CoSEM Master Thesis

Leveraging Indirect Indicators: Correlating Ransomware Attacks to Threat Actors

Ricky Kho

Delft University of Technology

TU Delft

CoSEM Master Thesis

Leveraging Indirect Indicators: Correlating Ransomware Attacks to Threat Actors

by

Ricky Kho

Submitted to Delft University of Technology in partial fulfilment of the requirements
to obtain the degree Master of Science
in Complex System Engineering and Management
at the Delft University of Technology,
Faculty of Technology Policy and Management,
to be defended publicly on Wednesday April 3, 2024 at 14:00.

Student number:	5627524	
Project duration:	September 11, 2023 – April 3, 2024	
Thesis committee:	Dr. Y. Zhauniarovich,	TU Delft, First supervisor
	Dr. A. Ding,	TU Delft, Second supervisor
	M. Mollema	Cybersecurity company, Supervisor
	R. Wajon,	Cybersecurity company, Supervisor

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Preface

Dear reader,

I am excited to share with you my thesis on Leveraging Indirect Indicators: Correlating Ransomware Attacks with Threat Actors. I am currently completing my MSc in Complex Systems Engineering and Management at Delft University of Technology.

The thesis has been an adventurous journey. I delved deeply into the world of academic research and learned extensively about conducting good research and the topic of attribution of cyber threat actors, especially ransomware threat actors. Initially, the goal was to develop a machine learning model to identify ransomware attackers based on indirect indicators. However, during the research it became clear that the use of indirect indicators for attributing ransomware threat actors required extensive research. Therefore, the scope was limited to whether indirect indicators could help correlate ransomware attacks to threat actors.

I would like to express my gratitude to the people who contributed to my research. First of all, I would like to thanks Yury, whose weekly meetings helped me streamline the thesis. He also gave me many tips to improve the master's thesis. Next, I would like to thank Aaron for providing critical feedback during the important milestone meetings. This helped me think critically about the changes I made during my journey. I would also like to thank Romy for her guidance and help in getting in touch with the interview participants. Additionally, I want to thank Michel for his guidance during my internship and also for his help in getting in touch with the interview participants. In addition, Michel provided me with a lot of information that contributed to improving the thesis. Furthermore, I would like to thank the interview participants for their helpfulness and for providing the necessary information regarding the attribution of the cyber-threat actors. Finally, I would like to thank my parents and Joris for reading my thesis and providing valuable feedback.

Now that I have reached the end of my student time, I think back with a big smile on the incredible time I had, the beautiful moments I created and the invaluable knowledge I gained. I look forward to what comes my way.

Ricky Kho
Delft, March 2024

Executive summary

The increasing dependence on technology has made society vulnerable to cyber threats, with ransomware becoming a major concern. The complex nature of the Ransomware-as-a-Service (RaaS) model makes identifying the attackers challenging. Traditional methods often rely on direct indicators, but these may not be readily available or reliable. This research explores the potential of utilizing indirect indicators to improve correlating ransomware attacks to specific threat actors. This results in the formulation of the following research question:

If and to what extent can the analysis of indirect indicator be utilized to improve correlating ransomware attacks with cyber-threat actors?

The research employs a mixed research approach. A literature review examines the techniques, indicators, and taxonomies used for attributing cyber-threat actors in general. Additionally, expert interviews explore differences in the attribution of ransomware threat actors compared to general cyber-threat actors. Furthermore, it highlights the need to use indirect indicators in the attribution process of ransomware threat actors. Therefore, a cybersecurity company's 2023 ransomware incident reports are analysed to understand how the ransomware attacks are investigated and how the conclusions are drawn.

This study identifies differences in attributing ransomware and general cyber-threat actors. While indirect indicators are crucial for attributing general cyber-threat actors, ransomware attackers often directly identify themselves through ransomware notes. These notes often provide access to communication channels and leak sites, offering substantial evidence for attribution. The study also finds that Tactics, Techniques, and Procedures (TTPs) tend to be generic in ransomware attacks, offering limited value for differentiating between different actors. However, based on the interviews, there is a need for a central database of observed indirect indicators to facilitate future research and attribution efforts. Consequently, the research finds some promising results for using indirect indicators in ransomware threat actor attribution. The first finding is that the TTPs are less generic as initially thought as 32% of the techniques and 47% of the sub-techniques were unique. In addition, analysing the specific tools and techniques used by different actors, such as Blackcat's use of ”nltest” for domain trust discovery, can help identify and differentiate them. Furthermore, threat actors observed only once in ransomware attacks of 2023 often used unique techniques, potentially allowing for differentiation based on this factor.

In conclusion, this study demonstrates that analysing indirect indicators can be a valuable tool in correlating ransomware attacks to specific threat actors. While certain limitations exist, continued research and development of this approach have the potential to significantly improve our ability to identify and track ransomware attackers.

Nomenclature

Abbreviations

Abbreviation	Definition
APT	Advanced Persistent Threat
C2	Command and Control server
CTA	Cyber-Threat Tctor
CTI	Cyber Threat Tntelligence
CoSEM	Complex System Engineering and Management
IoC	Indicator of Compromise
RTA	Ransomware Threat Actor
TTP	Tactics, Techniques and Procedures

Contents

List of Figures

List of Tables

1

Introduction

With the rapid advancement of technology over the past two decades, society has become increasingly dependent on digital means for various day-to-day tasks, including the storage of sensitive and valuable information. Consequently, the prevalence of malware, especially ransomware, has increased dramatically [28]. Studies conducted in 2017 estimate that there are more than 140 million variants of ransomware [6]. Generally, ransomware variants can be divided into two main groups: locker ransomware and crypto ransomware [6, 58]. Locker ransomware instances aim to deny users access to their machines by locking them, while crypto ransomware instances aim to encrypt user files, rendering them inaccessible. Consequently, the victims of these malicious programs face a dire threat, as the only viable way to regain access to their machines or files is often payment [58]. Moreover, these ransoms are usually paid with currencies such as Bitcoin [6, 58], making this scheme responsible for millions of dollars in damages each year [56].

This scenario presents a concerning picture. The cybersecurity threat posed by ransomware has emerged as one of the top ten threats. This is primarily due to the significant increase in attacks on companies and government institutions, as remote work necessitated employees to connect to corporate networks from home [2, 30]. Healthcare organizations have been particularly targeted during the pandemic. As the healthcare sector expands and adopts digitally-enabled healthcare services, it becomes more vulnerable to cyber-attacks, as these rapid shifts expose weaknesses and security vulnerabilities that can be exploited by digital criminals [51, 63]. Consequently, the rise in such attacks has prompted users, organizations, and governments to prioritize the protection and backup of critical data. However, due to the highly profitable nature of ransomware, attackers continuously evolve their tactics to bypass current protection mechanisms and enhance their encryption processes [31].

The increased ransomware attacks can also be observed through the growth of cybersecurity companies. In 2016, incidents occurred approximately once a month, whereas today, there are over 15-45 ransomware incidents per day. This number could be even higher as many ransomware incident remain unseen or unreported. When a company falls victim to a ransomware attack, some cybersecurity companies take on the responsibility of negotiating with and payments to the threat actors to restore the operations of the victimized company. However, governments impose sanctions on specific criminals or criminal organizations, which restrict payments to these entities [12].

Since payment to the sanctioned actors is prohibited, it is important to identify the cyber-threat actor you are dealing with. Cybersecurity companies that provide negotiations and payments to ransomware attacker use a sanction screening process in order to make sure if payment is allowed. An Incident Response Coordinator of a cybersecurity company provided insights into the challenges of the sanction screening process. Before making payments, the company must perform a sanction list check to identify if a cyber-threat actor is under sanctions. This check involves examining direct indicators like names and addresses associated with bitcoin wallets. If a match is found, payments to those entities are prohibited. However, threat actors commonly use aliases and create new cryptocurrency wallets. Consequently, relying solely on direct indicators often results in no matches, which allows the

cyber-security company to pay the cyber-threat actor.

Unfortunately, the complexity in the supply value of Ransomware-as-a-Service (RaaS) model makes it difficult to identify the ransomware threat actor, especially when assessing if you are dealing with a sanctioned threat actor. RaaS allows for the creation of customized ransomware based on existing code, enabling both skilled cyber criminals and non-technical individuals to participate in this unethical industry [41]. Contacting ransomware service providers using darknet markets, the criminals can cheaply obtain tailor-made ransomware ready to be used on their prospective victims [41]. The collaborative strategy gave rise to a value chain in which there are various roles involved [41]. Some identified roles are virus writers, website masters/crackers, envelope (account) stealers, virtual asset stealers and sellers, and players (buyers) [70]. Additional roles identified are malware distributors, mixers, and tumblers in the money laundering service [11, 49]. This ransomware supply chain allows achieving a faster rate of infections with a lower risk of getting caught [41]. As a result, ransomware has reached a dangerous degree, establishing a cooperative mechanism between computer-savvy criminals and non-skilled participants. This cooperative environment suggests that the prevalence of this type of malware will continue to rise in the future.

To identify cyber-threat actors reliably and efficiently, researchers are conducting research to indirect indicators. Examples of such indicators include techniques, tactics and procedures (TTP), software, and malware [48]. However, identifying ransomware-threat actors utilizing indirect indicators is noticeably absent in the literature. Therefore, the objective of this research is to map the ransomware threat actor attribution process. In addition, the research aims to extract and analyse indirect indicators. The goal is to determine the extent to which these indirect indicators can be utilized to identify cyber-threat actors. The analysis will be achieved by addressing both the quantitative and qualitative aspects of the problem.

This research is of great importance within the Master's program Complex System Engineering and Management (CoSEM), given the complexity for identifying the cyber threat actor. Ransomware-threat actor identification can be described as a complex system that includes various social and technical aspects [52]. The social aspects are the difficulties cybersecurity teams face in attributing ransomware threat actors. And the technical aspects are the technological aspect of a ransomware attack. This makes this problem a socio-technical problem, suitable for the master's program CoSEM.

2

Knowledge gap

The aim of this chapter is to identify a knowledge gap in academic papers concerning the identification of threat actors. This process of identifying a gap in knowledge is essential to guarantee that the research presented in this thesis makes a valuable scientific contribution. The identification process is accomplished through a PRISMA literature review, which is used for the formulation of the main research question.

2.1. Literature review process

Three databases were used in the identification step: Scopus, Worldcat and Google Scholar. Using these databases, two queries were identified, which are included in Table 2.1. The searches used resulted in a total of 17 articles that were assessed for eligibility, of which 6 were deemed not relevant to the main research question. Another article was not considered because it was a review. Therefore, 8 articles were included in this meta-analysis through database searches. Figure 2.1 provides an overview of the PRISMA framework and the number of records included in it.

Query	Database	Hits
Cyber-threat attribution	Scopus & Google Scholar	7
APT attribution	Scopus	10

Table 2.1: Used search queries in the PRISMA literature review

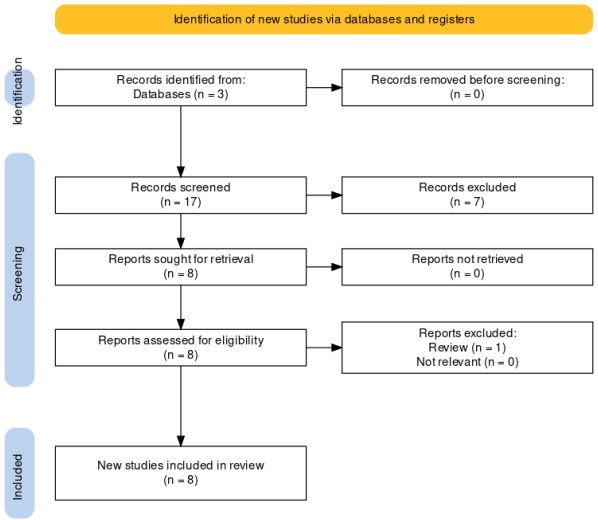

Figure 2.1: PRISMA steps results and schematic overview

2.1.1. Snowballing method
In addition to the 8 articles used for the meta-analysis, the snowballing method was applied, resulting in 1 more article. This resulted in a total of 9 articles in the literature search.

2.2. Results
An overview of the literature review findings are provided in the following paragraph and a summary is provided in Table 2.2. This table provides the relevant key findings for this thesis. Based on this information the knowledge gap can be identified.

2.2.1. Cyber-threat attribution based on high level Indicators of Compromise (IoC)
For the identification of threat actors, there are two different keywords in the literature that describe the identification of an adversary. The first is the Advanced Persistent Threat (APT) attribution, which is defined as the attacker's identification (name, organization name, or alias), location, or attack process [40]. [48]'s research explains that cyber threat attribution facilitates the identification of an attacker or his/her intermediary. To maintain consistency throughout this thesis, cyber-threat actor attribution will be used for the identification process of a ransomware attacker.

The article by [48] highlights the benefits of using high-level Indicators of Compromises (IoCs) when attributing cyber threats to their perpetrators. They profiled cyber-threat actors based on their attack patterns from Cyber Threat Intelligence (CTI) reports, using the distributive semantic technique of Natural Language Processing. Using the developed profiles, they trained and tested five machine learning classifiers on 327 CTI reports.

[23] developed a machine learning based tool that helps identifying the adversary having executed the attack described by cyber threat reports (CTR). The tool takes a CTR as input and extracts, among others, the techniques and tools described by the report to have been used during the attack. The tool then calculates the similarity to a set of previously learned adversary group profiles and outputs the calculated similarities in a sorted ranking.

[27] conducted research to improve a mechanism to attribute or profile cyber-threat actors. The authors tried to achieve this goal by extracting multiple features from CTI reports. In addition, a methodology to extract features from unstructured CTI reports was proposed by using natural language processing (NLP) techniques and then attributing cyber-threat actors by using machine learning algorithms.

2.2.2. Cyber-threat attribution based on TTPs
[60] proposed an Automated Reclassification for Threat Actors (ART), a Python-based analysis tool for automatically comparing Tactics, Techniques, Procedures (TTPs), extracted from MITRE's ATT&CK Framework, from different APT groups, to compare the similarity between different APT groups. Public reports that contained information about the APT groups were crawled from cyber reports in text format, and vector similarity was calculated to compare the APT groups.

In the research of [19], a cyber-threat attribution process is proposed by identifying, assessing, and visualize the relationship between APTs and their associated TTPs derived from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&ck) framework. The authors used association rule mining to identify statistical TTP relationships, and a weighted Jaccard similarity index for threat attribution. They created an extended threat playbook comprised of weighted associations between techniques used by APT groups to accomplish a tactical goal which can then be used to identify unknown APTs based on the TTPs they employ during a cyber attack.

2.2.3. Cyber-threat attribution based on Malware
In the research of [65], an APT attribution based on combining code features and string features is proposed. They used Natural Language Processing techniques such as paragraph vectors and bag-of-words vectors to represent function semantics and behavior reports. The model classification used for this type of APT attribution was achieved by implementing the machine learning technique Random Forest Classifier (RFC) and Local Interpretable Model-agnostic Explanations (LIME) was used to interpret the model results. In order to evaluate the method proposed, they used a data set collected from threat intelligence reports. One limitation in this research is that only APT samples are used without

adding non-APT samples to test the method's ability to identify APT samples and non-APT samples.

Another research that utilizes malware for APT attribution is the research of [66]. In this paper the authors attributes APT groups for malicious codes from the perspective of binary similarity. At first they extract raw features of the functions for classification. They employ the Shapelet model to select path shapelets, which are fragments representing paths and aiding in path-level interpretability for classification. Additionally, API calls are used to filter functions and generate specific paths to reduce resource consumption. To evaluate the method they collected APT malicious code based on publicly available threat intelligence reports.

[55] proposed a multi-view approach. The authors achieved this goal by creating eleven different views based on the extracted Opcode, Bytecode, and Header features to look at the files under observation from different aspects. Which they claimed made the system resilient against obfuscation and evasion techniques. Subsequently, they used five different machine learning algorithms to evaluate the created eleven views.

2.2.4. Cyber-threat attribution based on ontology

[52] discusses the lack of granularity with the current proposed APT attribution process. A framework is called a granular, when it comprises a large number of small, discrete components that can be combined and customized to perform more complex tasks [52]. The authors then propose a framework that asks primitive questions (What, How, Where, Who, When, Why) at various levels to structure and organize data about APT attribution in a way that is process-driven, comprehensive, consistent and explainable. At each level, the proposed framework produces a set of deliverables. As the framework progresses from enterprise level (victim) to the executive level (nation/state), the degree of confidence in accepting and rejecting hypotheses increases, assisting in the finalization of the APT attribution process.

Table 2.2: Overview of articles of the State of the Art

Ref	Attribution method	Indicators	Deficiencies
[48]	NLP[1], NB[2], KNN[3], DT[4], NN[5]	High level IoCs	Limited reports CTI reports used
[23] (snowballing)	Logistic regression classifiers	High level IoCs	No clear explanation of how the classifier works
[27]	DT[4], RF[6], SVM[7]	High level IoCs	Only used known APT data
[60]	Matrices Similarity Analysis	TTP	Small APT data set
[19]	Matrices Similarity Analysis	TTP	Need real world scenario testing
[65]	LIME[8]	String feature[9], Code feature[10]	Only classifies APT samples, without adding non-APT samples
[66]	Shapelet model	Dynamic and Static Features	Unreliable parameter selection
[55]	KNN[3], DT[4], SVM[7], Fair Clustering	Opcode, Binary, Count, Frequency, TFIDF[11], Eigenvector	Only tested in a controlled environment
[52]	Zachman ontology framework	Primitive questions	The framework has not been tested in a real world scenario

[1]Natural Language Processing, [2]Naive Bayes, [3]K-nearest neighbour algorithm, [4]Decision Tree, [5]Neural Networks, [6]Random Forest, [7]Support Vectore Machine,[8]Local Interpretable Modelagnostic Explanations , [9]Behavior features of malware, [10]Units of function that represent static features of malware, [11]Term Frequency-Inverse Document Frequency

As can be seen from Table 2.2, there is a limited number of papers conducting research to the identification of threat actors utilizing indirect indicators. In addition, the papers are primarily focused on identifying a threat actor within a broader scope of a cyber-threat in general. However, a specific investigation into the identification of threat actors in the context of ransomware attacks, leveraging the potential of indirect indicators, remains noticeably absent in the current literature. Therefore, the following research question is formulated:

If and to what extent can the analysis of indirect indicators be utilized to improve correlating ransomware attacks with cyber-threat actors?

3

Research design

This chapter presents a structured approach to the main research question by dividing it into sub-research questions. It contains details of the data requirements, data collection methods, analysis tools, and a flow diagram to demonstrate the relationship between the sub-research question and the main research question.

3.1. Main research question and sub-questions

Based on Section 2 the main research question is formulated as the following:

If and to what extent can the analysis of indirect indicator be utilized to improve correlating ransomware attacks with cyber-threat actors?

Sub-research questions are composed to structure this research, provide handholds, and answer the main research question:

1. SQ1: What techniques and indicators are currently used for cyber-threat actor attribution and what are their limitations?
2. SQ2: What techniques and indicators are currently used for ransomware threat actor attribution and what is the difference with cyber-threat actor attribution?
3. SQ3: To what extent are indirect indicators useful in the identification of ransomware groups?

The first sub-question provides a foundation by identifying established techniques, indicators and limitations in cyber-threat actor attribution. The second sub-question focuses specifically on ransomware threat attribution and provides expert insights on current practices and potential limitations. The final sub-question analyses the incident reports to identify indirect indicators and assess their usefulness in identifying ransomware groups. Answering all sub-questions results in a conclusion to the main research question.

3.2. Research approach

This section discusses the research approach of the study. The aim of the study is to discover the attribution process of ransomware threat actors and whether indirect indicators can help identify the ransomware threat actors. To achieve this, a mixed research approach is used. In particular, the explanatory sequential design fits well with the structure and objectives of the study. This approach allows for a comprehensive understanding of the problem space by combining qualitative and quantitative data collection and analysis

To address the sub-questions discussed, data is required. Data acquisition will be achieved by means of research methods. Selecting an appropriate research method is important as this will impact the usability of data to answer the sub-questions. Therefore, this paragraph discusses the selected research methods, and why it is suitable to answer the sub-questions. Firstly, the most suitable research

approach to answer the sub-question will be discussed. Secondly, the type of data which is required to answer the sub-question is discussed. Finally, a concise representation of the methodology is presented in the form of a research flow diagram which is provided in Figure 3.1.

3.2.1. Sub-question 1

Sub-question 1 examines the indicators, techniques and taxonomies used in the attribution process of cyber threat actors, including the limitations. This part focuses on understanding cyber-threat actor attribution. Currently, the attribution process of cyber-threat actors described in the knowledge gap is limited and described at an abstract level. The in-depth identification of the indicators and techniques used in attributing cyber-threat actors will aid in a comprehensive understanding of this process. The obtained knowledge will serve as a basis to develop interview questions as preparation for sub-question 2.

To answer this sub-question, a literature review is conducted using existing studies (secondary data) to identify the indicators and techniques used in attributing cyber threat actors.

3.2.2. Sub-question 2

The second sub-question examines the attribution process of ransomware threat actors using interviews. By analysing the interview results, the attribution process of the ransomware threat actors can be described. Highlighting the differences between the attribution of cyber-threat actors and ransomware threat actors provides a better understanding of the attribution process. The findings provide the basis for this research and ensure that the indirect indicators show potential to improve correlating ransomware attacks with cyber threat actors.

To answer this sub-question primary data is obtained by conducting semi-structured interviews with cybersecurity experts. During these interviews the goal is to identify the indicators and techniques used in the attribution process of ransomware threat actors and find out if indirect indicators are effective.

3.2.3. Sub-question 3

The purpose of this sub-question is to analyse the indirect indicators described in the ransomware incident reports of the cybersecurity company. However, before the analysis can take place, the extraction of the indirect indicators must take place. This is done manually by going through the incident reports and systematically recording the important indicators in Excel. Then the data analysis phase begins and the data is analysed by implementing data analysis techniques such as frequency analysis and weight contribution analysis. To make the data analysis more efficient, Python scripts will be written to standardise and analyse the data. After the analysis, a full understanding of the usefulness of indirect indicators to identify the ransomware group is obtained. The combination of these three sub-questions can provide an answer to the main research question.

To answer this sub-question, primary data is extracted by reviewing the cybersecurity company's 2023 ransomware incident reports. The analysis of these incident reports makes it possible to extract indirect indicators used by ransomware threat actors.

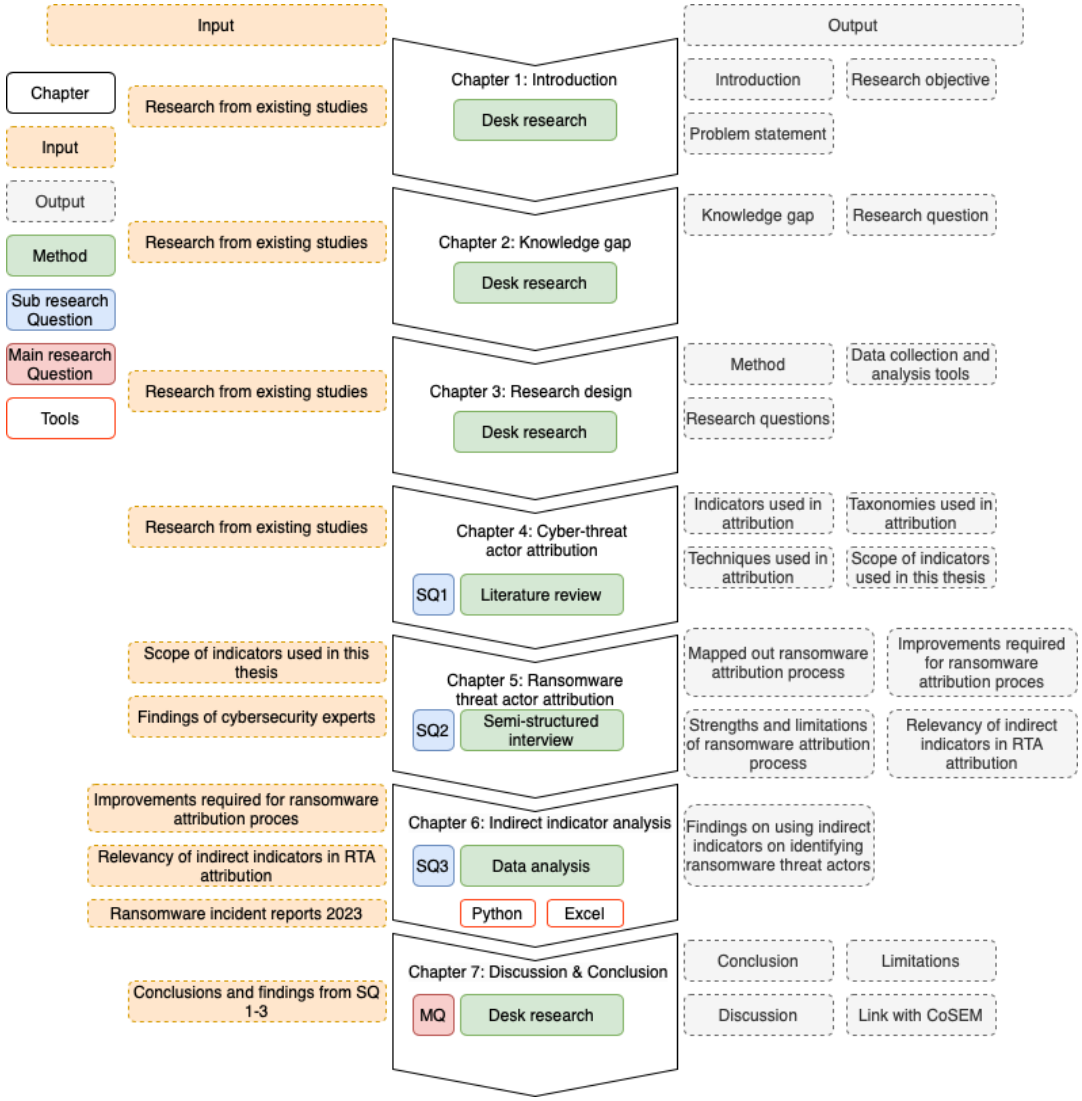

Figure 3.1: Research flow diagram

4

Cyber-threat actor attribution

Chapter 2 provides a generic and abstract definition of cyber threat actor attribution, drawn from existing literature. To determine the usefulness of indirect indicators in correlating ransomware attacks with cyber threat actors, it is important to gain a comprehensive understanding of the attribution process of cyber threat actors. The first step is to identify the important indicators used for the attribution process. The second step is to explore the techniques used for attribution, and finally to examine the taxonomies used in the attribution process. The selected taxonomy will define the scope of indicators that will be used in this thesis.

