Project Plan

Malware Classification

Student X | Company | Date

FONTYS UNIVERSITY OF APPLIED SCIENCES

Data Student	
Family name, initials	Student X
Student number	1234567
Project period (from-until)	
Data Company	
Name company/institution	Company
Department	Blue team
Address	
Project Leader	
Family name, initials	
Position	Manager
Company tutor	
Family name, initials	
Position	Cyber Security Specialist
University tutor	
Family name, initials	
Project Plan	
Title	Malware Classification
Date	
Version	
Approved and signed by university tutor	
Date	
Name and signature university tutor	
Approved and signed by company tutor	
Date	
Name and signature company tutor	
Signed by student	
Date	
Name and signature student	Student X

Table of Contents

1. INTRODUCTION 4
2. PROJECT STATEMENT 5
   2.1. Project Background 5
   2.2. Project Justification 5
3. PROJECT CONTENT 6
   3.1. Project Goal 6
   3.2. Project Approach 6
   3.3. Research Questions 7
   3.4. Research Approach 7
   3.5. Project Deliverables and Non-Deliverables 8
   3.6. Project Constraints 8
   3.7. Project Risks 8
4. PROJECT PHASING 10
   4.1. Detailed Planning 11
5. MANAGEMENT PLAN 14
   5.1. Money 14
   5.2. Quality 14
   5.3. Time 14
   5.4. Organization 14
6. COMMUNICATION PLAN 15

1. INTRODUCTION

The Company is a cyber security company who for nearly 10 years has been helping companies under digital attack. In the last few years, it has become crucial to take protective measures in which people, process and technology are always aligned. The Company has a 360 degrees approach trademark, which means they try to incorporate all the protective measures so their clients can outsource all the security management and measures.

They have various departments to ensure the 360 view on security, such as: Business Security, Cyber Security (Blue Team, Red Team, Dev Ops , Computer Emergency Response Team, Security Operations Center).

When working with different incidents and malware infections, the CERT team noticed that in the past year some ransomware groups specifically do not target former Commonwealth of Independent States (CIS) countries. One example that was found by a CERT member is this one: when the ransomware detects a Russian keyboard, it stops from executing itself. Hackers usually do this because they operate from these countries themselves, thereby ensuring that the local constitutional state does not prosecute them. However, this does come with a very interesting factor: if you can detect it, you will know exactly where to find the next type of ransomware, and perhaps even stop it in its first steps.

This is a great starting point for the project, because if this research leads to finding more of these kind of attributes before the encryption happens maybe it will be possible to utilize them to stop the encryption.

2. PROJECT STATEMENT

2.1. Project Background

As mentioned in 2020 State of Malware Report: “From an increase in enterprise-focused threats to diversification of sophisticated hacking, evasion, and stealth techniques to aggressive adware aimed at Androids, the 2019 threat landscape was shaped by a cybercrime industry that was all grown up.” This means that the security has to mature as well in order to keep up with the threats. Also, business-disrupting ransomware attacks have nearly doubled. Analysis on ransomware is crucial as it may reveal features that can be used to stop it from spreading.

2.2. Project Justification

The Company has a Security Operations Centre (SOC) that aims to detect and where possible prevent cyber-attacks. From hands-on experience in the field, it was discovered that the execution of ransomware is conditional for some malware samples. To keep their customers safe, The Company and their SOC are interested in using this research to detect and prevent ransomware before encryption occurs. They make use of Endpoint Detection and Response (EDR), so the outcome of this research might be useful to integrate with.

3. PROJECT CONTENT

3.1. Project Goal

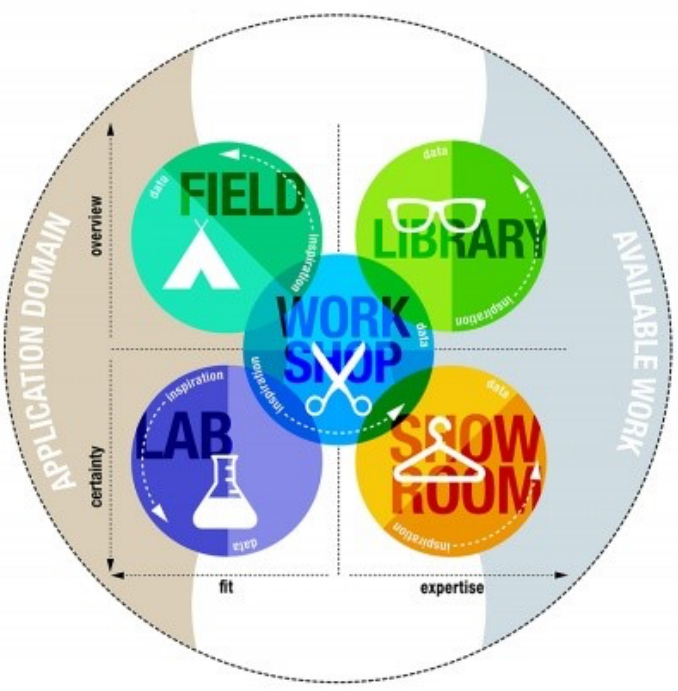
The desired outcome of this project is to have a classification method for the attributes of the malware using the available sources of the company and open-source products, within the specified time frame of the internship. This will enable the company to make use of these features found in malware in order to stop it or detect it in early stages of monitoring. The ideal situation would be if a ransomware could be stopped before the encryption part, however this is not part of the project, it is rather an idea that could work depending on the result of this research.

