HUMAN RESOURCE MANAGEMENT IN CYBERCRIMINAL ORGANIZATIONS: AN EXPLORATORY ANALYSIS

A thesis

Presented to

The School of Behavioral, Management and Social Sciences

University of Twente

In partial fulfillment of the requirement for the degree of Master of Science in Business Administration with the Digital Business & Analytics specialization track under the supervision of Dr. A. Abhishta, Dr. J.G. Meijerink, and external supervisor T. Meurs

By

Joost Hasper

12th of July 2024

ABSTRACT

This thesis explores the topic of human resource management (HRM) in cybercriminal organizations. From a business perspective, HRM is recognized for its role in value creation through means such as talent management and employee development. As a result, HRM processes and their involvement in organizational performance in a conventional setting have led to the topic being well-documented in literature. The HRM processes in criminal organizations, particularly those engaging in cybercrime, remain largely unexplored. This study aims to aid in filling this gap by investigating the HRM processes in cybercriminal organizations, focusing on the benefits the members of such organizations receive and how cybercriminal groups recruit, select, and retain new members with specialized skills.

To gain a better understanding of the workings of HRM processes and organizational structure in cybercriminal organizations, a systematic literature review was conducted. The review found that some of the most common methods of recruiting new members to cybercriminal organizations include posting vacancies on hacker forums and personal referrals. Furthermore, the review identified six main organizational structures within cybercriminal groups. These structures vary in their level of organization and coordination, often possessing a hierarchical nature similar to that of traditional organizations. The thesis further explored HRM processes within cybercriminal organizations through a textual analysis of leaked messages from the Russia-based ransomware group “Conti".

The analysis of the Conti leaks provided details regarding the roles and compensation of various members. Comparison between the salaries earned by Conti members and that of Russian citizens working in comparable sectors displayed the profitability of working for a cybercriminal organization. The multiple interviews and types of training applicants must go through before being full-fledged members are discussed as well. Other findings include the use of cryptocurrency for salary distribution and the monetary bonuses Conti awards for exceptional performance.

To conclude, cybercriminal organizations such as Conti employ certain sophisticated HRM strategies, similar to traditional organizations. These strategies include offering competitive compensation and having structured recruitment processes. Significant differences have been identified as well, such as maintaining anonymity during all communication through the usage of aliases. A better understanding of these HRM practices can aid law enforcement agencies to disrupt cybercriminal operations more effectively. The research suggests that the high-level compensation and recruitment practices are flaws that can be exploited to redirect talent to legal employment opportunities.

PREFACE & ACKNOWLEDGEMENTS

This thesis originates from my interests in cybersecurity and the process of organizing businesses. Searching for a method to combine these interests in one research, the idea of investigating cybercriminal organizations was created. This thesis is written in partial fulfillment of the requirements for the degree of MSc. in Business Administration.

I would like to take this opportunity to sincerely thank everyone who helped with the composition of my master's thesis. First and foremost, I would like to express my gratitude to Dr. Abhishta, my primary supervisor, for all his time, advice, and constructive criticism. His expertise and insightful inquiries helped me see several parts of my thesis in a different light. His passion for the subject aided me to stay motivated while writing the thesis. I am also very grateful to Dr. Meijerink for agreeing to be my second supervisor and helping the thesis further improve in quality. His fresh perspective and feedback helped significantly improve the content of this thesis.

Furthermore, I would like to thank Tom Meurs for his help in giving direction to the thesis and sharing his insights on the subject. Dr. Cardoso de Santanna and Raphael Hoheisel were of tremendous help in developing the methodology of this research. I would therefore like to thank both of them for their contribution to this thesis. The thesis would not have reached this level of quality without the guidance and support of all those mentioned above, for which I am deeply thankful to all of them.

Besides all the academics who were of help in the development of the thesis, I would like to thank my friends and family for supporting and motivating me during this process. Especially my mother, for always being supportive of me throughout my life and education.

Thank you all, and enjoy reading this thesis,

Joost Hasper

TABLE OF CONTENTS

1 INTRODUCTION

Human Resource Management (HRM), the process of recruiting, hiring, deploying, and managing an organization's employees, is an essential component of any organization. HRM was once only regarded as a cost to be minimized and a potential method to raise efficiency. The current view on HR has shifted, however, with many organizations recognizing the potential for benefitting a firm's bottom line through value creation. This is done through HR's contribution to aligning organizational objectives via talent management, fostering a positive workplace culture, and employee development (Becker & Gerhart, 1996). In order for an organization to maintain this competitive advantage, HR personnel have to ensure that their implemented strategies lead to both an external fit, where the HRM strategies align with the developmental stage of the organization, and an internal fit, where the various components of HRM in the organization complement and support each other (Baird & Meshoulam, 1988). This is not the only example of certain facets of HRM performance being linked to organizational performance. A linkage between well-organized recruitment and training practices and operational performance (i.e., employee productivity, machine efficiency, and customer alignment) has been observed in firms (Youndt et al., 1996).

One could argue that this necessity for well-organized HRM in traditional organizations also extends to criminal organizations aspiring to grow. However, HRM within criminal organizations is a topic to which literature has dedicated limited attention. Despite this, evidence on the recruitment into criminal groups displayed the importance of social relations, criminal background, and skills when being recruited in a criminal organization. The skillset sought after differs per criminal group. One group might have a need for a member with an inclination for violence, while another group might require someone with a more specific set of skills (Calderoni & Campedelli, 2020). Groups that focus on cybercrime are an example of this. Cybercrime can be defined as all criminal activity that utilizes computers or computer networks as a tool, a target, or a place of criminal activity. The crimes can range from the stealing of information to denial-of-service attacks. Cybercrime can also refer to traditional crimes if computers or computer networks were used during the illicit activity in question (Smith, 2007). The associations that utilize the means of cybercrime for their own goals are becoming increasingly infamous, with their actions impacting the lives of more and more people.

On the 30th of January 2023, a group of pro-Russian DDoS-attackers targeted UMCG, a Dutch hospital in the city of Groningen.[1] While the effects of this specific attack were limited, since the only consequence was a temporary unavailability of certain medical files, the potential results of such an attack could prove to be disastrous. The potential danger and media attention that accompanies these attacks by cybercriminals on innocent bystanders only further encourages law enforcement and academics alike to delve deeper into the minds of these criminals to predict and deter their next action. Many papers and articles write in-depth about various methods of cybercrime and the impact of this 'new' method of crime on society. Renu and Pawan (2019) investigated the effects of cybercrime on various sections of society, which are becoming increasingly reliant on computers and other interconnected devices. After analysis of all the sides of society affected by this type of crime, the paper found that society requires protection that can only be provided by commercial entities creating forms of protective software since governments and consumer education programs will only ever be able to reach and help a small subsection of the population.

This thesis contributes to addressing this issue by focusing on the cybercriminals, as opposed to the victims. Despite the ever-increasing prevalence of cybercrime, the literature on the inner workings of the groups involved in this form of crime is limited. The increase in cybercrime suggests that cybercriminal organizations are growing as well. This growth must be facilitated through the usage of various HRM processes, such as recruitment, selection, and retention methods. These

[1] https://nos.nl/artikel/2461833-pro-russische-ddos-aanvallers-hebben-het-gemunt-op-nederlandse-ziekenhuizen

processes are likely to be different in cybercriminal organizations than in traditional organizations due to having to keep a low profile to avoid the attention of law enforcement. An example of this includes interviews with new applicants. Both the interviewer and interviewee are likely to prefer to remain anonymous in this situation, making for a different type of interview than in traditional organizations. This illustrates how difficult it is to expand a workforce when both the employer and employee want to remain anonymous throughout the hiring process. Another issue cybercriminal organizations might face is finding IT specialists willing to break the law. One can assume that more people than not are unwilling to become criminals for a job, which might create difficulties for a cybercriminal organization trying to find new members. This thesis will contribute to the limited literature on this topic through the investigation of these HRM processes in cybercriminal organizations.

With the threat posed by these cybercriminal organizations ever-growing comes a need to analyze how these organizations operate and are structured. A characteristic most of these groups have in common is that they are extremely decentralized compared to traditional organizations (Broadhurst et al., 2013). Despite the challenges this decentralization brings, large groups of cybercrime criminals continue to form. To provide an example, in Nuh, a region in India, Indian law enforcement recently dismantled a so-called 'cybercrime hub'. This operation had 5,000 police officers raid a variety of villages in the region, making around 50 arrests. While the investigation is still ongoing, the suspects have already been linked to over 28,000 cases of cybercrime across all of India.[2] This specific group had a significant effect on countless lives, even though they were a relatively poorly organized and structured organization. The chaos and disruption a well-structured cybercriminal organization can cause greatly overshadows the harm the previously discussed group has caused. Shedding light on how these organizations are structured could help law enforcement and governments to disrupt their actions.

The threat of cybercrime is continuously growing, which has caused an increase in interest in how cybercriminal organizations operate. Academics can contribute to countering this threat through analysis of cybercriminals, their methods, and ways of operating. This thesis aims to contribute to solving this issue and expanding knowledge on the subject through the exploration of how human resource management works in an unconventional organization that commits various cybercrimes.

[2] https://economictimes.indiatimes.com/news/india/a-dark-web-of-crime-grows-in-delhis-shadow-28000-cases-and-counting/articleshow/100189728.cms

1.1 Rise of Cybercrime

In every field where opportunities to profit arise, there are those who seek to gain at the cost of others. Sometimes these individuals cause havoc without the prospect of any financial gain. This was no different when the internet was first introduced to the world. One of the first major crimes committed in cyberspace was the spread of the "Morris Worm" in 1988. Back then, only academics and the military had access to the World Wide Web. Even so, the worm caused a lot of damage by making approximately 6000 computers stop working.[3] Nowadays the digital landscape is vastly different from the one under attack of the Morris Worm, and its users have changed as well. Young people are becoming increasingly tech-savvy, with all the consequences that it brings. One such example is Arion Kurtaj, an 18-year-old man from Oxford, who is part of an organization being held responsible for a hacking spree against major tech firms such as Uber and Nvidia.[4]

Cybercrimes, criminal acts where digital devices and networks are both the means and target, are becoming more sophisticated and often more profit focused. Cybercriminals use techniques such as phishing scams, identity theft, and the usage of ransomware. Ransomware, a form of malicious software, refers to a program that is covertly inserted in a targeted system, with the goal of compromising the availability of the victim's data, applications, or operating system (Flick & Morehouse, 2011). Furthermore, the increase in popularity of cryptocurrency provides cybercriminals with a means to receive payment while minimizing risk of being tracked by law enforcement. In addition, cybercriminals tend to organize themselves in groups, gaining them the ability to execute more coordinated cyberattacks. One study found that coordinated cyber-attacks result in more harm and can lead to an increase in rewards for criminals at a lower cost (Meurs et al., 2022). The increased threat these organizations of cybercriminals pose requires them to be investigated thoroughly in order for law enforcement to understand and combat them better.

These cybercriminal organizations continue to grow with every lucrative opportunity they take. To illustrate, in 2015 the global cost of cybercrime was estimated to be around $3 trillion. This number increased to $6 trillion in 2021, with no signs of this trend slowing down.[5] This growth can only be sustained through an ongoing supply of IT specialists and professionals. For this stream to exist, such an organization would require a strong focus of management on recruitment and retention to obtain and sustain this workforce. However, these organizations prefer to keep a low profile due to their illicit actions. Avoiding attention from law enforcement organizations while attracting IT specialists as potential employees is a difficult challenge to overcome for these organizations. Furthermore, anonymity is key within these organizations, however, maintaining this anonymity when looking for new members to recruit must be an obstacle that these organizations have overcome. This thesis aims to shed light on how cybercriminal organizations deal with the issue of finding new and capable members.

[3] https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
[4] https://www.bbc.com/news/technology-66549159
[5] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

1.2 Problem Identification

Previous works on cybercriminal organizations mostly focus on the technological aspects of cybercrime. Common subjects of research include the multitude of hacking techniques, malware analysis, and profitability of these organizations. Studies such as those conducted by Mirkovich and Reiher (2004) and Huang et al. (2018) are prime examples that go into depth regarding the technicalities of cybercrime and the business behind it. However, limited attention has been paid to the organizational structure and HRM practices that enable cybercriminal organizations to function effectively. This is largely due to the way these enterprises operate, since keeping a low profile is preferred when avoiding contact with the law. Despite the challenge this poses during research, further investigation into their methods can aid law enforcement agencies and government in better understanding these organizations, and in turn disrupt, their operations.

Mirkovich and Reiher provide taxonomies of distributed denial-of-service (ddos) attacks and the defenses employed against these attacks with the purpose of introducing structure in the ever-evolving ddos field, highlighting important features of both attack and security mechanisms. This technical overview gives insight into the methods used by cybercriminals to achieve their goals, but this sole focus on the technical side of the issue gives an incomplete view when looking at the issue of cybercrime as a whole.

Huang et al. have created an extensive survey on the cyber-attack business by conducting a thorough literature review. They recognized that cybercrime is a chronic issue that will only grow over time. To contribute to combatting this issue, a survey of cybercrime services was created, aiding in understanding the cybercrime ecosystem as a business and how methods that counter cyber-attacks can be made better. Furthermore, the cybercriminal value chain model was created, consisting of all steps taken by these criminals when conducting illicit actions. Moreover, this model also highlights the need for human resource management in such an organization, fulfilling the need for new and talented IT specialists. The paper does not go in-depth regarding how these IT specialists are found and hired by cybercriminal organizations, leaving a gap to be filled by future research. Another point of interest is that cybercriminal organizations utilize various forms of organizational structure, not unlike traditional organizations. The significant difference in structure between traditional organizations and those involved in cybercrime is that the cybercriminal structures are highly adaptable, allowing for swift action within the dynamic world of tech. Despite the difference in the type of structure, the similarity of having an organizational structure between cybercriminal organizations and traditional organizations found by Huang et al. offers a new perspective on how cybercrime operations work. This thesis aims to provide insight into how cybercriminal organizations organize their HRM process, which should provide an opportunity to compare the HRM processes used by cybercriminal organizations to those of traditional organizations.

Another paper of interest is that of Putman et al. (2018). Unlike the previously mentioned works, this paper does not necessarily focus on the technical side of cybercrime but sheds light on the business model behind botnets. Using existing literature and four different case studies, Putman et al. not only want to give an estimate for the revenue generated by these botnets but also provide structure to this revenue stream. To create this structure, a cost-benefit analysis is conducted based on this business model, going over various potential botnet uses and their profitability. Besides the cost-benefit analysis, frameworks for a business model canvas and product life cycle analysis were used to illustrate a more elaborate image of this revenue stream. This research provides another valuable take on the subject of cybercrime and helps academics better understand how cybercriminal organizations function. Despite the unique viewpoint taken by Putman et al., the human factor within the organizations that utilize botnets is not discussed, while being of interest when attempting to fully understand cybercriminals.

Another point of view on this subject was explored in an article by Connoly and Wall (2019). This study focuses not just on the technical science, but also includes various social science factors involved in these issues. Utilizing in-depth interviews with victims and law enforcement officers

involved in crypto-ransomware attacks, the research looks at the actions taken as a response to these attacks. Development of adequate responses to such attacks was proven to be difficult, due to the complicated link between complex malware technology and social engineering that leads to infection of systems. As a result, there is no 'one' solution to this ever issue. The interviews with the victims and law enforcement officers provided a unique perspective, including new perspectives regarding the human factors that are present in ransomware attacks and cybersecurity. However, a rigorous investigation of these human factors on the criminal side of this issue is still lacking. This extends to a lack of literature on HRM within cybercriminal organizations.

In order to fill in this gap in the understanding of HRM within cybercriminal organizations, the following research question was formulated:

"How are Human Resource Management processes organized in cybercriminal organizations?"

By addressing this question, we aim to uncover the clandestine HRM practices employed by cybercriminal organizations, shedding light on the organizational structure of these enterprises, any benefits members of these organizations may receive, and the selection, recruitment, and retention methods they utilize. This investigation is crucial for developing a more nuanced understanding of cybercrime and the inner workings of these organizations.

Understanding the HRM processes within cybercriminal organizations is paramount for the creation and deployment of effective countermeasures. With a thorough understanding of their organizational structure, recruitment practices, and talent management strategies, insights into the motivations and dynamics that drive cybercriminal activities can be developed. Moreover, this research aims to yield practical implications that can aid law enforcement agencies, cybersecurity professionals, and policymakers seeking to influence cybercriminal networks.

