14-819 Homework #4

Assigned March-30-2019.
Due April-4-2019.

In class, we followed the manual unpacking procedure for a simple VB malware. In this homework you are to attempt a similar procedure on your own.
Consider an internet worm with a Trojan horse module called Zan. The worm is compressed using an algorithm that is somewhat similar to what we've done in class. **This is a life dangerous virus! For your computer safety, work only in a protected and isolated environment.**

For this assignment do the following:

1. Download password protected worm 'zan.zip' included with this assignment
2. Use password "infected" to open the archive.
3. Use Ollydbg runtime debugger and Import Table Reconstructor to unpack the virus. Produce a one-two page report on your accomplishment including the following:
   - Indicate calls to the unpacking routine, VirtualAlloc and VirtualFree functions.
   - Indicate starting and ending offsets of the packed code in memory that will be unpacked by the virus. What is the offset of buffer containing unpacked code? What is the size of the buffer?
   - Locate the Entry Point in the unpacked virus.

4. Make sure that the final unpacked virus runs silently and does not produce any errors.
5. Compress and password protect the file (password: "infected") and include with your solution.