SEC 150 Assignment: Detecting Viruses

Titus Barik (tbarik@staff.waynecc.edu)

Version 1.0

1 Assignment Description

In this assignment, you will learn some of the techniques that anti-virus software products use to detect viruses.

You will create a "virus" containing your name. You will then modify an actual open source anti-virus tool so that it recognizes your name and detects it as a virus (don't worry; it isn't permanent).

Upon completion of this assignment, you will be able to generate signatures for new viruses, and submit your signatures to anti-virus vendors.

2 Pre-Requisites

Before starting this assignment, watch the lecture video on ClamAV, and make sure that you have the PortableApps version of ClamAV installed on your system. Then read the document "Creating signatures for ClamAV", in particular, the sections marked Introduction (1), MD5 (3.1), and Body-based signatures (3.3).

3 Instructions

1. Create a file called `virus1.txt` with your last name in all capitals. For example, I would create a file with the contents `BARIK`.

2. Create a checksum-based signature file for `virus1.txt` using `sigtool`, and name the signature file `virus.hdb`.

3. Use `clamscan` to verify that your virus is actually detected by your checksum-based signature. You can do this with `clamscan -d virus.hdb virus1.txt` and examine the results.

4. Unfortunately, checksum-based signatures have a severe limitation in the way that they detect viruses. What is this limitation? Put your answer in a plain text file called `answers.txt`.

5. Create a file called `virus2.txt`. It should contain text such as `HELLO TITUS BARIK HOW ARE YOU`. The actual text doesn't matter, just make sure it contains your last name in all capitals somewhere in there.

6. Now, you want to create a body-based signature using the extended signature format as in section 3.3.4. The body-based signature should flag a file as a virus if it contains your last name anywhere in the document, and regardless of what else is in the document. (In my case, if the document has the word BARIK in it anywhere, it should be considered a virus).

7. To do this, set TargetType as 0, Offset as `*`, and generate a hex signature using `sigtool` with the `--hex-dump` argument. **Hint:** The output of `sigtool` might add the characters `0d0a` at the end of the string. If so, remove these characters.

8. Put this extended signature in a file called `virus.ndb`.

9. Test that ClamAV detects `virus2.txt` as a virus using the command `clamscan -d virus.ndb virus2.txt`. If it doesn't say `Infected files: 1`, then something is wrong and you should check your extended signature.

10. What is the advantage of an body-based signature when compared with a checksum-based signature? Document your answer in `answers.txt`.

4 Milestone

Submit a screen capture that shows ClamWin running on your machine.

5 Submission

Submit all of your files as a single zip archive. The archive should include the following files: `virus1.txt`, `virus2.txt`, `virus.hdb`, `virus.ndb`, and `answers.txt`.

Students are encouraged to help each other; please post issues to the Discussion Board.