The findings of this analysis provide the fundamental basis for understanding the following chapters. In addition, the information obtained is used to develop the interview questions. Therefore, this chapter addresses the sub-question:

What techniques and indicators are currently used for cyber-threat actor attribution and what are their limitations?

4.1. Summarized approach

To answer sub-question 1, a literature review is conducted to get an understanding of the following areas:

- Identify the indicators that are used for cyber-threat actor attribution and their limitations.
- Explore the attribution techniques for cyber-threat actors and their limitations.
- Investigate which taxonomies are used for cyber-threat actor attribution.
- Explore the limitations of each taxonomy.

To investigate the indicators, techniques and taxonomies used for attributing cyber threat actors, a literature review was conducted using the Scopus search engine. The terms used were: “Cyber-Threat Attribution”, “APT Attribution”, “Ransomware Family Attribution”, “False Flags” AND “APT”.

The search was conducted using title, abstract, and keywords to limit the number of articles. The initial search returned 23 articles published through December 24, 2023. The article set was then filtered based on inclusion and exclusion criteria, resulting in a final selection of 18 articles. Furthermore, 11 additional articles were obtained by using the snowballing technique. In addition, four additional academic papers were provided by the first supervisor. After assessment, all of them were relevant to this study. This brings the total number of articles in the overview to 33. The list of selected articles can be found in Appendix A.

4.2. Definition of cyber-threat actor attribution

Various definitions of cyber threat actors (CTAs) are given in the literature. Table 4.1 provides an overview of the definitions of CTA attribution that appear in the literature. For the purpose of this thesis, CTA is defined as follows: CTA attribution is the process that involves collecting data of cyber attacks, analysing it and match the findings to a profile of a threat actor.

CTA attribution is important for several reasons. First, attribution provides insight into patterns of threat actor behavior, which aids in cyber threat intelligence and decision making [60]. Furthermore, attribution makes it possible to impose sanctions on CTA [32]. Finally, the knowledge gained about the CTA can help deter future attacks by applying defense mechanisms [47].

Table 4.1: Definitions of cyber-threat actor attribution based on different sources

Source	Definition
[69]	The process of determining the identity or location of an attacker or an intermediary of an attacker, including the attacker's name, account, alias or identifying information associated with it, and location information including Geographic location or virtual address (e.g. IP or Ethernet address).
[40]	Attack attribution is a process of tracking, identifying and attributing blame to cyber attacks or hacking agents.
[27, 48, 52, 55]	Identifying the cyber-threat actor during or after an attack
[67]	The process that involves collecting data of a malicious cyber-activity, analysing it and then associating it with a threat actor

4.3. Levels of cyber-threat actor attribution

The main purpose of cyber threat attribution is to gain knowledge about the person or organization behind the attack [27]. However, identifying the person is not always possible. Therefore, there are different attribution levels, as shown in figure 4.1. Each attribution level can be linked to the parameters of a cyber attack, described by [27] and [39]. The first level is to obtain information about the tools and tactics, techniques and procedures (TTPs) used by the attacker, asking the questions 'what' and 'how'. In the second level, the main goal is to find the country behind the attack. This is achieved by answering the 'why' question, which results in information about the motives and objectives behind the attack. The last and most important level is knowing the person/organization behind the attack, where the question 'who' can be answered. This is the most difficult level, because attackers will use sophisticated methods to hide their identity [59, 27].

It is important to note that the goal of attribution is often to associate groups with a cyber attack, because attribution at the individual level is difficult to achieve [35]. This could be explained by the fact that individuals can change groups, making it difficult to identify them [62].

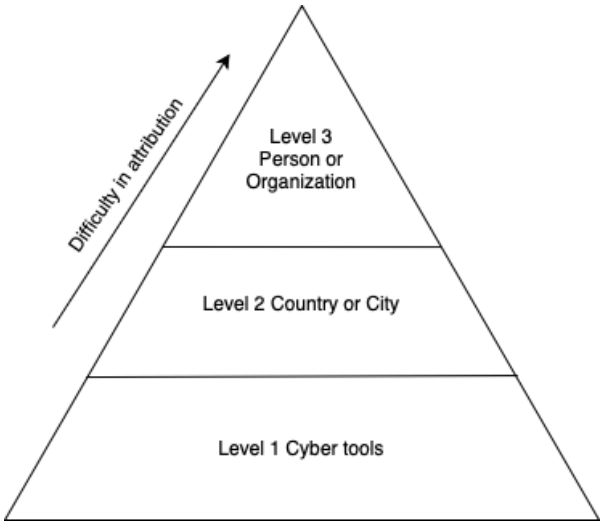

Figure 4.1: Levels of attribution

4.4. Indicators

Cyber-threat actor attribution is often a mix of technical attack analysis and threat actor profiling [62]. Indicators are needed to enable technical attack analysis and profiling of threat actors. Indicators are pieces of evidence or artifacts that can be used to identify and attribute cyber threats to specific actors, groups, or campaigns. Usually a distinction can be made between types of indicators. The literature distinguishes between low-level IoC and high-level IoC. Low-level IoC provides information about what type of artifacts are used during an attack, which can help discover the infrastructure used by the adversary [48, 27]. High-level IoC discovers how the attack was carried out and could lead to insights into the behavior of the CTA [48, 27]. Low-level IoC provides direct information about the CTA as the digital artifacts are used by the CTA. High-level IoC requires a translation layer, which means additional research is needed to obtain information about the behavior of the threat actor. An example is the use of software tools, the tool itself does not provide any information about the adversary. But finding out how they use it can give you information about its behavior. This is the translation layer. Therefore, low-level IoC will be referred to as direct indicators and high-level IoC as indirect indicators.

4.4.1. Direct indicators

Direct indicators refer to observable and verifiable evidence that indicates a security incident has occurred [3]. But they are often susceptible to changes from [48]. Examples of such direct indicators include hash values, IP addresses, domain names, network/host artifacts, and tools used. Analysing these direct indicators provides information about the infrastructure used by the adversary, such as Command and Control servers (C2s) [62].

- **Hash Values** Each file has a corresponding hash value which makes this file unique. Therefore, hash values can be seen as the fingerprints of files [8].
- **IP Addresses** an IP Address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol (IP) for communication [33].
- **Domain Names** A domain name is a human-readable and easy-to-remember identifier associated with an IP address on the Internet [8].
- **Network/Host Artifacts** A network artifact are indicators that looks at network level data and activities [8].
- **Command and Control servers (C2s)** A C2 server is a network that cybercriminals use to manage and control malware-infected devices. It acts as a communication hub that allows attackers to send commands to the infected devices [15].

4.4.2. Indirect indicators

In contrast, TTPs and how the tools are used emphasize the strategies and methods used by threat actors. This allows an analyst to get a broader perspective and provides insight into the adversary's modus operandi [3]. However, understanding the information provided by TTPs and the way the tools are used requires research into the modus operandi for finding relationships with a cyber threat actor. This is the translation layer and makes TTPs and the way tools are used an indirect indicator. A framework that helps with this translation is the MITRE ATT&CK framework, which provides a standardised language for these types of indicators [14].

- **Usage of software tools** The usage of software tools is how the adversary uses the tool, which can show specific behavior for the adversary. An example could be that an adversary uses WinZip to encrypt the files, and always end the zipfiles with ".gotyou".
- **Malware** Malware is a piece of malicious software found as digital evidence. However, research into the malware is necessary to obtain information about the opponent. Because this research is necessary, malware is considered an indirect indicator.
- **TTPs** Tactics, Techniques and Procedures (TTPs) is a typical behavior how the adversary accomplishes their mission. This means from reconnaissance all the way through data ex-filtration [8].

4.4.3. Impact of indicators on attribution

The first step in attribution is digital forensics, which collects direct and indirect indicators [7]. Direct indicators can provide information about the infrastructure used by the attacker [62]. The tools used provide information about an opponent's technical skills [62]. Combining the information results in a better understanding of an opponent's capabilities [62]. The direct indicators can therefore be used to map infrastructure and capabilities and infer the adversary's motives.

Attack patterns such as TTPs, specific use of software tools and malware can be categorized as indirect indicators. To demonstrate the importance of indirect indicators in cyber threat attribution, the example of the Democratic National Committee (DNC) email hack is used [4]. In this case, the CTA was an APT and used a persona as a decoy to divert digital forensics [68]. Similar tools and TTPs have been found in previous data breach incidents, such as the case of the German parliament [13], the French television network [57] and the World Anti-Doping Agency (WADA) [64]. After analysing these cases, a common pattern in the use of certain tools, TTPs and malware was found [48]. Based on the findings of Crowdstrike [42], ThreatConnect, FireEye and Mandiant [37], it was determined that the same CTA was responsible for several attack incidents targeting the government, military, media and other major organizations around the world [48]. Based on the similarity of the TTP patterns between the DNC email hack and the other data breach incidents, it was concluded that the threat actor behind the DNC email hack is Fancy bear [48]. This example shows the potential of using indirect indicators in cyber threat attribution.

4.4.4. Impact of indicators blocking on adversaries

"The Pyramid of Pain," described by [8], is a framework used in the field of cybersecurity to categorize different types of indicators based on their resistance to change for adversaries [43]. The Pyramid of Pain shows the different types of indicators that can be used to identify a Threat Actor's activity, and the pain it will cause a Threat Actor if one denies the ability to use those indicators [8]. The framework is given in Figure 4.2.

Based on the pain pyramid, it is concluded that direct indicators are not useful for hurting the opponent. However, currently it is common to use direct indicators such as IP addresses, ports, domains and hashes to detect data breach incidents. The direct indicators are fed into firewall rule sets to block malicious traffic coming from threat sources [48]. Furthermore, SIEM (Security Information and Event Management) systems are used to analyse and correlate these direct indicators to identify the attacker's geographic location and obtain real-time security alerts[48].

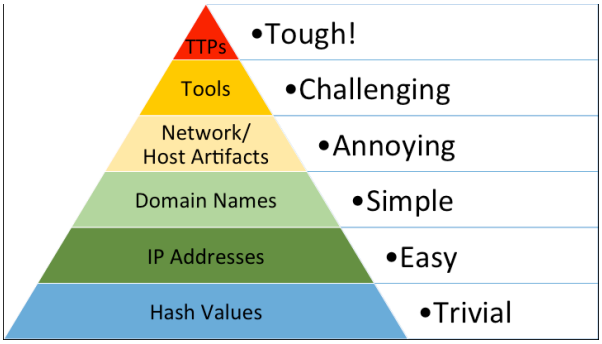

Figure 4.2: The pyramid of pain developed by [8]

4.5. Attribution techniques

In the cyber-threat actor attribution process, there are several techniques to identify the cyber-threat actor. Based on the literature, there are three major attribution techniques: digital forensics, malware-based attribution, and indirect attribution [59, 40, 45]. This section briefly summarises what the attribution techniques entail and what their limitations are.

4.5.1. Digital forensics

As mentioned in 4.4.3, digital forensics is the process of obtaining evidence such as direct and indirect indicators. Therefore, it plays a crucial role in attributing cyber-threat actors by providing evidence and insights from compromised systems. This technique collects digital artifacts during a cyber attack [61]. By analysing timestamps in log files, file changes, malware samples, registry entries, and network logs and activities, a reconstruction of the sequence of an attack can be made [50, 61]. This provides information about the attacker's entry points and time window of activity, which can be compared to known attack patterns of specific actors [3].

Digital forensics is the only technique that collects direct indicators, and according to [8] these are easy to change. Other limitations of digital forensics are that attackers can use techniques such as encryption [61] and file manipulation to delete or obscure evidence [59]. This makes attribution solely to digital forensics difficult. Table 4.2 provides an overview of the digital forensic techniques.

Digital forensics is considered the first step in the attribution of cyber-threat actors and is therefore considered a valuable tool [59]. This corresponds to the first attribution level based on Section 4.3. To increase the accuracy of the attribution process, it should be combined with other techniques [59].

Table 4.2: Overview of digital forensics techniques

Technique	Description	Limitation
Storage-based	Disk files are used to retrieve criminal activities	Analysing large storage disks becomes time consuming
RAM-based	Contents of RAM are analysed for malware	Time consuming due to the requirement of reading RAM contents across programs
Traceback	Network packets are marked and traced back to intermediate routers	Difficult to implement and execute on large scale
Logging deception	Using honeypots and sinkholes to deceive a criminal and analyse crime patterns	Information collected may not lead to full attribution

4.5.2. Malware-based attribution

Identifying the attacking group through malware-based analysis is challenging due to the complexity associated with the process of identifying the actual attacker. In most cases, malware-based attribution is used to identify the author of the code, and in some cases identifying the location is possible [59]. The malware analysis techniques are given in Table 4.3. A detailed explanation of the techniques is provided in Appendix B.

Malware attribution is a valuable tool for cyber threat actor attribution because it can provide information about the author and origin. This type of attribution corresponds to the second attribution level based on Section 4.3. However, with malware analysis alone, the information collected is limited. That is why it is important to combine this attribution technique with other techniques.

Table 4.3: Overview malware attribution techniques

Technique	**Description**	**Limitation**
Static analysis	A program code is analysed without execution	Code obfuscation techniques can deceive the analysis
Dynamic analysis	Inspecting a code through execution in a virtual environment	Code obfuscation techniques can deceive the analysis
Code similarity	Identifying similarities between malware	Resemblance does not necessarily lead to conclusive attribution as malware may have been stolen or copied
Reverse engineering	Analysing the malware to understand its behavior and characteristics	Requires specialized skills.

4.5.3. Indirect attribution

The biggest disadvantage of direct attribution techniques, is that adversaries can obscure the digital evidence [59]. Therefore, [34] concluded that indirect attribution techniques should be developed. Indirect models, which build attack models based on feature types rather than explicit features, provide more reliable attribution methods [34].

Feature types refer to the broader category or classification of attributes used for attribution [34]. It defines the type of information being analysed, rather than the specific details within that category. Common types of features include technical features, non-technical features, geospatial features, and targeted victim features [34].

There are two types of indirect attribution results: absolute attribution and relative attribution. With an absolute attribution the actual actor is identified, but in the latter case the attribution remains relative to a previous incident [59]. Indirect attribution often includes indirect indicators such as TTPs, malware and tools to generate criminal profiles. A disadvantage of indirect attribution is the extensive data required to generate accurate profiles of criminals [59]. Table 4.4 provides an overview of the indirect attribution techniques and their limitations. Appendix B provides an in-depth explanation of the indirect attribution techniques. Indirect attribution allows attribution at the personal/organization level, which is the highest level according to 4.3.

Table 4.4: Overview of indirect attribution techniques

Indirect attribution technique	Description	Limitation
Behavioral analysis	Behaviors of criminals, attacks, and intrudes are analysed to identify characteristics	Requires large amount of data
Linking with geo-political scenarios	Political scenarios are considered that may lead to improved attribution	Attribution is dubious
Cyber-threat intelligence	Evidence based knowledge	Inconsistencies in data quality across intelligence sources. Large volumes of data

4.5.4. Attribution challenges

One of the attribution challenges is false flag operations. A false flag operation occurs when the threat actor's intention is to blame a third party and hide their own malicious action behind someone else [62]. This makes the attribution process even more difficult.

4.6. Taxonomies

Taxonomies are used to perform classification and to describe characteristics of different classes. A taxonomy provides a standardised way to describe the traits and characteristics associated with cyber-threat actors, resulting in a basis for effective analysis and attribution [27]. Therefore, this section will identify the taxonomies used to attribute cyber-threat actors and their limitations.

4.6.1. Identified taxonomies in attribution

Based on the scientific literature, Table 4.5 provides an overview of the identified key attributes that have been used to attribute cyber-threat actors. Based on these findings, it can be noted that most of the attribution is done based on technical indicators. This can be classified as a technical taxonomy. However, there are also indicators such as speed of operating and target, which are non-technical indicators. This can be classified as a non-technical taxonomy. A specific form of non-technical attribution is the targeted victim taxonomy, which classifies threat actors based on their preferred targets. In the previous paragraphs it became clear that attribution at country level is important. This can be used to categorise the threat actors based on their geographic origin, which is called geospatial taxonomy. This section elaborate on the identified taxonomies and their limitations.

Table 4.5: Identified key features used in cyber-threat actor attribution

Source	Key feature used for cyber threat actor attribution	Actor
[19]	TTP	APT
[23]	High-level IoC (TTP, tools)	APT
[60]	High-level IoC, Low-level IoC	APT
[62]	High-level IoC (TTP, malware), Low-level IoC	APT
[66]	Malware (Binary similarity)	APT
[55]	Malware (Header features, Opcode, Bytecode)	APT
[65]	Malware	APT
[44]	Malware	Ransomware
[18]	Malware	Ransomware
[27]	High-level IoC (Malware, tools, TTP), low-level IoC (IP, hash)	CTA
[24]	Malware (signatures), tooling, speed of operating, Infrastructure, target	CTA
[48]	High-level IoC (TTp, software tools, malware)	Financially driven CTA

Technical taxonomy

A technical taxonomy is a classification system based on the technical characteristics of a cyber-threat actor (CTA). The goal is to categorise threat actors based on observable technical indicators and behaviors associated with their attacks. An overview of the identified technical indicators can be found in Table 4.6.

This taxonomy has its limitations, as obfuscation techniques can be applied to mask the direct indicators and malware [62]. As discussed, false flag campaigns are one of the challenges that make attribution more difficult. This is especially true for this type of taxonomy, as threat actors try to imitate other groups' malware and TTPs.

Table 4.6: Key features considered in a technical taxonomy

Key feature	Description	Limitation
Malware [66]	Analyses the code, functionality, and delivery methods	Prone to obfuscation and false flag campaign
IoCs [3]	Examining digital artifacts to launch attacks	Prone to obfuscation and false flag campaign
TTPs [48]	Classifying the specific methods attackers use to gain access, maintain persistence, and achieve their objective	Prone to false flag campaign

Non-technical taxonomy

In a non-technical taxonomy, threat actors are classified based on non-technical characteristics and behavior. Some of the most important characteristics are motivation, targets, victim selection, communication style and historical behavior. An overview of these features and their description can be found in Table 4.7.

This taxonomy provides a broader understanding of threat actors beyond their technical capabilities. It helps to understand the context behind the attack. This can be valuable in investigations as it provides clues and insights into the actor's potential identity or origins.

However, there are limitations to this taxonomy. First, the categorisation can be more subjective and open to interpretation compared to a technical taxonomy. Furthermore, collecting reliable and comprehensive non-technical data on threat actors can be challenging.

Overall, non-technical taxonomies are a valuable tool in the cyber-threat actor attribution process. They provide a holistic perspective by complementing technical analysis and offering insights into the motivational and behavioral aspects of the actors. However, it is crucial to acknowledge the limitations of these taxonomies and use them in conjunction with other sources of intelligence for a comprehensive and accurate attribution process.

Table 4.7: Key features considered in a non-technical taxonomy

Key feature	Description	Limitations
Target	Categorized based on their preferred target	Not all threat actors have a preferred target
Communication style	The language used, level of sophistication in communication, and preferred channels	Only apply for certain threat actors
Motivation	The primary driver behind the attack	More subjective

Geospatial taxonomy

In this type of taxonomy, threat actors are categorised based on their suspected geographic origin [59]. The key features in this taxonomy are IP addresses, language and cultural references, and geographic targeting [59]. An overview can be found in Table 4.8.

It is important to be cautious about relying solely on geospatial information for attribution. Factors such as proxy servers and intentional obfuscation can make accurate attribution based on location difficult. This information should be used in combination with other intelligence sources for a more complete picture.

Table 4.8: Key features considered in a geospatial taxonomy

Key feature	Description	Limitation
IP-address	Origin of IP used can provide info on location	Prone to anonymization techniques
Language	Provide info on geographical origin of the actor	Can use a different language
Geographical targeting	Observing patterns in targeting specific regions	Requires large amounts of data

Targeted victim taxonomy

This taxonomy classifies threat actors based on their preferred targets. This involves preferred sectors, victim selection methods and victim profile. An overview of the most important features can be found in Table 4.9.

One of the limitations of this taxonomy is that its scope is limited to the target selection process, neglecting other aspects. This narrow focus can lead to an incomplete understanding of the threat actor. This results in an oversimplification of the factors that influence the selection of victims. Finally, not all threat actors have specific targets, such as ransomware threat actors. Therefore, analysing targeted victim profiles is a valuable piece of the attribution process, but it should not be used in isolation. It should be combined with other evidence to avoid drawing inaccurate conclusions based on limited information.

Table 4.9: Key features in a targeted victim taxonomy

Key feature	Description	Limitation
Industry sectors	Observing a pattern of attacks targeting specific industries	Limited data
Victim selection	How the targets are chosen	Prone to subjectivity
Victim profile	Identifying characteristics shared by the victims	Limited scope

Limitations of the taxonomies

Each taxonomy has its limitations in which the technical taxonomy deals with false flag campaigns. The main limitation of the non-technical taxonomy is the subjectivity in its categorization. The geospatial taxonomy is sensitive to obfuscation techniques, which can lead to incorrect origins. Finally, the taxonomy of intended victims is limited in scope, resulting in an incomplete understanding of the threat actor. This shows that there are many challenges in the attribution process, and that a combination of taxonomies is often necessary to achieve a high level of confidence in attribution.

4.6.2. Suitable taxonomy

Several taxonomies can categorize relevant features. However, as this thesis focuses on analysing indirect indicators, a classification system based on technical indicators is most appropriate. The technical taxonomy includes a wide range of indicators relevant for indirect indicator analysis and fits well with the research goals.

4.7. Conclusion

This chapter explored: What techniques and indicators are currently used for cyber-threat actor attribution and what are their limitations? with the means of a literature review.

During the research it became clear that there are two types of indicators: direct and indirect. Direct indicators are susceptible to change, however provide valuable but limited information. In contrast, indirect indicators have been proven to have high attribution potential, but research is needed to establish a link with the cyber-threat actor.

The main attribution techniques found are digital forensics, malware-based attribution and indirect attribution. It was found that direct attribution is prone to obfuscation, and that indirect attribution could overcome this limitation. There are two types of outcomes in indirect attribution: absolute attribution (actual cyber-threat actor identified) and relative attribution (correlation with previous incident). However, the reliance on a large amount of data to create a profile makes it difficult to implement indirect attribution consistently for every cyber-threat actor. Despite these limitations, indirect attribution has the potential to be effective in attribution.

Finally, four types of taxonomies used for attributing cyber-threat actors have been identified. These are shown in table 4.10. The taxonomy chosen for this thesis is the technical taxonomy. This taxonomy uses key characteristics relevant to this study to categorize the threat actors.

In conclusion, this chapter shows that there are generally two types of indicators: direct and indirect. These indicators can be used for attribution, with the main attribution techniques being digital forensics, malware-based attribution and indirect attribution. Furthermore, it was determined that the technical

taxonomy is considered the most appropriate taxonomy for this study due to its focus on malware analysis and TTP analysis. This alignment allows for a more systematic analysis of ransomware threat actors based on technical indicators, which will be further explored in the following chapter. The use of the technical taxonomy will enable the categorization and analysis of threat actors based on their technical characteristics, providing valuable insights into their behavior and potential identification.

Table 4.10: Taxonomies and their limitations

Taxonomy	Limitation
Technical	Has to deal with false flag
Non-technical	Subjectivity in categorization
Geospatial	Obfuscation techniques are often used
Targeted victim taxonomy	Narrow scope

5

Ransomware threat actor attribution

After understanding the attribution process of cyber threat actors, this chapter aims to map the attribution process of ransomware threat actors. In addition, it aims to discover the challenges, limitations and improvement points of the attribution process of ransomware threat actors. By identifying these aspects, the goal is to discover the potential of the indirect indicators in the attribution process of ransomware threat actors. To achieve this goal, the following sub-research question will be answered:

What techniques and indicators are currently used for ransomware threat actor attribution and what is the difference with cyber-threat actor attribution?

The interview results from segment 1 are discussed to map the attribution process of the ransomware threat actor. To show the differences between the attribution process of the ransomware threat actor and the cyber threat actor, the differences between the literature and the interviews are highlighted. Segment 2 discusses the strengths and limitations of the ransomware threat actor attribution process, and helps identify the challenges experts face. Finally, the areas for improvement are discussed that will serve as a basis for the next chapter, where the indirect indicators are extracted and analysed to determine their usefulness in identifying the ransomware threat actors.