1.3 Research Questions

It is clear that cybercriminal organizations require a different approach to HRM practices when compared to traditional organizations. Law enforcement and governmental institutions can benefit from a deeper knowledge of how these organizations operate in order to combat them more efficiently. This research aims to further investigate these processes in cybercriminal organizations and the following research question was formulated to do so:

RQ: "How are Human Resource Management processes organized in a cybercriminal organization?"

HRM is an extremely broad concept, consisting of many activities. In order to make the scale of this research question more manageable, the question has been divided into smaller sub-research questions, with sub-questions two and three focusing on various essential HRM activities. The answers to each of these sub-questions will aid in answering the main research question.

SRQ1: "How are cybercriminal organizations structured?"

The first sub-research question will be answered through the literature review. The answer to this question will provide a baseline of knowledge that the results of the rest of the research can be compared to in order to determine whether there is a match between the findings of this research and existing literature. SRQ1 might also offer new perspectives on work culture and values in cybercriminal organizations, showcasing whether financial gain is prioritized over ethics and social responsibility.

SRQ2: "What benefits do employees of cybercriminal organizations receive?"

Being a member of a cybercriminal organization has its risks. Managers within these enterprises will attempt to offset these risks by offering certain benefits, both financial and non-financial. Gathering insights regarding the various forms of compensation employees of cybercriminal organizations receive provides information about the incentives that attract IT specialists to these criminal organizations. It is clear that cybercriminal organizations operate in rougher environments compared to most traditional organizations, making it even more interesting to discover what these organizations do to guarantee a steady stream of employees who want to keep working within the organization.

SRQ3: "What are selection, recruitment, and retention processes in cybercriminal organizations?"

While SRQ3 has some overlap with SRQ2, there are far more selection, recruitment, and retention processes than offering a large sum of capital or other benefits. Finding out how cybercriminal organizations are able to motivate IT specialists to join their ranks and commit cybercrimes will provide new insights into the operations of these organizations and yield helpful information for answering the final sub-question of this research.

SRQ4: "How can these Human Resource Management processes be influenced by law enforcement, governments, and cybersecurity firms using the findings of this research?"

Besides providing new insights into the workings of HRM in cybercriminal organizations, this thesis aims to deliver practical advice that can be used by law enforcement, cybersecurity providers, and governments to influence these processes within cybercriminal organizations. This last sub-research question aims to deliver this advice.

1.4 Methodology

This methodology section aims to present how the aforementioned research questions will be answered. Firstly, a systematic literature review will be conducted in order to provide an overview of the already existing knowledge regarding cybercriminal organizations and the way their HRM processes take place. Afterward, a text analysis will be performed on files leaked by members of a large-scale cybercriminal organization. The purpose of this analysis is to discover whether the HRM processes described in the literature are used by an actual cybercriminal organization. Furthermore, the flow chart displayed in Figure 1 was designed to provide a clear overview of each individual step during the research.

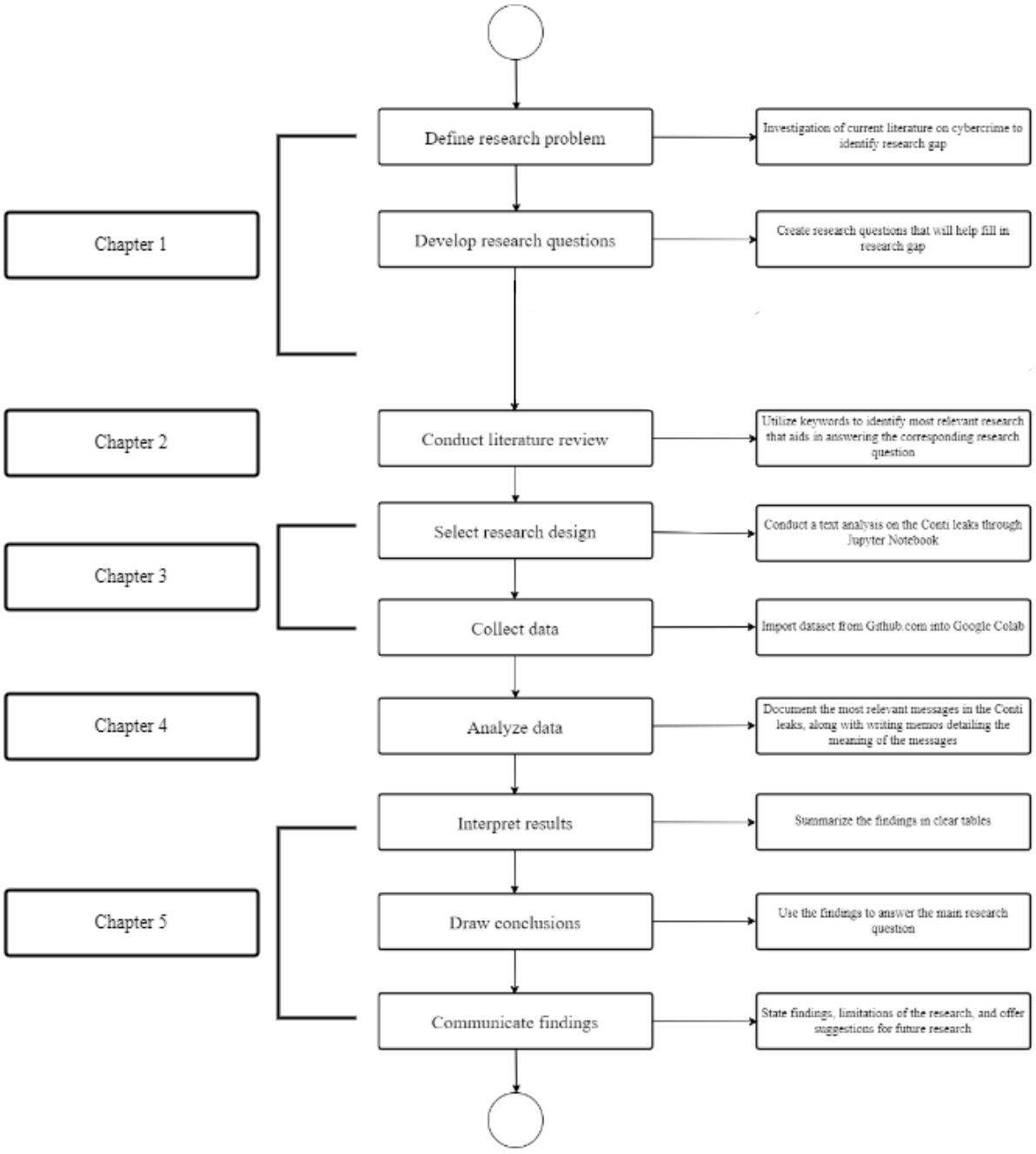

Figure 1. Research Steps

Literature Review

The objective of the literature review is to present a comprehensive survey of the current literature addressing HRM processes employed by both conventional and cybercriminal organizations in the recruitment of IT specialists. Additionally, this literature review seeks to compile pre-existing concerning the organizational structure of cybercriminal entities with the aim of addressing the first sub-research question: *"How are cybercriminal organizations structured?"* The literature review will be written following the framework proposed by Snyder (2019). This framework consists of four phases one must go through to successfully write an extensive literature review. The four phases are designing the review, conducting the review, analysis, and writing the review. Additionally, literature-gathering practices proposed by Webster and Watson (2002) are used to ensure that the literature review contains papers most relevant to the research.

Text Analysis

After completion of the literature review, the next step of the research will be conducted in the form of a text analysis. In order to acquire new insights regarding the workings of cybercriminal organizations, this text analysis will be performed on the "Conti" leaks. Conti is a pro-Russian cybercriminal group known for conducting ransomware attacks on a variety of organizations. The data included in these leaks contains information on their way of operating, victims, and internal communication. This in turn can lead to valuable insights into how such a cybercriminal group operates, how organizations can defend themselves against such a cybercriminal group and how law enforcement can combat them.

The text analysis will be performed using a combination of Python code in Google Colab and Excel. Python is a coding language that allows for the organization of the unstructured Conti leaks. Utilizing this method of structurization will yield tables that display the specific data required to answer the sub-research questions. In turn, the data most relevant to answering the sub-research questions will be imported into Excel for a more manageable overview. A more in-depth explanation of the text analysis will be provided in the method section of the thesis. The leaked files will be retrieved from Github, a code hosting platform.[6] The files here are in code and need to be transferred to a Jupyter Notebook service before the data can be further investigated utilizing the code language Python.

This text analysis aims to shed light on the level of financial compensation Conti provides its members, any additional benefits granted to members, and the selection, recruitment, and retention methods employed by Conti. This in turn will allow us to answer sub-research questions two, three, and four.

[6] https://github.com/ThePARMAK/conti-leaks-englished

1.5 Relevance

Proper research must have a level of academic and practical relevance in order to ensure that it contributes to the advancement of knowledge and that it has real-world implications. Academic relevance ensures that research is based on tested methodologies, builds on existing theories, and contributes to a certain field of knowledge. At the same time, research must also have practical relevance to ensure that it addresses real-world problems and has tangible outcomes that can benefit organizations or even society as a whole. Because of this, the research conducted in this paper has found relevance as well, both on an academic and practical level.

Academic Relevance

This research into the HRM practices of cybercriminal organizations has relevance from an academic perspective because it fills a gap in the existing literature on HRM practices. HRM is a common topic of research with there being plenty of literature and research on the HRM practices of legal organizations. This cannot be said about literature on the HRM practices of illegal organizations. Through investigation of the HRM practices of these cybercriminal organizations new insights into the ways that these organizations function can be found and may help to develop a more precise understanding of the broader field of HRM. Additionally, by studying these organizations, new HRM practices or approaches that could also be relevant for legal organizations could be found.

Practical Relevance

Understanding the HRM practices of cybercriminal organizations can also have significant implications from a practical perspective for governments and law enforcement. Law enforcement and governments can use the information gained in this research to better understand and influence cybercriminal-related operations. A more thorough comprehension of the HRM practices of cybercriminal organizations can therefore have significant practical implications for society as a whole. Furthermore, businesses might be able to learn from the recruitment methods used by cybercriminal organizations in order to improve their own recruitment and selection processes, further increasing the practical relevance of this research.

2 LITERATURE REVIEW

Human Resource Management is a widely investigated field of research, with plenty of papers explaining the details of the subject. HRM plays a crucial role in the recruitment of IT specialists and white hat hackers, as these individuals possess unique skills that are in high demand in the job market. In this literature review, several academic papers will be analyzed to provide an overview of the HRM processes involved during the recruitment of a strong workforce of professionals, with a focus on IT specialists. Furthermore, literature regarding cybercrime and the recruitment processes utilized by cybercriminal organizations will be investigated as well, despite the limited quantity of papers regarding these subjects.

The purpose of this review is to provide an overview of the existing literature on the various HRM processes used by both traditional and cybercriminal organizations regarding the employment of IT specialists. Furthermore, this literature review aims to gather relevant information regarding the structure of cybercriminal entities, in order to answer sub-research question one: *"How are cybercriminal organizations structured?"*

Besides this sub-research question, the following hypothesis was written to be tested. Cybercriminal organizations often exhibit a structured organizational framework that mirrors characteristics found in traditional organizations, albeit with reduced bureaucratic elements and a large likelihood of differences between various cybercriminal organizations. This hypothesis is largely based on the study conducted by Nguyen and Thanh Luong (2020), who found that structure differs largely between various cybercriminal organizations depending on the goal of the organization, but that most of the organizations did have a pyramidal, hierarchical structure.

2.1 Methodology of Literature Review

The first step of the research is acquiring literary information regarding the chosen topic. This means conducting an in-depth literature review of established HRM methods focused on hiring IT specialists. Furthermore, existing literature regarding how cybercriminal organizations operate and hire IT professionals is investigated in order to understand the topic better. The methodology behind gathering papers that contain useful information for the literature review can be understood through four phases, based on a framework proposed by Snyder (2019). Furthermore, additional methods of finding relevant literature in the information systems field were proposed by Webster and Watson (2002), which were used in the creation of this review as well.

Phase 1: Designing the Review

When conducting a literature review, it is essential to know what information to look for and how to find it. For this research, keywords relating to HRM practices and cybercrime were used to find relevant papers. Examples of these keywords include 'Human Resource Management', 'cybercrime', 'cybercriminal organizations', and 'recruitment and retention'. Combinations of the aforementioned examples and other variations were searched for as well. This step allows the researcher to make sure that the information they gather is relevant and properly relates to the chosen topic. Furthermore, a systematic literature review protocol was formulated to display how the used literature was found and examined. In order to find literature relating to the previously mentioned concepts, academic search engines such as Google Scholar and Scopus were used.

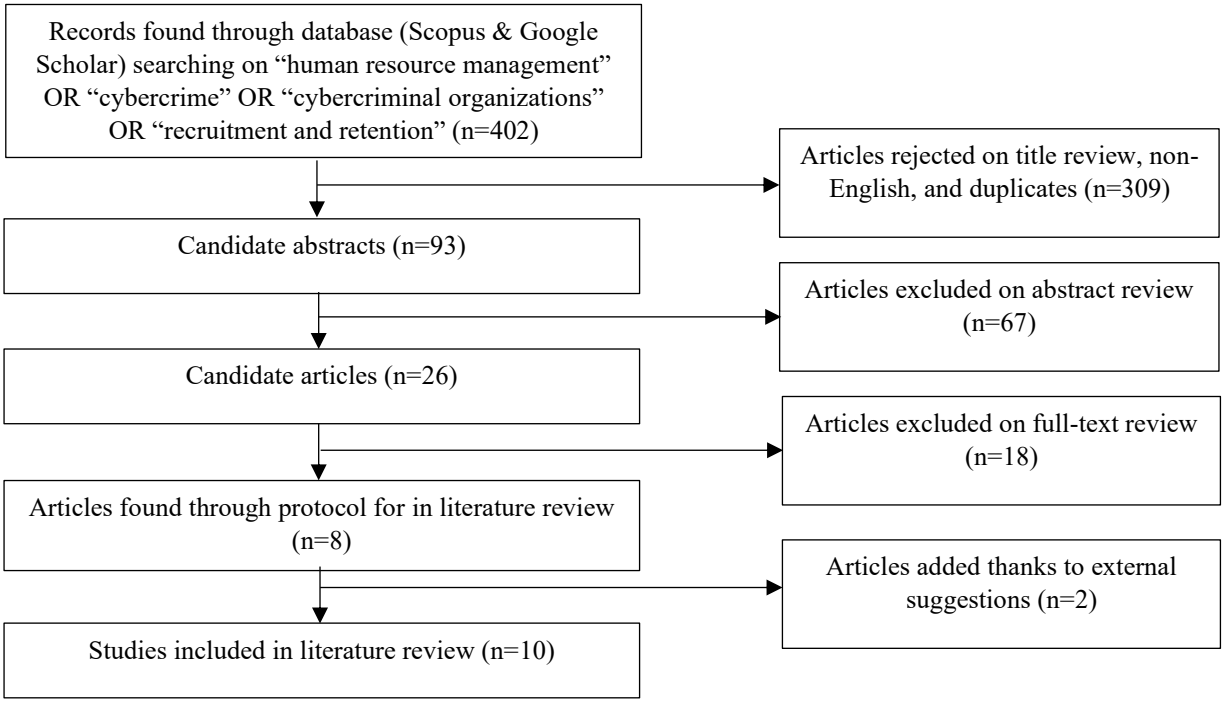

Figure 2. Systematic Literature Review Protocol

Providing structure to the literature review is essential, therefore a concept-centric matrix was used, as proposed by Webster and Watson (2002). The concepts in the tables include the main ideas discussed in the literature review and important methodologies required for conducting the research itself. In order to properly explain the concept matrix, the concepts derived from the three main ideas will be elaborated upon.

The first of these concepts is 'Human Resource Management'. This refers to the strategic and operational activities involved in managing an organization's workforce. It encompasses various functions relating to attracting, selecting, developing, motivating, and retaining employees and practices in line with the aforementioned functions.

Secondly, 'types of cybercrime' is a concept about the various forms digital criminal activities can take. Cybercrime involves the use of computers and networks to commit illegal acts. Examples of types of cybercrime include hacking, phishing, development and usage of ransomware, and Distributed Denial of Service (DDoS) attacks.

Thirdly, 'organized cybercrime' refers to criminal activities conducted by structured groups or networks that specialize in carrying out cybercrimes. The papers under this concept describe the various forms of structure utilized by these groups to carry out their malicious goals.

