Malware analysis and reverse engineering to provide knowledge transfer sessions to end users

Reflection

Bachelor in Electronics-ICT
Option: Cloud & Cybersecurity

Frederik Crauwels

Academic year 2022-2023

Campus: Kleinhoefstraat 4, BE-2440 Geel

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of my personal views and reflection on my internship assignment at Capgemini. As this was not only a "mandatory" requirement for completing my bachelor's degree, it is an opportunity to learn about the practical side. An opportunity to connect to like-minded people, learn a new subject and discover the consultancy world.

As someone who has prior experience in IT and cybersecurity, I discovered a new way of working within the IT domain. Throughout this journey I also discovered new things about myself which I can take with my for my future career.

Throughout my thirteen weeks I have gained new skills, new connections and new insights which will be reflected in this document. I have created an impact on both myself and the internship company as well.

In the first chapter you can read about a general reflection about the results of my internship. Did I complete my internship deliverables? What have I accomplished specifically? What did I do with all this new information? These are questions you will see answered In the first part.

In the second chapter you can read about a personal reflection of my internship assignment. What did I learn? How did this affect me personally? What problems did I encounter? And how did I overcome these problems?

1 SUBSTANTIVE REFLECTION

Looking back at the internship deliverables and what was to be expected of me, I can personally say I delivered more than what was originally expected of me.

Did I complete my internship deliverables?

Looking back at the primary internship deliverables, which I have been addressing in my realization documentation as well:

- The student will provide timeline at the beginning of the internship. (planning/WBS/retro planning) including the (intermediate) milestones.
- A document (playbook) explaining the steps taken during the research, as well as a demo package (incl. demo instructions and virtual harddisks)
- A demo will be provided on which a limited group of both Thomas More and Capgemini people are invited.

I can proudly say all of the above, and more, has been delivered.

- **Planning**: I have delivered not only one "planning" sheet, I have instead delivered three different templates: a specific deliverable sheet, a retro planning sheet and a day-to-day schedule. Each of these sheets complement one another. I even personalized the color scheme to the internship's internal corporate identity.
- **Document / playbook**: after completing the course material of my INE MAP course, I returned a 369-page document back to the internship company describing every single detail there is to know about malware (analysis). In addition this includes more than 20 labs / demo instructions. Aside from this documentation, I also documented my lab environment both in text and as a diagram. The advanced presentation even included the entire malware analysis of a ransomware called TeslaCrypt, which I provided to the audience after the session.
- **Demo**: originally we anticipated only one demo. We choose for two.
    - **Awareness session:** a generic and informative session which includes live malware demo's such as a keylogger and WannaCry (ransomware). This revolved mostly around understanding malware with some theory, defensive measurements you can take and how someone can get infected. The focus here was: keep it simple for users without prior knowledge of malware.
    - **Advanced malware analysis session:** an advanced deep dive into malware analysis. The focus for this presentation was providing live malware analysis on multiple samples as well as threat landscaping. The best defense is knowledge – and as such providing information about the recent threat landscape was key. Multiple malware samples were provided in multiple environments.

What have I accomplished specifically?

Aside from the above mentioned deliverables, I obtained a better understanding of malware (analysis) overall. At the end of the internship I analyzed advanced malware samples such as Whispergate (wiper used in cyberwarfare Russia vs Ukraine), WannaCry (ransomware causing 200.000+ infected computers), Play(crypt) (responsible for the cyberattack on the City of Antwerp) and crafted my own malware samples. This included a keylogger with a XAMP stack, sending all the logged keys to a "remote webserver". Custom Windows Defender disabling Python scripts, transformed into executables with the Pyinstaller library. A backdoor created with msfvenom / the Metasploit framework.

A malicious python / executable that can take the code required for a keylogger from OpenAI API services, similar to the BlackMamba PoC. All of the above was meant for a live demo during one of the sessions to display the real impact of malware to my audience.

