



Malware Inc.

Project Leader: Jay Guillard

Supervisor: Kimberly Tam

Contents

[Introduction (read to make sure) 4](#_Toc33611162)

[Project outcome (revenue and education) 4](#_Toc33611163)

[Processes: 4](#_Toc33611164)

[GitHub: 4](#_Toc33611165)

[Supervisor Meetings: 5](#_Toc33611166)

[Legal, Social, Ethical and Professional Issues 5](#_Toc33611167)

[Data Protection: 5](#_Toc33611168)

[Ethical Issues: 5](#_Toc33611169)

[Intellectual Property: 5](#_Toc33611170)

[Method of Approach 5](#_Toc33611171)

[Technologies: 5](#_Toc33611172)

[Risk Assessment: 6](#_Toc33611173)

[Design Diagrams: 7](#_Toc33611174)

[Interface Design 7](#_Toc33611175)

[Class Diagrams 7](#_Toc33611176)

[Country Class 7](#_Toc33611177)

[Malware Class 8](#_Toc33611178)

[Logic Design: 9](#_Toc33611179)

[Infection Devices and Unrestricting Countries: 9](#_Toc33611180)

[Upgrade Buttons (logic for both income and infection upgrades): 10](#_Toc33611181)

[Task Run Down 11](#_Toc33611182)

[Interface: 11](#_Toc33611183)

[Classes: 11](#_Toc33611184)

[Countries: 11](#_Toc33611185)

[Malware: 11](#_Toc33611186)

[Timers: 11](#_Toc33611187)

[Win and Lose Scenario: 11](#_Toc33611188)

[Income and Infection rate upgrades: 12](#_Toc33611189)

[Difficulty Levels: 12](#_Toc33611190)

[Casual: 12](#_Toc33611191)

[Normal: 12](#_Toc33611192)

[Hard: 12](#_Toc33611193)

[Infecting Restricted Countries: 12](#_Toc33611194)

[Leader board: 12](#_Toc33611195)

[Operating System Restrictions: 12](#_Toc33611196)

[Supervisor Meeting Summaries: 12](#_Toc33611197)

[Week 1: 12](#_Toc33611198)

[Week 2: 13](#_Toc33611199)

[Week 3: 13](#_Toc33611200)

[Week 4: 13](#_Toc33611201)

[Week 5: 13](#_Toc33611202)

[Week 6: 13](#_Toc33611203)

[Week 7: 13](#_Toc33611204)

[Week 8: 13](#_Toc33611205)

[Week 9: 13](#_Toc33611206)

[Brochure and Poster Design 13](#_Toc33611207)

[Testing 13](#_Toc33611208)

[Trello Boards: 13](#_Toc33611209)

[Trello Board 1: 14](#_Toc33611210)

[Trello Board 2: 14](#_Toc33611211)

[Trello Board 3: 14](#_Toc33611212)

[Trello Board 4: 15](#_Toc33611213)

[Trello Board 5: 15](#_Toc33611214)

[Trello Board 6: 15](#_Toc33611215)

[Trello Board 7: 15](#_Toc33611216)

[Trello Board 8: 15](#_Toc33611217)

[Trello Board 9: 15](#_Toc33611218)

[Testing: 16](#_Toc33611219)

[User Testing 16](#_Toc33611220)

[Summary: 16](#_Toc33611221)

[Alterations: 16](#_Toc33611222)

[Evaluation: 16](#_Toc33611223)

[What went well: 16](#_Toc33611224)

[Feedback: 16](#_Toc33611225)

[Future Improvement: 16](#_Toc33611226)

[Conclusion: 16](#_Toc33611227)

[Reference List: 16](#_Toc33611228)

# 

# Statement of Word Count

# Project Links

All code written will be submitted to the final submission point. If for whatever reason it is unavailable, the software is available via my GitHub repository linked below. Included is also a link of my trello board for the project:

Trello: <https://trello.com/b/dhhDBJbr/malware-inc>

GitHub: <https://github.com/JayKay202/Malware_Inc>

# 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.

# Project outcome (revenue and education)

The purpose of this project is to demonstrate how much we rely on technology and how one piece of malware can affect all of our lives. This should encourage people to go into cyber security roles to try and prevent these sorts of organizations from creating these pieces of malware. As this is an app there is also the potential for monetary gain in the form of pay once or with ads or with addition content that is hidden with a pay wall (freemium content). The purpose of this game is to therefore develop the users strategizing and resource management skills, while providing an enjoyable gaming experience.