TABLE 1
Concept Matrix

Authors \ Concepts	Research Methodologies	Human Resource Management	Types of Cybercrime	Organized Cybercrime
Broadhurst et al. (2013)				**X**
Caldwell (2011)		**X**		
Cloutier et al. (2015)		**X**		
Gazet (2008)			**X**	
Huang et al. (2018)			**X**	**X**
Lessig (1999)			**X**	
Lockwood & Ansari (1999)		**X**		
Meurs et al. (2022)			**X**	**X**
Mirkovic & Reiher (2004)			**X**	
Rogers (2018)	**X**			
Snyder (2019)	**X**			
Yadav et al. (2020)			**X**	

Phase 2: Conducting the Review

When deciding what papers to analyze for the review, certain criteria can be used to help find literature more beneficial to the review. These criteria are necessary since some articles might be more relevant to your research than others, even though both articles could have similar topics. Without these criteria, one would have to analyze countless articles and papers in order to find those most suited for the research. Criteria that were used for this review include date of release, number of citations, and general relevancy. A more recent release date tends to increase the likelihood of the literature containing information that is up to date. Furthermore, work that is cited frequently by other researchers tends to be of higher quality than literature that is rarely cited. This combination of criteria helped form a filter that led to relevant academic work of high quality.

Phase 3: Analysis

The selected papers also need to be read thoroughly. If the paper in question does not provide any information that could further the research, it is not to be included in the literature review. If the paper does provide useful information, it can be cited and included in the review. This is not only a necessary step for creating a literature review but helps develop a deeper understanding of the investigated topic.

Phase 4: Writing the Review

In the last phase, the gathered information is ready to be written about in the actual review. Furthermore, an explanation providing the motivation and need for the literature review needs to be written as well. All the aforementioned steps and criteria have led this research to include a variety of different sources, including scientific papers and articles, books, and regular internet articles in order to create a good understanding of the topic at hand. The literature review created using this method aids in answering the research question this thesis aims to answer.

2.2 HRM in IT Organizations

One paper by Lockwood & Ansari (1999) investigated the processes and challenges of recruitment and selection of IT specialists. Previous research suggested that companies that are not only able to recruit but also retain IT talent, have a competitive advantage. This advantage makes knowledge regarding IT talent recruitment and retention valuable. To gain these insights, Lockwood and Ansari utilized a focus group as their main methodology. They reasoned that the participants would be more motivated to share their experience in an academic setting among peers compared to other contact methods, such as phone and email.

This research found the key factors that IT job seekers consider when selecting an employer include salary, benefits, job security, work-life balance, and opportunities for career growth. The most common methods for recruitment of IT specialists include online platforms and personal referrals. The research also revealed that IT job seekers prioritize a positive work culture and meaningful work assignments over employer prestige. Besides factors that help with recruitment and retention of IT specialists, the study found factors that can lead to increased IT employee turnover. These factors include insufficient opportunities for career advancement, lack of work-life balance, a negative work environment, and insufficient compensation. To retain IT talent, organizations need to offer training and career development opportunities, flexible work arrangements, and fair compensation packages. The authors concluded that recruitment and retention of a strong IT workforce is a challenge and that understanding the needs of IT specialists is essential for the design of effective HRM practices.

Another study, conducted by Cloutier et al. (2015), took a deeper look at the importance of developing strategies for the retention of employees in organizations. Efficient employee retention methods are essential to create and maintain stability and growth within organizations. For their research, they wrote a literature review using 22 other studies on employee retention.

The study found that employee retention can be a critical factor for the success of an organization since high turnover rates lead to an increase in the cost of recruitment and talent. Besides these costs, there is the cost of loss of talent and reduced morale among remaining employees. These costs are more difficult to precisely measure, however. Common causes of high turnover rates include inadequate ineffective communication, lack of development opportunities, and hiring of inappropriately skilled people. The study offers some solutions that help avoid this issue, such as competitive salaries, the offering of training so employees can keep on developing, establishing a positive workplace culture, and the establishment of a diverse workforce. The authors conclude that the development of effective employee retention strategies is essential for long-term success within any organization. While this study did not focus specifically on the retention of IT specialists, the practices mentioned in this paper are of high importance for organizations interested in retaining a strong IT workforce, because of the scarcity of IT talent.

A paper by Caldwell (2011) focused on the role of white hat hackers in modern organizations. White hat hackers, also known as ethical hackers, are individuals who use their technical know-how for an ethical purpose. Examples of this include identifying security vulnerabilities in hardware, software, or networks, all while obeying the rule of law.[7] Caldwell goes into detail regarding the entry barriers for starting ethical hackers and goes into detail of how an 'amateur' hacker can develop oneself into a valuable asset to an organization.

Another subject discussed in the paper was that these ethical hackers use their skills to identify vulnerabilities in a system and report them to the organization, rather than exploit them for personal gain. Caldwell argues that ethical hackers can help organizations proactively identify and address security weaknesses, potentially saving the organization from costly data breaches or cyber-attacks. She also addresses some common concerns organizations may have about hiring ethical hackers, such as legal liability and potential conflicts of interest. These concerns are interesting to

[7] https://www.techtarget.com/searchsecurity/definition/white-hat

keep in mind when considering recruitment processes utilized by organizations interested in hiring white hat hackers. Organizations must be able to filter out individuals without strong moral and ethical principles in order to avoid forms of legal liability in the future.

In conclusion, some of the major HRM processes used to recruit IT specialists and white hat hackers include technology, using online job boards and social media platforms, and personal referrals. Furthermore, in order to retain these employees, processes such as comprehensive selection, granting the opportunity for employees to develop themselves, and being willing to pay competitive salaries are used. Competencies such as technical skill and experience are highly valued, but organizations do believe it is important for their IT specialists to have some level of ethical and moral principles, especially if they have the ability to disrupt information technology.

2.3 HRM in Cybercriminal Organizations

Not all IT specialists and hackers have an issue with breaking the law when searching for a way of earning their money. Unfortunately, the literature on Human Resource Management within cybercriminal organizations is limited when compared against HRM in traditional organizations, since few academic studies have been conducted in this area. However, there are some studies that grant insight into the way HRM operates within cybercriminal organizations.

A survey conducted by Huang, Siegel, and Madnick (2018) provides insight into the inner workings of the cyber attack business, including the role of HRM in this context. The purpose of their article is the development of an elaborate and repeatable survey, based on a literature review and publicly available reports, that enables the understanding of cyber attacks in a systematic manner. This survey intends to be a framework that can help study the cybercrime service economy, in which the services tend to be scattered and poorly described.

The authors found that the recruitment and retention of skilled personnel is a major challenge for cybercriminal organizations, as the highly specialized and technical nature of the work requires individuals with specific skills and knowledge. This challenge is compounded by the covert and decentralized nature of cybercriminal organizations, which often makes it difficult to attract and retain personnel. A common way of recruitment for cybercriminal organizations is the usage of hacker communities. These hacker forums use a hierarchical management system that helps with the organization of the community. In order to maintain the growth of members within these communities, tutorials are offered as a way in. This allows novice hackers to participate and benefit from cyberattacks, and in turn, become part of the community. All of this happens in such a structured way that hacker communities are able to provide Hacker Training as a Service (HTaaS) and Hacker Recruiting as a Service (HRaaS). HTaaS has grown exponentially in recent years and can now be considered an industry of its own. It is difficult for law enforcement to combat these services since the training that is offered is most often entirely legal, but great damage can be done utilizing the skills acquired during these training sessions. HRaaS is used for large-scale attacks that require additional hackers to collaborate.

Cybercriminal organizations are increasingly turning to the dark web as a source of skilled personnel, according to an article by Cyberscoop. The article, based on an analysis from cybersecurity firm Kaspersky[8], found that cybercriminal groups are offering job opportunities and seeking to attract talent through dark web forums and marketplaces. These job opportunities often include the promise of very high salaries and flexible work arrangements, as well as the opportunity to work on high-profile cyber attacks. The article suggests that cybercriminal organizations are becoming increasingly sophisticated in their HRM practices, using the dark web as a means to find and retain personnel.[9]

[8] https://securelist.com/darknet-it-headhunting/108526/
[9] https://cyberscoop.com/cybercrime-groups-jobs-talent-dark-web/

While there is not a large quantity of literature on HRM within the cybercrime industry, the discussed literature suggests that it is a complex and challenging issue, requiring cybercriminal organizations to set up complex networks during the task of recruiting and retaining skilled IT specialists. The covert and decentralized nature of cybercriminal organizations, as well as the highly specialized and technical nature of the work involved, make HRM a critical factor in the success of these organizations. The use of the dark web and personal referrals as a source of talent and as a means to attract and retain personnel highlights the sophisticated nature of HRM within cybercriminal organizations. A good understanding of how these organizations operate is essential for governments and law enforcement organizations that intend to counter the threat cybercriminals pose to society.

2.4 Overlap Cybercriminal & Traditional Organizations

When comparing these cybercriminal organizations and their HRM practices to traditional organizations, a clear contrast becomes visible. Cybercriminal organizations must operate in a more covert manner, requiring a different approach to the recruitment of IT specialists compared to traditional organizations, that seek a large amount of exposure when searching for new personnel. Besides this need for secrecy, cybercriminal organizations are often largely decentralized. This can cause issues during recruitment processes since the responsibility for finding and hiring new employees is shared among multiple individuals who are likely not to know each other. Additionally, the illegal nature of cybercrime activities can make it difficult to attract and retain personnel, as individuals may be concerned about the legal consequences of their involvement in these activities.

In conclusion, the existing literature suggests that HRM practices within cybercriminal organizations differ significantly from those in traditional organizations. This is largely due to the challenges that come with operating in secret and the decentralized nature of cybercriminal organizations. HRM practices within cybercriminal organizations have to be adapted in order to deal with these issues. Further research is needed to better chart the HRM methods of recruitment and retention within a cybercriminal organization. Moreover, these practices used by cybercriminal organizations can be useful to traditional organizations as well, providing more opportunities to attract, develop, and retain a skilled IT-focused workforce.

2.5 Cybercrime

Cybercrime has changed drastically since the deployment of the Morris Worm in 1988, which could be seen as the first cybercrime. A comparison could be made between cyberspace and the Wild West, a new frontier with a near endless number of opportunities. Lessig (1999) goes as far as to state the following: "*If there is any place where nature has no rule, it is in cyberspace. If there is any place that is constructed, cyberspace is it*". Similarly to the wild west, there are those who attempt to profit in an unethical manner. Nowadays this threat has gone global, and cybercrime encompasses a wide range of criminal activities. This literature review will discuss various forms of contemporary cybercrime. The primary source of information about these cybercrimes is retrieved from Various Types of Cybercrime and Its Affected Area by Yadav et al. (2020).

Types of Cybercrime

One of the more common and well-known forms of cybercrime to the general public is phishing. Phishing consists of manipulative methods that are used to trick victims into giving a criminal sensitive information. Examples of these types of information that criminals might be after include personal information, passwords, and financial information. There are various methods of phishing, but some of the most used methods include fake emails, phone calls, and websites. Criminals can profit from these situations by selling the gathered information or accessing personal accounts, for example, a victim's bank account.

Ransomware is another form of cybercrime that criminals use to limit the access of a victim to their data instead of attempting to access it for themselves. Ransomware is a type of malware that denies a

victim access to their data, giving the criminal a power position that can be abused for extortion. Hackers usually demand payment in trade for the decryption key that unlocks the encrypted data. Methods of delivering ransomware to targets include phishing emails and malvertising, advertisements that can be on legitimate websites but contain malware (Gazet, 2008). Ransomware has become more sophisticated over the years and a profitable business for those willing to break the law. So much so that cybercriminals have created a business model that offers Ransomware-as-a-Service (RaaS) in order to further monetize this form of cybercrime.
Another form of cybercrime that is frequently offered as a service is that of Distributed Denial of Service cyber-attacks, better known as DDoS attacks. Through DDoS attacks, a cybercriminal attempts to deny access to usage of a service, such as services provided by a website. DDoS attacks usually consist of multiple phases, the first being the recruitment of multiple agent machines. It consists of scanning for remote machines that can be infected with attack code, so these machines can be used in a DDoS attack. A common method of infecting such a machine is through the offering of what seems to be a useful downloadable application, but this application secretly contains this attack software. These forms of downloadable software are also called 'Trojans'. The remote machines, now considered subverted machines, can now be used in an attack by flooding the target with attack packets, in turn disabling the service the target is providing (Mirkovic & Reiher, 2004).

Structures of Cybercriminal Organizations

In 'Organizations and Cybercrime' by Broadhurst et al. (2013) an analysis is done on how cybercriminal organizations operate and are structured, through investigation of their methods of facilitating and enabling illegal activities in the digital world. They highlight the importance of the research by illustrating the large-scale effects of cyber attacks conducted by mere teenagers, such as manipulating trades on the NASDAQ stock exchange (US Securities and Exchange Commission, 2000). If a single adolescent is able to achieve such a feat, imagine what well-organized teams of weathered hackers are able to do. This realistic threat needs to be understood better, and Broadhurst et al. aim to contribute to this cause.
The paper explains that structures used in traditional organizations, such as networks, hierarchies, and market structures, are essential when facilitating cybercrime. These criminal organizations require elaborate networks of individuals with specialized skills to carry out specific tasks. Examples of such tasks include hacking, phishing, and money laundering. When the networks are well-developed, they can have a high level of adaptiveness, making them difficult to analyze and disrupt for governments and law enforcement. The research goes into more depth regarding these specializations and the division of labor within cybercrime. For example, some individuals may specialize in creating malware, while others may be responsible for distributing it or using it to carry out attacks. The motivation behind the actions of cybercrime was investigated by the authors as well. It was found that there is a wide range of factors that drive individuals and organizations to engage in cybercrime. One of the most common motivations was financial gain, as cybercriminals can profit large amounts of capital by stealing sensitive information or demanding ransom payments. Somewhat less common, but still high up the list were ideological or political motivations. Cybercriminals have the power to disrupt or undermine specific targets or organizations and might perform these actions for the aforementioned reasons. In short, the authors argue that cybercriminal organizations share similarities in structure to traditional organizations in the sense that there often is an established hierarchy combined with a clear discussion of tasks. Moreover, they offer insights into what drives cybercriminals to commit these digital crimes.

A survey conducted by Huang et al. (2018) goes in-depth on a variety of topics relating to cybercrime. One of these topics is about what the authors describe as a 'Hacker Organization', which describes the methods cybercriminals use to cooperate when starting an attack. The authors go over six basic structure types used by collaborating cybercriminals, which are listed in Table 2.

TABLE 2
Cybercriminal Organization Structures (Huang et al, 2018)

Structure Type	
Swarm.	A collaborative network of hackers operating in viral forms, characterized by a minimal or non-existent chain of command
Hub	A framework with a central group of hackers, around which peripheral associates congregate
Clustered Hybrid	A structure that integrates both online and offline activities, functioning similarly to Hub, focusing on specific activities or methodologies
Extended Hybrid	A structure that resembles the Clustered Hybrid model but encompasses numerous associates and subgroups, while maintaining a necessary level of coordination to ensure operational success
Hierarchy	A structure that bears resemblance to traditional organizations and criminal groups, leveraging online technology to streamline and enhance its activities
Aggregate Structure	A structure that refers to an informally organized collective of hackers, dedicated solely to temporary collaboration and frequently lacking a distinct objective

Each of these forms of organizational structure has its own merits and drawbacks. Consequently, a leader of a cybercriminal organization needs to consider carefully which structure to employ that is best suited for the given attack objective. The most common methods utilized in forming these groups include family ties, friendships, online relationships, and online forums.

2.6 Takeaway

The purpose of this literature review was to provide a baseline of knowledge regarding the HRM processes utilized by IT businesses and cybercriminal organizations, if there are significant differences between the two types of organizations regarding these processes, and to give an overview of cybercrime methods along with the basic principles of how cybercriminal organizations are structured. Furthermore, this literature review aimed to answer the first sub-research question: *"How are cybercriminal organizations structured?"*

According to the literature included in the review, cybercriminal organizations heavily rely on networks, hierarchies, and market structures in order to enable them to conduct their cybercrime activities. These organizations often utilize elaborate networks to recruit and use individuals with specialized skills to carry out specific tasks such as hacking, phishing, creating malware, and more. Furthermore, there have been six main structures of cybercriminal organizations identified, those being: Swarm, Hub, Clustered Hybrid, Extended Hybrid, Hierarchy, and Aggregate Structure. These structures differ greatly in the way they are organized and their levels of coordination. Cybercriminals choose the structure that is most suited for the objective they want to achieve. Moreover, the formation of these structures is often reliant on factors such as family ties, friendships, online relationships, and online forums.