In addition I obtained the opportunity to network and connect to others, and even provide a short session on AI safety (ChatGPT). Provide detailed documentation, share presentation formats, create professional invites and business emails, etc. I literally brought malware to my audience, and sincerely hope this was a great learning experience for them as well. The main goal was to transfer knowledge, and I believe I did just that.

What did I do with all this new information?

As mentioned already, this information was later shared with my internship company.

- **Presentation slides:** all of the slides provided have been shared internally. The advanced presentation included the complete analysis of a ransomware sample, explaining the malware analysis process in detail – in a picture format.
- **INE MAP documentation:** 369-page long documentation containing the entire contents of this learning course. Gladly shared this documentation with my cybersecurity colleagues!
- **Lab setup documentation:** some shorter documentation was provided on my malware lab setup. This hasn't been shared specifically, but could always be of use at a future stage. The visualization / diagram, for example, has been used during my presentations.
- **Additional learning resources:** there are more resources available aside from the provided learning resources. I shared more interesting sources to obtain knowledge on malware (analysis) as a whole.

I believe, solely from the perspective of expectations and deliverables, this internship was a major success. I delivered professional documentation and digital / live sessions to transfer all my knowledge to an audience and company.

2 PERSONAL REFLECTION

Not only on a professional level, but also on a personal level I discovered a lot and have learned a lot during this internship journey.

What has this internship meant to me personally?

With prior experience in a public company (company providing services to the public) and a private company, this internship provided me with yet another experience. At this stage I can gladly say I have experience in three different companies now.

The internship provided me with an opportunity to discover the world of consultancy. In my past experience(s) I felt like I was still missing a piece of the puzzle. As I was unsure of the consultancy world, since I'd rather compete against myself than others, I wanted to take the leap. Three major consultancy firms have taken up my request for an internship, of which one I choose in the end. Discovering the resources and way such a company works feels like I discovered what I may have been missing. An opportunity to learn and network with like-minded people, in addition to doing a cybersecurity job providing services to companies all over the world.

As my prior experience(s) were at non-IT companies – I now discovered you should absolutely start at an IT company in your career. What path you choose next is totally up to you – but the learning opportunities and networking is priceless. This internship delivered these exact expectations.

What did I learn?

I learned to become a malware analysis professional. At the time of typing I can proudly say I can analyze any type of malware, or at least try to. I'm not afraid to run malicious samples in a specialized environment. I learned to use REMnux (Reverse Engineering & Malware Analysis Linux) and discovered SIFT (used for digital forensics).

I increased my competences in delivered professional presentations, invitations and emails. I even learned about other IT-related topics which keeps the company occupied as well.

What problems did I encounter?

I didn't know anything about malware analysis as a whole. I didn't even know how to run them "safely" in a lab environment. These are obvious problems when you need to deliver a live demo to an audience.

Learning the Office 365 suite was also an interesting journey. Unaware how to create (non-)digital meetings in teams, extensively use teams vs OneDrive, Outlook in the browser / application, etc. So much to learn with regards to using this toolkit in a professional way.

Introverts don't always mix up well in an environment requiring networking. It is very much an environment that promotes me to be less introverted.

Learning the company policies and using them / adhering to them during my internship! This is very important to keep track of and do right.

Especially the French language remains a hurdle for me. If the other party doesn't speak English well enough, we're in for an interesting conversation.

How did I overcome these problems?

Learn by doing – and I love failing / trial-and-error approaches. If you didn't fail or encounter problems, that means you didn't try hard enough. With a bold, but moderate approach, I went for every opportunity I received and tried to make the best out of each problem creating a creative solution for each.

Simply doing the task and encountering the problems as they come is the way to go for me personally. A challenge, assignment or duty in which I don't encounter failure or mistakes isn't the right thing for me. This is one of the biggest and best ways a human being can transform forward. As such, I'd rather take the bold approach than play it safe. What is there to lose, if you can only grow?