Strategizing Skills: should they focus on making the malware produce more money or make the malware more infectious.

Resource management skills: as they will have to consider what advancements to make with their malware and the impacts/benefits of each change made.

Although there is no given client for this project, the possibility to sell this application to an app developer is a possibility.

# Processes:

Trello Board: This will be where all tasks that make up the project will be displayed and will be organised into three different categories. The first category is the backlog which is where all tasks for the project start. Once a task has been started it will be moved to the in-progress category, this is so you can see how many tasks are currently being worked on. Once a task has been complete it will be categorized as complete so that it is not mistaken as being in another category. All Trello boards can be found later in this report to demonstrate the project development over the weeks.

## GitHub:

This is how we will be organising are change management and are backups. This will allow for me to see how my application has change from previous pushes to GitHub. Therefore, if the application stop working after a change, we can look back at what exactly was changed and take the correct items to resolve the issue. As the application will additionally be stored online, if the machine that the application is being developed on is destroyed or lost. Then the application can be downloaded onto another machine, as long as you remember the username and password for the GitHub account.

## Supervisor Meetings:

The supervisor meeting is done in order to cover scrum meeting, which is needed given that we are doing agile project management. During these meeting we will be covering what we have done in the prior week and what we plan to do in the coming week. This will also allow for other students and supervisor to give advice on what feature can be add to the project and possible solutions to issues that I am experiencing with the project.

# Legal, Social, Ethical and Professional Issues

## Data Protection:

As We will not be storing any of the user’s information and all the information is stored locally and will not therefor be stored on any of our servers. Meaning that we will not have to worry about data protection when it comes to this project and can spend more time on other issues.

## Ethical Issues:

## Intellectual Property:

All code is written by me as the only member of the project and therefore all code/intellectual property belongs to me. If the program is sold to an organization then they are the owners of the code in question and will fold all rights.

# Method of Approach

Given the requirements of this cause the project is being managed using agile methodology with a scrum framework. Using Plague Inc feature a backlog of tasks that need to be complete in sprints. GitHub was used in order to do version control, which is in line with agile sprint to provide backups and evidence of sprints undertaken. In order to keep track of the progress of the project trello was used in order to see which task had or hadn’t been completed.

# 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. With the readymade assets (buttons, datagrids, etc.) this will reduce the amount of time need to create the interface and therefore allow for more time to be spent working on the logic behind the interface. This will also allow for more features that are not specifically require, but will improve it function, to be more likely to be completed before the end of the project.

I have not used a database as this would require the application to be connect to the internet at all times. As Plague Inc. is what my project is based upon, I have done testing to see what functionality it has. One such feature is that it does not require an internet connection to run. Therefore, I have stored the countries information within the code so that the user can still uses the application when not connected to the internet.

In order to backup and change manage the project all files are stored on GitHub, which will allow for changes made to be pushed to the master copy on the GitHub server. There is the device with all files goes missing or damaged all of the data can be recovered by downloading it from GitHub. There is also a log of all of the changes made to the program over the time of the project. If there was an error that was not present during the last chunk of code, you can check the log to see what has changed since the last instant and uses that to narrow down the cause of the error.

