Lecture 1: In-class Homework

Download zip file that contains hw\_1\_in.exe and hw\_1\_in.dll from the course website. Unzip them to a location in on your VM. Answer the following questions (attach screenshots if you can):

1. Upload the files to *VirtusTotal* and evaluate the reports. Does the consensus indicate they are malicious ? Any possibly in what type ?
2. When were the files compiled ?
3. Is the program packed ? How do you find it ? Show the proofs by snapshots
4. What are the imports ? Are there any imports that look suspicious ? Can you tell what the malware can do from the imports ?
5. Are there any network-based indicators ? If it is an IP address, what is it ? What can you tell from it ?
6. Can you guess the purpose of the malware ?