Studio 2

Spring Semester Report

By

OSINT Crew

Jeanette Fremmergård, Travis Clark & Selin Iren Aydin

In

UC2ST2103

Noroff University College

April 2021

Keywords: Teamwork, Studio2-project, OSINT

Attachments: Planning of Studio 2, Framework, Walmart report, mind map, Framework explanation, report template, example report.

Table of Contents

1 Project Summary

1.1 Scope:

Our Scope was to focus on the retail industry only and configure the threat intelligence products to give us an insight into threat intelligence for this industry. All other industries and threat intelligence not related to this area will be outside the scope.

1.2 Aim:

The team aimed to investigate how open-source threat intelligence could help businesses and organizations gain insight into real-time events and developing threats. We wanted to examine if open-source threat intelligence could help identify threat actors, their motives and plans. The project then hoped to answer the question: Can open-source threat intelligence compete with paid threat intelligence services?

1.3 Objectives:

Our objectives were to explore the tools, platforms, frameworks and techniques used to gather threat intelligence from different, open sources such as social media, forums, news feeds, etc.

1.4 Results and achievements

The team created a Framework with a step-by-step explanation, report template, and example report demonstrating the use of the framework. The Framework was created to visualize the steps necessary to start an OSINT investigation to produce Threat Intelligence. We wanted to make a template report so it could be easier for a business to start their OSINT investigation, and add an example report so it is easier to understand the steps taken towards a final report.

The original question for this project was "Can Open-Source Threat Intelligence compete with paid threat intelligence services?". We conclude that it is possible to find actionable Threat Intelligence. The road there is a long and rough one. It takes time to find the tools that work best and the right sources. The employers need to find time to train the right employees for the task. Being systematic and keeping order is key. Creating files and an orderly way to store the data as it moves through the analysis and cleaning process will help not only during the investigation, but after as well. In case questions come up about a source, or a reference for a future search is needed it will be easy to find if things are kept in order from the start.

1.5 The reason for why we choose this project

This project was inspired by the events that unfolded during the Black Lives Matter protests in USA. Many of the protests had "unforeseen" consequences regarding theft, vandalism, and arson. We were curious how much information was available before and during the events that would help a business forecast their threat level and hedge their potential economic loss. Many businesses cannot afford expensive intelligence services but were still affected by the events. We wanted to discover the alternatives that small and medium sized businesses have when facing threats.

1.6 Knowledge and skills acquired

OSINT is a new arena for our group. There are many open-source intelligence tools available. We tried as many as possible in order to better understand the tools that could be of interest. Not all the tools are easy to use and many take times to set up and monitor. Finding the right tools is important in the start. Twitter for example was relatively easy to use for searching keywords, while Facebook was more challenging especially finding an event that happened in the past. We all gained familiarity with some of the more popular tools like Facebook, Twitter, and SnapMap and the processes of how to use them. We have also learned the process of turning information gathered from these sources into intelligence.

Understanding OSINT investigations and familiarity with the relevant tools are important for both Cyber Security and Digital Forensics. Both study programs are reliant on finding information outside normal sources.

2 Project Challenges

2.1 Main Project Challenges

Learning about OSINT was a challenge. Espen was one of our main motivations for going forward with Threat Intelligence, as he has many years' experience with OSINT investigations. When Espen left school to take a job after Christmas, we were challenged with regrouping and continuing the project. We as a group took over the ownership of the project from Espen. Competencies and expertise had to be reshuffled, which resulted in us finding a new positive tone in our group. The group become more equal and cooperative. It turns out losing a group member was not necessarily a negative experience.

2.2 Unexpected Challenges

Losing a group member was not expected. We quickly regrouped and were forced to learn more about OSINT since we needed to find out ourselves instead of relying on Espen for guidance. Threat intelligence is a newer field so there is little guidance available. Especially threat intelligence for physical threats. It was unexpected that there was so little information available online or in research papers. We had to adapt existing knowledge of OSINT and cyber threat intelligence to our project.

2.3 Key lessons

We would have given everyone the same opportunity. Choosing a project that everyone can participate with from the start and not rely on 1 member to lead. In the end we all learned more when we needed to stand on our own two feet versus relying on 1 member to lead. There is almost a never-ending supply of tools being developed. The learning curve for some of them is quite steep, so becoming familiar with some of the tools has been a positive experience.