3.2. Project Approach

For this project, the agile approach to project management will be used because it allows to assess and examine the direction of the project during its life cycle. Agile planning is iterative, so there will be different iterations with set deliverables at the end of each iteration. More details can be seen below in Project Phasing section.

For the research part of the project the DOT research framework will be used. The researcher will make use of the different research strategies that it incorporates in order to get a better result.

Figure 1: DOT research framework



3.3. Research Questions

The research will be conducted around the main research question:

"How can we distinguish and classify ransomware characteristics that occur prior to encryption in the aid of stopping it from executing?"

Sub questions:

1. How to extract useful features?
2. (a) Are there related projects that can be (re)used for this research and (b) what are best practices recommended by professionals in this field to support this project?
3. How to do analysis on malware?
4. Which malware family is interesting to work with for future extraction?
5. What are relevant features that distinguish malware?

3.4. Research Approach

Sub Question	Strategy	Methods en Techniques	Expected Outcome
1. How to extract useful features?	Library	Literature research	Knowledge on the process of extracting features from malware
2.a. Are there related projects that can be (re)used for this research?	Library	Research related work	List of projects that can be related to this research
3. How to do analysis on malware?	Library Workshop	-Literature research -Hands-on experience on what was researched	Understanding on how malware analysis is done
2.b. What are best practices recommended by professionals in this field to support this project?	Field	Interview professionals from the company with experience in the field	Written results of the interviews
4. Which malware family is interesting to work with for feature extraction?	Lab Showroom	Test with different malware samples from different families	Find a type of malware that is best suitable for this research
5. What are relevant features that distinguish malware?	Workshop	Analyze begin files and compare the differences with malicious files	List of relevant elements that are distinguishable in malware

3.5. Project Deliverables and Non-Deliverables

Deliverables for Fontys

- Project Plan
- Project Report (Thesis)
- Assessment Form
- Personal Evaluation Form
- Final Presentation

Deliverables for Company

- Classification of ransomware/malware attributes that surface prior to encryption

Non-Deliverables

- Design document
- User requirement specification (URS)
- User manual
- Dutch version of the documentation
- Extracted features that are found after or during encryption

3.6. Project Constraints

Time will be one of the main constrains since the internship will be taking place from 1st of September until 29th of January. So, there will be five working months to finalize this project. Another constraint could be the cost, this project will be done with available free sources and tools that are already used within the company.
The resources could be another constraint because this project requires a large set of malware samples, possibly from the same category and it might be a challenge to find enough samples.

3.7. Project Risks

Risk	Likelihood x Impact	Chance	Mitigation Strategy	Responsible
1-Malware infection	High x Moderate	Moderate	Using a Sandbox environment	Project Leader
2-Poor data quality	Low x Moderate	Moderate	Make sure the dataset contains only useful data	Project Leader
3-Being late	Moderate x Low	Low	Stick to the project plan	Student X
4-Miscalculated deadline	Moderate x Low	Low	Rewrite the deadlines to fit the given tasks better	Student X

4. PROJECT PHASING

The project is divided into 5 phases, each phase resulting in different deliverables. Phases 2,3 and 4 will be repeated in each one of the 3 iterations. The iterations take place between Phase 1 and Phase 5. A general phasing overview can be found below.

A detailed overview of tasks and deliverables can be found at the end of this chapter.

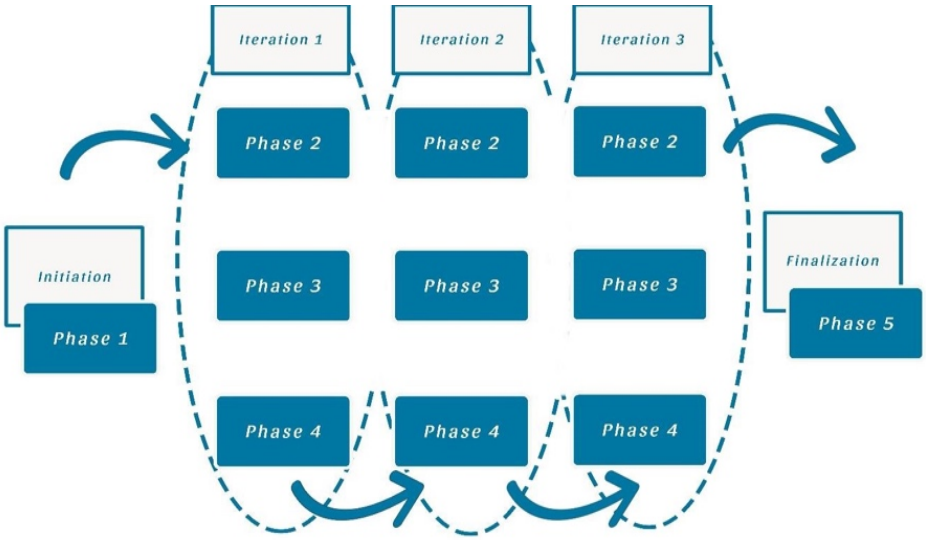


Fig.2: Phases and iterations in the development process

Phase 1: Initiation

- Iteration One, Two & Tree

Phase 2: Ransomware Sample Collection

Phase 3: Feature Extraction

Phase 4: Analyze findings

Phase 5: Finalization

4.1. Detailed Planning

The detailed planning can be found in this table:

