



Malware Inc.

Project Leader: Jay Guillard

Supervisor: Kimberly Tam

Contents

[Introduction (read to make sure) 3](#_Toc31881675)

[Project outcome (revenue and education) 3](#_Toc31881676)

[Processes: 3](#_Toc31881677)

[Trello 3](#_Toc31881678)

[GitHub 3](#_Toc31881679)

[Supervisor Meetings 3](#_Toc31881680)

[Technologies: 3](#_Toc31881681)

[Risk Assessment: 4](#_Toc31881682)

[Task Run Down (thought process) 4](#_Toc31881683)

[Interface: 4](#_Toc31881684)

[Classes: 4](#_Toc31881685)

[Countries: 4](#_Toc31881686)

[Malware: 4](#_Toc31881687)

[Timers: 4](#_Toc31881688)

[Win and Lose Scenario: 4](#_Toc31881689)

[Income and Infection rate upgrades: 4](#_Toc31881690)

[Difficulty Levels: 4](#_Toc31881691)

[Supervisor Meeting Summaries: 4](#_Toc31881692)

[Week 1: 4](#_Toc31881693)

[Week 2: 4](#_Toc31881694)

[Week 3: 4](#_Toc31881695)

[Week 4: 5](#_Toc31881696)

[Brochure and Poster Design 5](#_Toc31881697)

[Testing 5](#_Toc31881698)

[Conclusion 5](#_Toc31881699)

# Introduction (read to make sure)

This project is based on the popular mobile game Plague Inc which allows the player to develop their own virus and to facilitate its spread across the world, but with the idea of spreading malware rather than a virus. Just like in Plague Inc, the user will be able to develop their malware so that it can be spread using different formats (e.g. app stores, emails, etc.) and different devices (operating systems) that it can infect. From the originating country, other countries could potentially be infected by using email, the app store, etc, but countries that have restricted internet access (China, North Korea, etc) will only be accessible by physically transporting (plains/boats) the malware. The more people in a country with infected devices, the more likely that the infection will spread electronically and/or make it onto a plane or boat into a “restricted country”. The user will also be able to evolve the malware so that it becomes a different type of malware, making it difficult to track and eradicate. At the start it could be adware and by the end it could have evolved into ransomware and so generate a cash windfall for the creator. Like the game, you will have the ability to speed up time and which will advance the game quicker and so reduce the time taken to earn the money needed to buy enhancements to your malware. Once a certain number of days has passed, countries will start researching a solution to the malware and which will result in the malware being eradicated once the research reaches one hundred percent complete. If the malware spreads far enough and can infect modern operating systems, then it will start to infect devices being used to eradicate the malware and slow down their progress. The user will also have to strategize on how they develop their malware, i.e. should they focus on making the malware produce more money or make the malware more infectious? This strategizing will help the user to also develop their resource management skills, as they will have to consider what advancements to make with their malware and the impacts/benefits of each change made. The purpose of this game is to therefore develop the users strategizing and resource management skills, while providing an enjoyable gaming experience.

# Project outcome (revenue and education)

# Processes:

## Trello

## GitHub

## Supervisor Meetings

# Technologies:

This program will be done with the uses of C# windows forms, this is mainly as it is the solution that I am most familiar. There are some restrictions with using this technology like the fact I will not be able to have a graphics of the world with changing colours to show the spread of the virus. But I believe that this will be the technology that will allow for the greatest chance of project success given the limited time and limited resources (manpower). All other functionality will be achievable and the main display for the spread will be the world and countries summaries, that is included in Plague Inc. as a secondary means of checking the spread of the virus.

# Risk Assessment:

# Task Run Down (thought process)

## Interface:

## Classes:

### Countries:

### Malware:

## Timers:

There are two timers that are responsible for the majority of the applications functionality. The first timer (timer1) is responsible for the processes that take place during each simulated day in the applications. This involves how many devices are infected and how much they have made. The number of infected devices is randomly generated using the malware infection level to determine the minimum and maximum and uses that to generate a number in between. The income is determined by the number of infected devices overall and then multiplying that by a different value depending on the income level of the virus. The data grids are updated to show the changes and so is the money display.

The second timer (timer2) is responsible for the pausing and unpausing of timer1 when the user when the user goes to the upgrade tab. This is accomplished by checking what tab is currently selected and if the upgrade tab is currently selected then timer1 is enabled and if the world tab is selected it reactivates timer1 allowing for the game to continue.

## Win and Lose Scenario:

## Income and Infection rate upgrades:

## Difficulty Levels:

# Supervisor Meeting Summaries:

## Week 1:

During this meeting all participants of the meeting introduced themselves and what they are creating for there final year project. This session was more of an introduction with are supervisor and what we had to do for the start of the project (e.g. share trello and add them as a user to GitHub repository).

## Week 2:

This week involved the group sharing what we have accomplished during the following week and what we plan to do during the coming week. When it came to my plan for the coming week there where no suggestion as to do anything differently. We also discussed the layout of the report and what sort of content should be included.

## Week 3:

## Week 4:

# Brochure and Poster Design

# Testing

# Conclusion

Possible Reference

Top tier of infection:

<https://www.cisco.com/c/dam/assets/offers/pdfs/midyear-security-report-2016.pdf>

ransomware most profitable

<https://ieeexplore.ieee.org/abstract/document/7579103>

drive by infection