5.1. Summarized approach

In this comprehensive study, a total of 15 experts were interviewed by using semi-structured interviews. The details of the participants can be found Table 5.1. The primary objective of the interviews was to gather a comprehensive understanding of the ransomware threat actor attribution process. To achieve this, multiple cybersecurity experts were interviewed. The interview questions are provided in Table C.1 in Appendix C. To capture the experience and perspectives of cybersecurity experts, employees from cybersecurity companies and law enforcement were interviewed. These individuals have experience with the cyber-threat actor and ransomware threat actor attribution process. They provide valuable insights into the perspectives and issues of the attribution process faced by the experts. Moreover, the development process of the interviews can be found in Appendix C. Finally, a thematic content analysis is used in order to extract data from the interviews. The set up of this process is provided in Appendix D.

Table 5.1: Overview of the interviewees and their function

ID	Date	Function	Experience in cybersecurity
E1	09-11-2023	Lead Digital Forensics	13 years
E2	16-11-2023	Lead Cyber Threat Intelligence	16 years
E3	20-11-2023	Digital Forensics	3 years
E4	20-11-2023	Digital Forensics	3 years
E5	21-11-2023	Digital Forensics	3 years
E6	21-11-2023	Digital Forensics	4 years
E7	23-11-2023	Cyber Threat Intelligence Analyst	8 years
E8	27-11-2023	Digital Forensics	3 years
E9	08-12-2023	Reverse Engineer	8 years
E10	13-12-2023	Digital Forensics	4 years
E11	17-01-2024	Lead High Tech Crime	5 years
E12	17-01-2024	Manager	13 years
E13	18-01-2024	Cyber Resilience Consultant	6 months
E14	26-01-2024	Head Threat Intelligence	12 years
E15	08-02-2024	Digital Forensics	3 years

5.2. Interview findings segment 1

The interview questions of segment 1 mentioned in Appendix C Table C.1, provided insights in the techniques used to attribute ransomware attackers, the indicators which was most commonly used, and differences were highlighted between ransomware attackers and other cyber threat actors.

5.2.1. Indicators

During the interviews, five indicators were identified for the use of ransomware threat actor (RTA) attribution and one indicator was discussed that was not used. Table 5.2 provides an overview of the found indicators with a brief description of what the indicator entails. To demonstrate the importance of each indicator, Figure 5.1 shows the number of interviewees who mentioned the indicators.

Table 5.2: Indicators and their definition

Indicator	Description
Communication channel	A chatting platform on the darkweb to reach out to the ransomware attacker.
IoC's	Observable and verifiable evidence that indicates a security incident has occured.
Ransomware (Malware)	Software that encrypts files or the operating system.
Ransomnote	Read.me file with contacting addresses of the ransomware threat actor.
TTP	Strategies and tools employed by threat actors.
Leak site	Websites within the dark web used to leak stolen data and conduct ransom negotiations with victims.

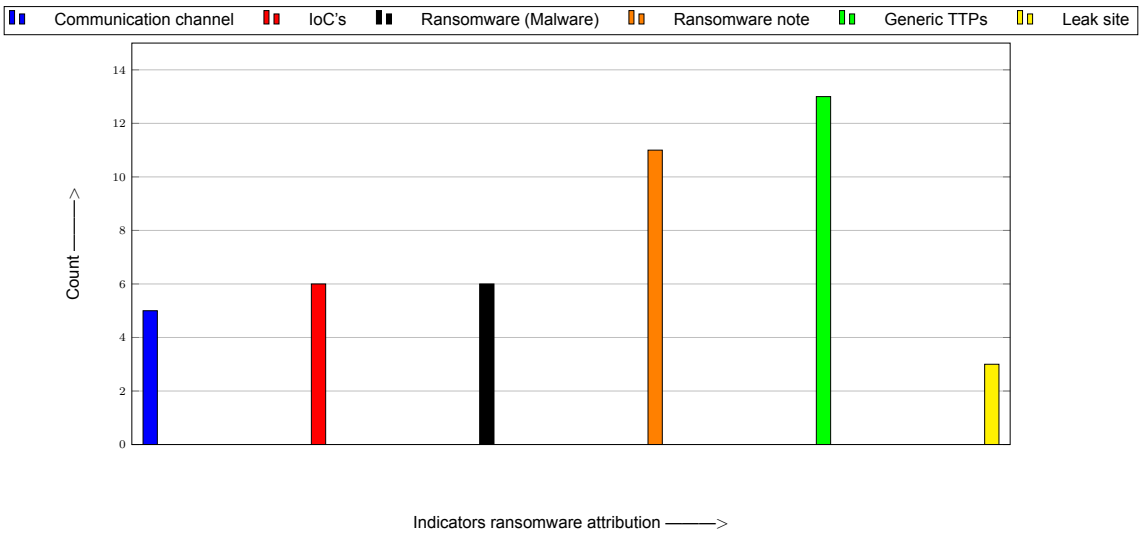

Figure 5.1: Indicators used in ransomware threat actor attribution

Direct indicators

Based on Table 5.2 direct indicators are of great importance in the attribution process of ransomware threat actors (RTAs) and will be discussed how these indicators impact the attribution process.

IoCs When IoCs are mentioned, it is often referred to network IoCs, such as the IP addresses, domains and servers used. These types of direct indicators can help reconstruct the infrastructure used by the adversary. Knowledge of the infrastructure used can help confirm the identity of the RTA, as they might use the same infrastructure in another attack.

Communication channel, ransomware note and leak site The main type of direct indicator observed is the ransomware note. A ransomware note is one of the most decisive indicators within the attribution of ransomware groups, as the ransomware actor presents itself in this note, as stated by participant E.3. The ransomware note contains contact information to contact the ransomware attackers via a communication channel on the dark web. That point of contact is recognizable with whom you are dealing, because such communication channels can only be managed by the specific group according to participant E.1. Additionally, during negotiations, ransomware threat actors provide evidence that they have stolen data through leak sites. Without a ransomware notification, it is difficult to negotiate and it is not possible to find out where your data has been leaked. Therefore, these direct indicators are linked to each other.

Ransomware (malware) Ransomware is an executable software program that is often responsible for system encryption. This type of indicator is often used to find errors in the encryptor so that the system can be decrypted without purchasing the decryptor. In some cases, the malware is used for the attribution process of ransomware threat actors (RTAs). Participant E.7 and participant E.2 both mentioned that this type of direct indicator is used to confirm the identity on the ransomware message. A more detailed explanation can be found in Section 5.2.2.

Indirect indicators

An interesting observation is the limited use of indirect indicators in the RTA attribution. One of the indirect indicators discussed are the TTPs and an explanation of why it is not utilized in the RTA attribution process.

TTPs Direct indicators such as the ransomware note and the communication channel provide conclusive evidence, so there is no incentive to attribute ransomware threat actors using the TTPs. Furthermore, the TTPs used by the ransomware attackers are usually too generic to make a clear distinction. The generic set of TTPs came into existence due to the prevalence of the RaaS model. This business model provides pre-built tools and infrastructure, making it easier for affiliates with limited technical skills to carry out ransomware attacks. According to participant E.3 and E.7, this reduces the variation in the use of TTPs in ransomware attacks. The TTPs are collected during the investigation to create mitigation measures against future attacks.

5.2.2. Methods and techniques

The interviews resulted in three different types of methods and techniques CTI, Forensic investigation, malware analysis and ransomware notes provided in Figure 5.2.

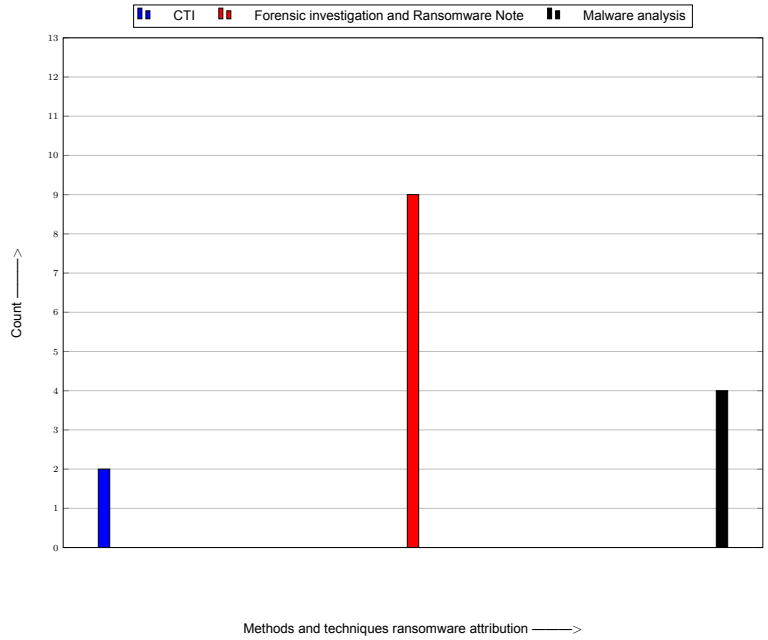

Figure 5.2: Methods and techniques used in ransomware threat actor attribution

Forensic investigation and ransomware note An interesting observation is that the attribution process starts with the analysis of the ransomware note. In this note, the ransomware threat actors often identify themselves and provide a way to contact them. Digital forensics is then used to find evidence that confirms the identity, such as the encryptor. During the forensic investigation, the TTPs are collected and the unified kill chain is used to create the attack pattern. This is important because the victim's vulnerabilities need to be patched.

Ransomware (Malware) analysis If the ransomware can be obtained, both dynamic analysis and code similarities can be performed. This can help identify the ransomware family.

Dynamic analysis
The ransomware can be analysed in a malware sandbox. This allows the malware to run in a safe environment and the malware's functionalities to be analysed. Such malware sandboxes often provide classification functionality that provides information about the ransomware family.

Code similarities
In addition to analysing the ransomware in a sandbox, the code can also be analysed and looked for code similarities. However, the code can be leaked or shared on online forums. This can result in code similarity, which does not necessarily mean it is the same author.

Cyber threat intelligence (CTI)
In some cases, the digital forensic team doubts whether certain direct indicators and TTPs found correspond to the RTA. These indicators are then sent to the CTI department, where they will provide confirmation whether the indicators correspond to the RTA. The main applications of CTI in the award of RTA are used for sanctions checks. However, this finding has its limitations, as the number of CTI specialists interviewed is only limited to three participants. Despite this limitation, CTI is considered part of the RTA attribution process.

5.2.3. Attribution process of ransomware threat actors (RTA)
To describe the attribution process of RTAs, a clear distinction must be made between ransomware and RTAs. An RTA is always financially motivated and therefore tries to make money from the attack. However, ransomware can be used by any CTA but for different purposes, such as using it as a decoy or destroying the data. It can therefore be concluded that making contact with the victim is a characteristic move of an RTA. Therefore, the scope of this attribution process is strictly limited to an RTA. The findings

from the indicators and methods are used to describe the attribution process of ransomware threat actors.

Features of ransomware threat actor used for attribution

The main attributes used for RTA attribution are mainly direct indicators, such as the ransomware note, the communication channel and the leak sites. These direct indicators provide conclusive information about the identity of the ransomware group. In some cases, the malware is analysed to obtain additional information. Therefore, the RTA attribution is based on a technical taxonomy with the focus on direct indicators. The literature reports that this type of feature is susceptible to obfuscation, *but according to participant E.9, obfuscation techniques are not commonly used in ransomware creation.*

False flag campaigns

Ransomware groups consider themselves a company that offers a service to the victim by providing the decryption key to get the data and system back. This means that the malware they use must generate a decryption key that actually works, *otherwise the reputation of the ransomware group will deteriorate and victims will not pay this group as explained by participant E.7.* Because reputation is important to ransomware groups, false flag campaigns are not used, as such campaigns would result in attribution to another group. This way they do not get the money and therefore they have no incentive to use false flag campaigns.

Impact of misattribution

The impact of misattribution is related to the purpose of the attribution. Subthemes have been identified in which misattribution has a major impact. Figure 5.3 provides an overview of the frequency analysis.

Of the fifteen participants, eleven said the impact of misattribution depends on the purpose. Three of these participants mentioned that misattribution depends on the target, without giving an example. The misattribution of an APT was reported as it could lead to geopolitical issues, making the attribution of APTs of great importance. The second goal mentioned was attribution at the individual level. Because this level of attribution is primarily performed by law enforcement agencies, individual misattribution must be avoided. Sanction checks was mentioned by three participants, this is important when making RTA attribution. The reason for this is that if a threat actor is prohibited from paying sanctions to such actors, a misattribution could lead to bankruptcy for the victim, as they can pay the sanctioned threat actor but also have to pay a fine because the payment has been made to a sanctioned threat actor.

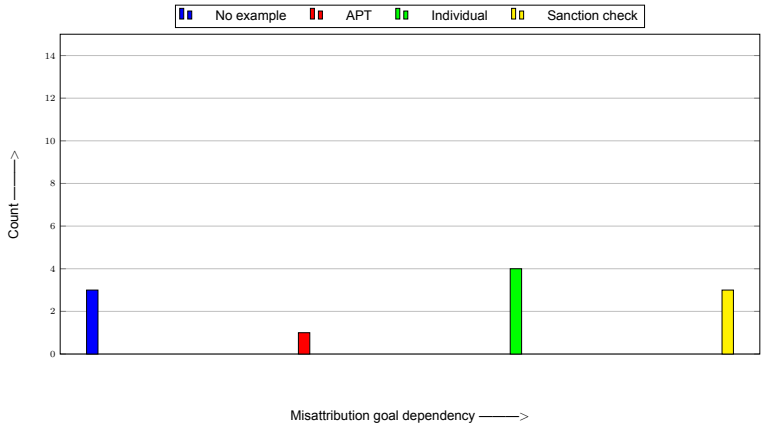

Figure 5.3: Misattribution and their goal dependencies

Levels of attribution in ransomware attacks

One level not mentioned in the RTA attribution is the country level. The reason the country level is not as important when attributing an RTA is because of the Ransomware-as-a-Service model. This model allows the affiliates to operate from different countries, making the country level with these types of threat actors not so relevant.

Clearly, differences exist between the level of attribution identified in the literature and the levels identified in the interviews. An overview of the attribution levels of RTAs is given in Figure 5.4. The first

observation is that the group identifier is placed at the lowest attribution level within the RTA attribution because the RTAs identify themselves using a ransomware note. A level higher is the identification of the cyber tools, which means conducting forensic investigations to gather information about the RTA's attack patterns to patch vulnerabilities. The last level is the person level, which is the most difficult to do and is not covered in this thesis.

There are two main differences between the RTA and CTA attribution levels. One of the differences with the attribution levels identified in the literature is that the identification of the group is recorded at the lowest level. Second, the country level is not used to assign the RTA because the attackers can be in multiple places at the same time.

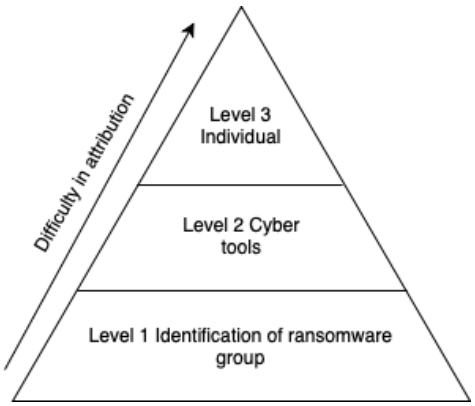

Figure 5.4: Levels of attribution in ransomware attacks

Attribution entities and cooperation

There are two major entities that do attribution: cybersecurity companies and law enforcement agencies. To explain the different attribution levels achieved by the identified entities, the diamond model will be used. The diamond model specifies the technical capabilities, infrastructure, the victims and information about the adversaries [10]. The diamond model can be found in Appendix F, Figure F.1. Based on this model, the attribution levels achieved by the various organizations are discussed. The frequency with which participants mention the attribution entities is shown in Figure 5.5.

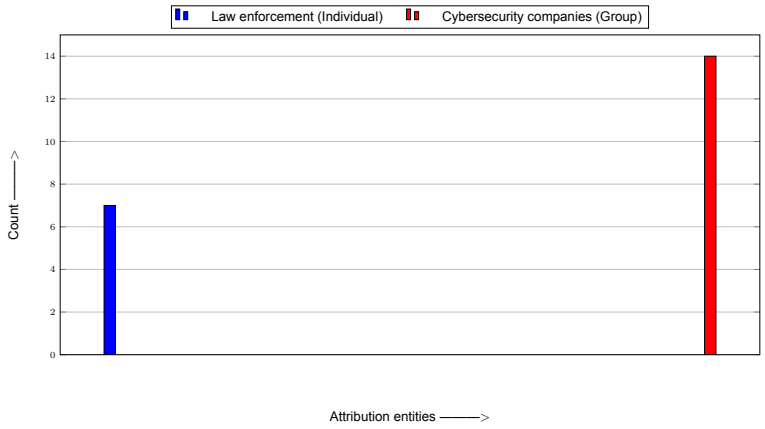

Figure 5.5: Identified attribution entities and their corresponding attribution level

Cybersecurity companies As shown in Figure 5.5, the cybersecurity company performs the attribution of ransomware threat actors at the group level. Cybersecurity companies use digital forensics to find out how the adversary penetrated the victim's infrastructure and what tools they used to carry out the attack. This type of information can help measure capabilities and discover certain parts of the infrastructure used by the adversary. Therefore, it can be said that cybersecurity companies tend to help the victim and explore the capabilities. Some cybersecurity companies facilitate payments, and

for these companies attribution is important, for the so-called sanctions control. By carrying out the sanctions check, all information found within the forensic investigation and the CTI is compared with information on a sanctions list. If it turns out that the threat actor is on a sanctions list, payment cannot be facilitated by the cybersecurity company. Therefore, it can be concluded that the level of attribution achieved by a cybersecurity company is on the lower level, as they identify the group and the cyber tools used.

Law enforcement Law enforcement officials conduct the attribution of ransomware threats at the individual level. The working method of such entities is different from that of the cybersecurity company. Law enforcement focuses on evidence and criminal offenses. Law enforcement tries to tie the evidence to a specific adversary. An example is investigating criminal forums and linking infrastructures used for nicknames. Therefore, it can be concluded that law enforcement focuses on the infrastructure used by the adversary and links it to a specific individual. As interviewee E.7 indicated, there must be a balance in the diamond model. This balance is achieved through collaboration between cybersecurity companies and law enforcement agencies. If necessary, the cybersecurity company will provide the evidence found during the investigation to law enforcement authorities, so that law enforcement authorities have more information to find the adversary. Therefore, law enforcement officials do attribution at the highest level possible.

Attribution process of ransomware threat actors

Ransomware threat actors are mainly attributed on group level. There are two situations that can take place a successful ransomware attack and early containment. In the case of a successful ransomware attack, the threat actors leave a ransomware note. This note is important as it contains information who the threat actor is. Additionally, a mean to negotiate with the threat actor is provided which is a communication channel on the darkweb. In addition, data is uploaded to a leak site to prove they exfiltrated the data. The combination of these direct indicators provide sufficient information on the RTA group behind the attack. Digital forensics is then used to find direct indicators that can confirm the identity of the ransomware threat actor such as the malware executable. Lastly, if there is doubt the findings are send to the CTI department that can help in confirming the identity.

The motive of a CTA become clear after the encryption process, however, in the case of an early containment the encryption process will not take place. There are two different scenarios possible. The first scenario is that the ransomware threat actor establish contact with the victim stating that certain data is stolen. This allows the victim to negotiate with the adversary and their identity still becomes known. The last scenario is that the adversary does not establish contact. *If this scenario is the case, then attribution is often not done as there is not enough unique evidence found to distinguish what type of threat actor is behind the attack. Since, there is no ransomware note and the TA is not reaching out to negotiate, it is likely that it was a different type of CTA.*

5.2.4. Comparison with the literature

Compared to the literature there are similarities and differences in the use of indicators in the attribution process. The similarity is that network IoCs can help in gaining insight in the infrastructure used by the RTA. A big difference is the significance of the direct indicators during the attribution process and the little utilization of the indirect indicators. This is explained by the fact that RTAs leave conclusive evidence of their group to start the negotiation process.

The fact that forensic research is one of the most important attribution techniques is consistent with the findings from the literature review. Because digital forensics is one of the main cyber-threat actor attribution techniques found in the literature. What is interesting, however, is that within ransomware actor attribution, forensics is primarily used to confirm the identity of the actor named in the ransomware note.

It it observed that the malware analysis techniques within ransomware threat actor attribution are similar to the literature. One of the limitations mentioned by the reverse engineer E.10 is that ransomware is relatively small and easy to build compared to other malware. As a result, there is often no signature in the code. Moreover, because of RaaS, the ransomware is shared between various connected parties. Therefore, performing a malware analysis helps assign the ransomware family, but does not provide information for absolute attribution.

Finally, CTI is mainly used for sanctions checks and only applied in certain cases of the RTA attribution process. This is expected because CTI is a form of indirect attribution, while RTA attribution involves more direct attribution.

Overall, it is observed that the attribution techniques are used to confirm the identity of the ransomware group as they already introduce themselves. This is stated differently in the literature, where the techniques are used to collect evidence and identify the threat actor.

5.3. Interview findings segment 2

The following sections explore the strengths and limitations of the RTA attribution process.

5.3.1. Strengths of attribution

A recurring theme as the strength of attribution is combining the knowledge to perform simulations, as mentioned by six participants. Participant E.7 discussed that the technical indicators should be linked to the behavior and motives of the threat actors. In total, there were five other participants who made statements about the usefulness of the knowledge acquired and the use of this knowledge when carrying out simulations. Participant E.2, E.5 and E.8 state that various departments collect knowledge during ransomware attacks, creating a solid knowledge base and the information found can be used immediately. Participants E.3 and E.12 then state that the information required during the investigation can be used by CTI to profile and prepare threat actor simulations to increase the level of cybersecurity. Running the simulations can increase the understanding between the technical indicators and the behavior and intentions of the threat actor. Therefore, one of the key themes identified as a strength of attribution is combining the knowledge gained during the attribution process to simulate the ransomware threat actor's strategies.

5.3.2. Weaknesses and limitations of attribution

Within the RTA attribution, no common theme was identified regarding the weaknesses of this process, as the weaknesses mentioned by the experts were diverse. Some clusters can be formed, such as limitations of the attribution process. *Participant E.6 states that attribution beyond the group level is not beneficial to the company because it costs more money to investigate, but does not generate more money.* Another limitation is mentioned by *participant E.11 and states that not all countries have extradition obligations, so you cannot simply catch the attacker. A second cluster that can be formed concerns the complexity of RTA attribution. Participant E.7 mentions that it is difficult to distinguish between an affiliate member or a core group member behind the attack. Participant E.9 states that ransomware provides limited information compared to other types of malware because the code is very small and leaves little room for signatures and patterns.* These examples demonstrate diversity in perspective and are valuable because they highlight the need for a multidisciplinary approach to the awarding of RTAs.

Legal and ethical limitations are also discussed, making it clear that such limitations depend on the level of attribution that takes place. The results are provided in 5.6. *The first observation is that law enforcement agencies have legal and ethical limitations in their work.* This is expected because Section 5.2.3 discusses that this entity focuses on the higher attribution level. Such entities must take into account the Code of Criminal Procedure, without it there are no legal actions. The majority of the cybersecurity company answered no. This answer is expected, because the attribution level achieved by cybersecurity companies is focused on the lower attribution levels elaborated in Section 5.2.3. However, there are participants from the cybersecurity company who answered yes, which is unexpected. *It is striking that two of the participants indicate that they sometimes find login details to log into the hacker's account to collect more personal information from this actor.* They are then faced with the ethical constraint of having to hand this evidence over to the police or do it themselves. It can therefore be said that these participants have personal motivation to attribute at a higher level, even if this is not the attribution goal of cybersecurity companies.

During the literature review it became evident that one of the limitations of attribution is the use of false flag campaigns of CTAs. *However, based on the identified weaknesses and limitations false flag were not mentioned, the reasoning is already explained in a previous section.*

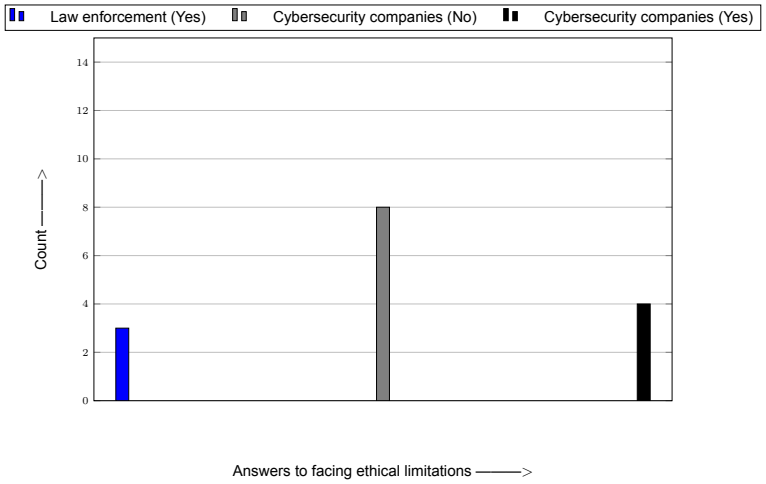

Figure 5.6: Facing ethical limitations

5.4. Interview findings segment 3

In this section we will discuss in more detail the points for improvement mentioned by the participants. For the improvement areas of RTA attribution, two main themes have been identified: creating a central database and sharing data with standardised language, as shown in Figure 5.7.

5.4.1. Create central database

One of the needs that several participants mentioned is the need of a central data base that contain the findings, both direct and indirect indicators, of previous investigations. This way the root cause analysis could be improved significantly. In addition, according to participant E.5 incorporating indirect indicators could help with identifying TTPs specific to a certain RTA. In addition, participant E.15 states that the implementation of the tooling might show the difference between ransomware groups or even affiliates. Therefore, analysing this data could help in correlating ransomware attacks to the same RTA of a previous attack.