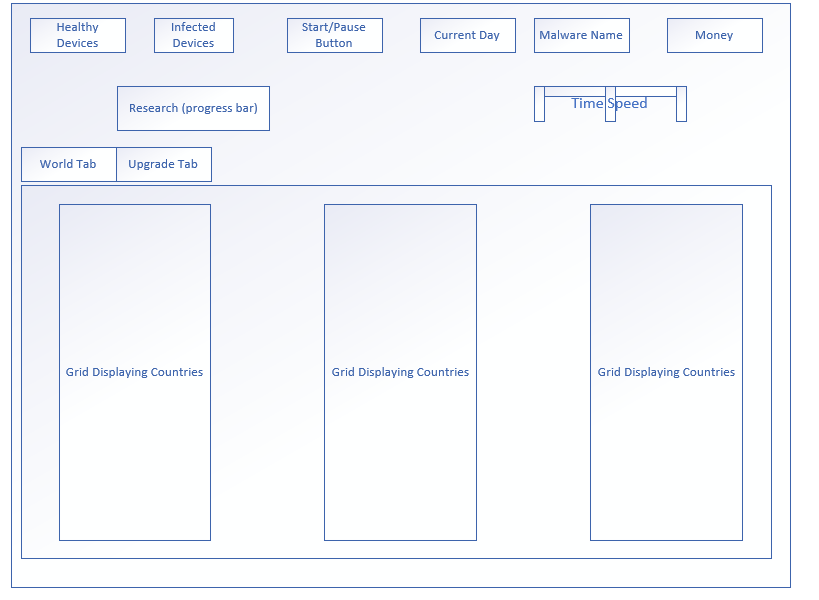
# Risk Assessment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Description | Likelihood | Impact | Overall Risk | Level | Action (if needed) |
| 1 | Requirements for the project change. | 1 | 7 | 7 | Ignore | N/A. This is because this project is based on an application that already exist and changing it to be malware rather than a virus. Also, as I do not have a client for this project, there is no possibility of them changing their mind. |
| 2 | Holidays and sickness. | 4 | 4 | 16 | Consider | Mitigation: The impact of this can be mitigated by ensuring that we account for extra time during the development of the game. |
| 3 | Coding delays caused by inaccurate estimates. | 6 | 6 | 36 | Consider | Mitigation: We can account for this by building in a degree of flexibility in the timings. |
| 4 | Errors discovered in module testing. | 3 | 8 | 24 | Consider | Mitigation: We can mitigate this by running tests throughout the project and so ensure that small errors do not become big errors. This will also make the error easier to locate as you will know that it is something you did after the previous test. |
| 5 | Having to change technologies mid project. | 6 | 10 | 60 | Take Action | This can be mitigated by researching beforehand to ensure that the technologies will be suitable for the project and allow for the project to be completed on time. |
| 6 | Loss of data/progress | 1 | 10 | 10 | Ignore | N/A. The reason the probability of this happening is so low is that the project is additionally stored on GitHub. All changes are pushed to GitHub, so if something happens to the device being used the code can be downloaded onto another machine. |

# Design Diagrams:

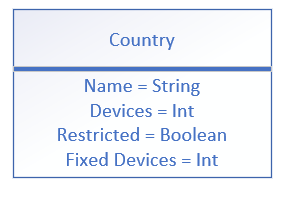
## Interface Design

All information that is stored in the application will be displayed on the interface. At all times the user will be able to see the overall healthy and infected devices, allowing them to make decisions of how to proceed given the information. The user can also pause the game at any point to allow for better strategizing.



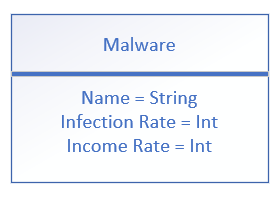
## Class Diagrams

### Country Class



At the start of the game the fixed device and the devices are the exact same values. During the game the devices will reduce as they become infected by the malware. The purpose of the fixed device is for the operating system restricts. As we need to know how many there were original for how many can be infected with the current restrictions of operating systems. The restricted variable is to determine which countries have restricted internet access and will be change to false once a certain condition has been met, at which time the country will start losing devices. The name will contain the countries name so that the name of the country can be seen in the data grid with the number of the devices.

### Malware Class



The malwares name is stored so that if a leader board is implemented, it will be a method for the user to identify which play through is what entry. The infection and income rate will increase as the user upgrades the virus. As the infection rate increases so will the number of devices infected per day and the income rate will increase the amount of money generated per day.

## Logic Design:

### Infection Devices and Unrestricting Countries:



### Upgrade Buttons (logic for both income and infection upgrades):



This code works by running through each of the possible outcomes of pressing the button until one is either met or it has reached the last possible outcome. As the only reason the button would not do anything is if the user has not got the money necessary for the upgrade. Once the code has decided which upgrade the user is buying the level is increased and the money for that upgrade is deducted. In case the user the user presses the button once they have fully upgrade a pop up will display to tell them they have already fully upgrade.

# Task Run Down

## Interface:

The user will be interacting with two forms when using this app. The first is the Malware Creation form, which will allow the user to come up with a name for their virus and the difficulty of the game. The second interface is the main game menu which will have multiple tabs, so the user does not have to keep opening different forms.

