NAME: **ALPHA:**

SY485J: Lab 10: What is this malware doing?

Go to http://courses.cyber.usna.edu/~debels/SY485J/Code/Lab10. There are two files: file3 and file1. Your goal is to find out what this malware is doing. Answer the following questions about the files. This lab is **due Monday, December 2, 2019 by 0855.**

1. (50 points) Is one of the files used to protect the other? If so, which file is doing the "protection" and how is this protection done? Be specific. Make sure to answer the following questions. Are common libraries and/or functions being used to perform the protection? If so, what are they? Are their constants in the code? If so, what is each being used to do? Is there a better way that you can think of to hide these constants from reverse engineers? If one of the files is protecting the other, how is the other file "liberated" and where is the "liberated" code placed?

NAME: **ALPHA:**

2. (50 points) What is the main functionality of this malware? Be specific. Describe exactly what the malware does, how it does it, and how it is called. Make sure to answer the following questions: What is the malware author trying to get the (unsuspecting) user to think he/she is doing? What information is the user (unknowingly) giving to an attacker and how does it get to the attacker? What do you think the attacker has to be doing in order to obtain this information? Does the victim (you) know if the attacker successfully accomplished their goal?