Besides these reoccurring structures, various roles within the hierarchy of cybercriminal organizations can be identified. While not all roles are represented in every structure, most roles are commonly filled. At the top of the hierarchy are the leaders or operators who coordinate and oversee the activities of the organization. They are responsible for setting goals, making strategic decisions, and managing the overall operation. Leaders may have advanced technical skills and deep knowledge of cybercrime tactics. They often have a significant level of authority and control over the organization. A large part of the cybercriminal workforce consists of specialists, who each have their own expertise and role. Examples of these specialists include hackers, programmers, and phishers. Besides these specialists, any large cybercriminal organization requires a sufficient number of facilitators, people who provide various support services. Examples of facilitators include money launderers, botnet operators, and more.

Lastly, every cybercriminal organization of scale needs one or more money handlers. A money handler's responsibility is to handle financial transactions, including receiving payments from victims of cybercrime, distributing funds to members, and managing accounts on virtual platforms used for money transfers.

It's important to note that the hierarchy and roles within cybercriminal organizations can vary. Some organizations may have a more centralized structure, while others may operate in a decentralized manner, with loosely connected individuals or groups collaborating on specific tasks. This large variation in organizational structure makes it difficult to give a definitive answer as to whether their structure is similar to that of traditional organizations. However, the hierarchical structure employed by the majority of investigated cybercriminal organizations allows us to accept the stated hypothesis.

Understanding the roles and hierarchy within cybercriminal organizations provides a foundation for exploring how these structures contribute to their operational effectiveness and the challenges they pose for law enforcement agencies. It also enables a comparison between the structures of cybercriminal organizations and those found in traditional organizations, which can inform strategies for countering cybercrime and developing effective HRM practices within legitimate organizations.

3 METHOD

The purpose of this chapter is to explain how the investigation of the cybercriminal organization's HRM processes is to be conducted. In order to acquire new findings, a text analysis will be conducted. The primary source of data for this analysis consists of the "Conti" leaks. These leaks are relatively recent, being released on Twitter around February 2022. It is essential that the source of information is recent when investigating a topic related to cybercrime, where constant change can make information outdated in months.

Conti is a pro-Russian cybercriminal group known for conducting ransomware attacks on a variety of organizations. The data included in these leaks contains information on their way of operating, victims, and internal communication. This in turn can lead to valuable insights into how such a cybercriminal group operates, how organizations can defend themselves against such a cybercriminal group, and how law enforcement can combat them.

3.1 Empirical Cycle

In order to ensure a structured and repeatable analysis of this phenomenon, De Groot's (1961) empirical cycle is used. This cycle consists of five phases, meant to systematize the methodology of research. These phases are observation, induction, deduction, testing, and evaluation. In the observation phase, a phenomenon is being recognized and an inquiry into the cause of the phenomenon is to be conducted. In the case of this study, the ever-growing threat of cybercriminal organizations is recognized, along with the gap in the literature regarding the HRM processes utilized by these enterprises. In turn, research questions can be formed, which attempt to fill up this gap in the literature. Moving on to the induction phase, the hypotheses, based on various pieces of literature, to the research questions can be formed. The newly formed hypotheses need to be tested, and this test is formulated in the deduction phase. This study employs a text analysis of leaked messages of a cybercriminal organization to shed light on the HRM processes used by such organizations. The test can then be performed, generating data to be evaluated during the evaluation phase. Furthermore, this evaluation phase leads to a theory that answers the research question and allows for new observations that can start the empirical cycle over again. To further illustrate this process, the following flowchart was created.

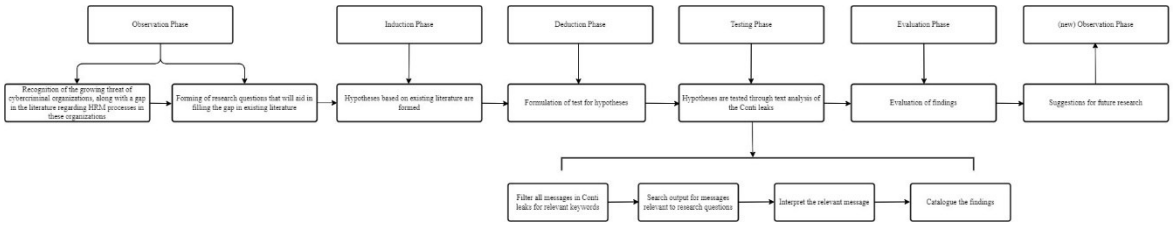

Figure 3. Empirical cycle analysis Conti leaks

3.2 Hypotheses

To answer the research question *"How are Human Resource Management processes organized in a cybercriminal organization?"*, the previously formulated sub-research questions must be answered. This text analysis focuses on answering sub-questions two and three. In order to achieve this, a text analysis approach using the Conti leaks as the primary source of information would be an appropriate qualitative research method. The text analysis will help to test the following hypotheses, formulated for these sub-research questions. The reasoning behind both of these hypotheses is based on the previously conducted literature review.

TABLE 3
Hypotheses for sub-research questions.

Hypotheses SRQ
H_{SRQ2}: Cybercriminal organizations provide large quantities of financial compensation compared to 'regular' IT organizations.
H_{SRQ3}: Cybercriminal organizations employ various unorthodox methods to select, recruit, and retain personnel compared to 'regular' IT organizations.

This research method of text analysis gives the opportunity to analyze this complex phenomenon. After completion of the text analysis, opportunities for comparison between the HRM practices of a cybercriminal organization and those of traditional organizations arise, giving this study the potential to grant insight into the differences between these two types of organizations regarding their HRM practices, including recruitment, selection, and retention methods. The use of the Conti leaks as a primary source of information allows for a deep examination of the inner workings of the cybercriminal organization.

The data analysis will be performed using a combination of Python code in Google Colab and Excel. Python is a coding language that allows for the organization of the unstructured Conti leaks. Utilizing this method of structurization will yield tables that display the specific data required to answer the sub-research questions. In turn, the data most relevant to answering the sub-research questions will be imported into Excel for a more manageable overview.

3.3 Existing Research on Conti Leaks

The Conti Leaks consist of a tremendous number of messages between members of the cybercriminal organization Conti. In order to narrow down the quantity of data, this research focuses on conversations between more high-ranking members of the organization and members specifically involved with HRM. The messages sent between these members have an increased likelihood of describing how the HRM practices are conducted compared to messages between "ordinary" members.

Existing literature on the Conti leaks provides insight into the various roles that the individuals have within the organization. One paper of particular interest is the research by Gray et al. on the business case behind Conti. This research delivers an empirical analysis of Conti, utilizing the same leaked files this thesis investigates. Gray et al. managed to identify the five main actors within the Conti leaks. These five actors can be seen as managers within the Conti organization, supervising all payments, operations, and malware builds. All users of these Jabber chats use aliases to protect their identity, and these managers are no exception. The aliases of the five main actors identified by Gray et al. are Defender, Stern, Buza, Mango, and Bentley.

A blog post by Northwave Cyber Security[10], written by Noël Keijzer, goes into detail regarding the Conti leaks. Firstly, they provide generic information about the dataset. The Conti leaks contain almost 169,000 messages, sent by 465 unique users. Utilizing information from the leaks, Northwave was able to identify one of the Conti members, exposing his anonymity.
Furthermore, Northwave shares the probable roles of actors who have sent the most messages. Most notably, they list 'Target' as one of the most active members of the organization, sending over 35,000 messages and being a HR manager within Conti. Using this knowledge, we can prioritize Target as a member of interest for our analysis of the HRM structure within the cybercriminal organization.

[10] https://northwave-cybersecurity.com/threat-intel-research/when-the-hackers-get-hacked-pt2

3.4 Data Collection and Importing

The first step in the method consisted of collecting the available data and moving it into Google Colab, a hosted Jupyter Notebook service that allows for the usage of Python code. In the case of this research, this meant collecting all available data regarding the aforementioned Conti leaks, which contain detailed information regarding the operating process of the cybercriminal organization Conti. Many of these leaked files are available on Github.com.[11] The leaked files have been translated into English as well. Using Jupyter Notebook, the files can be imported from Github.com. This is necessary in order to conduct the text analysis in Google Colab. The poster of the leaks provided the code required to load the Conti leaks data into a pandas dataframe, which displays the content of each message, the time at which the message was sent, and both the sender and receiver of said message.

3.5 Data Analysis

After the importing of the data is completed, the analysis of the data can begin. The first step in this process is forming a list of questions of which the answers help in answering the sub-research questions. This involves generating an extensive list of questions relevant to the various research questions. Furthermore, attempting to answer additional questions relating to how HRM is structured within Conti can help create a more complete overview of the organization structure. In turn, a full overview of these questions was created to streamline this process (Appendix A).

The questions will be difficult to answer directly from the dataset. Therefore, a list of simple sub-questions will be created that are more straightforward to answer. To illustrate, one question could be *'How much does a member of Conti earn?'* and the corresponding 'simple' question would be *'What words directly relate to salary?'*. This simple question instructs us to filter only for messages containing words relating to salary, in turn yielding insights into how much a member of Conti earns. In order to discover all the most relevant words to filter for, the following concept map was created.

[11] https://github.com/TheParmak/conti-leaks-englished

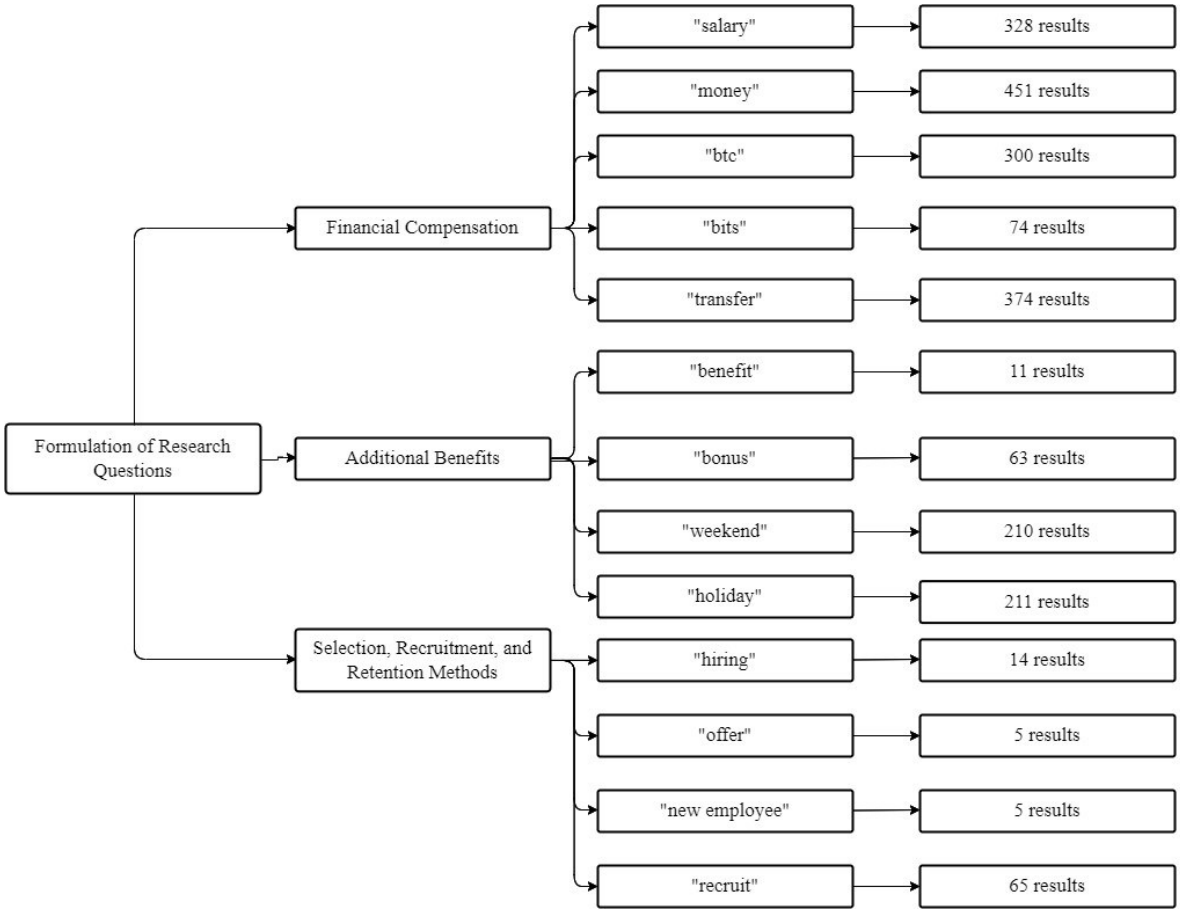

Figure 4. Concept map of relevant words

The figure above displays most of the words that were used to filter out meaningful messages from the enormous dataset. The words that were used as filters are based on the sub-research questions investigated in this part of the research. To illustrate, sub-research question two goes into detail regarding the financial compensation members of cybercriminal organizations receive. This led to using words such as “salary” and “transfer” as filters for relevant messages. Once such a relevant message was found, the entire conversation in which the message was sent was investigated. Furthermore, Rogers (2018) found that writing memos during text analysis can be beneficial to further capture thoughts and insights, providing additional data to study. Following this method, alongside each noted message a brief memo will be written, detailing why that message is of interest. One essential aspect to keep in mind during this procedure is to avoid making assumptions about the data and write it down as stated in the data.

Most of the Python code (Appendix F) was generated using ChatGPT, a generative artificial intelligence created and owned by OpenAI. The created tables will be analyzed for messages that can be helpful in answering our question. If such a message is found, it will be written down in Excel. Prior to this analysis, an investigation into individual actors was conducted. The purpose of this was to find out which actors play the largest role in the organization, and which actors are most involved in issues relating to HRM. Knowledge of what an actor’s role within Conti is provides valuable context when analyzing the messages these actors have sent. A table (Appendix B) containing this information was created.

3.6 Data Visualization and Interpretation

After completion of the analysis, the results will be a significant number of messages relevant to answering the sub-research questions. These messages will be grouped together in tables for each of the three questions they relate to. Afterward, the messages in the tables can be interpreted, which should provide helpful insights for testing our hypotheses.

Furthermore, the findings of the completed data analysis can then be compared against information gathered in the literature review to examine for similarities and differences between cybercriminal organization Conti and traditional organizations regarding their HRM processes.

4 RESULTS

The chapter focuses on the results of the HRM-focused analysis of the Conti leaks. The results will be used to answer the second, third, and fourth sub-research questions.

4.1 Dataset Description

The dataset investigated for this research includes the jabber chat logs used by the cybercriminal organization Conti from 2020, 2021, and 2022. Conti is a Russia-based group providing ransomware-as-a-service (RaaS). Previous research on Conti shows that some form of organizational structure is present. The cybercriminal group is led by someone who calls himself Stern (stern@q3mcco35auwcstmt.onion). Besides being the group leader, he is also in charge of distributing salaries among the other members of the organization. Another main character in the leaks is known as Mango (mango@q3mcco35auwcstmt.onion) and seems to be a general manager. For this research specifically, the member known as Target (target@q3mcco35auwcstmt.onion) is of interest as well. He can be seen as an HR manager and is involved in finding and recruiting new members. Besides these managers, some members focus on HR tasks within the organization who are of increased interest. Examples of them include Salamandra (salamandra@q3mcco35auwcstmt.onion) and Mavelek (mavelek@q3mcco35auwcstmt.onion). Within the leaks, 465 unique users were identified.[12]

The investigated chat logs were retrieved from Github and consisted of two compressed files 'Conti Chat Logs 2020.7z' and 'Conti Jabber Chat logs 2021 – 2022.7z'. The files contained 168,740 messages, all sent between the 21st of June 2020 and the 2nd of February 2022. For every one of the 168,740 messages, the index number, date and time when the message was sent, sender, receiver, the original message (mostly in Russian), and the English translation of the original message are displayed in separate columns. Table 4 gives an overview of these columns, illustrating what the investigated data looks like.