3 Collaboration & Professionalism

3.1 Planning, organizing and collaboration

There has not been contact with other studio groups or businesses, we were the only group working with OSINT and Threat Intelligence that we were aware of. Maryia and Ruan were our only contact outside of our group for guidance. We have had meetings with Ruan on how to organize this project and what their expectations are from us. This has helped our group tremendously to plan our project as best as we can.

3.2 Planning our work

We planned our work by setting up our internal goals and deadlines in a table. This table made it easy for every team member to follow the process and to visualize where we were in the process. By having our steps in a table visible for every team member made it easier to ensure that we stayed on track with our project. It was also possible for us to change the table if we met some unforeseen challenges or problems. One of these challenges was losing a team member as we had assigned who would do which tasks in the spring semester. This challenge forced us to re-think and work differently for the time ahead. From the start of our planning, we wanted to make this project equal – both workload and ownership wise. This did cause some issues that the team members did not bring up but was figured out after one member left the group. The group member that left sat with more knowledge about Threat Intelligence and that may have hindered the rest of the team members from doing research and to getting to know the project in an organic way. The internal communication changed drastically for the better.

A factor for our success has been communication and continuous work. The members have been active and dedicated to the studio weeks and participated equally. We have had internal deadlines so we could always stay ahead of the deadlines set by Noroff.

We have divided tasks between us and make sure that the workload has been fair. Communication between meetings has been via Skype, which allowed us to contact each other regarding the project.

3.3 Organizing our work within the team and collaboration with external parties

We organized our work according to our skill set. Though we did not discuss in the early stages what each person was good at or like to do, we quickly discovered each other's talents. Since the culture and dynamics were set early, we were able to regroup and change the culture in a very positive way after the loss of a group member. The group was then free to express their individual talents and was more democratic regarding direction and decision making.

3.4 Challenges faced working as a team

The project started out with most of us feeling it was one group members project and the other members were there to help. Having studio 100% online without the possibility to meet in person was a challenge and contributed to the dynamic. We were reliant on scheduling meeting times and that team members participated fully. As online students we are all used to interacting via Skype and Teams. However, it takes longer to establish the group dynamics and culture. Had we been able to meet in person even once or twice it could have expedited the process. In addition, we lost 25% of our team after the new year, which caused us to regroup and commit even more to the success of our group project. After losing a member of the group the remaining members refined the scope and took back ownership of the project. This was one of our biggest successes outside of the project itself.

3.5 Key lessons

Be open and have a clear communication so that each member of the group can contribute, and the group grows as a whole. Everyone is an expert in something and having a group culture that allows this expertise to flow is important to the groups culture. Once we had that in place project management was not an issue as all were willing to contribute with their best efforts. The most difficult challenge was probably managing everyone's enthusiasm. Having a group dynamic where the group feels equal and can contribute freely makes the work not only higher quality, but fun.

3.6 Future Team Projects

If we were to undertake a new project in the future with the knowledge we have now, we would choose a project that is not specific to one member of the group. A subject that all members can participate with and take ownership of from the start would be ideal. Time would not be lost figuring out group dynamics and a culture could be established much quicker. We would also be more efficient since we are now familiar with our individual strengths and weaknesses.

REFLECTIONS

4 Potential Legal, Ethical & Social Issues

4.1 Legal, ethical & social issues

OSINT can quite quickly go into grey areas. Both ethical and legal. It is important to create a scope that is both ethical and legal. Searching for information on social media platforms creates potential privacy issues if the search is to remain anonymous. Therefore, clear understanding of the tools and their scope of use is important. We did not run into any legal issues, as our goals were clear about finding information that was publicly available without the use of grey area tools such as sock puppet accounts and active information retrieval. We instead used tools to search existing information on the different public platforms. This kept our investigations within scope both ethically and legally.