5.4.2. Sharing data

As attribution is dependent on connecting information, data sharing is of great importance. However, the cyber-security community faces many problems regarding data sharing. Victims often do not report that they have been a victim to a ransomware attack. They are scared that their reputation might get damaged. This also impacts that investigation of law enforcement as they do not get the information on the incident. Therefore, research should be conducted to increase the efficiency of data sharing.

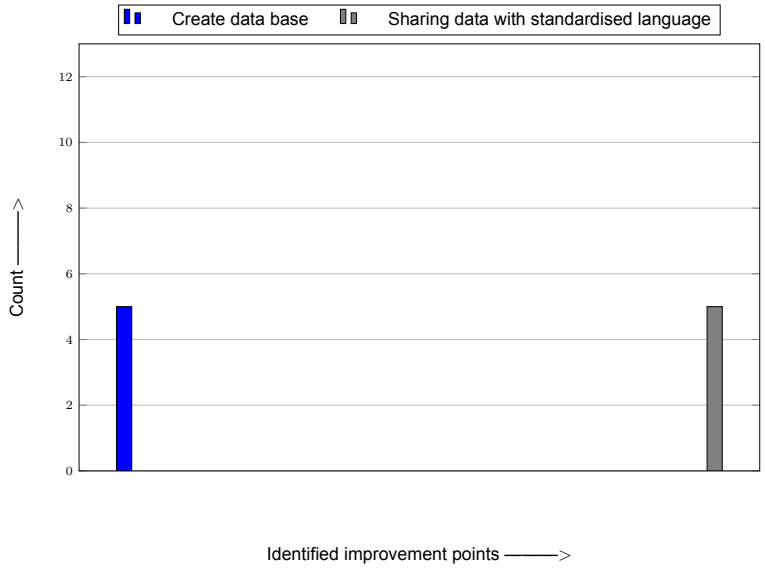

Figure 5.7: Improvement points Ransomware Threat Actor attribution

5.5. Conclusion

This chapter explored the ransomware threat actor attribution process and answered sub question 2: What techniques and indicators are currently used for ransomware threat actor attribution and what is the difference with cyber-threat actor attribution?

The major findings of the ransomware threat actor attribution process is the use of direct indicators that provide conclusive evidence, this results in no incentive to use TTPs. Obfuscation techniques poses no problem as ransomware group often do not use obfuscation techniques in their code. The attribution techniques that can be applied for ransomware threat actor and cyber-threat actor are the same, but the difference is in their application. During the digital investigation the TTPs of the ransomware threat actor are collected, but only to develop mitigation strategies and not for attribution. In some cases malware analysis and cyber threat intelligence are used for confirmation of the identity of the ransomware threat actor group. In cyber-threat actor attribution the malware analysis and cyber threat intelligence have more value, as they provide information on the origin of the attack and to behavior specific to an cyber-threat actor.

The ransomware threat actor attribution process consists of analysing direct indicators such as the ransomware note and the communication channel. In which digital forensics is used to find evidence to confirm the identity of the ransomware threat actor, such as an encryptor. The attribution levels of ransomware threat actor differ from that of a cyber-threat actor as the country level is not relevant for ransomware threat actors as the attackers can be scattered in multiple countries. In addition, the identification of the group of the ransomware threat actor is placed as the lowest level since they identify themselves, which is different for a cyber-threat actor in which identifying the group is placed as the highest level.

Attribution does not only help in identifying who is behind an attack, but it can also help in elevating the security level. The combined knowledge can create simulations of the attackers, that can be applied to test the security level of companies. There are multiple weaknesses mentioned, which show the need for a multidisciplinary approach to the attribution of ransomware threat actors. Interestingly, none of the limitations were false flag as mentioned in the literature. This can be explained by the fact that ransomware threat actor want to be known for their attacks, as their reputation of providing decryption keys is important to them. Therefore, ransomware threat actors do not have the incentive to use false flags.

An interesting finding is that multiple experts want to create a central data base with profiles including indirect indicators, as this could help with correlating ransomware attackers to other ransomware threat actors. The second improvement point that was found was sharing of the data. As attribution is depen-

dent on data, and often different companies hold different pieces of information, improving sharing the data could improve the attribution process in general.

In conclusion, the main indicators used in ransomware threat actor attribution are direct indicators such as ransomware notes, communication channel and leak sites. *The indirect indicators are not analysed as there is no incentive to use them in ransomware threat actor attribution, however, multiple experts mentioned that including these indirect indicators could help in correlating ransomware attackers to make a distinction between ransomware groups and even affiliates.*

After gaining knowledge of the relevant indicators and techniques in ransomware threat actor attribution, it became evident that there is a need to utilize indirect indicators in ransomware threat actor attribution. Therefore, the next chapter will analyse the indirect indicators to investigate whether such indicators can help correlating ransomware attacks to cyber-threat actors.

6

Indirect indicator analysis

Now that it became evident that there is a need to utilize indirect indicators in attributing ransomware threat actors, further research is being conducted into these types of indicators. To determine the usefulness of the indirect indicators in identifying the ransomware groups, the next step is to extract and analyse these indicators from the cybersecurity company's ransomware incident reports. This chapter aims to answer the following sub-question:

To what extent are indirect indicators useful in the identification of ransomware groups?

This chapter first explains how the data is extracted. The methods used to analyse the data are then discussed. The results are then presented and discussed.

6.1. Summarized approach

To answer sub-question 3, cybersecurity ransomware incidents from the year 2023 were analysed to extract the indirect indicators. Data analysis techniques are then applied to discover unique (sub-)techniques/tools used by ransomware threat actors. This is achieved by performing a frequency analysis, which helps visualize the (sub-)techniques/tools that have a frequency of one. To obtain information about the (sub-)techniques/tools that have a higher frequency than once, but are only used by a certain group, an additional contribution analysis is carried out to see whether a (sub-)technique/tools is typical for a threat actor. A Python code was written to assist in the results analysis.

6.2. Data extraction and analysis

To answer the question of whether indirect indicators are useful in identifying ransomware groups, data on ransomware incidents was taken from the incident reports of one cybersecurity company for the year 2023. This ensures that the analysis shows the latest techniques of threat actors. To protect sensitive information, extracted data was limited to indirect indicators, excluding personally identifiable or sensitive details. Additionally, all extracted data comes from the aforementioned cybersecurity company, to maintain consistency and control for potential biases associated with data collection methods from multiple sources.

In addition, during the analysis of the incident reports, it became clear that not all ransomware incident reports provided sufficient information. Therefore, the incident reports considered for the analysis contain information about how the threat actor entered the system, how they moved laterally through the system, how they exited the system, and who the threat actor was. If one element was missing, this report was not analysed. This resulted in a total of 27 ransomware incident reports analysed.

6.2.1. Data preparation

TTPs are a specific indirect indicator, often described in human-readable text [48]. This means that the data must be standardised before it is suitable for direct analysis. This is achieved by translating the TTPs described by humans into standardised language. Manually mapping them into the MITRE

ATT&CK framework, allows for a consistent and structured description of the TTPs used.

Thereafter, the data must be organized. This is accomplished by entering the translated TTPs into an Excel sheet. The organized data facilitates further analysis and creation of the threat actor's intrusion set. These are the specific combinations of TTPs observed in a ransomware attack.

6.2.2. Data filtration

During the frequency analysis, it became clear that there are common techniques that make the frequency analysis more complex by increasing the data volume, as shown in 6.1. To make analysing the data easier, data filtration is applied. The filtration process is explained in detail.

Initial access techniques

In the blog of [29], it is mentioned that for the initial access phase there are typically three key techniques of a ransomware attack: *Abuse weak credentials, Exploit vulnerability and Phishing.*

Threat actors often gain network access by purchasing leaked credentials from external remote services, such as VPN or remote desktop protocol (RDP) services [29]. This is also reflected in the results, as both valid accounts and external remote services are used for initial access. Therefore, these techniques can be seen as a set of the standard modus operandi of a ransomware threat actor. This results in the exclusion of these techniques in the indirect indicator analysis.

Second, vulnerabilities are exploited to gain a foothold in the network [29]. This activity is often observed according to the blog, but is only observed *9 times out of 27 in the results*. Therefore, this technique is included in the analysis. The last technique that is often used for initial access by threat actors are phishing techniques [29], however, *based on the results only two Threat Actors are using the phishing techniques.* This could be explained by the occurrence of RaaS, *in which the ransomware threat actor buys the credentials making phishing not part of the attack pattern.* Because there is a difference between the results and the information on [29]'s blog, the techniques exploit vulnerability and phishing are included in the analysis.

Obtaining control of the network techniques

[29] continues that the ransomware attackers try to gain control of the network by installing persistence, moving laterally, and escalating their privileges. This is consistent with the results as persistence is often created by using external remote services and installing a backdoor. Furthermore, the threat actors often use techniques to move within the system [29], based on the results this is often achieved by using remote services. Furthermore, privilege escalation is often achieved by obtaining credentials from valid accounts [29], which is also consistent with the results. Therefore, the techniques external remote services, remote services, and valid accounts are excluded from the analysis.

Extortion techniques

Finally, the threat actor attempts to obtain leverage over the victim through extortion. Data encryption is one of the techniques as it allows the negotiation process [29] to be initiated. This is clearly visible in the results, as each attack involved data encryption and therefore excluded from the analysis.

Data exfiltration is another tactic often used by the threat actor [29]. However, the exfiltration techniques are different among the threat actors, which is also reflected in the results, as three different exfiltration techniques are used in 2023. This technique is therefore not excluded because the technique may be unique to the threat actor.

The final tactic often used by ransomware threat actors is destroying backups [29]. This is not so often observed in the results, as only 5 out of 27 attacks show a low frequency.

Excluded techniques

To identify unique TTPs indicative of specific threat actors, techniques commonly observed in the analysed data and literature are excluded from further analysis. The excluded techniques considered part of many ransomware attackers' usual TTPs include:

- External Remote Services (Initial Access and Persistence)
- Valid Accounts (Initial Access)
- Remote Services (Lateral Movement)
- Valid Accounts (Privilege Escalation)

By excluding generic techniques, the analysis aims to focus on techniques that are less commonly observed. This aids in identifying techniques that can help distinguish between different groups.

6.2.3. Data limitations

The TTPs identified in each incident report vary widely. The variability is caused by several factors, the most important of which are missing logs. Without system/network logs, it becomes difficult to reconstruct the attack sequence and identify all TTPs used. Consequently, this results in an incomplete intrusion set, limiting insight into the threat actor's behavior. To mitigate this limitation, incident reports are scanned for completeness. As discussed in the previous section, ransomware threat actors have three phases: in, through, and out. If any of the stages were missing, the report was excluded from the analysis. Therefore, the data used provides valuable information.

6.2.4. Data analysis methods

This section discusses the key steps used to analyse and extract TTPs and identify potential indicators for ransomware threat actor attribution. The frequency analyses are performed on technique-level, sub-technique-level and tool-level.

For the (sub-)technique level, the overall frequency of unique techniques used for ransomware attacks are analysed. Low-frequency (sub-)techniques are investigated to assess their potential for ransomware threat actor attribution. The tool-level analysis follows a similar approach. This analysis helps identify tools that may be indicative of specific actors.

While frequency analysis provides insight into the unique TTPs used by threat actors, it does not reveal the distribution of usage among different groups. To overcome this limitation, an additional contribution analysis is performed. This analysis examines the contribution of each threat actor to the overall use of each technique and tool. This analysis focuses specifically on techniques and tools used at a frequency greater than 1 by a single threat actor, potentially indicating a unique characteristic relevant to ransomware threat actor attribution. Both of the analysis are achieved by writing a Python script.

6.3. Frequency of the threat actors

A total of 27 incident reports were analysed, with some ransomware groups more common than others. Table 6.1 shows an overview of the encounters of the ransomware groups in the 2023 dataset. Based on Table 6.1, eleven threat actors are observed once in the dataset. This limits the ability to draw definitive conclusions about these actors. However, investigating their presence is still relevant considering that affiliates can work in multiple groups.

Table 6.1: Threat actors and their corresponding encounters

Threat Actor	Frequency	Threat Actor	Frequency
Blackcat	5	Monti	1
Lockbit	3	Carver Phobos	1
Play	4	Ransomhouse	1
Blackbasta	2	Ragnar	1
Royal	2	Blacksuit	1
Mallox	1	INC	1
Hellokittycat	1	C3RB3R	1
ESXIArgs	1	8base	1

6.4. Frequency analysis based on techniques

The result of the frequency analysis is visualized in a bar chart in Figure 6.1. *Interestingly, 32% (16 out of 50) of the techniques observed were unique, meaning they were only used in one attack*. This result is in contrast with the findings of the interviews, which highlighted that the TTPs used by ransomware threat actors are very generic.

Table 6.2 shows the unique technique and the associated threat actor. An interesting observation is that the groups with a frequency greater than 1, *such as Blackcat, Lockbit, and Blackbasta, all used techniques not used by other groups*. Additionally, *some threat actors have multiple unique techniques*, such as Ransomhouse, Carver Phobos, and Lockbit. Ransomhouse has four techniques that are considered unique, Carver Phobos and Lockbit use two techniques that are unique. This finding is interesting because the interviews showed that the TTPs are too generic to attribute ransomware threat actors. However, based on these findings, there are differences in the techniques used between ransomware threat actors.

Therefore, despite the fact that some threat actors are observed only once in 2023, the techniques they use are considered a potential identifier for future attribution efforts. Especially considering the absence of these techniques among other actors within the analysed data. This finding highlights the potential of using indirect indicators to correlate ransomware attacks with cyber threat actors, despite limitations in the number of observations for certain threat actors.

Table 6.2: Threat actors and their unique technique

Threat Actor	Technique	Frequency of occurrence of TA
Blackcat	Hide Artifacs	5
Lockbit	Use Alternate Authenication Material, Account access removal	3
Blackbasta	User execution	2
Hellokittycat	Remote Service Session Hijacking	1
Mallox	System Network Configuration Discovery	1
Royal	Indicator Removal: Clear Windows Event Logs	1
INC	Credentials from password stores	1
Carver Phobos	Boot or Logon Autostart Execution, Network sniffing	1
Ransomhouse	Scheduled Task/Job: Scheduled Task, Event Triggered Execution, Network Share Discovery, Ingress Tool Transfer	1
Ragnar	Use Alternate Authentication Material	1
Blacksuit	Drive-by Compromise	1

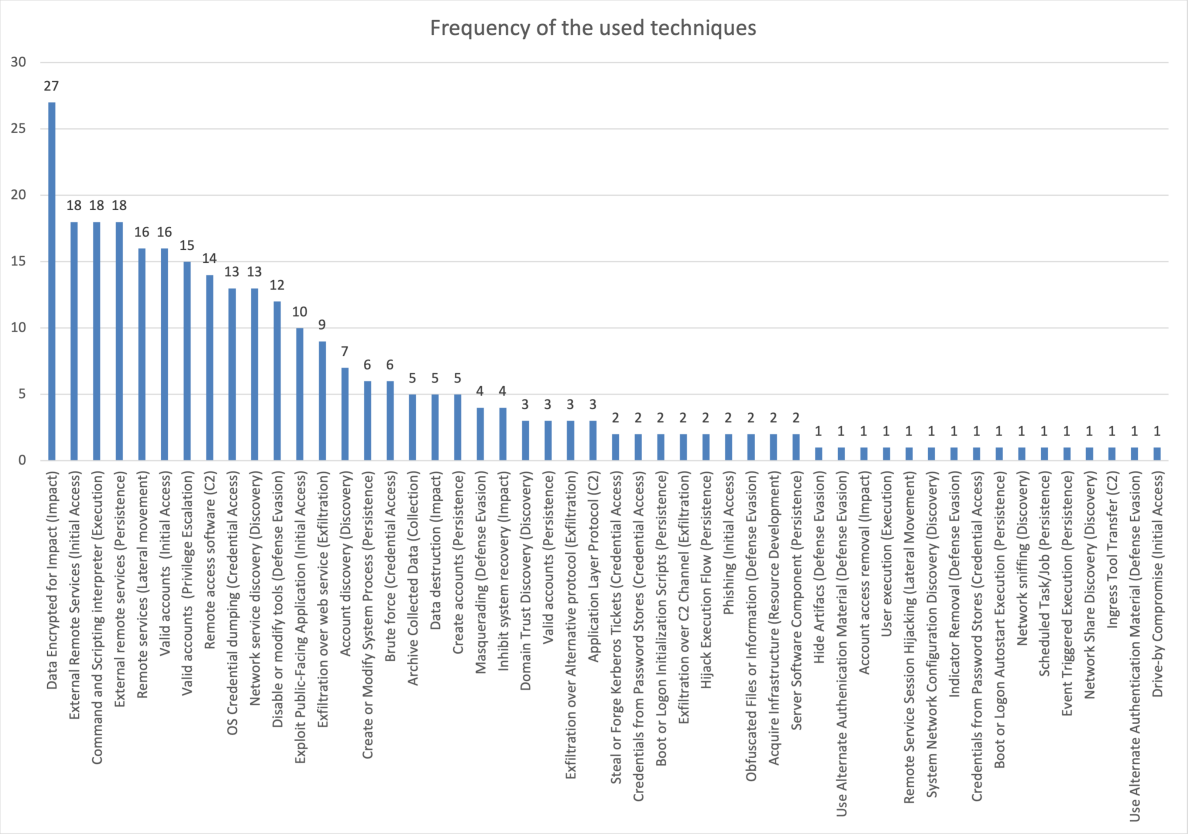

Figure 6.1: Frequency of the used techniques

6.4.1. Technique Contribution Analysis

Further analysis is conducted by examining what percentage of threat actors use the identified techniques. This is done because there may be techniques that have a frequency higher than 1, but are only performed by a certain threat actor. The techniques that appear only once are excluded because the threat actor would have a weight of 100%.

The results can be found in Table G.1 in Appendix G. It is observed that Blackcat are often the largest contributors to the use of a given technique, which is to be expected as they are the most commonly observed group. However, the Domain Trust Discovery (Discovery) technique, which refers to the process of identifying connections between networks [14], is not observed in other threat actor activities. The absence of this technique among other known threat actors makes it a potentially strong unique identifier for Blackcat attacks.

6.5. Frequency based on sub-techniques

Figure 6.2 visualizes the results of the frequency analysis for sub-techniques in a bar chart. *The findings are similar to the analysis without sub-techniques. Notably, 21 out of the 45 sub-techniques (around 47%) were used only once. Table 6.3 lists these unique sub-techniques and the associated threat actors, representing distinct attacks.* If a threat actor used unique techniques in multiple attacks, the table indicates this with a bracketed number after the actor name.

An interesting observation is that compared to the threat actors identified in the technique section, there are different unique threat actors. *This indicates that the sub-techniques can provide additional information on the behavior of a threat actor.* An example is Lockbit (1), if only the technique level is analysed they have no unique behavior. *However, with including the level of sub-techniques they show unique behavior even among the Lockbit group themselves. This could provide information on affiliates within the groups.*

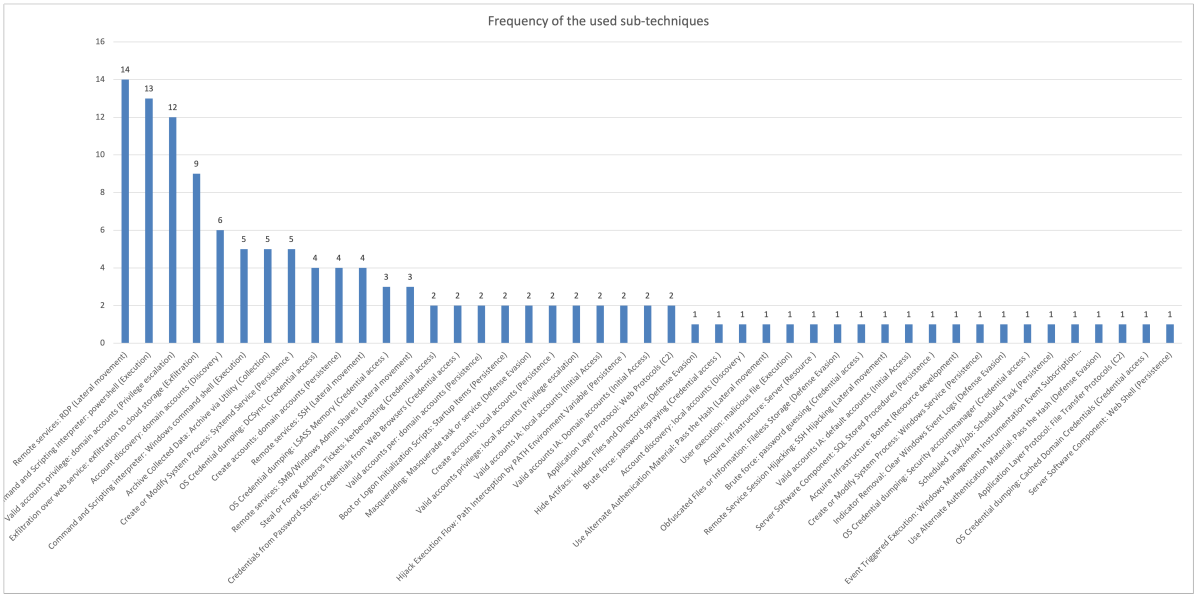

Figure 6.2: Frequency of the used sub-techniques

Table 6.3: Threat actors and their unique sub-techniques

Threat Actor	Sub-Technique	Frequency of occurrence of TA
Blackcat	Hide Artifacs: Hidden Files and Directories	5
Lockbit (1)	Brute force: password spraying, Account discovery: local accounts	3
Lockbit (2)	Use Alternate Authenication Material: Pass the Hash	3
Blackbasta	User execution: malicious file	2
Hellokittycat	Acquire Infrastructure: Server, Obfuscated Files or Information: Fileless Storage, Brute force: password guessing, Remote Service Session Hijacking: SSH Hijacking	1
Mallox	Valid accounts: default accounts, Server Software Component: SQL Stored Procedures	1
Royal (1)	Acquire Infrastructure: Botnet	1
Royal (2)	Create or Modify System Process: Windows Service, Indicator Removal: Clear Windows Event Logs	1
Monti	OS credential dumping: Security accountmanager	1
Ransomhouse	Scheduled Task/Job: Scheduled Task, Event Triggered Execution: Windows Management Instrumentation Event Subscription	1
Ragnar	Use Alternate Authentication Material: Pass the Hash, Application Layer Protocol: File Transfer Protocols	1
Blacksuit	OS credential dumping: Cached Domain Credentials	1
C3RB3R	Server Software Component: Web Shell	1

6.5.1. Sub-Technique Contribution Analysis

In Table G.2 in Appendix G, the results of the attack contribution analysis is provided. One of the first observation is that there is not a sub-technique that only a specific threat actor uses. This means that none of the sub-techniques used by themselves can be considered as a strong indicator to identify a specific threat actor.

While there are no techniques that are 100% associated with a single threat actor, the OS Credential dumping: DCSync sub-technique is 75% used by the Blackcat threat actor group. This finding suggests that analysing the sub-techniques used in an attack can be a valuable indicator for identifying the threat actor. However, sub-techniques alone cannot identify the threat actor, but in combination with other indirect indicators this could help improve the attribution process. Therefore, such sub-techniques can be considered as a potentially weak unique identifier.

6.6. Tools used frequency

The frequency analysis bar chart in Figure 6.3 shows that 18 tools are used by only one Threat Actor. Of the eighteen tools, six are utilized by threat actors that appear only once. Even though the threat actors only appear once, it is still interesting because none of the other threat actors used these tools. This demonstrates the uniqueness of the tools used and can be an indication of the correlation of a tool with a specific threat actor. Table 6.4 provides an overview of the identified unique tools used.

Interestingly, Blackcat, Lockbit, and Play, which were commonly observed in 2023 incident reports, all used unique tools in each of their attacks, as shown in table 6.4. This suggests that analysing the specific tools used can not only identify the main group of threat actors, but also provide clues that the attacker is a specific affiliate within the group. However, further research is required with a larger sample size to strengthen the connection between the tools and techniques used by these groups and their partners.