TABLE 4
High-level statistics of the investigated data

Column Name	Description	Unique Values	Missing Values
ts	Time series: displays both the date and time when the message was sent	168740	0
from	Displays the address of the sender of the message	346	0
to	Displays the address of the recipient of the message	463	0
body	Displays the original message	98406	0
body_en	Displays the message in English	95721	0
body_language	Displays the language of the original message (note: this process is not flawless, e.g., the message "yo" is recognized as Spanish. This is what causes a large number of unique values for this column)	89	28453

[12] https://northwave-cybersecurity.com/threat-intel-research/when-the-hackers-get-hacked-pt2

4.2 Ransomware Group Conti

To learn more about the HRM processes of cybercriminal organizations, a contemporary organization involved in cybercrime must be investigated. The group that is being analyzed in this thesis is the ransomware group Conti.

Most cybercriminal organizations that offer ransomware as a service (RaaS) develop this ransomware and offer this malicious software to affiliates who pay the organization to use it. The affiliates do not need significant technical knowledge to use this ransomware, making cybercrime more accessible to criminals without a background in information technology.[13] Conti is also seen as a RaaS model variant; however, the way Conti interacts with their affiliates has been observed to be different. It is probable that Conti developers compensate the ransomware deployers with a salary instead of a percentage of the proceeds, which is the typical arrangement for affiliate cyber actors, and then receive a share of the profits from a successful attack.[14] After obtaining sensitive information, a double extortion technique is utilized by the cybercriminals. Firstly, the accessed files of the target are encrypted, after which a cybercriminal organization demands payment to restore the target's access to the files. The second part of this technique involves the threat of releasing the victim's data to the public if they are not willing to pay an additional ransom. This method is especially effective if the accessed data is classified.[15]

Gray et al. (2022) have found that Conti has various departments in which members have their own set of tasks. The departments they found include management, development and infrastructure, access operations, and negotiations. Management oversees the organization as a whole and is responsible for human resources, recruitment, finance, and payroll. System administrators and software developers are part of the development and infrastructure department. Their main responsibility is to ensure that the RaaS operations are able to continue at all times. Other responsibilities include acquiring and developing software and other tools necessary to conduct the organization's operations. Access operations are in charge of selling access to their victim networks to affiliates. The negotiations department is responsible for contact with victims. They also run the public leak website, which is the place where the details of the victim are recorded. Most new members are recruited through hacker forums and legitimate job boards and trained by team leaders.

4.3 Finding Relevant Messages

Using keywords to filter the dataset containing all messages sent by Conti members led to interesting messages and conversations between members, revealing information about the HRM processes in the cybercriminal organization. The flowchart on the next page illustrates this process, using the word "salary" as an example. One of the topics investigated was the level of financial compensation members of cybercriminal organizations receive. This led to various keywords to filter for, "salary" being one of them. Afterward, all the relevant messages containing the word salary were noted, along with their index number. Furthermore, for each of these messages, a memo was written explaining the relevance of the message. This process was repeated for other keywords relating to financial compensation, and for keywords relating to additional benefits provided for members of Conti and the selection, recruitment, and retention methods employed by 'manager-level' members of the organization. The findings derived from these queries can be found in tables in the appendix. The tables provide a more concise overview of the results and in turn aid in the ease of comparison and analysis. In order to structure the information more clearly, the tables are sorted per answered sub-research question.

[13] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[14] https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware
[15] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

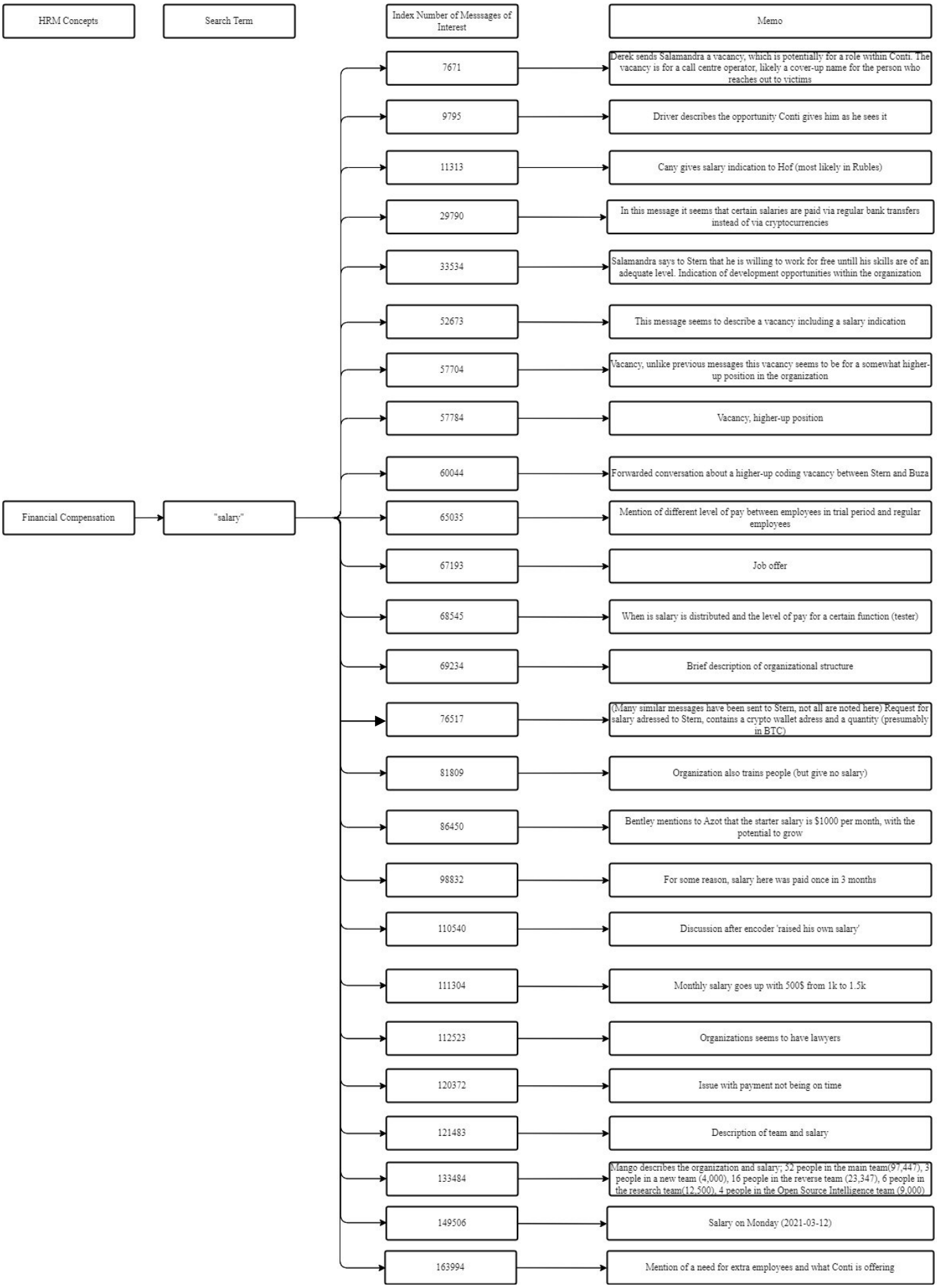

Figure 5. Flowchart illustrating relevant messages containing "salary"

4.4 Findings on Benefits

In order to find out more about the HRM processes within cybercriminal organizations, the thesis aimed to uncover what type of benefits these organizations provide to their members. To do this, the following sub-question was formulated:

SRQ2: "What benefits do employees of cybercriminal organizations receive?"

During the analysis of the Conti leaks, information regarding the benefits received by various members of the organization was found. The analysis was first focused on uncovering the level of financial compensation received by members of Conti. The messages which were most useful in acquiring the following information can be found in Appendix C. Similar to non-criminal organizations, salary differed depending on function, experience, and qualifications. Table 5 displays two salaries mentioned in vacancies. Therefore, these salaries are for starter positions and are therefore likely lower than salaries earned by long-term members of the organization. The columns in Table 5 represent the role within the organization, the salary for that role per month, and the index number of the messages that included relevant information regarding this salary.

TABLE 5
Financial compensation within cybercriminal organization Conti

Role	Salary	Index number
Call Center Operator	$900-$1,600	7671
(Junior) Accountant	$2,500	57784

The messages suggest that the role of call center operator is a cover-up name for the role of negotiator. This will be one of the members who will reach out to the victims of their ransomware to discuss the terms of payment.

Of course, there are many more roles than the two mentioned above within Conti. The data did not contain specifics regarding the level of financial compensation rewarded for those roles. However, messages were sent regarding organization-wide salary days and the salary that was distributed on those days among various teams. Using this information, average salaries for other roles within Conti can be determined.

TABLE 6
Financial compensation among teams within cybercriminal organization Conti

Team	Total salary	No. members	Average salary	Index number
Main team	$97,447	52	$1,873.98	133484
New team	$4,000	3	$1,333.33	
Reverse team	$23,347	16	$1,459.18	
Research team	$12,500	6	$2,083.33	
OSINT team	$9,000	4	$2,250	

The columns in Table 6 represent the team within the organization, the total salary that the team received, the number of team members, the average salary per team member, and the index number of the message that included the information used in this table.

The numbers shown in the tables above have little meaning without context. To provide this, the salaries mentioned by Conti will be compared against the median salaries in certain sectors in Russia. See Table 7 for this information. The median salary expressed in USD was calculated using the RUB to USD exchange rate of April 2022.

TABLE 7
Median salary for various fields Russia 2022[16]

Field	Median Salary in Russia 2022 (RUB)	Median Salary in Russia 2022 (USD)
Mining	62.284,00 ₽	$ 809,69
Finance and Insurance	51.189,00 ₽	$ 665,46
IT and Communications	48.769,00 ₽	$ 634,00
Scientific Field	48.508,00 ₽	$ 630,60
Construction	43.927,00 ₽	$ 571,05
Transportation and Storage	42.933,00 ₽	$ 558,13
State Control	39.932,00 ₽	$ 519,12
Housing and Communal Service	39.590,00 ₽	$ 514,67
Manufacturing Industries	39.091,00 ₽	$ 508,18
All Industries	37.650,00 ₽	$ 489,45
Trade	34.598,00 ₽	$ 449,77
Healthcare	33.347,00 ₽	$ 433,51
Water Supply	32.241,00 ₽	$ 419,13
Agriculture	31.899,00 ₽	$ 414,69
Real Estate	31.246,00 ₽	$ 406,20
Education	31.243,00 ₽	$ 406,16
Sports and Leisure	30.611,00 ₽	$ 397,94
Administrative Activities	28.655,00 ₽	$ 372,52
Hotels and Catering	26.811,00 ₽	$ 348,54

The fields of interest of this research are finance and insurance, IT and communications, and administrative activities, since most work done within Conti relates to these fields. The median salary in these fields is $665.43, $634, and $372.52 respectively. Comparing these numbers to the salaries offered by Conti leads to the conclusion that Conti offers exceptional wages. To illustrate, Conti offers $900 per month for an administrative position that would earn someone around $372.52 per month in a traditional organization. Similar ratios are found when comparing positions in Conti in the fields of finance and IT to traditional organizations. The bar chart in Figure 6 displays this difference in salary more clearly.

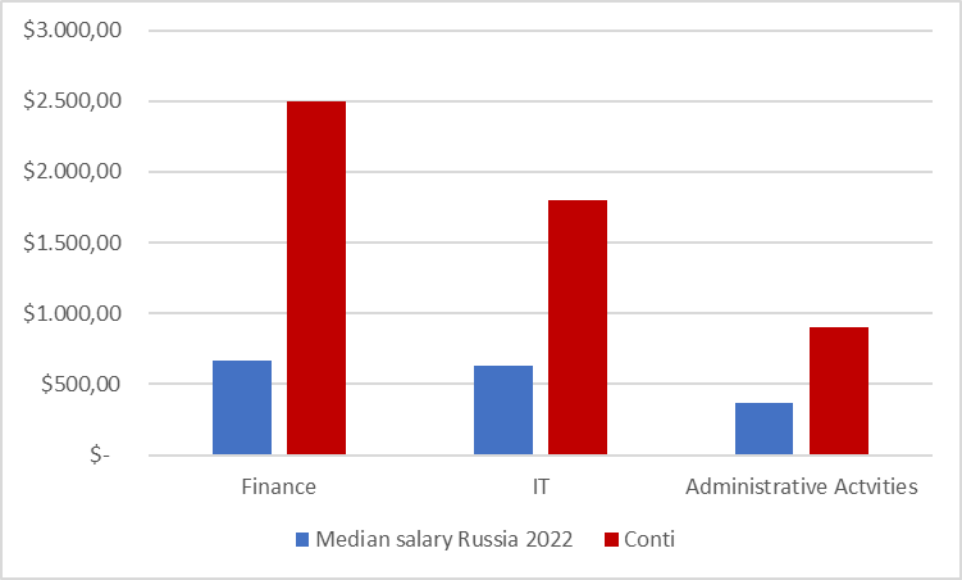

Figure 6. Comparison of salaries in Russia vs Conti

[16] https://vc.ru/money/441150-naskolko-vyrosli-zarplaty-v-2022-godu-v-kakih-sferah-samye-vysokie-i-nizkie-zarplaty

Various indications of salaries for various positions are given, but the method of distribution of these salaries is equally relevant. Most of the time salary is distributed via a crypto transfer, paid in bitcoin. This is clearly indicated by the large number of messages similar to message 76517: "hello, send salary plz 3BWQhLHVWwm57jdhCTnZzD9XrYa4CYabiL 0.13541791", in which a member of Conti asks Stern for his salary and provides the crypto wallet address his salary can be sent to, along with the quantity of bitcoin he expects to get paid. Despite most salaries being distributed in cryptocurrency, there is evidence that the organization uses bank transfers as well. In message 29790, Van asks Bentley the following: "I wanted to ask this... Stern transfers my salary to my bank card. A bank will not prepare trouble? Are there any other ways to get money?". Bentley responds to this with the following: "I get through the services of exchanging cue ball for rubles. And how are you?". This is clearly translated incorrectly, and when translating the original Russian message in Google Translate 'cue ball' is replaced with bitcoin. Bentley continues by reassuring Van that he will not be 'burned' through this method of payment. A further explanation of this method is absent, however. In short, most salary payments within Conti are conducted using cryptocurrency, but it appears that the organization has methods to pay in cash without leaving clear traces for law enforcement agencies.

During analysis of the Conti leaks, various messages were found that included information about benefits that members of Conti can receive. Certain benefits were granted to every member of the organization, but others were only received by those able to perform well. The messages that were most useful in acquiring the following information can be found in Appendix D. Table 8 was created to visualize these benefits.

TABLE 8
Benefits within cybercriminal organization Conti

Type of benefit	Additional information	Index number
Monetary bonuses	Various mentions of bonuses of different magnitudes. Bonuses range from ₽10,000 (about $100) to ₽140,000 (about $1,400). These bonuses are mostly performance related, but a holiday bonus is also being handed out	9782, 25001, 53000, 57704, 100790, 106104, 133185
Off days	Vacancies put out by Conti mention that a paid vacation is a part of that role. Furthermore, Saturdays and Sundays are regarded as weekends, and therefore off days	7671
Legal support	During a discussion of an investigation into Conti, company lawyers are mentioned	112523

The columns in Table 8 represent the type of benefit provided by Conti, additional information providing some context relating to the type of benefit, and the index number of the message that included the information used in this table.

Besides the salaries within Conti, an overview of various bonuses is displayed. These bonuses can be earned by members for exceptional performance, but whether exceptional performance in a cybercriminal organization is the same as that in a traditional organization is still unclear. In message 35641 Target promises a bonus to a member named Deploy. Further investigation in the conversation that precedes this promise of a bonus on top of a salary of $2,500 (message 35525 Deploy demands: "Stern $ 2.5k for two weeks") for agreeing to work on a 'crypt'. Crypt is short for crypter, which is software used for encryption, obfuscation, and manipulation of malware.[17] The main purpose of a crypter is to make malware harder to be identified by security programs. Target agrees to this demand. Another indication of Deploy's exceptional performance within Conti is the following message (35413) sent by Target: "you are the smartest crypter in the world whom I know personally". In this

[17] https://www.trendmicro.com/vinfo/us/security/definition/crypter

case, exceptional performance can be defined as being exceptionally good at software creation, specifically the creation of crypter software in the case of Deploy.

