Initial Plan

CM3203 – One Semester Individual Project

Machine Learning Scanner to Detect Phishing Emails that Contain Malware

Author: Uthman Shaikh

Supervisor: Amir Javed

Moderator: Hiroyuki Kido

School of Computer Science and Informatics

Cardiff University

2021

Contents

Introduction

Today we are becoming more digitally connected every day, hence why 50% of the global population own more than one email account. [1] Phishing attacks have significantly increased over the last year some companies are experiencing an average of 1,185 attacks per month. From the statistical evidence found in 2020 that 22% of the data breaches that year were caused by phishing attacks. [2] Another statistic showed that 97% of people are unable to recognise sophisticated phishing emails therefore a tool that could detect these specific emails would be extremely beneficial for large organisations and the public.

There is a clear desire for a tool with these capabilities therefore the aim of this project is to develop a tool that can scan emails for phishing attacks based upon its content and scan for any malicious files within the attachments of emails. This tool will also incorporate machine learning to classify any emails that have a high probability of being harmful.

From this project I would like to find out the percentage probability for detecting these emails and its effectiveness this tool will have with detection. There are many machine learning API tools that can be used for this program, but which has the right capabilities for this specific model. With regards to its capabilities how will the devices performance be affective during its standby monitoring.

During this project all the implementation and testing will be held on a Windows Device. The most likely programming language that I will be using is python as there are many machine leaning tools that support this language, but I will be exploring other possible solutions. As this tool will be used for detecting harmful emails a large data set will need to be acquired to train the model with detection.

Aims and Objectives

This section will provide the aims and objectives for this project.

Research Objectives:

- Identify the different types of attacks from E-Mail.
- Establish an understanding of different ML API models.
- Understand different classification models.
- Establish an understanding of how malicious emails can be detected.
  - Within the content.
  - Within the attachments.

Primary Objectives:

- Gather larger testing datasets of emails.
- Develop a program that can scan the contents of incoming emails.
- Develop an MVP (minimum viable product) that can differentiate malicious emails with phishing links from non-malicious emails.
- Implement Machine Learning into the program so that the detection classification is more accurate.
- Train the model with Large datasets to improve its accuracy.

Secondary Objectives:

- After identifying a malicious email respond by blocking all incoming emails from that address.

- Improve accuracy further by training the model with multiple large datasets

Evaluation Objectives:

- Test the accuracy of the tool with multiple datasets to verify its efficiency.
- Carry out a performance analysis.
- Find part of the tool that can be developed or improved.

Ethics

With regards to ethical procedure, consideration will be taken if the handling of any personal data is required during the testing and developing for this tool. I do not believe that any personal data will be stored or used by this program but if circumstances occur with handling personal data then I will immediately file for an ethical approval.

From the best of my ability, I will aim ensure that all decisions are ethically assessed. The only area I am currently aware of that may be handling personal or CID data are the datasets that will be used for detecting phishing and malware links.