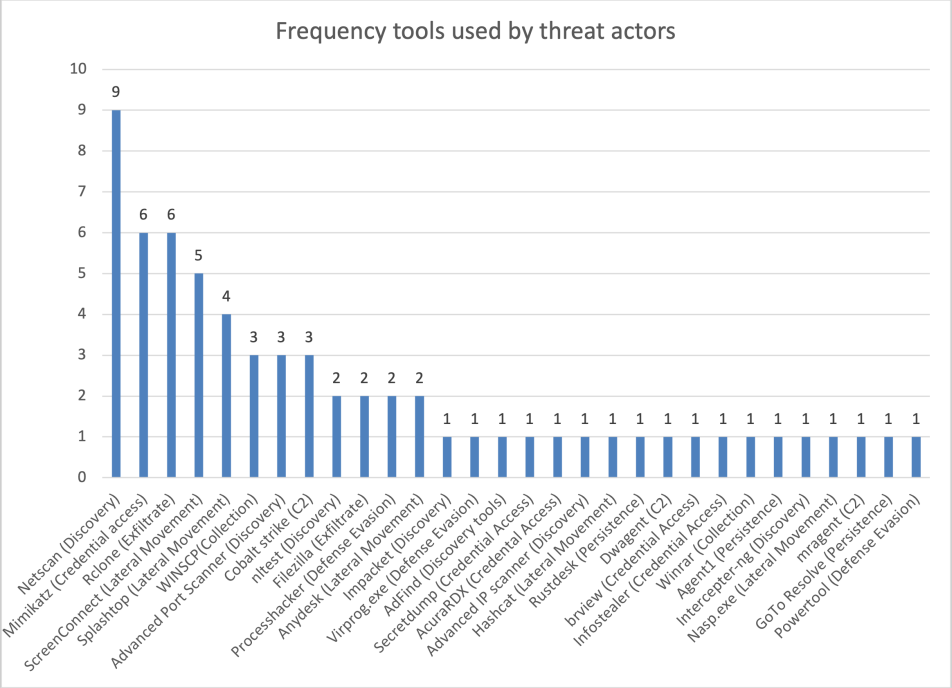

Figure 6.3: Frequency of tools used by threat actors

Table 6.4: Unique tools used by the Threat Actor

Threat Actor	Tool	TA Frequency
Blackcat	Virprog.exe (Defense Evasion), AdFind (Discovery),	5
Play	Rustdesk (Persistence)	4
Lockbit (1)	Hashcat (Lateral Movement)	3
Lockbit (2)	Secretdump (Credential Access), AcuraRDX (Credential Access), Advanced IP Scanner (Discovery)	3
Royal	Dwagent (C2), Brview (Credential Access), Infostealer (Credential Access), Winrar (Collection),	2
Ransomhouse	Impacket (Discovery), Nasp.exe (Lateral Movement), mragent (C2)	1
Monti	Agent 1 (Persistence)	1
Carver	Intercepter-ng (Discovery)	1
Blacksuit	GoTo Resolve (Persistence), Powertool (Defense Evasion)	1

6.6.1. Tool Contribution Analysis

Based on the results of the contribution analysis of the tools used, provided in Table 6.5, it can be observed that Blackcat is the only threat actor using the nltest (Discovery) tool. In Table 6.4 it became clear that Blackcat also uses AdFind (Discovery). Both tools are used to achieve Domain Trust Discovery (Discovery), which is only done by Blackcat. Therefore, the combination of using nltest and AdFind to achieve Domain Trust Discovery is considered a potentially strong indicator to correlate ransomware attacks to Blackcat.

The second observation is that Lockbit uses Filezilla (Exfiltrate) to achieve the tactic data exfiltration. As data exfiltration is a tactic that is common within ransomware attacks, the uniqueness of this tool makes this a strong indicator that can be correlated to Lockbit.

Table 6.5: Tools used by threat actors

	Blackcat	Lockbit	Play	Royal	Ransomhouse	8base	Monti	Carver	INC	ESXIArgs
Netscan (Discovery)	33,33%	11,11%	22,22%	11,11%	11,11%	11,11%	∼	∼	∼	∼
Mimikatz (Credential access)	50,00%	16,67%	∼	∼	∼	∼	16,67%	16,67%	∼	∼
Rclone (Exfiltrate)	33,33%	16,67%	16,67%	16,67%	∼	16,67%	∼	∼	∼	∼
ScreenConnect (Lateral Movement)	60,00%	20,00%	∼	20,00%	∼	∼	∼	∼	∼	∼
Splashtop (Lateral Movement)	50,00%	∼	∼	∼	∼	∼	25,00%	∼	25,00%	∼
WINSCP(Collection)	33,33%	∼	33,33%	∼	∼	∼	33,33%	∼	∼	∼
Advanced Port Scanner (Discovery)	33,33%	∼	∼	33,33%	∼	∼	∼	∼	∼	33,33%
Cobalt strike (C2)	66,67%	∼	∼	33,33%	∼	∼	∼	∼	∼	∼
nltest (Discovery)	100,00%	∼	∼	∼	∼	∼	∼	∼	∼	∼
Filezilla (Exfiltrate)	∼	100,00%	∼	∼	∼	∼	∼	∼	∼	∼
Processhacker (Defense Evasion)	∼	50,00%	∼	∼	∼	50,00%	∼	∼	∼	∼

6.7. Conclusion

In this chapter the following sub-question is explored: To what extent are indirect indicators useful in the identification of ransomware groups? The required data was extracted from incident reports of a cyber-security company, and the data was manually prepared in an excel file. Subsequently, the data was further prepared by writing a script in python to do a frequency analysis and a contribution analysis.

First, the frequency analysis was conducted separately on the techniques, sub-techniques and tools used by the threat actors, revealing that there were several techniques and tools that occurred only once. The high percentage of unique techniques (32%) and sub-techniques (47%) was the first notable observation. Especially since the interviews revealed that TTPs are too generic to be used for attributing ransomware threat actors. As many of those techniques corresponded to a threat actor that only occurred once, it was still an interesting finding as none of the other groups used these techniques. Therefore, the techniques that occurred only once are regarded as unique identifiers of the groups. In addition, in some cases the technique and tools correspond to a threat actor that has a higher frequency which makes this a strong indicator for this group.

After all the unique values were analysed, further analysis was conducted called the contribution analysis. It was analysed if a threat actor was the only user to utilize a tool/technique. In the case of the techniques and tools, it was found that Blackcat was the only threat actor using Domain Trust Discovery utilizing nltest and AdFind. Lockbit was the only threat actor to utilize the tool 'filezilla'. Making both a strong indicator for their respective groups. In the case of the sub-techniques it was found that Blackcat used OS Credential dumping: DCSync 75% of the times, therefore, this was considered as a weak indicator for Blackcat.

Lastly, it was observed that some techniques/tools were unique among the groups themselves. This insight could be a potential indicator for investigation of affiliates within ransomware groups. However, as the data was limited on these groups, further research and more data of the group is required in order to provide a conclusion.

Overall, based on these results in can be concluded that unique techniques and tools can be strong indicators for identifying ransomware groups. If these techniques/tools are encountered, then these can be used as strong indicators for the identification of ransomware groups.

7

Discussion and Conclusion

This thesis explores the research question:

> If and to what extent can the analysis of indirect indicator be utilized to improve correlating ransomware attacks with cyber-threat actors?

The aim of this research is to analyse whether indirect indicators are useful for identifying ransomware threat actors. Literature review is used to gain the basic knowledge of the attribution process of cyber-threat actors. Interviews are then used to gain knowledge of the ransomware threat actor (RTA) attribution process. Lastly, data analysis techniques, such as frequency analysis, are used to determine the impact of analysing indirect indicators on the RTA attribution process. Direct indicators are mainly used in the RTA attribution process. However, the analysis of indirect indicators showed that RTA show specific behavior that could improve the attribution process.

7.1. Discussion of findings

Throughout the research, multiple new findings and insights were discovered on ransomware threat actor attribution which enhances the overall understanding of the topic. The study highlighted the differences between cyber-threat actor attribution and ransomware threat actor attribution, showcasing the different limitations of the attribution process. The research also investigated the usefulness of the indirect indicators in the ransomware threat actor attribution process. It was shown that the tactics, techniques and procedures (TTPs) can be unique for a ransomware threat actor, opposing the statements of the experts stating that these are too generic to attribute ransomware threat actors. While the findings are promising, they are not without limitations. Therefore, this section will discuss the findings and their limitations.

7.1.1. Ransomware Threat Actor attribution process

In this research, a key contribution lies in exploring the attribution process of Ransomware Threat Actor (RTA) and Cyber-Threat Actors (CTA). The attribution process of CTA, was explored by the means of literature review, while for RTA, interviews with experts were conducted. The main findings for the CTA attribution process reveals that indirect indicators play a crucial role for the attribution process as the direct indicators are easily changed, as discussed in Section 4.4.3. This reinforces the significance of considering the behavior of CTA in the attribution process. However, in the RTA attribution process it was found that RTAs introduce themselves and mainly direct indicators were used, such as ransomware notes, communication channels and leak sites as elaborated in 5.2.3. Consequently, there is a notable absence of incentive to use indirect indicators to attribute RTAs on group level. This difference in attribution approaches is further highlighted, as in Section 4.3 it is shown that for CTA attribution identifying the country is important and that identifying the organization is most challenging. In contrast, RTA attribution, as detailed in Section 5.2.3 show that identification of group level is the lowest level and country level is not included. The understanding of attribution levels contributes to a more comprehension of the attribution processes for both CTA and RTA.

One of the limitations of this key finding is that the knowledge of the RTA attribution process is mainly based on the perspective of a cybersecurity company that does negotiation services. Since there is no standardised way to do attribution, other cybersecurity companies might have a different approach to their RTA attribution process. Therefore, the RTA attribution process might not be complete and can be expanded by considering multiple cybersecurity companies.

7.1.2. Usefulness indirect indicators

Another contribution lies in the exploration of analysing indirect indicators for the ransomware threat actor (RTA) attribution process. As discussed in the previous paragraph, direct indicators were identified as sufficient evidence for attributing RTAs at the group level. However, in Section 5.2.1 it was revealed that, according to the majority of experts, TTPs were deemed too generic for effective RTA attribution. Interestingly, a pattern emerged from experts' suggestions for improving RTA attribution, particularly emphasizing the creation of a centralized database. This database would facilitate the correlation of TTPs to RTAs, as outlined by participant E.15. Therefore, further research was conducted to what extend indirect indicators could help in the identification of ransomware groups.

The relevant data was obtained from incident reports of a cybersecurity company. The data was prepared by manual translation of human-described TTPs to universally defined TTPs, aided by the MITRE ATT&CK framework. Subsequently, a Python script was developed to structure the data, enabling a comprehensive frequency analysis presented in a bar chart. This analysis revealed unique indirect indicators that could be easily observed through the frequency distribution. Additionally, a contribution analysis was undertaken to identify whether threat actors exhibited unique techniques or tools serving as potential identifiers. The results confirmed the existence of tools/techniques unique to specific threat actors, aligning with the insights from participant E.15. Moreover, the research uncovered instances where certain techniques/tools were unique among ransomware groups, suggesting that, with a larger sample size, this could aid in correlating attacks to specific affiliates. This comprehensive analysis of indirect indicators not only contributes to refining RTA attribution processes but also lays the groundwork for advancing the understanding of affiliations within ransomware groups.

A limitation of this analysis was the size of the dataset, as there were only 27 viable ransomware incident reports in 2023. The evidence found during the digital forensics are dependent on the capabilities of the threat actor. In some cases, traces of digital evidence were deleted, resulting in an incomplete reconstruction of the cyber kill chain. This limitation highlights the improvement points of data sharing mentioned in section 5.4.2. If the data had been shared between cybersecurity companies, a more complete analysis could have been conducted and more patterns could have been found. However, the dataset used was still viable as it showed that in addition to the generic tactics, techniques and tools used, there are unique tools and techniques corresponding to a threat actor, even within the groups themselves.

A second limitation is that not all groups are observed equally in 2023. Of the total 17 threat actors identified, there were 11 which were only encountered once. Nonetheless, the data showed interesting results as the groups that were observed only once showed unique techniques not utilized by any other threat actors. This implies that of all the 27 attacks, these threat actors showed unique behavior. Therefore, the unique techniques that were used by a group with frequency one, was still considered as a unique identifier.

7.1.3. TTPs

The findings of the interviews indicated that the TTPs that are utilized by the RTAs are very generic. In addition, direct indicators were considered as sufficient as the RTAs identify themselves. This is in contrast with the findings of the literature discussed in Section 4.4.3, as it was stated that indirect indicators showed great potential. The results of this research are in line with the literature as it was observed that indirect indicators such as the tools and techniques, can be unique to RTAs. This finding can be the first step to start experimenting with machine learning techniques to develop a tool that can assist in the attribution process of RTA based on indirect indicators. While experts usually characterise ransomware Tactics, Techniques, and Procedures (TTPs) as largely generic, analysis of incident reports results in a large number of unique techniques.

One possible explanation lies in the challenges of interpreting human-written descriptions of TTPs.

These descriptions may be prone to misinterpretation due to factors such as the author's writing style and the analyst's individual perspective. This subjectivity can affect the number of unique techniques observed if different analysts interpret the same information differently.

As there was awareness of this potential bias, measures were taken to minimise its impact. Cybersecurity experts were consulted to refine our understanding of common TTPs and provide a basis for accurate identification. However, the translation of human described TTP to universal TTPs seems to be a challenge as CTI expert in Summary E.7 mentioned that the cybersecurity community should speak the same language. Therefore, further research to policies around the attribution can be conducted. This could greatly increase the consistency of the incident reports in the cybersecurity community.

7.1.4. Limited time

One of the limitations in this research was time, as in the current research the techniques, sub-techniques and tools are all analysed separately. There could be a correlation between the tool used and the technique applied, if this is the case a bigger part of the behavior of a ransomware threat actor can be found resulting in the discovery of a strong indicator. This is one way this research could be improved. In addition, this research can be expanded by considering both direct and indirect indicators. With the help of MISP, a correlation graph could be developed which provides a detailed visualisation of the cyber kill chain of an adversary. Thus, further research could be researching the effectiveness of combining direct and indirect indicators on the attribution of RTAs.

7.2. Conclusion

This section summarizes the conclusion of each sub-research questions of this study and answer the main research question.

7.2.1. Sub-question 1

The study started by answering the sub-research question:

What techniques and indicators are currently used for cyber-threat actor attribution and what are their limitations?

This research identified two indicator types for cyber-threat actor attribution: direct and indirect. Although direct indicators are susceptible to manipulation, they provide valuable but limited information. Conversely, indirect indicators have high attribution potential but require further research to definitively link them to specific actors.

The analysis revealed three primary attribution techniques: digital forensics, malware-based attribution, and indirect attribution. Direct attribution methods were found to be vulnerable to obfuscation techniques used by attackers. However, indirect attribution offers the opportunity to overcome this limitation. Within indirect attribution, two types of outcomes exist: absolute attribution, which identifies the specific actor, and relative attribution, which establishes a correlation with a previous incident. However, the reliance on extensive data for profiling makes the consistent application of indirect attribution a challenge for all threat actors. Despite these limitations, indirect attribution holds great promise for effective attribution.

Finally, this study identified four taxonomies used for cyber-threat actor attribution, as shown in table 4.10. This thesis used the technical taxonomy, which categorizes threat actors based on key characteristics relevant to the specific investigation.

7.2.2. Sub-question 2

The second sub-question of the research explores the following:

What techniques and indicators are currently used for ransomware threat actor attribution and what is the difference with cyber-threat actor attribution?

This research examined the ransomware threat actor attribution process, revealing key distinctions from cyber-threat actor attribution. While both utilize similar techniques (digital forensics, malware analysis, Cyber Threat Intelligence), their application differs. For ransomware threat actors, the focus is on direct

indicators like ransom notes and communication channels, with digital forensics employed to confirm identity through evidence like the encryptor. Conversely, for cyber-threat actors, malware analysis and cyber threat intelligence hold greater value, providing insights into attack origin and actor-specific behaviors.

This research also identified unique aspects of ransomware threat actor attribution levels. Unlike cyber-threat actors, where country-level attribution might be relevant, ransomware threat actors often operate transnationally. Additionally, identifying the specific ransomware threat actor group becomes the lowest attribution level, as they often self-identify.

Beyond identification, attribution offers broader security benefits. By combining knowledge of ransomware threat actors, simulations can be developed to test organizational defenses. This research identified weaknesses in the process, highlighting the need for a multidisciplinary approach to ransomware threat actor attribution. Notably, the absence of false flags (a tactic mentioned in literature) suggests ransomware threat actors prioritize maintaining a reputation for providing decryption keys, disincentivizing false flag campaigns.

Finally, the research identified two potential improvements:

- Centralized database with indirect indicators: Experts advocate for a central database containing ransomware threat actor profiles with indirect indicators, facilitating correlations between threat actors.
- Enhanced data sharing: As attribution relies heavily on data often spread across organizations, improved data sharing practices could significantly enhance the overall attribution process.

7.2.3. Sub-question 3

The third sub-question of the research went as follows:

To what extent are indirect indicators useful in the identification of ransomware groups?

The extent of the usefulness of indirect indicators in the identification of ransomware groups is investigated. This was achieved by extracting data from ransomware incident reports of 2023 from a cyber-security company. The data was then structured by writing a code in python to do a frequency analysis and contribution analysis.

The frequency analysis found that of the identified techniques used by ransomware threat actors, 32% were unique. For the sub-techniques, 47% of the techniques were unique. These results contradict the statements of the experts, who stated that the tactics, techniques and procedures were too generic to be used for attributing ransomware threats. Second, the techniques observed once often corresponded to a threat actor observed only once. However, they used techniques that no one else used and is therefore still considered a unique technique for that threat actor.

The second analysis was the contribution analysis, which analysed how many threat actors used a technique/tool with a frequency higher than 1. Then it was observed that groups like Blackcat and Lockbit used techniques/tools that were not used by any other group. It is therefore likely that these techniques/tools are unique to Blackcat and Lockbit. These analyses therefore show that indirect indicators can help identify ransomware groups.

7.2.4. Main research question

To answer the main research question:

If and to what extent can the analysis of indirect indicator be utilized to improve correlating ransomware attacks with cyber-threat actors?

The results of sub-question 3 showed that a significant number of (sub-)techniques (32% of the techniques and 47% of the sub-techniques) were unique to specific ransomware groups. This contradicts claims that indirect indicators are too generic to attribute ransomware threat actors. However, as highlighted in sub-question 1, challenges exist, such as the need for extensive data and the difficulty of establishing a definitive correlation.

Despite these limitations, indirect indicators offer a valuable path forward. They could potentially lead to relative attribution, identifying links between attacks without necessarily pinpointing the exact perpetrator. Furthermore, the areas for improvement identified in sub-question 2, such as setting up a centralized database with indirect indicators, could significantly improve the effectiveness of this approach. By creating and expanding the centralized database, the analysis of indirect indicators holds great promise for improving the correlation between ransomware attacks and cyber-threat actors.

7.3. Scientific contribution

The outlining of the ransomware threat actor attribution process is considered an important contribution of this study to the existing literature. While most literature explore the attribution of cyber-threat actors and their challenges, it often lacks the attribution of ransomware threat actors. This study serves as a good starting point in filling this gap, by interviewing experts and providing an overview of the ransomware threat actor attribution process.

Furthermore, this study contributes by investigating the effect of indirect indicators on correlating ransomware attacks to cyber-threat actors. The results showed that there are unique indirect indicators for RTAs, meaning that this study can be the first step to the development of an automated tool to correlate ransomware attacks to cyber-threat actors.

7.4. Societal contribution

This research contributes to society by potentially improving the effectiveness of the attribution process, which increases the chance to hold groups behind ransomware attacks accountable. By demonstrating the usefulness of indirect indicators in correlating attacks to specific actors, this research offers valuable tools for investigators. This can result in a swift recovery of the victim. Faster and more accurate attribution minimizes the impact and financial losses associated with ransomware attacks. Secondly, holding cybercriminals accountable can enhance digital public safety by potentially disrupt and dismantle criminal organization.

7.5. Future work

This section presents the recommendation for future research, drawing on both the findings and limitations of this study.

7.5.1. Direct and Indirect indicator analysis

In this work, research can be conducted to ransomware attacks to find out if analysing both direct and indirect indicators could help in correlating ransomware attacks to cyber-threat actors. With the combination of direct and indirect indicators a correlation graph could be created, in which patterns could be found that is specific to a certain cyber-threat actor.

7.5.2. Unique TTP for a group

This future work suggests the analysis of TTPs of groups that have a high frequency in the cyber landscape. One of the findings of the current research was that certain threat actors with a high frequency had unique TTPs even among the attacks of the same groups. By analysing these TTPs it might be discovered if a specific TTP could be linked to an affiliate.

7.5.3. Policies for attribution

Due to the lack of a industry standard of how the attribution process should look like, there is no guideline of what is considered a sufficient level of attribution. Developing a policy to create a standardised attribution process could greatly increase the cyber-security level. This could also help in a standardised format, in which interpreting the shared data would be made easier. Such a policy would not only improve attribution accuracy and efficiency but also contribute to a safer cyberspace for all.

7.6. Reflection on research process

The journey through this research is filled with many lessons and insights, not only about the subject, but also about the research process itself. The researcher strongly believes that the mixed research methods, specifically the explanatory sequential design, was the appropriate method to use for this topic. This method allowed for a structured approach to understanding the topic by analysing qualitative data obtained through literature review and interviews. With this knowledge, the quantitative data was extracted and explained.

However, some improvements could be made in the research process. The first important lesson from this journey is the importance of a clear definition of the research problem. This became especially apparent after changes were made to the original plan but the research design was not adjusted accordingly. This resulted in some inconsistency in the research approach and the actual narrative of the thesis. Therefore, updating and rethinking the research approach after changing the original idea would have helped streamline the process and ensure a more consistent narrative and efficient use of time.

The literature review has yielded a lot of information. The temptation to read extensively on the subject was driven by the researcher's interest in the subject and by increasing his own understanding of the subject. However, this resulted in the inclusion of information that was useful to the researcher's own understanding, but was not necessary to answer the sub-question. This experience highlighted the importance of prioritizing quality information over quantity. In the future, adopting a methodology that helps select relevant and high-quality literature could be beneficial for future research.

The data collection process taught the researcher another important lesson about balance. During the thesis, data was collected through interviews, which required a significant amount of time to conduct, analyse and summarise. Additionally, data was pulled from ransomware incident reports, which required translating the information from human-readable text into standardised cybersecurity language. Since both tasks were very demanding, long working hours were required. In the future, a more selective approach to data collection would be taken to ensure a manageable analysis process while ensuring sufficient rest.

7.7. Link with CoSEM

This graduation project examined the attribution process of cyber-threat actors from a socio-technical perspective. Based on the input from the experts, the technical needs were identified. It then analysed technical information to examine the effect of indirect indicators. This shows that the research requires a combination of technical and social knowledge to understand the attribution process of cyber-threat actors.

Furthermore, the study successfully explored the attribution process of ransomware threat actors by mapping this process and addressing its limitations. With the knowledge obtained, the study explored the potential of indirect indicators for the attribution process of ransomware threat actors. This demonstrates a typical mixed research problem-solving approach of the CoSEM program.

References

[1] Omolola A Adeoye-Olatunde and Nicole L Olenik. “Research and scholarly methods: Semi-structured interviews”. In: *Journal of the american college of clinical pharmacy* 4.10 (2021), pp. 1358–1367.

[2] Tabrez Ahmad. “Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity”. In: *Available at SSRN 3568830* (2020).

[3] Ibrahim Akdag. *Tips for Threat Hunters: Comparison of Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs)*. https://ibrahimakkdag.medium.com/tips-for-threat-hunters-comparison-of-indicators-of-compromise-iocs-and-tactics-techniques-and-47bc268fe7ff. Online; accessed 14 January 2024. 2022.

[4] Dmitri Alperovitch. *Our work with the DNC: Setting the record straight*. June 2020. URL: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[5] Hamza Alshenqeeti. “Interviewing as a data collection method: A critical review”. In: *English linguistics research* 3.1 (2014), pp. 39–45.

[6] Sana Aurangzeb et al. “Ransomware: a survey and trends”. In: *J. Inf. Assur. Secur* 6.2 (2017), pp. 48–58.

[7] Brian Bartholomew and Juan Andres Guerrero-Saade. “Wave your false flags! deception tactics muddying attribution in targeted attacks”. In: *Virus Bulletin Conference*. Vol. 9. 2016.

[8] David J Bianco. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html. Online; accessed 20 October 2023. 2013.

[9] Virginia Braun and Victoria Clarke. “Using thematic analysis in psychology”. In: *Qualitative research in psychology* 3.2 (2006), pp. 77–101.

[10] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. “The diamond model of intrusion analysis”. In: *Threat Connect* 298.0704 (2013), pp. 1–61.

[11] Alvaro Cárdenas et al. *An economic map of cybercrime*. TPRC, 2009.

[12] NW-CERT. *CERT Introduction slides*. 2023.

[13] Laurens Cerulus. *EU sanctions Russian hackers for 2015 Bundestag breach*. https://www.politico.eu/article/eu-sanctions-russias-fancy-bear-hackers-for-2015-bundestag-breach/. Online; accessed 26 februari 2024. 2022.

[14] The MITRE Corporation. *MITRE ATT&CK*. https://attack.mitre.org/resources/faq/#faq-5-0-header. Online; accessed 4 January 2024. 2016.

[15] Cryxnet. *Command and Control Servers: How They Operate and Why They’re Dangerous*. https://cryxnet.medium.com/command-and-control-servers-how-they-operate-and-why-theyre-dangerous-8b52f7032b26. Online; accessed 31 January 2024. 2023.

[16] Brian Donohue et al. *Is North Korea really behind the Sony breach?* Dec. 2014. URL: https://www.kaspersky.com/blog/sony-hack-north-korea/7072/.

[17] Maximillian Dornseif, Thorsten Holz, and Sven Müller. “Honeypots and limitations of deception”. In: *„Heute schon das Morgen sehen “, 19. DFN-Arbeitstagung über Kommunikationsnetze in Düsseldorf* (2005).

[18] H. Van Dyke Parunak. “A Grammar-Based Behavioral Distance Measure Between Ransomware Variants”. In: *IEEE Transactions on Computational Social Systems* 9.1 (2022), pp. 8–17. DOI: 10.1109/TCSS.2021.3060972.

[19] Kelsie Edie, Cole Mckee, and Adam Duby. “Extending Threat Playbooks for Cyber Threat Intelligence: A Novel Approach for APT Attribution”. In: *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE. 2023, pp. 1–6.

[20] Manuel Egele et al. “A survey on automated dynamic malware-analysis techniques and tools”. In: *ACM computing surveys (CSUR)* 44.2 (2008), pp. 1–42.

[21] Cheng Fu et al. “Coda: An end-to-end neural program decompiler”. In: *Advances in Neural Information Processing Systems* 32 (2019).

[22] Simson L Garfinkel. “Digital forensics research: The next 10 years”. In: *digital investigation* 7 (2010), S64–S73.

