Description of Unknown Executable

This unknown executable appears to be a calculator with multiple options to select from that also has malicious code intermixed with the main code. There are multiple stages of the malicious code. Upon execution in a Windows 10 VM, the program first starts a repetitive cycle of opening a YouTube video 19 times on both Microsoft Edge and Google Chrome. The program then shows the menu options, prompting the user for input (example: “1”, “2” Etc.) The calculator section contains 10 mathematical functions options and one guessing game mode for the user to select. Upon entering the valid instructions, the program will then print out “wrong answer” 500 times. The program then reprints the menu options, and then automatically inputs “-1” while printing “choice = -1”. The program again displays “wrong answer” 500 times. The process repeats until in the fourth iteration, the program prints “don’t do it again” 1,000 times to the screen after reprinting the menu. The program automatically inputs “-1” once more while printing “choice = -1”, and again outputs “wrong answer” 500 times. On the next iteration, after printing the menu, the words “I warned you” are output 1000 times. The executable then starts to open the programs Outlook, Paint, Photos, Notepad, along with html page of corndogs floating on Microsoft Edge and Google Chrome on the user’s computer that loops for 1000 times.

Upon circumventing the above mentioned loop structure, options 1 through 4 prompt the user to enter two numbers and calculate the result based on the selected mathematical operation. Option 5 prompts the user to enter a base and exponent and outputs the correct calculation. Option 6 takes the user input and calculates the natural log of that number. Originally, when the user enters “7”, the program prints “Hello” followed by the user’s student id. The program then prints “It’s too bad that you decided to run this program…” and “There’s still time to turn back”. Multiple command lines are then opened on the user’s machine. After circumventing the malicious code option 7 prompts the user to enter the principle dollar amount, the yearly interest rate, and the number to years. The program then computes the compound interest rate and outputs the result. Option 8 prompt the user to enter a number and calculates the factorial of the input. If the user enters a negative number, an error message is displayed saying that the input must be non-negative. Options 9 and 10 calculates the combination and permutation respectively of the user inputted n and m values. If m is larger than n, then an error message is output stating that n must be larger than m. Option 11 starts a guessing game. First the program calculates a random value between 1-100. The user is then prompted for a guess. The program displays if the input is too low, too high, or the correct number. After three incorrect guesses, the program outputs if the random value is divisible by 3 or not. After the 7th incorrect guess, the program outputs whether the value is divisible by 2. Once the user enters the correct value, the program prints “Wow! You got it!” followed by the correct number. The number of tries it took to find the correct answer is then output.