Another topic of interest is that of the working hours mentioned in the vacancy of message 7671. The work schedule is from 18:00 to 2:00 in Moscow time. Given that many members of Conti originate from Russia and certain neighboring countries, this work schedule is different from that of many traditional organizations. The reason for these unusual working hours could be that the call center operators of Conti must reach out to businesses located in other time zones, suggesting Conti is operating globally.

Lastly, the vacancy mentions that the position is not registered according to the 'Labor code'. Once again, we assume that the Russian Labor Code is of used here since Conti is an originally Russia-based organization. In other words, someone in this position at Conti does not have the rights mentioned in this code. These rights are about a range of employment conditions and labor rights and liberties of Russian citizens, such as increases in salary after fulfilling a position for a certain amount of time, working hours, and more.[18]

[18] https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_363.pdf

4.5 Findings on Selections, Recruitment, and Retention

Besides the various forms of benefits, the selection, recruitment, and retention methods of these organizations were investigated as well. To learn more about these methods in the cybercriminal world, the answer to the following sub-question was sought:

SRQ3: "What are selection, recruitment, and retention processes in cybercriminal organizations?"

During the analysis of the Conti leaks, various messages were found that included information about the selection, recruitment, and retention techniques employed by Conti. Table 9 contains information regarding how these processes take place within the cybercriminal organization. The messages which were most useful in acquiring the following information can be found in Appendix E.

TABLE 9
Description of selection, recruitment, and retention procedures used by cybercriminal organization Conti

Type of process	Description of process	Index number
Selection	Conti has various selection criteria, which differ for different roles within the organization. • Call Center Operator: good knowledge of spoken English (level B2-C1); age from 18-25 • (Junior) Accountant: college degree or equivalent experience; proficiency in the use of computer and office applications; knowledge of accounting basics; strong communicative and analytic skills • Tester/Developer: basic knowledge regarding scripting languages or control systems is a must; high proficiency in these skills results in a higher base salary	7671, 14548, 57704
Recruitment	There are mentions of forums on which vacancies are posted. The names of the forums are not mentioned in the leaks. Candidates who meet the aforementioned selection criteria are invited for a conversation with one of Conti's HR managers to test them. If HR sees potential, they will be sent through to a trainer in their respective department. The candidate will answer questions to determine his capabilities and will be trained using a manual, getting them up to speed within the organization. Candidates that show potential, but lack some of the required skills will be offered the opportunity to work for free at first, in order to develop their skills	2898, 2966, 2992, 10683, 20809
Retention	Little to no mentions of a thought-out retention plan for employees. However, it is clear that good work is rewarded with monetary bonuses, which can be seen as a retention method	9782, 25001, 53000, 57704, 100790, 106104, 133185

The columns in Table 9 represent the type of process being described, a description of how this process takes place within Conti, and the index number of the message that included the information used in this table.

Conti mentions the posting of their vacancies on a ‘hack forum’ but does not specify which forum they utilize to recruit new members to their organization. This might be to reduce the risk of exposure to law enforcement. There can be multiple reasons as to why the name of this hack forum is not mentioned within the internal communication of Conti. One of these reasons could be that most of the members are not aware of the specific hack forum used by Conti. This reasoning is flawed, however, since many members of the organization are likely to have been recruited from such a forum. A more reasonable explanation would be that higher-ranking members of Conti have imposed a rule that states that the hack forums should not be mentioned by name. This reduces the exposure of these hack forums, in turn reducing the risk of being exposed to law enforcement agencies. Furthermore, the hack forums used by Conti might utilize a so-called ‘closed’ model. A forum organized following this methodology can only be joined by new members if they receive a recommendation from an existing member. This decreases the chance of infiltration by law enforcement agencies and can help improve the quality of interaction and trade within these communities (Motoyama et al., 2011).

The vacancy described in message 7671 also mentions a specific age group of 18 to 25 for the function of call center operator. There seem to be no messages giving an explanation of why the cybercriminal organization has these specific age selection criteria.

The methods used for selection and recruitment by Conti align with existing HRM theories, namely with principles from both human capital theory and the person-job fit theory. Human capital theory is a framework to understand the role of education, training, skills, and experience in enhancing a person's productivity, which in turn can help increase overall profitability. Furthermore, it suggests that investments in education and training can be compared to investments in physical capital, like machinery or equipment, and thus can increase returns in the form of increased productivity and earnings over time (Becker, 1975). The person-job fit theory proposes that individuals are more likely to perform well and remain in a job when there is compatibility between their characteristics and the requirements of the job. This theory suggests that a good match between an individual's skills, abilities, and values and the demands and characteristics of the job leads to positive outcomes for both the employee and the organization (Kristof-brown et al., 2005).

From the human capital theory perspective, Conti understands the strategic benefit of investing in top personnel by paying high wages and offering bonuses. These monetary rewards have the power to draw in competent workers, providing the company with a large pool of human resources. Consistent with the human capital theory, Conti's approach recognizes that people possessing relevant skills and experience may make a substantial contribution to the success of the firm. Another way that Conti's actions align with the human capital theory is through its readiness to invest in members' additional training to enhance their expertise in their specialized sectors. Moreover, Conti is well-known for the amount of funds they have been able to extort from organizations and is a sizable company by cybercriminal standards. The number of hackers hoping to work for Conti may rise as a result of this achievement in the realm of cybercrime. This finding is consistent with the person-job fit hypothesis, as Conti looks for candidates whose goals and beliefs mesh well with the high-stakes world of cybercrime. Conti appeals to those who want a sense of distinction and belonging in their workplace in addition to financial benefits since it is an exclusive group within the hacking world. Therefore, Conti's hiring procedures show a strategic connection with person-job fit and human capital theories, highlighting the significance of luring and keeping talent that supports the goals of the company.

4.6 HR Canvas

This collection of tables gives insight into various aspects relating to how HR processes are managed within cybercriminal organization Conti. The tables do lack a clear overview of HRM within the organization as a whole. A common tool to describe how an organization creates, delivers, and captures value is the business model canvas, originally described in a work by Osterwalder & Pigneur (2010). This canvas goes over nine 'building blocks', essential components involved in a business' value creation. Examples of these components include the customer segment, which explains who it is value is being created for, and the value proposition, which explains what value it is you deliver and which problems you are solving.

Vulpen & Veldsman (2023) recognized the business model canvas' potential as a descriptive tool for organizations and alignment within businesses. However, when faced with the issue of HR solutions often not aligning with businesses' key challenges, a new solution was found. The business model canvas was transformed from a commonly used business tool into a tool for strategic HR management. More specifically, the HR canvas helps provide a clear strategic overview of the HR organization, its customers, value proposition, activities, strategic differentiators, and cost drivers. Taking the time and effort to clarify all of these elements will help HR professionals define their service delivery while articulating HR's strategic impact and value (Vulpen & Veldsman, 2023). While this HR canvas is originally intended as a management tool, it can also be used as a means to describe HR in an organization, similar to how the original business model canvas does this for an entire organization. Using the information found during the analysis of the Conti leaks, the HR canvas can be filled in for the cybercriminal organization Conti, giving an overview of their key HRM practices.

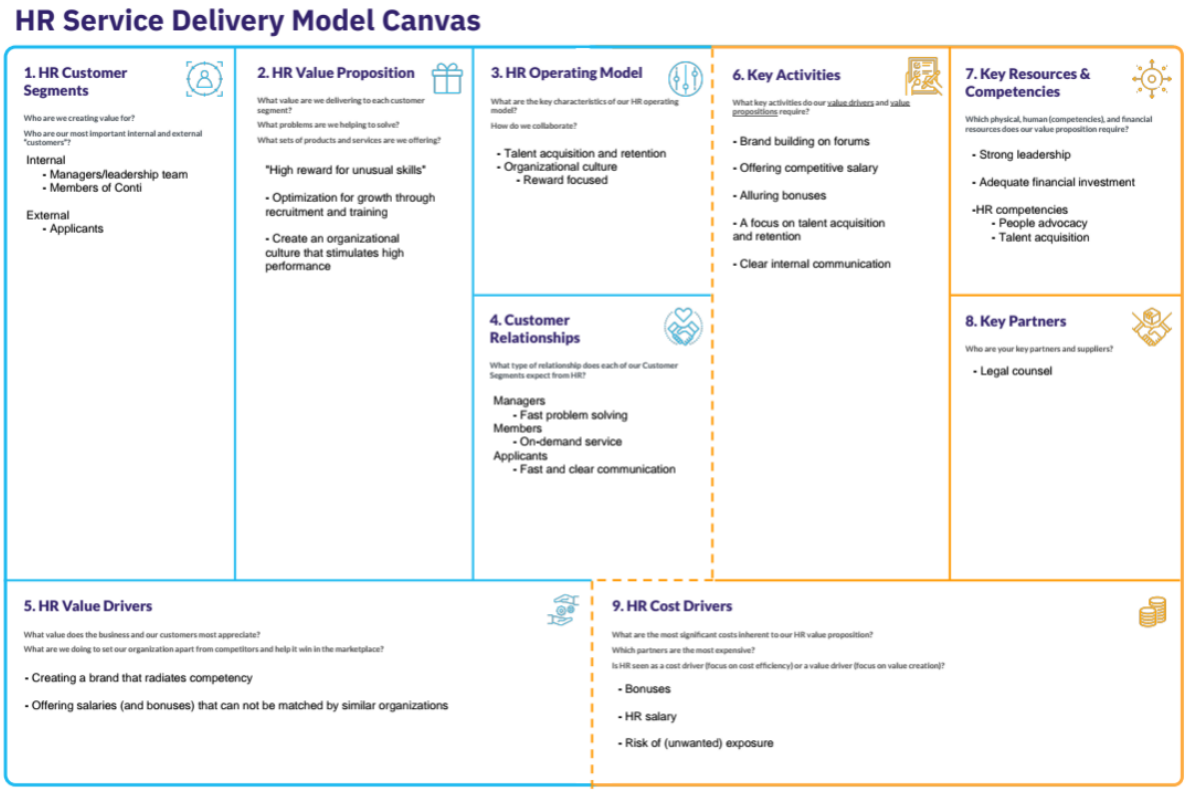

Figure 7. HR Canvas Conti

The nine segments of the original business model canvas have been replaced with segments linking to HR, of which the first five segments are related to the strategy employed by the organization, while segments six through nine display how this is executed in reality. The first of these segments is the HR customer segment. This includes all relevant stakeholder groups in and outside of the organization for which HR is of value. This includes employees, managers, customers, shareholders, employee representation groups, and so on. The aim here is to create value for external stakeholders through value creation for internal stakeholders. For Conti, this is somewhat different, however. Conti has limited external stakeholders it wants to create value for, thanks to its business model being cybercrime. The internal customer segment here includes the management of Conti and all other members. Furthermore, HR has the task of recruiting new members, making applicants external stakeholders. Secondly, even a non-traditional organization such as Conti has an HR value proposition. Their HR value proposition can be summarized as offering high rewards for unusual skill sets. In order to promote this type of organizational culture, the organization must display a willingness to offer bonuses to members who excel at their functions. Moving onto the HR operating model and its key characteristics, two key characteristics have been identified. The first is talent acquisition and retention. For Conti to be profitable, the organization must stay ahead of law enforcement and cybersecurity providers. To sustain that advantage, a constant stream of new talent must be acquired and retained. Furthermore, there is a high priority for strong employee development. This employee development has the same goal as talent acquisition, contributing to a highly competitive workforce. The second key characteristic related to organizational culture, which promotes excellence. The main way this is outed is through rewarding this excellence via bonuses. The fourth segment is about the relationship between each of the customers from the customer segment and HR. Firstly, there is management, which requires fast problem-solving from HR. To illustrate, if there is a sudden need to upscale the workforce because of an upcoming large project, HR must have the ability to work on and resolve this issue. Secondly, the members of Conti require on-demand service. This is mostly seen in the availability of HR when a member has a question. These questions can be about a wide range of topics but tend to mostly be salary related. The last of the customer relationships is the one between HR and applicants. This relationship is about clear communication, HR wants to send out a detailed message to all applicants of what they require of a potential applicant and what Conti can offer in return. The fifth and last strategy related segment is about HR value drivers. This segment explains what HR contributes to value creation. In the case of Conti, HR is tasked with creating a competent brand, that attracts talented IT specialists. Furthermore, the organization must offer financial compensation that is hard to be matched by other organizations. The talent this attracts contributes to creating an advantage over law enforcement and cybersecurity providers.

The last four segments are about HR in practice and how the strategy that the organization came up with is executed. The first of those four are the key activities done by HR that enable the HR value drivers. Secondly, there are the key resources and competencies HR must have. In the case of Conti, strong leadership is required. HR must be able to get the required financial resources in order to be able to attract, recruit, and retain the needed talent. However, the way these funds are acquired is through negotiation with upper management, therefore requiring these strong personalities with the ability to convince others. The eighth segment lists HR's external key partners. Cooperation with other organizations is rarely mentioned in the studied files, except for the legal counsel used by the organization. Lastly, HR's cost drivers are described. These drivers are the main costs made by HR within the organization. Within Conti, these costs are mostly made up of financial costs that are needed to support the talent acquisition and organizational culture that rewards high-performing individuals through bonuses. Another, non-financial, cost that must be considered, is the unwanted exposure that comes with brand building. Conti wants to be known as a competent organization to the right people, namely people interested in working with them. However, with marketing to these people, the risk of exposure to law enforcement and cybersecurity providers grows as well.

5 DISCUSSION & CONCLUSIONS

This chapter provides a summary and discussion of the findings of the thesis. Firstly, the motivation of the thesis is revisited, and the main findings are summarized by answering the main research question in accordance with the sub-research questions. Subsequently, the limitations of this study are addressed along with suggestions being given for future research.

5.1 Discussion of Main Findings

Human Resource Management plays a crucial role in organizations, encompassing tasks such as recruitment, deployment, and management of employees. Initially seen as a cost to minimize, HRM now holds significance in value creation for organizations by aligning objectives, nurturing workplace culture, and fostering employee development. Ensuring both external and internal fit of HRM strategies is vital for maintaining a competitive edge.

This necessity extends beyond traditional organizations to include criminal organizations, particularly those involved in cybercrime. Cybercrime poses a significant threat, to governments and businesses alike. These criminal groups require specific skill sets, leading to extensive recruitment practices, as seen in cybercrime-focused organizations. Despite their decentralized nature, these groups can cause widespread disruption, underscoring the importance of understanding their structure for effective law enforcement. Academic inquiry into cybercriminal organizations aids in countering the growing threat of cybercrime. To shed more light on this issue, the following main research question was developed:

RQ: "How are Human Resource Management processes organized in a cybercriminal organization?"

To answer this research question, three sub-research questions were formulated. Each of these questions will be revisited to provide a coherent overview of the main findings. The first sub-question aims to describe the structure of cybercriminal organizations. Understanding of the organizational structure in cybercriminal organizations will aid in the comprehension of other processes within the organization. In order to answer this sub-question, a systematic literature review was conducted. The following sub-question was formulated for this purpose:

SRQ1: "How are cybercriminal organizations structured?"

The research found that cybercriminal organizations rely on intricate networks, hierarchies, and market structures to facilitate their illicit activities. These entities recruit individuals with specialized skills, such as hacking and phishing, through extensive networks. Various organizational structures have been identified, including Swarm, Hub, Clustered Hybrid, Extended Hybrid, Hierarchy, and Aggregate Structure, each tailored to specific objectives and coordinated through factors like family ties and online relationships.

Within these structures, distinct roles emerge, with leaders orchestrating operations, specialists executing tasks like hacking, and facilitators providing support services. Money handlers manage financial transactions, underscoring the complex organization of cybercriminal groups. While structures can vary from centralized to decentralized, a hierarchical framework predominates, influencing operational effectiveness. This variation in organizational structure between cybercriminal organizations poses a challenge for law enforcement and cybersecurity providers when attempting to form a 'silver bullet' solution to this issue.

With this overview of cybercriminal organizational structure provided, the focus of the research shifted to the HRM processes within these organizations. Membership in a cybercriminal organization comes with inherent risks, prompting managers to offer compensatory benefits, both monetary and non-monetary, to mitigate these risks. Understanding the diverse forms of compensation provided to employees sheds light on the incentives attracting IT specialists to these illicit enterprises. Given the harsh operational landscapes of cybercriminal organizations compared to conventional ones,

exploring the strategies employed to maintain a consistent workforce becomes particularly intriguing. To further analyze the nature of these benefits, the following sub-question was formed:

SRQ2: "What benefits do employees of cybercriminal organizations receive?"

