# CSC 471 Spring 2025 Final Project

Dr. Si Chen

## Topic: Malware Analysis: Zeus

## 1 Introduction

The final project for this course is to analyze the notorious Trojan malware, Zeus. You will be required to use the provided memory dump file (`zeus.vmem`) and analyze it with the Volatility framework. This part of the project is similar to what we covered in Class 20. Subsequently, you will need to use the leaked source code of the malware to justify your analysis.

## 2 Group Formation

This project involves group collaboration, with each group consisting of up to 3 students. Alternatively, you may work individually if you prefer. If you decide to work as a team, **please send an email to me before 04/29, 2025, including your group members' names and WCU IDs.** After 04/29, 2025, **you will NOT be able to claim team membership**. However, you can still work on this project individually.

## 3 Final Report

Each team must submit one detailed malware analysis report (in PDF format) on D2L. The team leader is responsible for submitting the report using their student account. On the first page of your group report, indicate how your team has divided the tasks among the members.

In your report, use both text and figures (e.g., screenshots) to demonstrate what you have done. Do **NOT** copy or reuse screenshots from other groups or students.

### 3.1 Malware Analysis Report

A malware analysis report is a document that provides an in-depth breakdown of the functionality and risk of a new or evolving cyber threat. Your malware analysis report should include the following sections:

- **Introduction**: Provide a brief introduction to the malware.
- **Findings**: Describe what the malware is designed to do, using the following two methods:
    1. Use Volatility to analyze the malware memory dump and report how Volatility can be employed to find relevant artifacts of the activity within memory (e.g., identify all API Hooks of Zeus).
    2. Use the leaked malware source code to justify such activity (e.g., pinpoint which function/line of code is responsible for the API Hooks). Note that this part is crucial; your group must identify the functions/lines of code for each malware activity found in the memory dump.
- **Summary**: Summarize your work and provide best practices for preventing infections and recovering from them.

## Submission

- Each team must submit a detailed report (in PDF format) on D2L. The team leader should submit the report using their student account to D2L. On the first page of your group report, please indicate how your team allocated tasks among its members.
- Your submission should include:
    1. A comprehensive project report detailing your work, complete with screenshots and code snippets. Include explanations for any interesting or surprising observations. You are encouraged to explore beyond the project description's requirements. Bonus points may be awarded for extra efforts.
    2. Your program's source files (compressed into a .zip file) in the programming language of your choice. Note: DO NOT submit binary results or raw data files.
    3. Academic integrity is expected. If your work is based on others', provide clear attribution. Failure to do so may result in failing the course.