CS495/595 In-class Homework 2

Download zip file that contains hw\_2\_in.exe from the course website. Unzip to a location on your VM. Answer the following questions (attach screenshots and notes):

1. Can you guess what the program do using only static analysis? (Hints: use PEView to see the imports, string.exe and PEiD to check if it is packed). Provide evidence for the following questions (attach screenshots if you can):
   1. What are the imports?
   2. Are there any network-based indicators? Such as URLs
   3. Are there any Registry Keys being modified?

If the gathered evidence is not sufficient to draw a conclusion, proceed to the dynamic analysis in the following.

1. Use basic dynamic analysis learned in this lecture to figure out what the program does. Follow the hints below (take a snapshot of the VM before running it):

2.1 When you use string, what interesting strings did you see? List a few strings you think interesting (similar to Question 1.2).

2.2 Let’s use the Process Explorer. Search for the process name hw\_2\_in.exe. Select View->Lower Pane View Handles/DLL (look for mutant, what did you see? What mutex is created? Which DLLs are loaded?

2.3 Kill the process hw\_2\_in.exe in Process Explorer and Open ProcMon. Set a filter on the process name hw\_2\_in.exe, and operation: RegSetValue to see results, open the program again. Which file can you see the program has created under system32? Find it and compare the SHA hash on onlinemd5.com with hw\_2\_in.exe. What can you conclude?

2.4 Use ApateDNS to capture any DNS request. What did you see?

Summarize what the malware does in one or two sentences.