4.2 Stakeholders of the project

The main stakeholders of our work would be small to medium sized retail businesses. They could be potentially interested in Threat Intelligence at a lower or no cost if it meant protecting their business from harm. Using free OSINT tools to gather information and then process that information into intelligence that can be acted on for little or no cost other than time used is an empowering knowledge. A business could be overwhelmed by the amount of information that can be gathered. Having the tools and knowledge to distill the information down without craving to many new resources is helpful. Regardless of the amount of time invested and results we feel a little intelligence gathered is better than none. Therefore, it is worthwhile for the businesses to train themselves on how to use the framework and the tools.

4.3 Encountered issues

A stakeholder, as does anyone using OSINT tools to gather information, needs to start the process with an ethical scope. Ethical and legal boundaries could easily be crossed for the sake of “saving” the business. However, those boundaries are important to stay on the correct side of. Any information gathered or intelligence acted upon could have ramifications for the business or the individuals implicated. We did not encounter any of these issues, however we all experienced situations where it would have been easy to cross such a line using sock puppet accounts or actively contacting individuals trying to extract information from them.

4.4 Other issues

Our project could have encountered greater issues with a person leaving if the topic of our project had been even more dependent on that person's competencies. We should have considered this more when picking our subject. It was a risk. And in hindsight we should have listened to our gut feelings more than we did. That alone was a valuable lesson.

RESEARCH

4.5 Future issues

If our project were to continue, we could see the maintenance of real time searching and updates would need to be addressed. Some free tools are set it and forget it, others take time. There are several OSINT platforms that take time to set up and calibrate. The issue of a platforms value would need to question compared to the intelligence it can help produce. Gathering the information is one challenge. Processing it is another. Processing the information into useable intelligence faster will hopefully also be addressed in the future by newer technology or software.

5 Project Review & Evaluation

5.1 Achieving the aim and objectives

Our team achieved the goals by putting together a framework that could give threat intelligence to businesses in the retail industry as well as a report template. Originally, we intended to compare the kind of information that is possible to find vs what a client of an expensive paid service could expect to receive. This became out of scope, so the objectives were more manageable.

5.2 Changes to the project

Our scope did change throughout the project. The scope of OSINT and Threat Intelligence can be quite large. Producing a framework and making a comparison with a large paid service became out of scope for our project. With guidance from Ruan we were able to narrow our scope, so the objectives and deliverables were manageable in the timeframe of Studio 2. We refined our scope to production of a framework, step-by-step guide, and report template.

5.3 Success of the project

Our project set out to prove if Open-Source Threat Intelligence could compete in giving actionable threat intelligence compared to paid services. We feel we were successful in finding actionable Threat Intelligence for Walmart store #2648. In addition, we have not found a step-by-step guide for retail businesses to use OSINT tools to gather information and produce Threat Intelligence online. We have created a framework and example report that can be used as a guide for companies that are interested in starting a threat intelligence gathering program. XXX

5.4 Achievements of the project

Our main achievements have been the creation of a simple framework and step by step guide for using OSINT to gather information and demonstrating that actionable Threat Intelligence from publicly available sources for small to medium sized retail businesses.

5.5 Skills developed and lesson learned

We have learned the importance of focusing our curiosity. We have learned how to connect dots and fill in the blanks. Often one source will produce a question that is answered by another source. The dots keep connecting until the web gets bigger and bigger. Take a step back and try to understand the whole story by looking at the bigger picture.

5.6 Future project development

If we were allowed to continue another 3 months on this project we could have gone even more in depth with more advanced tools. There are several OSINT platforms that are open source and take time to set up and calibrate. We did not investigate using them as time did not allow. If we had more time, we could have explored some of these tools. It is not guaranteed the results would have been of a higher quality; however, a comparison could have been made. A more in-depth analysis of ROI regarding time used and output generated at different levels of investment could have been interesting to see.

6 Resources

https://awesomeopensource.com/projects/threat-intelligence

https://blog.eccouncil.org/what-is-threat-intelligence-8-steps-to-create-a-ti-program/

https://www.researchgate.net/publication/312415710_Legal_Considerations_for_Using_Open_Source_Intelligence_in_the_Context_of_Cybercrime_and_Cyberterrorism

https://www.uk-osint.net/legalcases.html

https://www.tandfonline.com/doi/abs/10.1080/08850607.2014.900295

Legal aspects of open-source intelligence – Results of the VIRTUOSO project. October 1st 2013. Computer Law & Security Review, ELSEVIER