[23] Cyrill Gössi. “IDENTIFYING ATTACKERS BY USING MACHINE LEARNING ON UNSTRUCTURED CYBER THREAT INTELLIGENCE”. In: (2020).

[24] Juan Andres Guerrero-Saade. “Draw me like one of your french apts—expanding our descriptive palette for cyber threat actors”. In: *Virus Bulletin Conference, Montreal*. 2018, pp. 1–20.

[25] Hackerone. *Human Research Ethics*. https://www.tudelft.nl/over-tu-delft/strategie/integriteitsbeleid/human-research-ethics. Online; accessed 10 January 2024. N.D.

[26] Ray Hunt and Sherali Zeadally. “Network forensics: an analysis of techniques, tools, and trends”. In: *Computer* 45.12 (2012), pp. 36–43.

[27] Ehtsham Irshad and Abdul Basit Siddiqui. “Cyber threat attribution using unstructured reports in cyber threat intelligence”. In: *Egyptian Informatics Journal* 24.1 (2023), pp. 43–59.

[28] Taran Cyriac John et al. “Evolving malice scoring models for ransomware detection: An automated approach by utilising genetic programming and cooperative coevolution”. In: *Computers & Security* 129 (2023), p. 103215.

[29] Noel Keijzer. *Inside The World Of Ransomware, Part 1/3: Dissecting The Attack*. https://northwave-cybersecurity.com/threat-intel-research/inside-the-world-of-ransomware-dissecting-the-attack. Online; accessed 5 februari 2024. 2023.

[30] Navid Ali Khan, Sarfraz Nawaz Brohi, and Noor Zaman. “Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic”. In: (May 2020). DOI: 10.36227/techrxiv.12278792.v1. URL: https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792.

[31] Eugene Kolodenker et al. “Paybreak: Defense against cryptographic ransomware”. In: *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 2017, pp. 599–611.

[32] Ferdinand Kpieleh. *A Review of Attacker Attribution Book Chapter Series on Research Nexus in IT, Law, Cyber Security Forensics*. Creative Research Publishers, 2022, pp. 197–202. DOI: dx.doi.org/10.22624/AIMS/CRP-BK3-P32.

[33] Finn Kuusisto. “IP addresses”. In: *XRDS: Crossroads, The ACM Magazine for Students* 22.2 (2015), pp. 71–71.

[34] Robert Layton and Paul A Watters. “Indirect attribution in cyberspace”. In: *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (2015), pp. 246–262.

[35] Antoine Lemay et al. “Survey of publicly available reports on advanced persistent threat actors”. In: *Computers & Security* 72 (2018), pp. 26–59.

[36] Moira Maguire and Brid Delahunt. “Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars.” In: *All Ireland Journal of Higher Education* 9.3 (2017).

[37] FireEye Mandiant. *APT28 malware: Russia’s Cyber Espionage Operations Report*. Oct. 2014. URL: https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

[38] G Manohar Venkat, Saranya Chandran, and TU Arjun. “Malware Reverse Engineering to Find the Malicious Activity of Emotet”. In: *Recent Developments in Electronics and Communication Systems: Proceedings of the First International Conference on Recent Developments in Electronics and Communication Systems (RDECS-2022)*. Vol. 32. IOS Press. 2023, pp. 167–168.

[39] Vasileios Mavroeidis et al. “Threat actor type inference and characterization within cyber threat intelligence”. In: *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE. 2021, pp. 327–352.

[40] Yangyang Mei et al. “A Review of Attribution Technical for APT Attacks”. In: *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*. IEEE. 2022, pp. 512–518.

[41] Per Håkon Meland, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. “The Ransomware-as-a-Service economy within the darknet”. In: *Computers & Security* 92 (2020), p. 101762.

[42] Adam Meyers. *Danger close: Fancy bear tracking of ukrainian field artillery units*. Dec. 2016. URL: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[43] Hamad Al-Mohannadi, Irfan Awan, and Jassim Al Hamar. “Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence”. In: *Service Oriented Computing and Applications* 14 (2020), pp. 175–187.

[44] Ricardo Misael Ayala Molina et al. “On Ransomware Family Attribution Using Pre-Attack Paranoia Activities”. In: *IEEE Transactions on Network and Service Management* 19.1 (2022), pp. 19–36. DOI: 10.1109/TNSM.2021.3112056.

[45] Milton Mueller et al. “Cyber attribution”. In: *The Cyber Defense Review* 4.1 (2019), pp. 107–122.

[46] Andrew Nicholson, Helge Janicke, and Tim Watson. “An initial investigation into attribution in SCADA systems”. In: *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*. 2013, pp. 56–65.

[47] Umara Noor et al. “A Machine Learning based Empirical Evaluation of Cyber Threat Actors High Level Attack Patterns over Low level Attack Patterns in Attributing Attacks”. In: *arXiv preprint arXiv:2307.10252* (2023).

[48] Umara Noor et al. “A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise”. In: *Future Generation Computer Systems* 96 (2019), pp. 227–242.

[49] Philip O’Kane, Sakir Sezer, and Domhnall Carlin. “Evolution of ransomware”. In: *Iet Networks* 7.5 (2018), pp. 321–327.

[50] Ayodeji Ogundiran et al. “A Framework to Reconstruct Digital Forensics Evidence via Goal-Oriented Modeling”. In: *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*. IEEE. 2023, pp. 1–11.

[51] Bernardi Pranggono and Abdullahi Arabo. “COVID-19 pandemic cybersecurity issues”. In: *Internet Technology Letters* 4.2 (2021), e247.

[52] Venkata Sai Charan Putrevu et al. “A Framework for Advanced Persistent Threat Attribution using Zachman Ontology”. In: *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*. 2023, pp. 34–41.

[53] Li Qiang et al. “Framework of cyber attack attribution based on threat intelligence”. In: *Interoperability, Safety and Security in IoT: Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers 2*. Springer. 2017, pp. 92–103.

[54] Klaus-Peter Saalbach. “Attribution of cyber attacks”. In: *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (2019), pp. 279–303.

[55] Dilip Sahoo. “Cyber threat attribution with multi-view heuristic analysis”. In: *Handbook of Big Data Analytics and Forensics* (2022), pp. 53–73.

[56] Nolen Scaife et al. “Cryptolock (and drop it): stopping ransomware attacks on user data”. In: *2016 IEEE 36th international conference on distributed computing systems (ICDCS)*. IEEE. 2016, pp. 303–312.

[57] Mathew Schwartz. *French Officials Detail ’Fancy Bear’ Hack of TV5Monde*. https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983. Online; accessed 26 februari 2024. 2017.

[58] Daniele Sgandurra et al. “Automated dynamic analysis of ransomware: Benefits, limitations and use for detection”. In: *arXiv preprint arXiv:1609.03020* (2016).

[59] Jawwad A Shamsi et al. “Attribution in cyberspace: techniques and legal implications”. In: *Security and Communication Networks* 9.15 (2016), pp. 2886–2900.

[60] Youngsup Shin et al. “ART: automated reclassification for threat actors based on ATT&CK matrix similarity”. In: *2021 world automation congress (WAC)*. IEEE. 2021, pp. 15–20.

[61] Sikich. *THE ROLE OF DIGITAL FORENSICS IN FIGHTING AND PREVENTING CYBERCRIME*. https://www.sikich.com/insight/the-role-of-digital-forensics-in-fighting-and-preventing-cybercrime/. Online; accessed 26 februari 2024. 2023.

[62] Florian Skopik and Timea Pahi. “Under false flag: using technical artifacts for cyber attack attribution”. In: *Cybersecurity* 3 (2020), pp. 1–20.

[63] Noor Thamer and Raaid Alubady. “A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research”. In: *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. IEEE. 2021, pp. 210–216.

[64] *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. `https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and`. Online; accessed 26 februari 2024. 2018.

[65] Qinqin Wang, Hanbing Yan, and Zhihui Han. “Explainable apt attribution for malware using nlp techniques”. In: *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*. IEEE. 2021, pp. 70–80.

[66] Qinqin Wang et al. “APT attribution for malware based on time series shapelets”. In: *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. 2022, pp. 769–777.

[67] Arun Warikoo. “The triangle model for cyber threat attribution”. In: *Journal of Cyber Security Technology* 5.3-4 (2021), pp. 191–208.

[68] Mike Wendling. *Conversations with a hacker: What Guccifer 2.0 Told me*. Jan. 2017. URL: `https://www.bbc.com/news/blogs-trending-38610402`.

[69] David A Wheeler and Gregory N Larsen. “Techniques for cyber attack attribution”. In: *Institute for Defense Analysis* (2003), p. 2.

[70] Jianwei Zhuge et al. *Studying malicious websites and the underground economy on the Chinese web*. Springer, 2009.

A

Overview of used articles for sub-question 1

Table A.1: Overview of all used articles used in the cyber-threat actor attribution research

Author	Title	From query?
[40]	A Review of Attribution Technical for APT Attacks	Yes
[54]	Attribution of Cyber Attacks	Yes
[48]	A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise	Yes
[27]	Cyber threat attribution using unstructured reports in cyber threat intelligence	Yes
[55]	Cyber Threat Attribution with Multi-View Heuristic Analysis	Yes
[60]	ART: Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity	Yes
[59]	Attribution in cyberspace: techniques and legal implications	Yes
[7]	Wave your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks	No
[42]	Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units	No
[47]	A Machine Learning Based Empirical Evaluation of Cyber Threat Actors High Level Attack Patterns over Low Level Attack Patterns in Attributing Attacks.	Yes
[43]	Analysis of Adversary Activities Using Cloud-Based Web Services to Enhance Cyber Threat Intelligence	No
[32]	A Review of Attacker Attribution Book Chapter Series on Research in Nexus in IT, Cyber Security Forensics.	Yes
[33]	IP Adrresses	No
[34]	Indirect Attribution in Cyberspace	No
[39]	Threat Actor Type Inference and Characterization within Cyber Threat Intelligence	No
[45]	Cyber Attribution	Yes
[50]	A Framework to Reconstruct Digital Forensics Evidence via Goal-Oriented Modeling	Yes
[52]	A Framework for Advanced PersistentThreat Attribution using Zachman Ontology	Yes
[62]	Under Flasge FLag: Using Technical Artifacts for Cyber Attack Attribution	No
[67]	The Trianle Model for Cyber Threat Attribution	Yes
[17]	Honeypots and Limitations of Deception	No
[18]	A Grammar-Based Behavioral Distance Measure Between Ransomware Variants	Yes
[19]	Extending Threat Playbooks for Cyber Threat Intelligence: A Novel Approach for APT Attribution	Yes
[20]	A Survey on Automated Dynamic Malware-analysis Techniques and Tools	No
[21]	Coda: An end-to-end Neural Program Decompiler	No
[22]	Digital Forensics Research: The next 10 years	No
[24]	Draw Me Like One of Your French APTs-Expanding our Descriptive Palette for Cyber Threat Actors	No
[26]	Network Forensics: an Analysis of Techniques, Tools, and Trends.	No
[35]	Survey of Publicly Available Reports on Advanced Persistent Threat Actors.	Yes
[39]	Threat Actor Type Inference and Characterization within Cyber Threat Intelligence	Yes
[44]	On Ransomware Family Attribution Using Pre-attack Paranoia Activities	Yes
[53]	Framework of Cyber Attack Attribution Based on Threat Intelligence	No
[69]	Techniques for Cyber Attack Attribution	No

B

In depth explanation of the attribution techniques

B.1. Digital forensics

[59] explains that when the process of forensics is executed over already stored information (static data), the process can be described as dead forensics. Two common examples of forensics on static data are storage-based analysis and RAM-based analysis. However, both cases are deemed expensive and infeasible because of the increase storage capacity and data distribution techniques such as the cloud. In addition, RAM-based analysis is expensive because they require data layout to be conserved across different programs [22].

B.1.1. Forensics on dynamic data or Network forensics

Forensics on dynamic data is defined as digital forensics applied over streaming and dynamic data [59]. Network forensics is an active example of live forensics when attributes such as network packets or network logs are analyzed in real time to detect intrusion and collect criminal activities.

Traceback and logging

This technique involves tracing an IP packet back to its original source. To accomplish this there are two methods that can be applied: packet marking and packet logging. In packet marking, the original source can be traced back by attaching specific information to every packet of each network device (like routers or switches). Packet logging stores valuable data at the network device, which allows for tracing the packet to its source [59]. However, these methods are limited in their use of attribution, because of techniques like spoofing and anonymization [46].

Deceptive techniques

A honeypot can be set up to deceive attackers. A honey pot is a system or a set of resources, which is purposely set up to analyze and study attack patterns. This can then be used to closely monitor the network decoy that is used for distracting adversaries and analyzing their behavior [59]. The effectiveness of this techniques is related to the ability of the attacker to detect the environment of the honeypot. An experienced attacker may be able to detect honeypot environment which makes it more difficult to track the attacker's activities [17].

Obtained information from the system and network logs could vary in usability and their amount. It is unlikely that an attacker leaves clear identification marks in logs. However, the logs can be used in order to obtain information about the attacker such as the methods used [59].

Network forensics has many opportunities for advancements, however, it requires extensive experience and skill to attribute the origin of an attack [59]. Network forensics can be integrated with other techniques such as adaptive firewalls and malware and social network analysis [26].

B.1.2. Malware analysis

Static analysis

In static analysis, the malware code is analysed without executing the program. It could either be the source code of the malware or the disassembled binary. Then known signatures of the code are compared in order to detect malicious code [59]. The usability of static analysis is limited because of anonymity, privacy providing tools, code obfuscation techniques [66]. This makes it difficult to find or identify useful information from a malicious activity [59]. Therefore, because of the obfuscation techniques static analysis becomes limited.

Dynamic analysis

In contrast to static analysis, dynamic analysis analyses the malware in a controlled environment such as a virtual machine (VM) [59]. This allows dynamic analysis to overcome the limitation of static analysis, since the code can be directly executed in the VM environment. Various techniques such as function parameter tracking and function call monitoring are utilized in order to detect malicious activity within the malware [66]. In Table B.1 and overview of the major techniques of dynamic analysis is provided.

Dynamic analysis also has limitations. The analysis will be conducted while the program is being executed which limits the malware analysis only to the executed paths in the code [20]. Specifically, due to the fact that dynamic analysis is largely performed in an isolated environment such as a VM or a debugger, malware can be obfuscated by alternating the execution path upon detection of the execution environment [66].

Table B.1: Techniques for dynamic malware analysis by [20].

Technique	Description
Function call monitoring	Function calls form a program are intercepted and monitored for malicious activity.
Parameters' tracking	Analyze input and output parameters of a function.
Information flow tracking	Track the flow of data in the program.
Instruction trace	Analyze sequence of machine instructions while the program is being analysed.

Similarity-based attribution

Comparing malware used in an attack can be compared to previous cases to identify the source of an attack. This concept is known as similarity-based attribution. [16] explains a case in which similarities were found between in malware code during the hack of Sony and other hacks attributed to North Korea.

Despite the successful case described by [16], there are limitation to similarity-based attribution. A limitation of similarity-based attribution is that similarity with a previously known malware does not necessarily attribute an attack to the previously attributed attacker [59]. The reason for this is because signatures of previously used malware can also be stolen or copied in order to mislead an attack [59].

Reverse engineering

Reverse engineering is the process of analysing the malware to understand its behavior and characteristics [38]. One of the limitation of reverse engineering is the required specialized knowledge and skills. The available expertise in reverse engineering is limited, which makes the reverse engineering process challenging [21].

B.1.3. Indirect attribution techniques

Behavioral analysis

Behavioral analysis can be useful in identifying malicious sources, however, it is depended on the availability of data. Therefore, this technique is often combined with other techniques [59].

Linking with geo-political scenarios

In some cases, cybercrimes are motivated by political ideologies. Correlating a cyberattack to a geo-political motive may provide some information about the origin of a cyberattack [59]. This link is often not a strong one, however, it might be a valuable source to initiate an attribution process.

Cyber-threat intelligence

Threat intelligence is a type of evidence-based knowledge, including the context of the threat, the mechanism of attack, the threat indicators and impact of the attack, the threat or danger that exists or may occur to the item in question, and the countermeasures made by the subject in response to that threat or danger [40]. Cyber-threat intelligence attribution currently faces challenges such as differences in threat intelligence sources, fluctuating threat intelligence data quality, large data volumes, and complex correlation relationships [53].

C

Generating the interviews

C.1. Interview setup

As discussed in Section 3.2 conducting interviews with experts regarding cyber-threat attribution is part in solving sub-question 2. In addition, during the literature review it was observed that there is an absence of extensive publications on the topic of attributing ransomware groups [5]. Therefore, conducting interviews proves to be an effective method for generating insights into experiences and obtaining expert information.

The process of developing the interviews will be discussed. Section C.1.1 discusses the roadmap of the development of the interview. In Section C.1.2 the difference phases of the interview is outlined.

C.1.1. Generating the interviews: The Roadmap

Because the interviews also involve humans, it is very important to gain knowledge about the potential risks of collecting data from human subjects. Therefore, the first stage of generating the interviews was to comply with the rules of the TU Delft Human Research Ethics Committee. This step ensures that legal requirements for data privacy are met, as well as all professional and ethical standards relevant to this research. [25].

The second phase of this interview development is selecting the appropriate structure for the empirical research. The goal of the interviews is to increase the understanding of the perspective of the experts on cyber-threat attribution. According to [1] the best framework to achieve such a goal would be the semi-structured interviews. As this would allow the interviewer to ask specific questions but provides freedom to the interviewee to elaborate on specific details, sharing experiences, and provide insights [1]. Therefore, the semi-structure interview is chosen as the foundational framework.

In phase three the questions were formulated based on information that could not be found in the literature. These questions were first checked by the first supervisor of TU Delft. Subsequently, the interview questions were sent to the supervisor of the cybersecurity company. By doing this, it was made sure that the question would provide sufficient information to answer sub-question 1. Lastly, during the interviews some minor alterations were made to further clarify the questions.

C.1.2. Generating the interviews: the content

The first step in each interview was providing transparency regarding the information processing. This was accomplished by going through the informed consent which provides the participants insights about how the data is processed.

C.1.3. Semi-structured

The semi-structured interviews allows to gather diverse data. The questions were designed based on questions that raised during the literature review of sub-question 1. Therefore, the questions are formulated based on the information that could not be found in the literature review. To avoid biased

answers of the participants the questions are designed in such a way that the interviewee can freely discuss details, share experiences and provide insights.

In order to give structure to the interview, the questions are separated in segments based on the area of interest. This resulted in six different segments, in which the goal of the segments is to progressively explore different aspects of cyber threat attribution. This helps in obtaining a comprehensive and nuanced understanding of the interviewee's expertise and experiences in the field. The questions and the segments are provided in Table C.1. Furthermore, for all participants the questions were the same.

Segment one is designed to cover the questions that raised during the literature review. Since it was observed that there was limited information regarding the attribution process of ransomware threat actors (RTA), this segment will put an emphasis on RTA. In addition, the differences between other CTA are explored. Understanding the attribution process regarding RTAs is crucial in determining the feasibility and the scope of this research.

In segment two emphasis was put on the strength and limitations of the attribution process from the perspective of the experts. These questions allowed the participant to share their experiences and challenges which can lead to valuable information regarding the attribution process of ransomware groups. In addition, these type of questions can help the expert think of unique situations that required a different approach.

The last segment provides information on the experts opinion on how to improve the attribution process.

Table C.1: Interview questions

Segment 1: Overview of Cyber Threat Attribution
1. How are cyber threat actors typically categorized based on their characteristics and traits?
2. Can you describe the techniques or methods that your organization currently employs for cyber threat actor attribution of ransomware groups?
3. In your experience, which indicators are typically considered when attributing a cyber threat to a ransomware actor or group?
4. Are there differences in cyber threat attribution techniques when dealing with different types of threat actors, such as state-sponsored groups, cybercriminals, or hacktivists?
5. Are there different levels of attribution? If so, do you observe differences in the level of attribution when comparing different organizations, such as law enforcement and cybersecurity companies?
6. At what level is the ransomware attacker identified?
Segment 2: Strengths and Limitations
7. What do you consider the main strengths of the attribution techniques or methods you use?
8. What limitations or challenges have you encountered when attempting to attribute cyber threats to specific actors or groups?
9. Can you provide an example of a recent or notable case of cyber threat attribution you have worked on, and walk through the process of attribution, including the techniques and indicators used?
10. In your opinion, how important is it to consider the potential risk of false attribution in the field of attributing cyber threat actors, and how do you mitigate this risk?
11. Are there specific legal or ethical considerations that impact your approach to attributing cyber threat actors, and if so, how do they influence your work?
12. Can you share examples of cases where attribution efforts did not lead to a clear identification of the threat actor? What were the main challenges in these cases?
Segment 3: Adaptation and Future Developments
13. How do you stay informed about evolving techniques and indicators in the field of attributing cyber threat actors, and how do you adjust your methods accordingly?
14. In your opinion, what are the most significant areas of improvement or development needed in the field of attributing cyber threat actors?

D

Thematic Analysis: Setup

The thematic analysis is utilized in order to analyse the findings of the interviews. This analysis, as described by [9], is a six-phased guide for thematic analysis. Section D.1 will explain these steps and link them to the own obtained data in this research. Subsequently, the results of the thematic analysis will be discussed.

D.1. Explanation of the six phases

D.1.1. Phase 1: Become familiar with the data

The first step in the thematic analysis is becoming familiar with the data. This is achieved by reading and re-reading the transcripts. This step was applied in this research by going over the interview transcripts multiple times. To further help the process of familiarization, notes and early impressions were made.

D.1.2. Phase 2: Generate initial codes

The next step was systematically coding interesting and relevant data. [9] states that the coding depends on whether the themes are more 'data-driven' or 'theory driven'. Since the interview was designed based on the questions that raised during the literature review, this research had the emphasis on theory driven approach. Therefore, each segment of data that was relevant to or captured something interesting about the research question was coded. In addition, open coding was applied, indicating the there were no pre-set of codes, but the codes were created and modified as the coding process progressed.

D.1.3. Phase 3: Searching for themes

In this step themes are identified based on patterns, connections and recurring concepts within the coded data. Codes that clearly fitted together were put together in a theme.

D.1.4. Phase 4: Review themes

Phase four included the refinement of the themes. The themes should be coherent and they should be distinct from each other. Therefore, the following questions were asked during the refinement of the themes inspired by the research of [36].

- Do the themes make sense?
- Does the data support the themes?
- Am I trying to fit too much into a theme?
- If themes overlap, are they really separate themes?
- Are there themes within themes (subthemes)?
- Are there other themes within the data?

D.1.5. Phase 5 & 6: Defining and naming themes & Report

The final steps of the analysis are to develop the final themes that will be discussed in the coming sections. Frequency analysis is added to strengthen the identified and formulated themes. The addition of the frequency analysis makes it visible how many participants mention a theme, which helps clarify the meaning of a specific theme.

E

Summary of Interviews

E.1. Lead Digital Forensics

The interviewee provides insights into the difficult process of attributing cyber threats, particularly focusing on ransomware attacks and the challenges posed by advanced persistent threats (APTs). They start by emphasizing the significance of ransom notes left by attackers, which often contain contact details and communication channels. These channels, usually on the dark web, serve as identifiers for specific threat groups.

Communication platforms become critical in understanding the identity of threat actors, with ransomware notes offering initial clues. The interviewee states that the communication platform can only be managed by the specific groups. However, the interviewee acknowledges the need for validation, as copycats can replicate ransom notes. They highlight the reliability of communication channels, assuming that each group manages distinct channels.

In cases where ransomware note details are insufficient, the interviewee discusses the option of analyzing the ransomware itself. This involves identifying characteristic pieces of code, requiring the establishment of a reference base. The interviewee mentions running ransomware in a secure environment for analysis and interpretation, emphasizing the unique challenges posed by ransomware developers and affiliates.

Attribution complexities arise, particularly in distinguishing between nation-state goals (disruption or espionage) and financially motivated ransomware actors. Group-level identification is often prioritized, with affiliates intentionally remaining unidentified. The interviewee touches on the use of affiliate IDs embedded in ransomware and the challenges of accessing relevant databases.

The interviewee underscores the binding nature of sanction lists at the group level. They discuss the assumption of communication channel reliability, though cautioning about potential copycats. The challenge arises in cases with limited threat actor information, prompting consideration of the effort required for a thorough investigation.

E.2. CTI Lead

The interviewee detailed the organization's approach to attribution, involving in-house research, collaboration with partners, and reliance on MITRE techniques. Emphasis was placed on profiling behavior, utilizing intelligence networks, and accessing the latest research from intelligence providers.

The interviewee discusses the challenges and nuances of cyber threat intelligence, emphasizing that intelligence work is not straightforward and often involves assessing probabilities rather than certainty. The focus is on Tactics, Techniques, and Procedures (TTPs) as crucial indicators, acting like fingerprints for cyber threat groups. The interviewee highlights the importance of key elements in cyber investigations, such as ransom notes and pieces malware. The Pyramid of Pain, a framework for categorizing indicators based on their persistence, is mentioned, indicating its significance in the investigation pro-

cess. The discussion suggests a dynamic and layered approach to cyber threat investigations, where the choice of where to begin depends on the specifics of each case. The text also touches on the challenges of attributing cyber threats to specific groups and the need to carefully analyze evidence, especially when dealing with closely related threat families.

The interviewee discusses the influence of motivation on the Tactics, Techniques, and Procedures (TTPs) employed by different threat actor groups. It contrasts the characteristics of ransomware groups, primarily driven by financial motives and engaging in quick and noisy activities, with nation-state groups focused on gathering information and maintaining undetected access. The distinction is made between ransomware groups purchasing access and cybercriminals encrypting data rapidly, while nation-states independently ensure access, completing the cyber-kill chain through Advanced Persistent Threats (APTs). The central idea is that the motives of threat actors play a crucial role in shaping their TTPs.

