Statement of Work

The purpose of this project is to identify what the provided unknown executable ECS.exe does when opened. To aid in our investigation, we will find and use online reverse engineering tools, including disassemblers and decompilers. After using them, we will compile a list with the tools used, in which we describe where to find them, their ease of use, advantages, disadvantages, and lessons learned using the program. Our initial investigation has led us to believe that this executable is a mix of a simple calculator function intermixed with malicious code. We will make the add, subtract, multiply, divide, power, natural log, compound interest, factorial, combination, permutation, and the guessing game work correctly. To do this, we will isolate the dangerous code in the file. We will modify the guessing game to allow the user to automatically win when a secret key is entered. To complete this project, we will meet both online as well as in person. To safety analyze the executable, we will use a Windows 10 virtual machine so that we do not risk infecting our own systems. We will start the project on October 21, 2020 and will finish by December 1, 2020.

We submitted a Progress Report to our client on October 29, 2020, documenting our initial findings and project plan. We will submit our final executable, final report, and present our findings, on December 1, 2020.