Iteration	Phase	Tasks	Deliverables	Deadline
Initiation	1	• Company introduction • Finalize the Project Plan • Research (Literature) all the needed topics • Gain access to all the needed resources • Make sure the needed resources are available (ex: enough malware samples can be found)	• Project plan • Initial version research paper	22/09/2020
One	2	• Find a few malware samples • Interview people from the company with knowledge on the subject (Field) • First company visit of university mentor • Find a methodology for approaching feature extraction	• Collection of at least 5 malware samples • Extended research paper	2/10/2020
One	3	• Extract features from the samples • Design dataset structure • Add the features to a dataset	• Dataset with extracted features from the samples	16/10/2020
One	4	• Research findings • Analyze and classify the features	• Classified malware attributes • Extended research paper	30/10/2020

Two	2	• Find a few malware samples	• Collection of at least 5 malware samples	6/11/2020
Two	3	• Extract features from the samples • Add the features to a dataset	• Extended dataset with extracted features from the samples	20/11/2020
Two	4	• Research findings • Analyze and classify the features	• Classified malware attributes • Extended research paper	27/11/2020
Three	2	• Find a few malware samples • Add benign files and analyze them	• Collection of at least 5 malware samples	4/12/2020
Three	3	• Extract features from the samples • Add the features to a dataset • Compare the features of benign files vs. malicious files	• Extended dataset with extracted features from the samples	18/12/2020
Three	4	• Research findings • Analyze and classify the features	• Classified malware attributes • Extended research paper	29/12/2020
Finalization	5	• Answer the main research question and sub-questions • Finalize the project and documentation • Second company visit of university mentor • Thesis submission (11-15jan)	• Handover of the project • Thesis submitted	29/01/2021

Sub-question phasing can be found in this table:

Sub Question	Phase
1. How to extract useful features?	Initiation Phase1
2.a. Are there related projects that can be (re)used for this research?	Initiation Phase 1
3. How to do analysis on malware?	Initiation Phase 1 Iteration 2 Phase 2
2.b. What are best practices recommended by professionals in this field to support this project?	Iteration 1 Phase 2
4. Which malware family is interesting to work with for feature extraction?	Iteration 2 Phase 4
5. What are relevant features that distinguish malware?	Iteration 3 Phase 3

5. MANAGEMENT PLAN

5.1. Money

The finances incurred in the project are accumulated in five months, the duration of the internship. The costs derive mostly from the payment of the project members.

5.2. Quality

The quality will be checked by the Company mentor by giving feedback in different stages of the development.

5.3. Time

The project's lifespan is five months. The period is split into 5 phases: *Initiation, Design, Implementation & Testing, Finalization*. The project requires 40 hours of work each week.

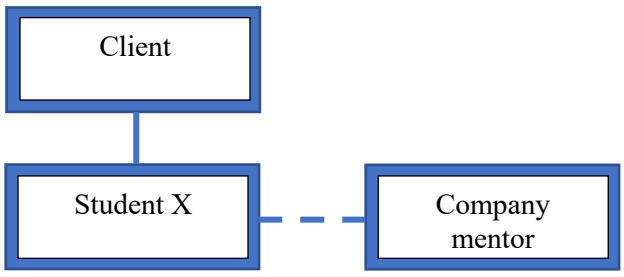
The official duration of the internship is 20 weeks.

Start date: 1st of September

End date: 29th of January

5.4. Organization

Since this is not a team project, and there are no other stakeholders involved than the Client and Company mentor, the organization is quite simple. I report only to the Client who is the project leader, and the Company mentor.



6. COMMUNICATION PLAN

The information will be communicated amongst the company tutor, the intern and the university tutor. Verbal communication will be used for critical decisions and tasks, whereas written reports and weekly updates will be sent via email.

The communication between the student and the university tutor will be done weekly via email. In case of emergency, a meeting will be organized between the participants.

	Project Plan	Process Report	Prototype	Documentation
Intern	Dr, S, Di	Dr, S, Di	Ex	Dr, S, Di
University mentor	R, Di, A	R, Di, A	Di	R, Di, A
Company mentor	R, Di, A	R, Di, A	Di	R, Di

Legend (Di = Discuss, A = Approve, S = Send, R = Receive, Dr = Draw up, Ex = Execute)

The final presentation will take place for both the Client and the Company mentor as well the University tutor.