Group-level attribution was deemed more practical, with identifying the country challenging and often speculative. Ransomware as a Service (RaaS) and the diverse origins of group members highlighted the complexity of pinpointing geographical origins.

The interviewee underscored the strengths in experience, leveraging accumulated knowledge, incident responses, and archives. The organization's holistic approach, encompassing a Security Operations Center (SOC), Red Team, and Cyber Threat Intelligence (CTI), contributed to effective attribution techniques.

Challenges included encountering new scenarios, relying on premium services or potentially outdated open-source information, and the time-consuming nature of such processes. However, a robust network compensated for these limitations.

An espionage case involving APT actors posing as ransomware groups illustrated the challenges of attribution. The importance of motives, the use of counter techniques, and the concealment of true objectives showcased the complexities faced in such scenarios.

The text highlights the risks associated with misattribution in the context of threat attribution for sanction controls. Specifically, the concern is about attributing a threat group incorrectly, which could lead to unintended consequences, especially when dealing with sanctioned entities. The potential impacts include legal scrutiny and non-compliance with regulations, posing significant risks for both the organization and the victim. The interviewee also notes that in cases where threat actor attribution is not linked to ransomware payments but is associated with reputational damage, the severity of consequences depends on the specific circumstances.

Legal and ethical considerations were acknowledged, with ethical dilemmas arising from potential hacking into criminal infrastructures and the use of investigation data. The interviewee highlighted the need for careful decision-making and adherence to legal frameworks.

Attribution challenges occurred when dealing with insufficient data, restricted access, or trails leading to countries with no available answers. The consideration to stop attribution efforts depended on the feasibility of obtaining the last puzzle piece.

Staying informed about evolving techniques involved following the threat intelligence lifecycle, understanding consumer needs, utilizing relevant sources, analyzing data, and constant evaluation. Continuous learning is crucial to adapt methods accordingly.

The interviewee identified areas for improvement, including efficiently utilizing past data for Cyber Threat Intelligence (CTI), navigating legal aspects, and extracting knowledge from past incidents. These improvements could enhance forensic readiness and contribute to attributing currently unattributable actors.

E.3. Digital Forensics

The interviewee highlighted the organization's current methods for cyber threat actor attribution. Ransomware attribution is relatively straightforward since they identify themselves by leaving a ransom note. If this is not the case, then the use of similar tools and methods by ransomware groups makes it difficult to make a distinction. If there is a case that where attribution must be done on individual level,

the evidence will be forwarded to the law enforcements. APT cases are more difficult to spot, so it is rarely encountered.

The interviewee emphasizes the unique challenges posed by APT cases. While APT hunting involves using the pyramid of pain, ransomware groups, structured as RaaS with various roles, make it difficult to apply typical Tactics, Techniques, and Procedures (TTPs) distinctions. Nation-states, on the other hand, present a more stable environment.

Distinguishing cyber actors extends beyond groups like ransomware, which are categorized based on their motives. Some of these actors engage in business email compromise for financial gains. Such actors, are often individuals or groups of individuals and exhibit consistent operational styles, making the pyramid of pain a valuable tool.

Attribution is a difficult process, with group-level identification being more common, occasionally extending to a country level. Indicators like IP addresses, negotiation styles, and language nuances may provide clues, but attribution at an individual level remains challenging. In addition, configuration files of the adversary are often found on the system of the victim, this can provide indicators, such as the keyboard lay out, on the origin of the attacker. In that sense is country level doable but not relevant.

Forensic investigation emerges as a vital tool, aiding in understanding the modus operandi, tactics, and tools of threat actors. The evolving trend in cyber threats, where groups adopt diverse methods over time, necessitates continuous adaptation.

Within the red team, realistic scenarios are simulated, highlighting the need for continuous engagement in hacking methodologies. However, the cybersecurity company faces limitations due to its youth, necessitating 24/7 dedication, coupled with legal restrictions.

The interviewee shares a notable case involving a client who paid a ransom without initially detecting sanctions. Three years later, complications arose when the insurance company sought to recover the money after placing the group on the sanctions list. This emphasizes the critical importance of accurate attribution for legal and mitigation purposes.

Ethical challenges arise in investigating hacker login credentials, with the interviewee acknowledging the limitations on enhancing attribution by placing a tap in a threat actor's system.

The interviewee underscores the significance of staying updated through various sources, including news, Twitter, websites, and blogs. Furthermore, the interviewee emphasizes the importance of effective collaboration between private and public entities, such as the police and NCSC, highlighting the potential risks associated with information being leaked on the internet.

E.4. Digital Forensics

The interviewee highlights multiple methods for attributing cyber threats. They begin with the basic attribution obtained from ransomware notes, where threat groups often disclose their identity. Communication channels and Tor websites further validate their claims. Additionally, analyzing ransomware executables, including examining keyboard layouts, provides indicators for potential geographic origins. The importance of forensic investigation and monitoring post-incident is emphasized.

The Pyramid of Pain is introduced as a framework for attribution, with IP addresses and TTPs considered significant. While IP addresses can be indicative, the emphasis is on Tactics, Techniques, and Procedures (TTPs) for a more accurate attribution. The interviewee mentions the challenges of false flags, such as groups setting different keyboards to mislead attribution. However, the interviewee states that TTPs are not often looked at with ransomware threat actors due to high similarities caused by the RaaS model.

Attribution involves different levels, including country, group, affiliate group, and individual. In ransomware cases, identification is primarily at the group level due to the structure of ransomware operations. Country-level attribution is often an assumption based on working hours and other characteristics.

Precise attribution is crucial for understanding the threat landscape, negotiating with threat actors effectively, and determining the appropriate response. However, the interviewee notes that within their

organization, the priority for precise attribution is higher for processes like payment and sanction checks rather than overall investigation and reporting.

The interviewee acknowledges the difficulty of initially determining the identity of threat actors. They stress the need to know who is involved to find relevant indicators but recognize the paradox that indicators are required to identify threat actors. Challenges arise when dealing with small or unknown groups that don't explicitly identify themselves, leading to low-confidence indicators.

Considering the potential risk of false attribution is essential, but the interviewee notes that the importance depends on the objective. If the goal is apprehension, a high level of certainty is required. However, for general identification, there can be a margin of error, with a willingness to reevaluate and correct assumptions.

The interviewee mentions limited legal and ethical considerations within their role, emphasizing that sensitive information, if discovered (like an IP address linked to a physical location), would be handed over to law enforcement.

Staying informed about evolving techniques is crucial. The interviewee keeps updated through blog posts, professional networks, and shared information from colleagues.

Actors are categorized into state-sponsored groups (espionage), financially motivated groups (ransomware), politically motivated groups, and script kiddies. The interviewee notes the blurred line between state-sponsored actors and financially motivated groups.

E.5. Digital Forensics

The interviewee discussed their organization's cyber threat attribution methods. Currently, Google, article reading, and forensic investigation are employed as there's no dedicated tool, with ongoing efforts in that direction. The tools include MISP, IntelForce 1, Google searches, and exploring forensics, sigma/yara rules, and IP lookup websites.

In attributing ransomware threats, indicators like IP addresses, directories, ransomware notes, communication channels and tools play a crucial role. Notably, HelloKittyCat's hit-and-run style and Revil's use of Qbot phishing, Cobalt Strike, and ransomware serve as examples. The interviewee stressed the significance of analysing TTPs translated into the MITRE ATT&CK matrix. This could help in determining the use of specific TTPs to certain RTAs.

Regarding different threat actors, the interviewee mentioned that while techniques remain similar, APTs may mimic cybercriminals to conceal their objectives.

Attribution levels were discussed, with identification primarily at the group level. Specific examples included detecting an IP address from KPN or Ziggo (home IP address) and finding a pseudonym on the dark web.

Strengths of their attribution techniques include the ability for individuals to gather significant intelligence. Challenges, on the other hand, involve the lack of a central platform/database storing indicators, impacting the efficiency of incident response.

An illustrative case involved attributing HelloKittyKat instead of HelloKitty based on the ransomware note and wormable nature of the sample. The FBI's report and the discrepancy in modus operandi further supported this attribution.

The interviewee acknowledged the potential risk of misattribution, especially with APTs' slow operations affecting data theft estimates.

In terms of legal or ethical considerations, the interviewee stated it doesn't significantly impact their work.

Challenges in attribution efforts were discussed, specifically in a case involving the use of ransomware but with suspected APT activity. The nature of the ransomware, the lack of demand of ransom and the only information left behind was a text with "contact me" lead towards a potential APT actor instead of a ransomware actor. The lack of online information and an outdated exploit added to the challenges of attributing this actor, and lead to no result.

Staying informed involves gaining experience and collaborating with colleagues.

A proposed improvement is the creation of a shared database to enhance efficiency in searching for TTPs specific to ransomware threat actors.

E.6. Digital Forensics

In the interview, the expert outlines the organization's techniques for cyber threat actor attribution. The process often begins with ransomware notes, indicating the group's identity. Communication channels provided in these notes, along with banners and icons and indicators emerging during negotiations, contribute to the identification of threat actors. Additionally, infrastructure shared by multiple victims points to attacks by the same group.

When attributing cyber threats, indicators like Command and Control (C2) servers and bitcoin wallets are considered. While C2 servers are encountered frequently, attributing based solely on these indicators can be challenging. Bitcoin wallets, split and consolidated in a specific manner, offer an alternative for attribution.

The interviewee emphasizes that the attribution process is primarily driven by the need for sanction checks, ensuring money is not transferred to sanctioned entities. They discuss the importance of precision in this process to avoid legal consequences.

Differences in attribution techniques for various threat actors are highlighted. Ransomware groups, characterized as opportunistic, differ from state-sponsored actors with more prolonged objectives. The noisy nature of ransomware attackers contrasts with the stealthy operations of state actors.

The interviewee points out the difficulty in attributing at the individual level due to frequent name changes by ransomware groups. Building profiles for individuals requires consistent incidents, which is challenging in a dynamic operational environment. This makes identifying ransomware attackers on group level more viable. Determining the country level in a ransomware attack is difficult, especially due to RaaS which created multiple roles in a ransomware attack. However, in the case of an APT looking at a country level is viable since you can look at working hours and at the malware. For example, Russians and Chinese use very different malwares.

Strengths of the organization's attribution methods lie in their simplicity and reliance on direct information from ransomware notes. However, limitations include the reluctance to invest in proactive measures such as server searches and fingerprinting due to financial constraints.

A notable case is presented, where the organization follows the cyber-kill chain in a ransomware incident. Examining intrusion, movement within the network, and monetization stages helps in attribution. At the end of the technical summary a summary of the general steps to solve a case is provided.

The potential risk of false attribution is acknowledged, particularly concerning sanction checks. From a forensic perspective, misattribution impacts the investigation's goals and efficiency. So, the goal of your attribution is a determining factor in severity of consequences of misattribution.

Legal and ethical considerations arise, particularly regarding sanction checks. Ethical dilemmas include the transparency of attribution processes and the inability to use reports in court due to misattribution.

Cases where attribution efforts do not lead to a clear identification of the threat actor are mentioned, emphasizing minimal effort in such instances.

Staying informed about evolving techniques involves relying on blogs and work experience. The need for infrastructure tracking and actor profiling is identified as a significant area for improvement in the field of cyber threat actor attribution.

E.7. CTI analyst

In the realm of cyber threat attribution, the techniques and methods employed vary significantly between law enforcement and the private sector. The police prioritize evidence, seeking to convincingly link specific individuals to committed crimes. Their approach involves a root cause analysis, scrutinizing the exact actions of the attackers and assessing the criminal offenses committed.

Indicators such as Indicators of Compromise (IoCs), IP addresses, Tactics, Techniques, and Procedures (TTPs), and tools play a crucial role in attributing cyber threats to specific actors or groups. While cybersecurity companies focus on the victim's side, climbing higher in the attacker's infrastructure aids law enforcement in their investigations.

The interviewee discussed the crucial elements of cybersecurity investigations, emphasizing the significance of Indicators of Compromise (IoCs), IP addresses, and Tactics, Techniques, and Procedures (TTPs). It describes how attackers typically control malware externally, establishing connections within their network infrastructure and forming distinct tiers within their structure.

Observing Command and Control servers (C2s) at the infrastructure's bottom is highlighted for cybersecurity companies, while law enforcement focuses on climbing higher in the infrastructure to trace attackers. IoCs, including domain names, play a key role in understanding infrastructures, and studying TTPs involves analyzing how attackers operate within networks.

The Pyramid of Pain concept underscores the importance of investigating C2 servers lower in the infrastructure for disruption, acknowledging that even higher servers may not be in contact but can impact threat actors when disrupted. The interviewee also notes the significant impact of disrupting servers, as demonstrated by the takedown of Emotet's entire infrastructure.

Moreover, the interviewee discusses the additional pain inflicted on threat actors when their unique malware methods are analyzed and published. This publication forces threat actors to devise new approaches, contributing to the overall understanding and disruption of cyber threats.

Ransomware groups often reveal their identity in ransom notes, verified through Indicators of Compromise (IoCs) and negotiation details. Challenges emerge when dealing with undisclosed or new groups, resulting in the use of multiple names. Sanction checks involve verifying actors against lists using indicators like emails, while newly formed groups may adopt Tactics, Techniques, and Procedures (TTPs) from others, complicating attribution. Ransomware groups generally avoid deceiving their identity due to reputation concerns.

Hacktivists commonly disclose their identity, except when posing as Advanced Persistent Threat (APT) groups.

Advanced Persistent Threats (APTs) aim for prolonged, unnoticed presence for information gathering. Attributing APT attacks raises questions about certainty in associating them with specific countries. Established APTs with a history may be linked to countries based on language, working hours, and holidays. Attribution of new APTs is challenging, and scrutiny of their Tactics, Techniques, and Procedures (TTPs) is crucial. The technical challenges in attribution vary across threat actor groups, with factors such as disclosed identity, TTP adoption, and historical context influencing the process.

The levels of attribution vary among different entities. Balancing both aspects provides a comprehensive understanding, with each entity looking at different parts of the Diamond Model.

Ransomware attackers are typically identified at the group level, with cybersecurity companies rarely reaching the individual level in the infrastructure.

The key strengths of attribution techniques lie in obtaining threat actor profiles, understanding negotiation techniques, and comprehending cyberattacks as more than technical issues.

However, challenges arise in distinguishing between affiliates and core group members. The core group, responsible for creating and distributing ransomware, have a major impact on the environment. So, identification of the core group is of great significance.

Mitigating the risk of false attribution is crucial, and conclusions based on a single indicator should be avoided. Attribution guides the investigation's direction, but a balance is necessary to avoid tracking the wrong actor.

Legal or ethical considerations have not been encountered, and there is limited experience in cases where attribution efforts did not lead to a clear identification of the threat actor.

Staying informed about evolving techniques involves reading blogs and collaborating with Cyber Threat Intelligence (CTI) colleagues.

The most significant areas of improvement in the field include standardizing language across the cybersecurity sector and translating information into common Tactics, Techniques, and Procedures (TTPs) for global sharing.

Cyber threat actors are categorized based on characteristics such as motivation, capabilities, tactics, techniques, and procedures. Nation-states operate for national interests, cybercriminals pursue financial gain, hacktivists act based on political ideology, and terrorists operate with political motives.

E.8. Digital Forensics

The discussion commenced with an exploration of the techniques employed by the organization for cyber threat actor attribution. The interviewee emphasized that while clear indicators often emerge, especially in cases like ransomware, attribution remains a complex task. Ransomware, being adaptive and frequently utilizing existing server tools, poses challenges due to its generic indicators and overlapping TTPs employed by different affiliates.

The interviewee shed light on the indicators considered during attribution, citing examples like Exchange exploitation, RDP brute force, VPN compromise, Mimikatz usage, Rclone for data exfiltration, Mega as a preferred destination for ransomware data, and the details found in ransomware notes. Each method, distinct in its approach, contributes unique indicators for attribution.

A notable theme emerged regarding the differences in cyber threat attribution techniques between APTs and ransomware attacks. APTs were characterized as more straightforward due to custom tooling, slow-paced operations, and a focus on prolonged infiltration. On the contrary, ransomware, driven by speed and immediate impact, posed challenges in attribution, with most affiliates resorting to similar tools from the dark web.

The discussion touched upon a fascinating case where two distinct threat actors—an APT group and a ransomware group—were discovered concurrently. The identification hinged on discerning differences in steps and TTPs employed by each actor.

Attribution levels were explored, revealing a predominant focus on the group level, occasionally hinting at affiliations through negotiation styles—providing a partial individual-level identification.

The interviewee underscored the strengths of their attribution methods, highlighting the importance of swift investigations in the face of advanced attackers. The need for attribution becomes critical, particularly when dealing with custom tooling, as standard indicators may fall short.

Challenges in attribution, especially in ransomware contexts, were acknowledged. The interviewee proposed the establishment of a centralized database within the cybersecurity community, containing actor profiles for enhanced attribution. Internal communication, particularly insights from negotiators recognizing similar actors, was deemed crucial for more efficient investigations.

False attribution was considered a significant risk, emphasizing the importance of maintaining an open-minded investigative approach and avoiding tunnel vision. Ethical and legal considerations were deemed less impactful in the context of the interviewee's experiences.

In terms of staying updated, the interviewee highlighted real-time incident involvement as the primary source of awareness, diminishing the need for external readings. Looking ahead, the interviewee expressed a need for a platform with a central database to facilitate easy identification of similar cases.

The interview concluded with insights into how cyber threat actors are categorized based on their characteristics and motives. Actions played a pivotal role in categorization, with ransomware gangs identified by their rapid extortion tactics and APTs characterized by prolonged network presence. An insider threat example was the case of Rotterdam Haven, in which a USB stick was planted in the main OS which created a backdoor.

E.9. Reverse Engineer

The interviewee begins by discussing the techniques employed for cyber threat actor attribution in ransomware attacks. They delve into the difficulties of deciphering the source code of ransomware, highlighting the use of patterns in functions as a crucial clue. The expert emphasizes the significance

of recognizing specific functions that are unique to a particular piece of software, forming a recognition code for identification.

As the conversation progresses, the interviewee introduces the concept of ransomware hierarchy, distinguishing between core groups and affiliates. They explain that while affiliates can modify configuration parameters, it's not a foolproof method for attribution due to limited adjustments. The discussion touches upon the role of configuration details as indicators, emphasizing their contribution to a broader understanding of the attack.

The interviewee addresses the challenge of attributing attacks to specific groups with absolute certainty. They underscore the reluctance in the cybersecurity community to claim 100% certainty, emphasizing the complexities and nuances involved in attribution. The interviewee touches upon the exceptional cases where the U.S. government exhibits a rare level of certainty in attributing attacks to specific individuals.

Moving on to indicators considered in attribution, the expert emphasizes function reuse in older malware and analyzes metadata in binary files, including headers and timestamps. IP addresses, often significant in other types of attacks, play a lesser role in ransomware. The interviewee also mentions the variation in the sophistication of ransomware binaries as an essential aspect of analysis.

The conversation widens to address differences in attribution techniques concerning various threat actors, such as state-sponsored groups, cybercriminals, and hacktivists. The interviewee notes similarities in tools used by ransomware actors but acknowledges differences in the sophistication of ransomware binaries. While IP addresses and attack setup nuances may vary, the primary focus remains on analyzing the ransomware binary.

The interviewee candidly discusses challenges associated with cyber threat attribution, emphasizing the anonymity of the internet, false flags used by attackers, and the evolving nature of malware and attack techniques. They underscore legal and geopolitical factors as additional challenges, highlighting the caution required in attributing attacks to specific nations.

Concluding the discussion, the expert provides recommendations for enhancing cyber threat attribution capabilities. Suggestions include enhancing forensic capabilities, active participation in threat intelligence sharing, deploying advanced security solutions, continuous training for cybersecurity professionals, collaboration with law enforcement, and adopting a zero-trust security model.

E.10. Digital Forensics

In the interview, the focus is on the organization's methods for attributing cyber threats, specifically ransomware groups. The interviewee mentions relying on Indicator of Compromise (IoC) matching to identify threat actors, looking broadly to discover indicative pieces such as ransomware notes, regardless of their source or format.

When asked about the indicators considered in cyber threat actor attribution, the interviewee notes the importance of looking beyond Tactics, Techniques, and Procedures (TTPs) due to their generality. Instead, they emphasize concentrating on the ransomware note, assuming the involvement of a specific group

Regarding differences in attribution techniques for various threat actors, the interviewee acknowledges that the core methodology remains the same, but motives differ. They reference the diamond model and mention variations among organizations in terms of attribution approaches. For example, Mandiant uses activity clustering, while Microsoft associates attacks with countries through storm names.

The interviewee dismisses the relevance of country-level attribution for ransomware attacks, highlighting that these groups may not operate exclusively from one country, unlike Advanced Persistent Threats (APTs) employed by states.

Levels of attribution are discussed, with a distinction made between ransomware attacks and APTs. County level is relevant for APT attribution, however, for ransomware groups this is not relevant at all since such groups do not work from one country. The interviewee proposes considering tactical,

operational, and strategic attribution levels instead of the standard ones. They emphasize attributing at the group level for ransomware attacks.

They also mention the importance of considering the potential risk of misattribution and stress the need to provide attribution with a certain level of certainty.

Legal and ethical considerations are deemed not applicable in their context. The interviewee suggests that every attribution attempt they've made has faced challenges, emphasizing the difficulty in identifying ransomware actors.

In terms of staying informed, the interviewee relies on news, blogs, and private communities. They highlight the significance of standardizing methodologies within cybersecurity companies and encoding data, suggesting that Incident Reports (IRs) often lack follow-up.

E.11. Team lead high tech crime

The interviewee, an expert in cyber threat attribution within their organization, provided insights into the diverse methods employed for investigating and attributing cyber threats, with a particular focus on ransomware groups. Rather than limiting the scope to ransomware, their approach encompasses a broader view of the criminal ecosystem, emphasizing the need for comprehensive investigations.

The techniques employed involve tapping into networks, seizing assets, and, at times, resorting to hacking. Central to their methodology is the meticulous collection of information, incorporating Open Source Intelligence (OSINT) and establishing contacts with private parties and other law enforcement agencies. The interviewee highlighted the importance of data analysis, connecting disparate pieces of information to reveal a comprehensive picture.

A key aspect of their work involves attributing cyber threats to specific individuals or groups. The interviewee noted the combination of various techniques, such as technical analysis, identifying IP addresses, and examining user accounts. They discussed instances where mistakes made by threat actors, like logging in without a VPN or engaging in a cash-out, become pivotal in linking pieces of information together. Accessing communication platforms and forums used by these groups also plays a crucial role, providing historical context and linking to past investigations.

In terms of indicators, the interviewee emphasized the dynamic nature of cyber threats, with distinctive elements varying from case to case. They discussed the significance of infrastructure changes, the use of specific botnets, and the tighter security of ransomware groups compared to botnets. The interviewee stressed the combination of technical data and investigative work, involving everything from IP addresses to specific typos.

The international dimension of their work was underlined, with collaboration and information-sharing playing a pivotal role. The interviewee acknowledged the challenges of attribution on a global scale, citing differences in analytical approaches, resources, and law enforcement capabilities among countries. The collaboration, particularly with the United States, was emphasized as essential for effective attribution efforts.

The interviewee emphasizes that attributing ransomware actors are in general the same, and that these types of actors are aware of leaving digital traces. A comparison is drawn between ransomware activities, characterized as more criminally significant, and less severe activities like running a botnet for spam.

Furthermore, he highlights the ongoing international collaboration in attributing cyber threats, which is consistently data-driven. It dismisses the interest in isolated individuals making mistakes and directs attention toward organized criminal activities. Overall, the emphasis is on the technical and strategic aspects of attributing cyber threats through data-driven international cooperation.

The interviewee delves into the nuanced levels of cyber threat attribution. They acknowledge the inherent complexity in investigations, where a simple name change can lead to a significant shift in perceived threat groups. The distinction lies in the challenge of correctly identifying and attributing cyber activities, emphasizing the need for precision in a dynamic landscape.

When discussing variations in attribution levels among different organizations, the interviewee notes that journalists, for example, may approach attribution differently due to their distinct roles and responsibilities. Law enforcement, on the other hand, faces the delicate task of avoiding premature conclusions, emphasizing the importance of thorough documentation and alignment with legal authorities to prevent missteps.

Regarding ransomware attacks, the interviewee highlights the multifaceted nature of their involvement, ranging from broad network assessments to individual actors. The international dimension adds another layer of complexity, raising questions about the sources of information and the intricate details involved in the investigative process.

The interviewee distinguishes between law enforcement's primary concentration on individual actors and their involvement in criminal collaborations. The necessity for targeted investigations emerges, with an understanding that, in the realm of ransomware, addressing a broader network becomes crucial. The goal is not solely pinpointing specific individuals but unraveling the complexities of the entire group involved.

The interviewee discusses the strengths of their organization's attribution methods for ransomware groups. They highlight the importance of broader investigations, such as the Title 5 inquiry and 1.4a, focusing on criminal collaborations.

The significance of international collaboration and leveraging national strengths is highlighted by the interviewee. They stress the Dutch infrastructure and skilled team members as key assets. Public-private partnerships, especially with entities like Cybersecurity companies, contribute significantly to their operational efficiency.

In response to a question about sharing evidence, the interviewee confirms that collaborators like Cybersecurity companies provide evidence and encourage filing reports. They emphasize the need to understand the scale of the problem, considering both the forensic information and the number of reports received. The interviewee stresses the importance of collaboration for effectively addressing the massive and intricate challenges posed by ransomware.