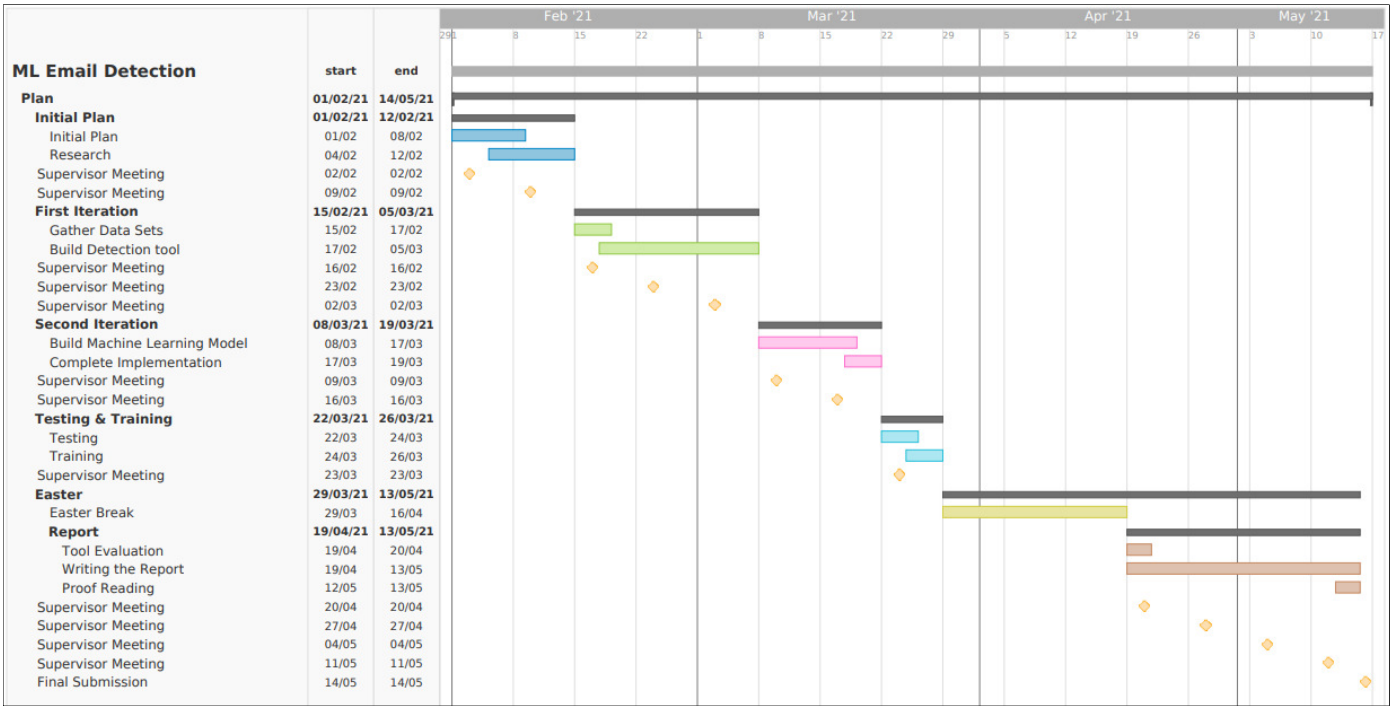
Work Plan

As part of my plan once a week myself and my supervisor will have a one-to-one meeting where we discuss my progress with this project. The meetings will be 15 to 30 mins long if needed.

Dates	Objectives	Milestones
Week 1 1st Feb to 7th Feb	• Complete Initial Report Plan • Research types of phishing attacks to defend against	• Start Initial Plan
Week 2 8th Feb to 14th Feb	• Research machine learning models to use and sources of datasets for application testing. • Research different types of phishing attacks and methods of detection.	• Submit Initial plan (8th Feb)
Week 3 15th Feb - 21st Feb	• Gather various datasets to use for testing. • Build the first iteration of the program, scanning emails, modelling the detection of malicious emails, and testing different types of attacks.	• Gather Datasets • Starting building Detection tool
Week 4 22nd Feb - 28th Feb		
Week 5 1st Mar - 7th Mar		• Finish the Detection tool
Week 6 8th Mar - 14th Mar	• The Second iteration will focus on the	• Start building the ML program

Week 7 15th Mar - 21st Mar	Machine Learning implementation, expanding on the scanning and detection.	
Week 8 22nd Mar - 28th Mar	• Test and debug the machine learning model • Train the machine learning model with datasets • Complete implementation • Record programs results and performance.	• Finish the ML program • Train the ML model with datasets
Easter Break 29th Mar - 18th Apr	• Nothing set for this period. • Complete any unfinished parts of the program	
Week 9 19th Apr - 25th Apr	• Evaluation of the tool's strengths and weaknesses • Writing the Report	Start on Report
Week 10 26th Apr - 2nd May	• Writing the report	
Week 11 3rd May - 9th May		Finish Report
Week 12 10th May - 14th May	• Proof read submission and report	Submit Final Report & Tool (14th May)

Gantt Chart



ML Email Detection	start	end
Plan	**01/02/21**	**14/05/21**
Initial Plan	**01/02/21**	**12/02/21**
Initial Plan	01/02	08/02
Research	04/02	12/02
Supervisor Meeting	02/02	02/02
Supervisor Meeting	09/02	09/02
First Iteration	**15/02/21**	**05/03/21**
Gather Data Sets	15/02	17/02
Build Detection tool	17/02	05/03
Supervisor Meeting	16/02	16/02
Supervisor Meeting	23/02	23/02
Supervisor Meeting	02/03	02/03
Second Iteration	**08/03/21**	**19/03/21**
Build Machine Learning Model	08/03	17/03
Complete Implementation	17/03	19/03
Supervisor Meeting	09/03	09/03
Supervisor Meeting	16/03	16/03
Testing & Training	**22/03/21**	**26/03/21**
Testing	22/03	24/03
Training	24/03	26/03
Supervisor Meeting	23/03	23/03
Easter	**29/03/21**	**13/05/21**
Easter Break	29/03	16/04
Report	**19/04/21**	**13/05/21**
Tool Evaluation	19/04	20/04
Writing the Report	19/04	13/05
Proof Reading	12/05	13/05
Supervisor Meeting	20/04	20/04
Supervisor Meeting	27/04	27/04
Supervisor Meeting	04/05	04/05
Supervisor Meeting	11/05	11/05
Final Submission	14/05	14/05

Risk Plan

Risk	Level (low, medium, high)	Likelihood (certainty, likely, somewhat Likely and Unlikely)	Avoidance Solution
Sickness	Medium (Increased risk due to COVID-19)	Likely	Spread the work out evenly throughout this semester. This strategy will avoid my work piling up if I fall ill.
Data Loss	High	Somewhat Likely	I will make sure to save every file in my Cloud One Drive account in case of any corruption on my storage device or data loss.
Falling behind in work	Medium	Likely	The easter break has been left blank so if I fall behind in any of my work this time slot can be used for catch up.

References

[1] Security Magazine, New research shows significant increase in phishing attacks since the pandemic began straining corporate IT security teams, [Online] Available at: https://www.securitymagazine.com/articles/93194-new-research-shows-significant-increase-in-phishing-attacks-since-the-pandemic-began-straining-corporate-it-security-teams [Accessed 3rd Feb. 2021]

[2] Security Boulevard, Staggering Phishing Statistics in 2020, by Dhwani Meharchandani, [Online] Available at: https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/ [Accessed 3rd Feb. 2021]