NAME: **ALPHA:**

SY485J: Lab 9: What is this malware doing?

Go to http://courses.cyber.usna.edu/~debels/SY485J/Code/Lab9. There is one executable, runmenow. Your goal is to find out what this malware is doing. The malware is obscured in some way. You first need to find out how it is obscured so that you can see the actual executable. There are multiple ways the malware is infecting your machine once it in un-obscured and run on your laptop. This lab is **due Thursday, November 21, 2019 by 0955**. Have a nice day!

1. (50 points) How is the malware obscured? Describe in detail how it is hidden and what you did (step by step) to get to the underlying executable.

NAME: **ALPHA:**

2. (50 points) Describe in detail all of the malicious things you found that the malware is doing. Be specific. For example if the malware is placing a file on your system, give the file name, exactly what the file does, the actual file type (jpg, doc, pdf), etc.