Malware Analysis Project 2
CSCI 4976 - Fall 2015
Malware Analysis

Overview

After the incident at your last job you were laid off and have been looking for work since. You met someone in League of Legends who claims to do security work, and can put in a word for you, but you need to demonstrate your skills to his boss. Apparently his boss is a jerk who spends all day every day playing, and failing at, minesweeper. You'd rather have a boss you like, but you need the money. You remember hearing of "trainers" for video games, and you decide to make one so mr. boss can finally win a game of minesweeper, and you can get a job.

A trainer is a name for a program that hacks a game (usually) in order to perform certain tasks, such as infinite health, one shot kills, revealing enemies on a mini-map, etc. You will do something similar to minesweeper in order to aid mr. boss in his endeavors. Your trainer must be able to…

1. Extract the layout of the tiles
2. Make the mines visible in the game
3. Freeze the timer
4. Render mine tiles inert
5. Auto-win
6. User interface
    - For output or for choosing which task to enable/disable/perform
    - This can be terminal-style or graphical

Your submission will be broken into two parts, source code and a small report. I recommend using Visual Studio to make a DLL that, when injected into minesweeper, has the ability to perform these tasks. You may use your own DLL injection program or a third-party's as long as it is included in your submission. **You will NOT receive credit for patching the minesweeper binary on disk.** This must work with a vanilla copy of Windows XP Minesweeper.

Rubric

Below is the point breakdown for what is expected of you in this assignment.

Pts	Title	Description
10	**Advanced Analysis**	Document your analysis process. How did you find where/how minesweeper stores its grid? Describe this representation. How did you perform each of the tasks, and what analysis was needed for each? This should be similar in style to the Advanced Static/Dynamic Analysis sections of the Project 1 Report.
5	**README**	How do I use your trainer? This can be plain text file.
10	**Extract Tile Layout**	Extract the tiles from memory, and calculate the values of any hidden tiles. This should be an ASCII table of the minesweeper grid that shows empty tiles, numbered tiles, and mines.
10	**Show Mines**	Make the mines visible in game. This involves changing all of the hidden mine tiles to display the mines they hide, like what happens when you lose.
10	**Freeze Timer**	Freeze the in-game timer. In other words, prevent it from changing any further.
10	**Inert Mine Tiles**	Clicking on a mine tile does not make you lose the game.
15	**Auto Win**	Auto solve the game. All mines must be marked and all tiles revealed. DO NOT just call minesweeper's “win” function.
5	**Usability**	Make your trainer easy to use and interact with. Does it crash minesweeper?
75	**Total**	