**CMSC 491/691 Malware Analysis Final**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assigned: 5/13/2020

Due: 5/18/2020 by 8:00pm

Download final2020.7z and extract it. The password is “infected”. Answer the following questions about final2020.exe. There are 105 points available and the final will be graded out of 100. **Make sure to run Immunity debugger in administrator mode or the malware will not run properly!**

1. Is this final2020.exe packed? List 3 indicators that it is or is not packed. (8 pts)  
     
   a.  
     
   b.  
     
   c.  
     
   Packed (Y/N): \_\_\_\_\_
2. What file is copied by CopyFileA at 0x402067? Where is it copied to? (6 pts)
3. Which file has its attributes modified when SetFileAttributes is called at 0x402077? What attributes are given to the file? Please provide the names of the attributes, not a number. (8 pts)
4. For what purpose does the malware call RegOpenKey at 0x402092 and then RegSetValueEx at 0x4020BF? Justify your answer in detail. (10 pts)
5. What is the value of the string being passed as the first argument (lpCmdLine) to WinExec at 0x4020D9? Why is the malware doing this? (8 pts)

1. If execution reaches the call to FUN\_00403186 at 0x4020E0, the malware will terminate its own process. Use Immunity Debugger to force execution to reach 0x4020EA. Describe how you did this and provide a screenshot showing execution paused at 0x4020EA. (10 pts)
2. Describe what the function FUN\_401DF0 does in detail. What does the function return? (16 pts)
3. What is the value of the argument passed to FUN\_401DF0 when it is called at 0x4020EA? (4 pts)
4. What is the value returned by FUN\_401DF0 when it is called at 0x4020E5? Provide a screenshot of this value in Immunity debugger. (5 pts)
5. When FUN\_402FDC is called at 0x40213C, the first argument of is a pointer to a sequence of bytes and the third argument is the length of the byte sequence. Investigate this byte sequence. What is interesting / unusual about it? (5 pts)
6. The malware calls FUN\_401CF0 at 0x40215F. This function performs one of the covert malware launching techniques described in chapter 12 of PMA. State which technique is used (be specific) and describe what this function is doing – a very detailed analysis is expected. Make sure to explain what both parameters and any important Windows API functions are used for. (25 pts)