To answer this sub-question, leaks of internal communication within the cybercriminal organization Conti were investigated. This analysis yielded insight into the various benefits members of this organization receive, with most of these benefits being of a financial nature. Similarly to traditional organizations, salary differs per role, tasks, and responsibilities within the organization. Furthermore, excelling performance within Conti is rewarded with significant financial bonuses.

Salaries ranged from $900 to $2,500 per month. The salary of $900 was offered for a starting position as a call center operator, while the position that offered $2,500 was for the role of junior accountant. When looking at these numbers, one must consider that these salaries are taken from descriptions of job positions. In other words, a long-time member of Conti is likely to have received multiple raises and will earn more.

In the results chapter, these wages are compared to the median salaries earned by Russian citizens in their respective fields. The clear outcome of this comparison was that Conti offers salaries that cannot be matched by traditional organizations in Russia. This might increase the appeal of joining such a cybercriminal organization, especially when one considers that most of the salaries given out by Conti found in this research are for starter positions within the organization, leaving potential for growth. Besides salary, Conti is keen to reward high-performing individuals through monetary bonuses. These bonuses range from ₽10,000 (circa $100) to ₽140,000 (circa $1,400). Besides these performance related bonuses, holiday bonuses are given out by Conti as well. Not all bonuses are financial in nature, however. Vacancies put out by Conti also have mentions of paid vacation. Furthermore, Saturdays and Sundays are regarded as weekends, and therefore off days. Legal support is also provided by Conti when needed.

Human resource management consists of more than just offering adequate compensation for your employees for their efforts. The various methods utilized by organizations to attract and maintain are other key components of HRM. To further investigate these methods within cybercriminal organizations, the following sub-question was formulated:

SRQ3: "What are selection, recruitment, and retention processes in cybercriminal organizations?"

This sub-question can be divided into three components, the first being selection criteria within Conti. Vacancies described by HR employees of Conti contain various selection criteria. Similar to traditional organizations, these criteria vary per position. Aspiring call center operators must have a good knowledge of spoken English, more specifically a level ranging from B2 to C1. Furthermore, an age preference was given from 18 to 25. Criteria for the role of accountant are stricter. A college degree or equivalent experience is a must. Moreover, one must have proficiency in the use of computer and office applications and strong communicative and analytic skills are required. For the position of tester or developer, the criteria are more lenient, with the organization displaying a willingness to help someone develop his skills further if he has a grasp of the basics of scripting languages or control systems. However, a higher proficiency in these fields can lead to a higher starting salary within Conti.

The second component of this sub-question is about the recruitment process utilized by cybercriminal organizations. The criteria and compensation for a specific position are posted on forums of illicit nature. In the case of Conti, candidates who fulfill the stated selection criteria will be invited for an interview with one of Conti's HR managers for assessment. If the HR team identifies potential in the candidates, they will proceed to be evaluated by a trainer from their respective departments. During this evaluation, candidates will respond to inquiries to assess their capabilities and will receive training utilizing a manual to familiarize them with the organization's operations. For candidates demonstrating potential but lacking certain skills, the opportunity to work initially without

pay will be extended to facilitate skill development.

The last of the processes investigated is that of retention methods within cybercriminal organizations. Despite Conti's need for a sustainable and talented workforce, there is no well-structured retention for members of the organization. Nevertheless, it is evident that exceptional performance is acknowledged through monetary bonuses, serving as a potential means of retention.

These findings give an insight into HRM processes within cybercriminal organizations. To give the findings not only academic purpose but also practical purpose, the following sub-question was formulated:

SRQ4: "How can these Human Resource Management processes be influenced by law enforcement, governments, and cybersecurity firms using the findings of this research?"

Multiple methods of influencing the HRM processes can be created utilizing this research. One potential method could be employed by governments and law enforcement agencies by focusing on organizational structure within a previously identified cybercriminal organization. This research contributes to the categorization of the various types of structures, dynamics, and roles in cybercriminal organizations. By comprehending what a law enforcement agency is facing, strategies can be devised to disrupt their operations more effectively.

A significant part of the organizational culture and HRM processes in cybercriminal organizations revolve around monetary compensation. Recognizing that compensation serves as a significant incentive for individuals to engage in cybercrime, gives the opportunity to disrupt these organizations. Cooperation between governments and cybersecurity firms can lead to IT specialists becoming tentative about joining a cybercriminal organization and opting for alternative career paths. This cooperation makes it easier to create incentives to dissuade individuals from pursuing illicit avenues. Moreover, monetary bonuses given out by these organizations for rewarding exceptional performance can be exploited as a vulnerability. Law enforcement agencies can target key individuals within these organizations by offering incentives for cooperation or providing opportunities for rehabilitation and legal employment. Another potential method to influence these practices can be to post advertisements on these Russian hacker forums. These advertisements would contain vacancies for jobs in the IT sector in countries. The vacancies should be from organizations that offer better salaries than those in Russia, making organizations based in Western countries strong contenders. In short, IT organizations based in high-paying countries could post vacancies on Russian forums to siphon this talent from cybercriminal organizations.

The recruitment methods are a potential target of influence as well. Law enforcement agencies can monitor and disrupt the recruitment practices of cybercriminal organizations through the investigation of online forums and other platforms where recruitment efforts of cybercriminal organizations take place. By identifying and intercepting potential recruits early in the process, efforts can be made to divert them toward legal employment opportunities within cybersecurity or other sectors. Furthermore, collaborative efforts between governments, educational institutions, and cybersecurity firms can focus on promoting ethical behavior among these IT specialists. By shifting the focus of those individuals from a desire to get rich quickly to a more ethical-oriented culture and responsible use of technology, the allure of cybercrime may be diminished.

The answers to these sub-questions provided the information necessary to answer the main research question of this thesis*: "How are Human Resource Management processes organized in a cybercriminal organization?"*. To provide a structured overview of the findings, an HR canvas was developed, giving an overview of HRM in the investigated cybercriminal organization.

The HR canvas is divided into nine segments showcasing HR-related strategy and execution. The first five of these segments outline the HR strategy of the organization. Essential components included here are the identification of stakeholders, the HR value proposition, the HR operating model, customer relationships, and the value drivers of HR within Conti. Aspects of the organization that are highlighted in these segments include the high rewards given for unique skills, the promotion of a culture of excellence through bonuses, the need for strong talent acquisition and retention, and a focus on building a competent brand to attract top IT talent with unmatched financial compensation.

The last four segments cover HR in practice. Topics discussed include key HR activities, key resources and competencies, external key partners, and cost drivers. Key takeaways from the canvas are the need for strong leadership, access to adequate financial resources, the financial costs for talent acquisitions and bonuses, and the non-financial risk of exposure during brand building.

5.2 Limitations and Future Research

Limitations

The conducted study has its limitations. Firstly, the reliance on translation for Russian messages within the Conti introduces potential inaccuracies and biases. While the investigated files have been translated using the API from Google, translation errors can persist and nuances lost in translation may distort the interpretation of messages, leading to misinterpretation of key information and findings. Furthermore, the memos written to interpret the messages between members of Conti can introduce bias into the analysis. A researcher's subjective interpretation of messages can influence the conclusions drawn from the data, potentially skewing the findings in favor of a certain perspective.

The issue of a limited sample size must also be considered. The research exclusively examines the cybercriminal organization Conti, thereby limiting the generalizability of the findings. The practices and dynamics observed within Conti may not be representative of other cybercriminal organizations, leading to potential biases in extrapolating the findings to the broader landscape of cybercrime. Furthermore, findings about the salaries of Conti members were compared against that of the Russian population to create a fair comparison. The information regarding the salary earned by Russians in various sectors was taken from a Russian news site, which may introduce bias due to potential influence or censorship by the Russian government.

Future Research

This study utilized a text analysis of the Conti leaks, conducted by a single person. While this form of qualitative analysis can give deep insight into the inner workings of the cybercriminal organization Conti, conducting such a form of analysis by one person can make the study prone to bias. A recommendation would therefore be to conduct a follow-up study, in which multiple researchers are giving their interpretation of the internal communications of Conti separately.

Another suggestion for future research would be to conduct a longitudinal study on Conti. Cybercrime is a constantly evolving and changing field, creating challenges for law enforcement and cybersecurity providers to overcome. When a new method of combatting cybercrime is deployed, cybercriminals are already working on a means to circumvent that method. A longitudinal study would give insight into how cybercriminals deal with setbacks and work on new methods to sustain their organization and workforce. This study would be difficult to conduct, considering detailed leaks of internal communications as investigated in this thesis are a rare occurrence. Despite that, a longitudinal study would yield new information regarding the inner workings of cybercriminal organizations, furthering understanding of the subject. Another component of this could be to look at a different method of communication within Conti. This thesis investigated the internal communication of the organization, but researching the messages that are posted on the forums used by Conti might yield another perspective on the method of operations.

Lastly, this research focused on certain specific components of HRM when investigating Conti, namely salary and additional benefits. These aspects only cover a small section of HRM, however. This is illustrated in the additional findings section, where messages of interest were found that were not directly relevant to any of the sub-questions but could improve further understanding of the HRM practices within cybercriminal organizations and these organizations as a whole. Conducting further research on aspects such as performance management and rule setting increases the literature on cybercriminal organizations, which will allow for a better understanding of these groups and in turn aid law enforcement agencies and governments in finding methods to disrupt their operations.

6 REFERENCES

Baird, L., & Meshoulam, I. (1988). Managing two fits of Strategic Human Resource Management. Academy of Management Review, 13(1), 116–128. https://doi.org/10.5465/amr.1988.4306802

Becker, B., & Gerhart, B. (1996). The impact of Human Resource Management on Organizational Performance: Progress and Prospects. Academy of Management Journal, 39(4), 779–801. https://doi.org/10.5465/256712

Becker,G.S. (1975) Human capital: A theoretical and empirical analysis, with special reference to Education. New York, National Bureau of Economic Research

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2013). Organizations and cybercrime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2345525

Calderoni, F., & Campedelli, G. M. (2020). Recruitment into Organised Criminal Groups: A Systematic Review. https://doi.org/10.52922/ti04183

Caldwell, T. (2011). Ethical hackers: putting on the white hat. Network Security, 2011(7), 10-13. https://doi.org/10.1016/S1353-4858(11)70075-7

Cloutier, O., Felusiak, L., Hill, C., & Pemberton-Jones, E. J. (2015). The importance of developing strategies for employee retention. Journal of Leadership, Accountability & Ethics, 12(2).

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. Global Crime, 13(3), 160–175. https://doi.org/10.1080/17440572.2012.702523

de Groot, A. D. (1961). Methodologie. Mouton.

Flick, T., & Morehouse, J. (2011). Securing the smart grid: Next generation power grid security. Syngress.

Gazet, A. (2008). Comparative analysis of various ransomware virii. Journal in Computer Virology, 6(1), 77–90. https://doi.org/10.1007/s11416-008-0092-2

Gray, I. W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2022). Money over morals: A business analysis of Conti Ransomware. 2022 APWG Symposium on Electronic Crime Research (eCrime). https://doi.org/10.1109/ecrime57793.2022.10142119

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR), 51(4), 1-36. https://dl.acm.org/doi/pdf/10.1145/3199674

Hwang, S. (2008). Utilizing Qualitative Data Analysis Software: A Review of Atlas.ti. Social Science Computer Review, 26(4), 519–527. https://doi.org/10.1177/0894439307312485

Kristof-brown, A. L., Zimmerman, R. D., & Johnson, E. C. (2005). CONSEQUENCES OF INDIVIDUALS' FIT AT WORK: a META-ANALYSIS OF PERSON–JOB, PERSON–ORGANIZATION, PERSON–GROUP, AND PERSON–SUPERVISOR FIT. Personnel Psychology, 58(2), 281–342. https://doi.org/10.1111/j.1744-6570.2005.00672.x

Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books. 18-26

Lockwood, D., & Ansari, A. (1999). Recruiting and retaining scarce information technology talent: a focus group study. Industrial Management & Data Systems, 99(6), 251-256.

Meurs, T., Junger, M., Abhishta, A., Tews, E., & Ratia, E. (2022). COORDINATE: A model to analyse the benefits and costs of coordinating cybercrime. Journal of internet services and information security, 12(4). https://doi.org/10.58346/JISIS.2022.I4.001

Mirkovic, J., & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39–53. https://doi.org/10.1145/997150.997156

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. https://doi.org/10.1145/2068816.2068824

Osterwalder, A., & Pigneur, Y. (2010). Business model generation: A handbook of visionaries, game changers, and Challengers. John Wiley & Sons.

Putman, C. G. J., Abhishta, A., & Nieuwenhuis, L. J. M. (2018). Business model of a botnet. 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 441–445. https://doi.org/10.1109/pdp2018.2018.00077

Renu and Pawan (2019) 'Impact of cyber crime: Issues and challenges', International Journal of Trend in Scientific Research and Development, Volume-3(Issue-3), pp. 1569–1572. doi:10.31142/ijtsrd23456

Rogers, R. (2018). Coding and Writing Analytic Memos on Qualitative Data: A Review of Johnny Saldana's The Coding Manual for Qualitative Researchers. The Qualitative Report, 23(4), 889+.

Smith, R. G. (2007). Crime Control in the Digital Age: An exploration of Human Rights Implications. International Journal of Cyber Criminology, 1(2), 167–179.

Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

US Securities and Exchange Commission. In the Matter of Jonathan G. Lebed (2000). Retrieved from http://www.sec.gov/litigation/admin/33-7891.htm;http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm ; http://cbc.ca/cgibin/templates/view.cgi?/news/2001/01/18/mafiaboy010118

Vulpen, E. van, & Veldsman, D. (2023, February 20). The HR CANVAS: A strategic human resources management tool. AIHR. https://www.aihr.com/blog/hr-canvas/

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2), xiii–xxiii. http://www.jstor.org/stable/4132319

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2020). Various Types of Cybercrime and Its Affected Area. In Emerging Technologies in Data Mining and Information Security (Vol. 3, pp. 305–315). essay, Springer Verlag, Singapore.

Y. Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Youndt, M. A., Snell, S. A., Dean, J. W., & Lepak, D. P. (1996). Human Resource Management, manufacturing strategy, and firm performance. Academy of Management Journal, 39(4), 836–866. https://doi.org/10.5465/256714

7 APPENDICES

During the preparation of this work the author(s) used ChatGPT in order to assist in writing code in the coding language 'Python'. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the work.