When considering the limitations and challenges of attributing ransomware groups, the interviewee highlights the geographical obstacles. Ransomware actors often operate from countries like Russia, where extradition is difficult. This significantly delays the investigative process, limiting its effectiveness until the perpetrators make a move, such as traveling.

Attribution is crucial for law enforcement to utilize their powers effectively. Broader investigations allow authorities to disrupt the criminal business model swiftly. However, the interviewee notes the time-consuming nature of individual attributions, especially when identifying specific actors. This extended timeline can impede the timely disruption of criminal operations.

Information sharing emerges as a significant challenge. While cooperation between law enforcement agencies is generally effective, challenges arise in sharing information with private entities. The interviewee emphasizes the importance of better sharing mechanisms, suggesting that smoother information exchange could contribute to minimizing damages.

Legally, the interviewee underscores the strict adherence to criminal procedure laws. Ethical considerations also play a role, particularly in deciding when and how much information to share with the public to prevent potential harm.

The interviewee provides insight into the effectiveness of their attribution efforts. They emphasize that attributing cyber threats involves continuous research, collaboration with various sectors, and adapting methods strategically. Staying informed about evolving techniques and indicators is crucial for maintaining effectiveness.

The interviewee suggests that improved international diplomatic agreements are necessary for smoother collaboration. Additionally, there is a need for a more strategic approach to investigations, focusing on international contributions rather than isolated national efforts.

The challenges of companies hesitating to report incidents to the police are discussed. The interviewee notes that some organizations fear that reporting may not yield immediate benefits, but law enforcement

actively engages in notifying potential victims and believes that cooperation is crucial.

Regarding the categorization of cyber actors, the interviewee mentions that they prioritize factors like methodologies, motivations, and the impact of their actions. While they consider capabilities, these aspects are factored into a prioritization strategy rather than forming a strict categorization.

E.12. Cyber resilience consultant

The interviewee begins by discussing the techniques and methods used within their organization for attributing threats. They highlight the use of MITRE as a core tool and the establishment of a generic threat landscape specifically tailored to the financial sector. This approach provides insight into relevant threat actors and the tactics, techniques, and procedures (TTPs) they employ. Both private source information and open-source intelligence (OSINT) contribute to these analyses, while experts within the organization make connections with critical functions within the financial sector.

The interviewer then inquires about the indicators considered when attributing cyber threats to ransomware actors. The expert notes that TTPs within ransomware are generally generic but emphasizes the specific behavior of these groups, such as data exfiltration for extortion.

Responding to the question of whether attribution techniques differ depending on the type of threat actor, the expert affirms this, illustrating the distinction between cybercriminals targeting direct financial exfiltration and advanced, state-sponsored groups (APTs) with a broader range of capabilities. He highlights the challenge of profiling APTs due to their advanced capabilities.

Asked if there are different levels of attribution, the expert confirms this, although he notes that, in their specific context, attribution at the group level is sufficient. He emphasizes the importance of caution in attribution, given the risk of misattribution and its impact on resources and reputation.

The expert then outlines the strengths of their attribution methods, focusing on the use of cyber threat intelligence (CTI) for advanced actor simulations. He emphasizes the ability to provide creativity to the red team for effective simulations.

The interviewee also discusses limitations and challenges, particularly related to emulating realistic situations and the risk of recognizing red team activities as threat actors.

The importance of avoiding misattribution is addressed, with the expert emphasizing that caution is warranted in attribution decisions. Political considerations come into play when profiling APTs, as this implies a statement about another country.

The interview concludes with a discussion on the need for improvement in attributing threat actors, with specific attention to creating links between technical, tactical, and strategic levels of CTI. The lack of actionable perspective for less technically inclined clients is highlighted, and it is suggested to provide advice on translating from tactical to operational levels.

Finally, the expert stresses that keeping up with evolving techniques primarily occurs through open-source intelligence and identifies the need for more coherence between different levels of CTI as a significant area of improvement within the field of cyber threat actor attribution.

E.13. Manager

In discussing the cyber threat actor attribution methods employed within the organization, the interviewee differentiates between technical and political attribution. Technical attribution, pertinent to ransomware, involves scrutinizing elements such as ransomware notes and phishing campaigns, focusing on domains and their specific details. While these provide a basis to connect various attacks, it's emphasized that linking an attack to a specific actor requires more nuanced analysis. Political attribution, focusses on country attribution which is especially useful in APT attribution.

The conversation shifts to indicators considered during attribution, highlighting the importance of recognizing that a single indicator does not constitute sufficient evidence. To overcome this limitation, a spectrum of indicators is evaluated, aligning with the Pyramid of Pain. Significantly, it's noted that attributing ransomware requires contemplating the groups crafting the malware versus those executing the attacks.

Distinctions emerge when dealing with diverse threat actors, including state-sponsored groups, cybercriminals, or hacktivists. Advanced Persistent Threats (APTs) are characterized by known malware and a combination of identifiable malware within a network, indicating a specific quest for information. Conversely, ransomware groups exhibit a more dynamic and less targeted approach. The interviewee underscores the challenge of attributing ransomware groups due to their ever-changing dynamics and propensity to offer services like Ransomware as a Service (RaaS).

The discussion extends to different levels of attribution, emphasizing a pivotal difference between technical and political attribution. While technical attribution involves associating technical indicators with specific groups, political attribution operates at the geopolitical level. Strategic attribution, combining technical and political aspects, enhances certainty. Law enforcement predominantly focuses on attributing threats at the individual level, a complex task with ransomware groups. For cybersecurity, the attribution might be less crucial. The interviewee continues that APTs can mimic the modus operandi of ransomware groups to obfuscate their true objectives.

Key strengths in the attribution process include the retrieval of encryption keys and negotiations with threat actors when communication is established. However, challenges arise due to the evolving nature of ransomware groups, often leading to decisions to abstain from attribution.

Regarding potential misattribution risks, the interviewee stresses caution, especially when considering the level at which attribution is utilized. The consequences for law enforcement, aiming for legal actions, differ significantly from those for cybersecurity firms assisting clients in recovering encrypted data.

The interviewee, while maintaining that specific legal and ethical considerations are not applicable in their context, acknowledges the sensitivity of attributing ransomware groups. Privacy concerns and the potential impact on legal proceedings underscore the need for a nuanced approach.

Addressing unsuccessful attribution cases, the interviewee refrains from providing specific examples but attributes such failures to a lack of comprehensive information. Remaining informed involves continuous research from both public and private sources, as well as national and international collaborations.

Lastly, the interviewee states that the cyber threat actors are distinguished based on their motives. Hacktivists often have political goals, ransomware groups are financially driven and APTs often strive for espionage.

E.14. Head Threat intelligence

The interviewee starts off with stating that the RTA attribution process is easy if you wait long enough, as the ransomware group would introduce themselves in are ransomware note. Which makes attributing ransomware on group level not that difficult. The difficulty is in who you are dealing with. He continues that in the case of Revil affiliates ID number in the malware were analysed and a pattern was found in which affiliate ID belongs to a specific affiliate. It is emphasised that there should be made a difference between the ransomware builders (developers) and the attackers (Affiliates), as the former gives the brand name and the latter conducts the attack.

Within the ransomware ecosystem it is often observed that certain actor execute a specific part of the kill chain. Resulting in a dependency on each other, and communication is required. This can be done via forums, chat platforms and is also a big difference between APT and RTA. Finally he states that they do everything they can that falls within the framework of the law.

The indicators which are considered in RTA attribution was stated as malware, network IoCs and certificates. The interviewee adds to this that the combination of tools used can be important to find clues about the attacker's identity. TTPs used in ransomware attacks are very generic, since affiliates move between groups. It is further explained that the TTPs used also depend on the victim's security system.

Reputation is very important in the ransomware business. There are a few things that are important for a ransomware group to have a good reputation:

External marketing: This includes the leak site, which is used to publish information about the victim's data if the ransom is not paid.

Internal marketing: This includes individual status, which is the reputation of the individual affiliates within the group.

Good malware: This includes a well-working encryptor and decryptor. The encryptor should be strong enough to make it difficult for victims to decrypt their data without paying the ransom.

The interviewee states that the techniques used for RTA attribution as the same as other CTA attribution.

For a cybersecurity company, group level is enough. Country level attribution is difficult. It is possible to determine which country the developers come from, but this does not say anything about who is behind the attack, because an affiliate can purchase the ransomware. As for individual level attribution, cybersecurity companies will go as far as possible, but if it leads to nothing, they will stop. The goals of the individual can sometimes differ from the goals of the group. Personal drive could be an explanation for why an individual would attribute an attack to an individual level instead of a group level.

Strong attribution requires answering the 5 Ws and explaining all elements using the diamond model. If a cybersecurity company can answer the 5 Ws (who, what, when, where, and why) from multiple sources and explain all elements of the attack using the diamond model, then they have a strong attribution.

The challenges of attribution is that RTAs do everything they can to remain anonymous at the individual level.

The interviewee explains that misattribution depends on the depth of the attribution. If the evidence found is going to the police, they must be sure the evidence is correct. This can be prevented by conducting an analysis of competing hypotheses. Ransomware actors have no incentive to use false flags.

The interviewee continues that, they have to deal with the legal framework. That is what they simply have to adhere to.

Lastly, the interviewee states that he is staying updated on new techniques and indicators based on work experience, reading blogs and x, and talk to colleagues. He continues that and improvement to the attribution process would be that the Whois data base should not be GDPR sensitive.

E.15. Digital Forensics

The interviewee explains that attributing a RTA is not challenging because they do not conceal their identity, aiming to receive payment. Typically, they provide a ransomware note explicitly stating their ransomware group.

Distinguishing between ransomware and a ransomware threat actor is crucial. Ransomware may be used as a decoy by other CTA, whereas a RTA actor employs ransomware for financial gain. Attribution to a RTA is relatively straightforward as they are usually explicit about their identity, prioritizing their reputation.

Digital forensics are employed to find evidence, such as the encryptor, confirming the identity on the ransomware note. While Tactics, Techniques, and Procedures (TTPs) may be generic, the encryptor's unique development by groups differentiates them. In cases without a ransom note, suspicion arises about a different CTA, as monetary gain is not the objective.

Moving to attribution indicators, the interviewee underscores the importance of ransom notes, communication channels, and leak sites. In dealing with ransomware threat actors, direct indicators are usually sufficient, and false flags are rare.

Ransomware groups seek recognition, while APT groups avoid it, resorting to false flags. APT groups exhibit unique behaviors, sticking to specific groups, limited resources, and infrastructure. Malware analysis serves as part of APT attribution, while in RTA analysis, usually flaws in the encryptor are explored.

Attribution levels are typically achieved at the group level within cybersecurity companies, with country-level attribution being less relevant due to the potential for affiliates worldwide.

Early containment scenarios may lack ransom notes and encryptors, relying on intrusion sets and TTPs. The interviewee highlights the need to investigate the effectiveness of TTPs in such cases.

Ransomware operations involve reconnaissance, lateral movement, ransomware deployment, and data exfiltration. TTPs are collected for mitigation but are less relevant for attribution, given the open acknowledgment by threat actors.

Attribution strengths include insights for mitigation, emphasizing the importance of cooperation for validation. Limitations include the need for substantial intelligence, contextual information, and community sharing. Public-private cooperation is proposed to enhance attribution, setting an industry standard for attribution.

Misattribution impacts vary by actor type, with APT misattribution potentially causing geopolitical issues. Legal and ethical considerations shape the attribution approach, with varying perspectives on what constitutes a good attribution.

The interviewee stays informed through experience and blog reading. Cyber threat actors are categorized based on motivation, sophistication, resources, and technical skills.

The interviewee states that attribution of an RTA is not that difficult, since they do not hide who they are since they want to get paid. They often have a ransomware note that explicitly identifies what group it is.

The interviewee continues, a distinction should be made between ransomware and a ransomware threat actor. Ransomware can be used as a decoy by other CTA and can be used by anyone. A ransomware threat actor is an actor that uses ransomware to get financial gain out of it. Attribution to a ransomware threat actor is therefore not difficult as they always let you know who they are. Since reputation is important to them.

Digital forensics are used to find evidence such as the encryptor to confirm the identity on the ransomware note. The TTPs are generic, but the encryptor is developed by the groups themselves so that is different. The TTP might be same, but the implementation of the tooling can show the difference between the ransomware groups/affiliates.

In the case of a cyber attack in which no ransomnote is left behind, it is often not a ransomware threat actor as they want to gain money. Without the ransomnote, money cannot be paid, thus the suspicion is that it would be a different CTA.

Moving on to the indicators considered in attribution, the expert emphasises the use of ransomware note, communication channel and leak sites. In case of ransomware threat actors it is really rare that you do not know who you are dealing with, therefore, the use of direct indicators is sufficient. False flags are often not used as this is to put blame on another group this would work against them.

Ransomware groups want themselves to be known, and APT groups do not, therefore, they do false flagging. APT have an unique behaviour as they do not switch groups as much, in addition, they are bound by limited resources and infrastructure used. In APT malware analysis functions as part of the attribution, in RTA malware analysis it is often to discover the flaws of the encryptor. It is investigated if you can break the encryption without buying the decryptor.

The interviewee continues talking about the attribution level of the RTAs. Group level is usually what is achieved within cybersecurity companies. Country level is not as relevant, since anyone can be an affiliate and they can be anywhere.

In the case of an early containment, you will not have a ransomnote, you will not find the encryptor. You only have the intrusion set, then TTPs can come into play. If this is the case it is not known to what extend TTPs can help, this is worth investigating.

Ransomware do reconnaissance to find domain controllers and do lateral movement to access sensitive data. Then roll out ransomware and do data exfiltration.

There is an incentive to collect the TTPs to form mitigation rules, but not for attribution since they clearly state who they are already.

The main strengths of attribution mentioned by the interviewee are the following, it provides more insights to take mitigation measures. Cooperation between different entities is a strong point as multiple entities can confirm your findings which you then can be sure you did it correctly. The interviewee also mentions the limitations of attribution, the intelligence, you need quite a lot of them to get enough contextual information surrounding a particular actor or group. To do a significant analysis on the TTP. You also need enough sharing of the community where you can confirm or refute your hypothesis of your attribution. Not all important information is shared for good reasons, but this inhibits the attribution process of other attribution entities. He continues talking about the main improvement points, Public and private cooperation would improve the attribution process. A lot of cybersecurity companies are private companies and have the most of these cases. A lot of information in the private sector can help assist the public entities in the attribution processes. In addition, There should come an industry standard of what is regarded as a highly like attribution.

Then misattribution is discussed. Impact of misattributions differ per actor type, if you misattribute and APT to a wrong country then it can cause geopolitical issues. The impact of misattribution is dependent on the goal.

The conversation continues with legal or ethical consideration that impact the approach of attributing CTA. There is a different perspective on what a good attribution looks like, therefore, the conclusion of highly likely can differ for each person.

The interviewee stays up to date through experience and reading blogs.

F

Diamond model

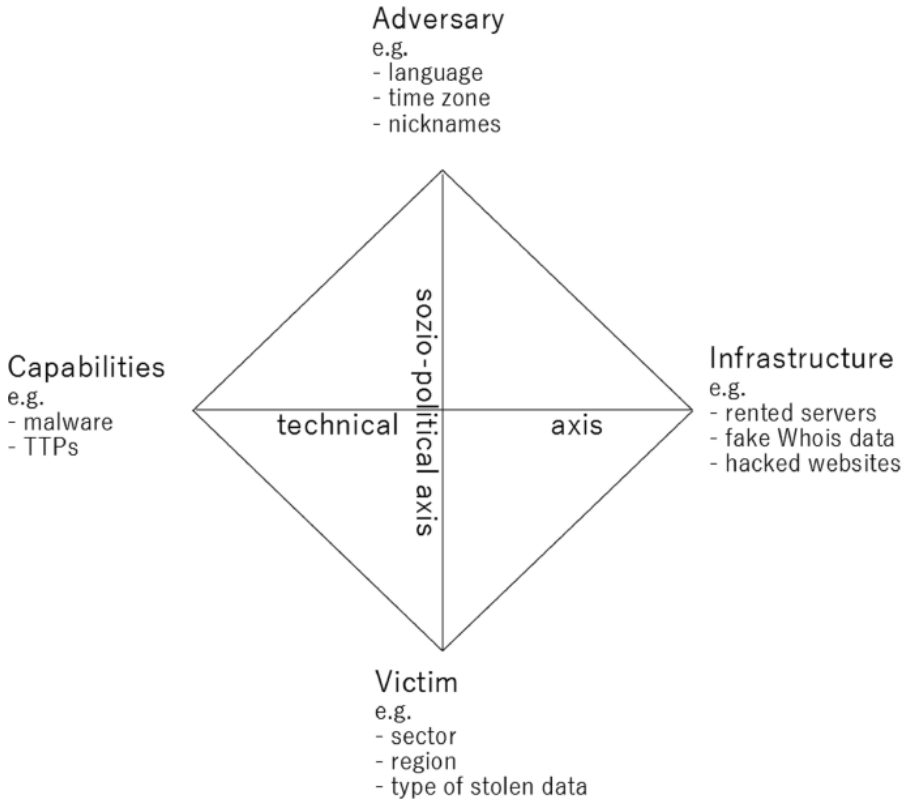

Figure F.1: The diamond model

G

Results contribution analysis

G.1. Results contribution analysis techniques

Table G.1: Weight of techniques used per threat actors

	Blackcat	Lockbit	Play	Blackbasta	Mallox	Hellokittycat	Royal	INC	Monti	Carver	Ransomhouse	Ragner	Blacksuit	8base	ESXIArgs	C3RB3R
Command and Scripting interpreter (Execution)	27,78%	11,11%	11,11%	11,11%	5,56%	5,56%	5,56%	5,56%	5,56%	~	5,56%	~	5,56%	~	~	~
Remote access software (C2)	28,57%	14,29%	7,14%	~	~	~	14,29%	7,14%	7,14%	~	7,14%	~	7,14%	7,14%	~	~
OS Credential dumping (Credential Access)	30,77%	15,38%	15,38%	~	~	~	~	~	15,38%	7,69%	~	~	15,38%	~	~	~
Network service discovery (Discovery)	23,08%	23,08%	15,38%	~	~	~	15,38%	~	~	~	7,69%	~	~	7,69%	7,69%	~
Disable or modify tools (Defense Evasion)	8,33%	8,33%	16,67%	16,67%	~	~	~	8,33%	8,33%	8,33%	~	8,33%	8,33%	8,33%	~	~
Exploit Public-Facing Application (Initial Access)	30,00%	10,00%	10,00%	~	~	10,00%	~	~	10,00%	~	~	10,00%	~	~	10,00%	10,00%
Exfiltration over web service (Exfiltration)	44,44%	11,11%	11,11%	11,11%	~	~	11,11%	~	~	~	~	~	~	11,11%	~	~
Account discovery (Discovery)	42,86%	42,86%	14,29%	~	~	~	~	~	~	~	~	~	~	~	~	~
Create or Modify System Process (Persistence)	16,67%	16,67%	~	33,33%	~	~	33,33%	~	~	~	~	~	~	~	~	~
Brute force (Credential Access)	~	33,33%	~	~	16,67%	16,67%	~	~	~	16,67%	16,67%	~	~	~	~	~
Archive Collected Data (Collection)	40,00%	~	20,00%	~	~	~	20,00%	~	20,00%	~	~	~	~	~	~	~
Data destruction (Impact)	20,00%	20,00%	~	~	~	~	~	20,00%	20,00%	20,00%	~	~	~	~	~	~
Create accounts (Persistence)	~	40,00%	20,00%	~	~	~	20,00%	~	20,00%	~	~	~	~	~	~	~
Masquerading (Defense Evasion)	50,00%	~	~	~	25,00%	~	~	~	~	25,00%	~	~	~	~	~	~
Inhibit system recovery (Impact)	~	~	25,00%	~	~	~	25,00%	25,00%	~	25,00%	~	~	~	~	~	~
Domain Trust Discovery (Discovery)	100,00%	~	~	~	~	~	~	~	~	~	~	~	~	~	~	~
Valid accounts (Persistence)	33,33%	33,33%	33,33%	~	~	~	~	~	~	~	~	~	~	~	~	~
Exfiltration over Alternative protocol (Exfiltration)	~	66,67%	~	~	~	~	~	~	~	~	~	33,33%	~	~	~	~
Application Layer Protocol (C2)	~	~	~	~	~	~	~	~	~	~	33,33%	33,33%	~	~	~	33,33%
Steal or Forge Kerberos Tickets (Credential Access)	50,00%	50,00%	~	~	~	~	~	~	~	~	~	~	~	~	~	~
Credentials from Password Stores (Credential Access)	50,00%	~	~	~	~	~	50,00%	~	~	~	~	~	~	~	~	~
Boot or Logon Initialization Scripts (Persistence)	50,00%	~	~	~	~	~	~	~	~	~	~	~	50,00%	~	~	~
Exfiltration over C2 Channel (Exfiltration)	~	~	50,00%	~	~	~	~	~	~	~	~	~	50,00%	~	~	~
Hijack Execution Flow (Persistence)	~	~	50,00%	50,00%	~	~	~	~	~	~	~	~	~	~	~	~
Phishing (Initial Access)	~	~	~	50,00%	~	~	50,00%	~	~	~	~	~	~	~	~	~
Obfuscated Files or Information (Defense Evasion)	~	~	~	50,00%	~	50,00%	~	~	~	~	~	~	~	~	~	~
Acquire Infrastructure (Resource Development)	~	~	~	~	~	50,00%	50,00%	~	~	~	~	~	~	~	~	~
Server Software Component (Persistence)	~	~	~	~	50,00%	~	~	~	~	~	~	~	~	~	~	50,00%

G.2. Results contribution analysis sub-techniques

Table G.2: Weight of sub-techniques used per Threat Actor

	Blackcat	Lockbit	Play	Blackbasta	Royal	INC	Monti	Ransomhouse	Ragner	8base	Mallox	Blacksuit	HelloKittyCat	Carver	C3RB3r
Remote services: RDP (Lateral movement)	28,57%	14,29%	14,29%	~	7,14%	7,14%	7,14%	7,14%	7,14%	7,14%	~	~	~	~	~
Command and Scripting interpreter: Powershell (Execution)	23,08%	7,69%	15,38%	15,38%	7,69%	7,69%	7,69%	~	~	~	7,69%	7,69%	~	~	~
Valid accounts privilege: Domain accounts (Privilege escalation)	25,00%	16,67%	25,00%	8,33%	8,33%	8,33%	~	~	~	8,33%	~	~	~	~	~
Exfiltration over web service: Exfiltration to cloud storage (Exfiltration)	44,44%	11,11%	11,11%	11,11%	11,11%	~	~	~	~	11,11%	~	~	~	~	~
Account discovery: Domain accounts (Discovery)	50,00%	33,33%	16,67%	~	~	~	~	~	~	~	~	~	~	~	~
Command and Scripting interpreter: Windows command shell (Execution)	40,00%	20,00%	~	~	~	~	~	20,00%	~	~	~	~	20,00%	~	~
Archive Collected Data: Archive via Utility (Collection)	40,00%	~	20,00%	~	20,00%	~	20,00%	~	~	~	~	~	~	~	~
Create or Modify System Process: Systemd Service (Persistence)	20,00%	~	20,00%	40,00%	20,00%	~	~	~	~	~	~	~	~	~	~
OS Credential dumping: DCSync (Credential access)	75,00%	~	~	~	~	~	25,00%	~	~	~	~	~	~	~	~
Create accounts: Domain accounts (Persistence)	~	25,00%	25,00%	~	25,00%	~	25,00%	~	~	~	~	~	~	~	~
Remote services: SSH (Lateral movement)	~	25,00%	~	~	~	~	~	25,00%	25,00%	25,00%	~	~	~	~	~
OS Credential dumping: LSASS Memory (Credential access)	~	~	66,67%	~	~	~	~	~	~	~	~	33,33%	~	~	~
Remote services: SMB/Windows Admin Shares (Lateral movement)	~	~	33,33%	~	~	~	~	33,33%	~	~	~	33,33%	~	~	~
Steal or Forge Kerberos Tickets: Kerberoasting (Credential access)	50,00%	50,00%	~	~	~	~	~	~	~	~	~	~	~	~	~
Credentials from Password Stores: Credentials from Web Browsers (Credential access)	50,00%	~	~	~	50,00%	~	~	~	~	~	~	~	~	~	~
Valid accounts: Domain accounts (Persistence)	50,00%	50,00%	~	~	~	~	~	~	~	~	~	~	~	~	~
Boot or Logon Initialization Scripts: Startup Items (Persistence)	50,00%	~	~	~	~	~	~	~	~	~	~	50,00%	~	~	~
Masquerading: Masquerade task or service (Defense Evasion)	50,00%	~	~	~	~	~	~	~	~	~	~	~	~	50,00%	~
Create accounts: Local accounts (Persistence)	~	50,00%	~	~	~	~	50,00%	~	~	~	~	~	~	~	~
Valid accounts privilege: Local accounts (Privilege escalation)	~	50,00%	~	~	~	~	~	~	~	~	~	~	~	50,00%	~
Valid accounts IA: Local accounts (Initial Access)	~	50,00%	~	~	~	~	~	~	~	50,00%	~	~	~	~	~
Hijack Execution Flow: Path Interception by PATH Environment Variable (Persistence)	~	50,00%	~	50,00%	~	~	~	~	~	~	~	~	~	~	~
Valid accounts IA: Domain accounts (Initial Access)	~	~	~	~	~	50,00%	~	50,00%	~	~	~	~	~	~	~
Application Layer Protocol: Web Protocols (C2)	~	~	~	~	~	~	~	50,00%	~	~	~	~	~	~	50,00%