## Classes:

One of the feature of C# is that it allows for the coder to create there own class inorder to store data, this is mainly to make the code easier to read and to also reduce

### Countries:

All countries are made up of the name of the country and how many devices are within each country. The value of the device will reduce as the virus spreads. All this information is then saved to a list and displayed in a data grid.

### Malware:

Although there is only one malware that will be created, I still thought that creating its own class for the malware would allow for the code to be more readable and easier to understand. The malware is made of it name, which is displayed in on the interface. It will also be used later in the leader board in order to identify which virus is which. It also includes an income and infection level, which are the type integer. These will affect how many devices are infected per day and how much money the virus also produces during the day. These levels will increase as the user purchases updates.

## 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:

Theses scenario’s will only happen if either the research or the infection has reached one hundred percent. In both scenario’s the user will either be congratulated or condoned for there lose. If the user wins the states for the game will be save in the leader board so the user can look back on there most successful games.

## Income and Infection rate upgrades:

## Difficulty Levels:

The level that the user selects will change the conditions that cause research to commence and how quickly it is complete by default. There are three different difficulty levels which are Casual, Normal and Hard. The user can select the difficulty when they start the game and enter a name for the malware.

### Casual:

For this difficulty level research will start as soon as either days has reached 100 or the user has upgraded the malware infection level have reached 6 or income level to 5. Once research has started it will increase by 0.1% per day and this may change if the user upgrades the virus to make it harder to research.

### Normal:

For this difficulty level research will start as soon as either days has reached 75 or the user has upgraded the malware income or infection level have reached 4. Once research has started it will increase by 0.25% per day and this may change if the user upgrades the virus to make it harder to research.

### Hard:

For this difficulty level research will start as soon as either days has reached 50 or the user has upgraded the malware income or infection level have reached 3. Once research has started it will increase by 0.40% per day and this may change if the user upgrades the virus to make it harder to research.

## Infecting Restricted Countries:

As there are some countries in the world that have restricted internet access, in order to make the game more challenging theses countries cannot be infected until a certain condition has been met. Once that condition has been met each day there is a 1 in 4 chance that a country will be infected by the malware.

<https://eu.usatoday.com/story/news/world/2014/02/05/top-ten-internet-censors/5222385/>

## Leader board:

## Operating System Restrictions:

Not all malware is affective against every type of device, which is why the user will have to upgrade what devices they can infected. At the start of the game the user can only infect fifteen percent of all devices and by upgrading they will be able to infect all operating systems eventually.

# Supervisor Meeting Summaries:

## Week 1:

During this meeting all participants of the meeting introduced themselves and what they are creating for their 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 were 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:

During this meeting it was suggested that I implement operating systems into my program, so that the virus is limited by what device it can infect until it unlocks other operating systems. This was a good suggestion so I have now added it to my trello board and will be testing to see how exactly I will go ahead with this new feature.

## Week 4:

During this meeting it was brought up about games and the need for persistent data. It was decided that if it is not necessary for you game then it is not required to have a database in place to store any data.

## Week 5:

## Week 6:

## Week 7:

## Week 8:

## Week 9:

# Brochure and Poster Design

## Logo

The logo is a traditional danger of infection logo, but with the yellow background removed and replacing the curves of the sign with lines.

A picture containing clipart

Description automatically generated

# Testing

# Trello Boards:

The trello board is used to keep track of how the project is progressing, by seeing what tasks have been completed, in progress or have yet to be started. This means that as the end of the project grows nearer, we will be able to see how many tasks we have left and tell if we will be able to complete all of the them or if the project will run over.

## Trello Board 1:

A screenshot of a cell phone

Description automatically generated

## Trello Board 2:

A screenshot of a cell phone

Description automatically generated

## Trello Board 3:

A screenshot of a cell phone

Description automatically generated

## Trello Board 4:

A screenshot of a cell phone

Description automatically generated

## Trello Board 5:

## Trello Board 6:

## Trello Board 7:

## Trello Board 8:

## Trello Board 9:

# Testing:

## User Testing

By getting other users to test the game we will be able to find error and get their feedback on how to improve the application.

## Summary:

## Alterations:

# Evaluation:

## What went well:

## Feedback:

## Future Improvement:

# Conclusion:

# Reference List:

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

uses interview on the 7th feb as reference for using the easy option.