7.1 Appendix A

Question	Sub-Questions	Purpose
How much does a member of Conti earn?	What words directly relate to salary? (salary, crypto, bitcoin, bits, transfer, etc.)	Insight regarding salary within Conti
What specific benefits for are there for employees?	What words directly relate to additional benefits? (bonus, benefits, etc.)	Insight regarding benefits within Conti
What recruitment methods are mentioned (e.g., what platforms are used)?	What words directly relate to these processes? (hire, hiring, (job) offer, new employee, recruit, etc.)	Insight regarding recruitment methods within Conti
What selection methods are mentioned (e.g., what criteria are used to select employees)?	^	Insight regarding selection methods within Conti
What retention methods are mentioned (e.g., additional benefits, increase in salary)?	^	Insight regarding retention methods within Conti
What actors are involved in HRM?	What words directly relate to HR and who sends/receives these messages?	Finding actors most relevant to this research
When do actors send their messages?	*Analyze at what time actors usually send messages*	Analyze whether they follow regular working hours
What working days do members of Conti have (e.g., holidays, days off, weekends)?	What words directly relate to working days? (working days, weekend, holiday, days/time-off, etc.)	Insight regarding working days within Conti
What payment methods are used by Conti (e.g., bank transfer, cash, cryptocurrency)?	What words directly relate to payment methods? (transfer, salary, payment, etc.)	Insight regarding payment methods used within Conti
What actions do HR actors take regarding employee well-being?	What words directly relate to employee well-being? (well-being, feel, help, etc.)	Insight regarding how employee well-being is dealt with in Conti
What type of performance management does Conti employ?	What words directly relate to employee performance? (metric, content, good, etc.)	Insight regarding how performance is measured within Conti
What messages regarding learning/development of employees are being sent?	What words directly relate to employee development? (training, development, etc.)	What opportunities does Conti provide for employees to further develop themselves
What struggles are discussed by actors relating to HR?	*Analyze whether HR-actors mention struggles*	Display issues faced by HR employees within Conti
Are there messages about Non-Disclosure Agreement being sent, if so, what is in them?	What words directly relate to NDAs? (NDA, disclosure, etc.)	Does Conti utilize NDAs?
Are there messages about employees violating internal rules, if so, what is in them?	What words directly relate the violation of rules? (sanction, fire, firing, etc.)	Insight into what Conti does with employees unable to follow their established rules
What is being discussed about other communication channels than Jabber?	What words directly relate to communication channels? (message, channel, via, etc.)	Insight into various communication methods used by Conti
How many employees does Conti have?	What words directly relate to the scale of the organization? (size, members, etc.)	Determining the scale of the organization

7.2 Appendix B

Actor	Role	Username
Target	HR manager	target@q3mcco35auwcstmt.onion
Stern	Accountant/task manager	stern@q3mcco35auwcstmt.onion
Bentley	Manager/tester	bentley@q3mcco35auwcstmt.onion
Buza	Manager role/tester	buza@q3mcco35auwcstmt.onion
Ali	Developer	ali@q3mcco35auwcstmt.onion
Mango	General manager	mango@q3mcco35auwcstmt.onion
Bio	Negotiator	bio@q3mcco35auwcstmt.onion
Salamandra	HR manager/employee	salamandra@q3mcco35auwcstmt.onion
Mavelek	HR manager/employee	mavelek@q3mcco35auwcstmt.onion

7.3 Appendix C

Index	Message (English)	Memo
7671	Hello, I want to offer you a job in our team that is engaged in the maintenance of an online store abroad. in self-isolation mode, our team offers you a current vacancy for a fully remote job for the position of a call center operator. Responsibilities: Taking calls and communicating with clients Required skills: Good knowledge of spoken English (level B2-C1) Age from 18 to 25 Conditions: -We offer you timely wages in the amount of 450-500$ (Increase in salary by 100$ - 200 $ - $ 300, depending on the success in the work of the call center) - Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation - WITHOUT registration according to the Labor Code If you are interested in the offer, send your resume by replying to this letter. [31.08.2020 16:10:58]<derek> got a message bro? [31.08.2020 16:11:01]<derek> [13:52:29]<derek> Hello, I want to offer you a job in our team that is engaged in the maintenance of an online store abroad. in self-isolation mode, our team offers you a current vacancy for a fully remote job for the position of a call center operator. Responsibilities: Taking calls and communicating with clients Required skills: Good knowledge of spoken English (level B2-C1) Age from 18 to 25 Conditions: -We offer you timely wages in the amount of 450-500$ (Increase in salary by 100$ - 200 $ - $ 300, depending on the success in the work of the call center) - Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation - WITHOUT registration according to the Labor Code If you are interested in the offer, send your resume by replying to this letter.	Derek sends Salamandra a vacancy, which is potentially for a role within Conti. The vacancy is for a call centre operator, likely a cover-up name for the person who reaches out to victims
9795	Gone, now here. Look, in general, I'm leaving another project now, I'll be leaving on November 4th. On this day in the evening I will be able to make a final decision on work, I will need to finish my business and on 9 I will be able to go to work already. Do I understand correctly that you are ready to make an offer, you are satisfied with my experience, and based on the agreements with Maria, then this is 100 tr. to map. The absence of any official contract in any form, salary 2 times a month, well, here is such a specificity associated with the torus, and most likely there will be something else. You have my resume, phone (Well, in general), on the other hand, I will not know who I work with, and is this part of our agreements? That is, what I either agree to or not Do I understand correctly?	Driver describes the opportunity Conti gives him as he sees it
11313	The salary level is determined based on the results of the test task and interview (60 thousand-200 thousand)	Cany gives salary indication to Hof (most likely in Rubles)
29790	I wanted to ask this... Stern transfers my salary to my bank card. A bank will not prepare trouble? Are there any other ways to get money?	In this message it seems that certain salaries are paid via regular bank transfers instead of via cryptocurrencies
33534	Good afternoon. Very little programming experience. Is it possible to work in your company for free? So that the mentor gave me tasks, I fulfilled them. When I more or less begin to meet the requirements of your team, I will join for a salary.	Salamandra says to stern that he is willing to work for free untill his skills are of an adequate level. Indication of development opportunities within the organization

52673	1. Salary $450-500 (Salary increase by $100 - $200 - $300, depending on the Supervisor's position) 2. Work schedule 18:00 - 2:00 Moscow time. 5/2. 3. English language Upper intermediate 4. Age from 18 to 25 5. The point is to receive calls and communicate with clients. 6. Calls per day per operator from 10 to 40. 7. The duration of a successful call is 15-16 minutes.	This message seems to describe a vacancy including a salary indication
57704	ОБНАЛ 1к: {Bookkeeping | Accounting} {company|firm} is {looking for|seeking} a {Finance|Accounting} {Clerk|Assistant} to {perform|maintain} daily {accounting|bookkeeping} {operations|procedures}. {This|The} {position|job} is {focused|targeted} on {developing|improving} {company's|firm's}{projects|annual plans}. {Duties|Responsibilities}: - {Assistance|Taking part} i n the {preparation|calculation} of monthly financial {reports|schedules}; - {Reconcile|Examine|Study} {invoices|reports|ledgers} and {identify|point out|determine} {discrepancies|deviations|differences}; - {Verify|Track} accounts {receivable|payable}; - {Maintaining|Updating} the {market|business} {research|spreadsheets}; - {Other|Additional} {related|associated} {duties|tasks} as {assigned|required}. {JOB REQUIREMENTS|REQUIRED QUALIFICATIONS} College degree/School diploma or equivalent experience; {Proficiency|Excellent} in the use of {computer|office applications}; Knowledge of {accounting|bookkeeping} {principles|basis}; {Strong|High} {communication|analytic} skills; {Salary|Wage}: $2,500 + {monthly bonuses|percentage} Accounting firm is seeking Financial Clerks who will carry out financial analysis tasks, including costing and presentation of financial data by managing their daily schedule and undertaking general administration tasks to ensure the effective running of the finance team and to assist the Director of Finance in overseeing and directing all aspects and operations with regards to the processing and distribution of payroll and the accounting operations of the organization. The main duties include: - Create and update Excel spreadsheets; - Monitor bank balances on a daily basis; - Verify and post accounts payable and receivable to ledgers; - Notifying customers of insufficient and due payments; - Assist with preparation of payroll reports; - Assist senior accountants as needed; - Other duties as assigned. Required Skills and Qualifications: School diploma/Bachelors degree; Good verbal, written, and telephone communication skills; Proficient in Word, Outlook, and knowledge of Excel. Compensation: $2,500 + bonuses.	Vacancy, unlike previous messages this vacancy seems to be for a somewhat higher-up position in the organization

57784	Bookkeeping | Accounting} {company|firm} is {looking for|seeking} a {Finance|Accounting} {Clerk|Assistant} to {perform|maintain} daily {accounting|bookkeeping} {operations|procedures}. {This|The} {position|job} is {focused|targeted} on {developing|improving} {company's|firm's}{projects|annual plans}. {Duties|Responsibilities}: - {Assistance|Taking part} in the {preparation|calculation} of monthly financial {reports|schedules}; - {Reconcile|Examine|Study} {invoices|reports|ledgers} and {identify|point out|determine} {discrep ancies|deviations|differences}; - {Verify|Track} accounts {receivable|payable}; - {Maintaining|Updating} the {market|business} {research|spreadsheets}; - {Other|Additional} {related|associated} {duties|tasks} as {assigned|required}. {JOB REQUIREMENTS|REQUIRED QUALIFICATIONS} College degree/School diploma or equivalent experience; {Proficiency|Excellent} in the use of {computer|office applications}; Knowledge of {accounting|bookkeeping} {principles|basis}; {Strong|High} {communication|analytic} skills; {Salary|Wage}: $2,500 + {monthly bonuses|percentage} If you are interested, please, {do not hesitate|feel free} to leave {a call-back|the best} number and one of our HR-managers will get in touch with you. Accounting firm is seeking Financial Clerks who will carry out financial analysis tasks, including costing and presentation of financial data by managing their daily schedule and undertaking general administration tasks to ensure the effective running of the finance team and to assist the Director of Finance in overseeing and directing all aspects and operations with regards to the processing and distribution of payroll and the accounting operations of the organization. The main duties include: - Create and update Excel spreadsheets; - Monitor bank balances on a daily basis; - Verify and post accounts payable and receivable to ledgers; - Notifying customers of insufficient and due payments; - Assist with preparation of payroll reports; - Assist senior accountants as needed; - Other duties as assigned. Required Skills and Qualifications: School diploma/Bachelors degree; Good verbal, written, and telephone communication skills; Proficient in Word, Outlook, and knowledge of Excel. Compensation: $2,500 + bonuses. If you are interested, please, do not hesitate to leave a call-back number and one of our HR-managers will get in touch with you.	Vacancy, higher-up position

60044	[13:29:39]<buza> hello [13:29:41]<buza> [16:34:40]<salamandra> and cp he wants 200 [13:30:00]<buza> well, you said that we also consider candidates from the point of view of leaders [13:30:03]<Stern> yes [13:30:05]<Stern> that's right [13:30:18]<buza> I looked at the dude's resume, he has about 20 years of experience in IT, the last years all leadership positions [13:30:21]<Stern> but for this, people must prove that he is a 1. high-level encoder [13:30:23] <Stern> 2. stable [13:30:28]<buza> absolutely right [13:30:36]<buza> no one says to give him those 200k right away [13:30:38]<Stern> 3. knows how to manage, is loyal [13:30:56]<Stern> good [13:31:00]<Stern> then the first 2 months 150 [13:31:00]<buza> you can just agree that here he shows all this, shows himself as a pro coder, and on the horizon of six months receives a leadership position and salary [13:31:01]<Stern> beyond 200 [13:31:28]<buza> well then tell the salamander to connect it - I'll talk to him myself and find out how [13:32:03]<Stern> OK	Forwarded conversation about a higher-up coding vacancy between Stern and Buza
65035	naned needs to raise his salary to 140, he got 80 during the trial period	Mention of different level of pay between employees in trial period and regular employees
67193	Hello, I want to offer you a job in our team that deals with ....., in self-isolation mode, our team offers you a current vacancy for a completely remote job for the position of ..... Responsibilities : Receiving calls and communicating with clients Required skills: Good knowledge of spoken English Age from 18 to 25 Conditions: - We offer you a timely salary in the amount of $450-500 (Increase in salary by $100 - $200 - $300, depending on positions of the Supervisor) - Work is co mpletely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation - WITHOUT registration according to the TC If you are interested in the offer, send your resume by replying to this letter.	Job offer
68545	So. Zp is issued 2 times a month on the 1st and 15th. Salary 1000$ per month	When is salary is distributed and the level of pay for a certain function (tester)

69284	now money is flowing like a river in three directions 1) these are operators current expenses + expansion = total 2 offices with large teams - one main and one new for training 2) hacker offices (3 pcs) - interviews, equipment, rent, interviews, deposits, servers inside, equipment, hiring and assistance in hiring and a whole lot more, and in a week another salary will be added for those who will work there (20+ hackers) 3) an office with programmers and equipment for everything for them + a good team leader has already been hired and he is the team to collect there will be a pro, this is an important devops for a pro, a pro is happy with everything and he really needs it + we hire third-party specialists with a pro to speed up various processes, I'm sure that everything will pay off, so I'm not nervous	Brief description of organizational structure
76517	hello, send salary plz 3BWQhLHVWwm57jdhCTnZzD9XrYa4CYabiL 0.13541791	(Many similar messages have been sent to Stern, not all are noted here) Request for salary addressed to Stern, contains a crypto wallet address and a quantity (presumably in BTC)
81809	he is still on training without salary	Organization also trains people (but give no salary)
86450	$1000 per month salary to start. Then there is the possibility of growth	Bentley mentions to Azot that the starter salary is $1000 per month, with the potential to grow
98832	and in terms of salary, you started paying once every 3 months, I don’t complain much, but at least I told you what the reason was	For some reason, salary here was paid once in 3 months
110540	right now, a situation arose that one of the encoders raised his own salary from 2 to 2.5k, I say, who raised it to you with whom you coordinated it? And he says the headhunter is constantly bombing mailings from our company and he has been tracking the rate for a long time, supposedly from a job offer that comes from work))))	Encoder 'raised his own salary'
111304	1.5k salary the first month of probation 1k	Salary description

112523	Hello, I am writing to you off. Our old case was resumed, the investigator said why it was resumed, the Americans officially requested information about Russian hackers, not only about us, but in general who was caught in the country. Actually, they are interested in the trickbot, and some other viruses. On the following Tuesday, the investigator called us for a conversation, but for the time being, like as witnesses. But for now we will be at 51. Even as the investigator said, the case was extended until the end of October in order to have a conversation with us. Since if the case is suspended, they cannot interrogate us in any way, and, as a matter of fact, because of this, they resumed it. We have already contacted our lawyers. Question: Would it be possible to get a salary? What would I do to extend my lawyer right now and go on vacation until the end of October? To destroy all this bullshit. The only thing I will go to issuing routers every day. I give them to thunder and defu.	Does the organization have lawyers?
120372	hello, I turned to the defender to clarify the situation with the salary, he replied that now it's really tight with money, he said that he would write to you and [18:14:16]<defender> write a mango [18:15:42]<defender> he will send you thanks for February 1, that the possibility of payment was still found, I will revise my budget somehow. this is the first time I have had a force payout at this job, so I didn't expect it, otherwise I'll be more patient	Issue with payment not being on time
121483	ZP bande here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df sum total 85k _____ _____ 99947 main team 62 people, salary I get 54 33847 - reverse team, 23 people 3000 for expenses (servers \ pads \ test tasks for new people) 164.8k total per month	Description of team and salary
133484	Tomorrow is salary day: main team - 97 447; 52 people new team - 4000; 3 people, one has not yet started the reverse team - 23,347; 16 people research team - 12,500; 6 people team of osint intelligence - 9,000; 4 people total 146 294 \ 2 = 73 147 for salary + 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and 3-4k are needed for expenses on routers / servers / gaskets bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8	Mango describes the organization and salary; 52 people in the main team(97,447), 3 people in a new team (4,000), 16 people in the reverse team (23,347), 6 people in the research team(12,500), 4 people in the Open Source Intelligence team (9,000)
149506	there will be a salary in Mon. will you be in touch?	Salary on Monday (2021-03-12)

163994	right now we are looking for new people on the hack forums. in the announcement, a salary of 2k is indicated, there are a lot of comments that we are recruiting galley slaves) of course, how can we dispute that they say those who work and bear results get more, etc., etc. 10k earn .. in short, it's difficult to negotiate with them all	Mention of a need for extra employees and what Conti is offering

7.4 Appendix D

Index	Message (English)	Memo
7671	Hello, I want to offer you a job in our team that is engaged in the maintenance of an online store abroad. in self-isolation mode, our team offers you a current vacancy for a fully remote job for the position of a call center operator. Responsibilities: Taking calls and communicating with clients Required skills: Good knowledge of spoken English (level B2-C1) Age from 18 to 25 Conditions: -We offer you timely wages in the amount of 450-500$ (Increase in salary by 100$ - 200 $ - $ 300, depending on the success in the work of the call center) - Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation - WITHOUT registration according to the Labor Code If you are interested in the offer, send your resume by replying to this letter. [31.08.2020 16:10:58]<derek> got a message bro? [31.08.2020 16:11:01]<derek> [13:52:29]<derek> Hello, I want to offer you a job in our team that is engaged in the maintenance of an online store abroad. in self-isolation mode, our team offers you a current vacancy for a fully remote job for the position of a call center operator. Responsibilities: Taking calls and communicating with clients Required skills: Good knowledge of spoken English (level B2-C1) Age from 18 to 25 Conditions: -We offer you timely wages in the amount of 450-500$ (Increase in salary by 100$ - 200 $ - $ 300, depending on the success in the work of the call center) - Work is completely REMOTE, Work schedule 18:00 - 2:00 Moscow time. 5/2. Sat and Sun weekend. - Paid vacation - WITHOUT registration according to the Labor Code If you are interested in the offer, send your resume by replying to this letter.	Vacancy describes various benefits (off-days, holidays)
9782	I financially support all the guys with bonuses, everyone is trying	Target says to Stern that 'guys' are supported with bonuses
25001	and for testers, I'll make you a separate bonus	Indication of separate bonus for testers
25002	for education	(follow-up previous message) reason for bonus mentioned in previous message
53000	hello create another 100k bonus	100k bonus (100k rubles is about 1,000 usd)
57704	ОБНАