CPE457/557 Software Reverse Engineering

**19 - Dynamic API code obfuscation**

# Reverse Engineering Activity

**Lab Description:** The goal of this lab is to reverse engineer a program that dynamically resolves all the addresses for the functions (from the Windows API) that it uses. It does this by first finding the base address of the DLL/module that it needs functions from, then walks the exports of the module to find the addresses. This complicates the process of analysis by obfuscating the function calls, making it more complex to determine the purpose of the program.

**This is a malicious file - do NOT execute the sample unless in a sandbox or lab environment.** The sample has been provided without an extension to help prevent accidental execution. You can analyze this sample with tools like IDA Pro, since it performs static analysis only, without infecting yourself.

**Lab Environment:** Use of a virtual machine is recommended.

**Lab zip File Needed:**

The password to the zip is ‘infected’, which is industry standard for archives that contain malicious files.

Sample MD5: 30d3307779016426d24f3077d8f33514

You may need to disable Windows Defender: <https://support.microsoft.com/en-us/windows/turn-off-antivirus-protection-in-windows-security-99e6004f-c54c-8509-773c-a4d776b77960>

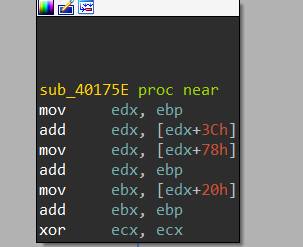
### **Part 1 – finding modules**

*Learning Outcomes 1 and 2*

Answer the following questions using unknown file:

1. What function is responsible for resolving the base of a required DLL?

sub\_40175E



1. Briefly describe how this function works - discuss structures used, how it utilizes any data in the executable and any other relevant information. Please provide screenshots of your analysis.

### **part 2 – resolving apis**

*Learning Outcomes 2, 3 and 4*

1. What function is responsible for resolving the address of an API?
2. Does this function depend on the previous function? If so, how?
3. Briefly describe how this function works - discuss structures used, how it utilizes any data in the executable and any other relevant information. Please provide screenshots of your analysis.

### **Part 3 – Calling functions**

*Learning Outcomes 4*

1. How does this program make the API call?  Summarize the technique used, provide the name of an API called, and show where the API call is made.

# What to submit

Submissions should be neatly organized. Each question should include at least one screenshot and a brief explanation if possible.