briefly justify your decision. This should be written as an "executive summary," without rehashing all the details, but getting at the most relevant information you uncovered.

4. [Reversing] Carefully download the "Free File Viewer" from the page http://file.org/free-download/free-file-viewer.

   (a) (5 points) What is the MD5 code of the downloaded program (FreeFileViewerSetup.exe)?

   (b) (5 points) Does the program use any DLLs in ways that one should be concerned about?

   (c) (5 points) What do virus scanners say about the file?

   (d) (5 points) Is the file packed? (Give a brief justification.)

   (e) (10 points) What does the file do when you run it (carefully, in a VM)?

   (f) (10 points) Summarize whether you think the file is malware or not and briefly justify your decision. This should be written as an "executive summary," without rehashing all the details, but getting at the most relevant information you uncovered.

Points

This homework's total points: 125.

References

[SH12] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, San Francisco, 2012.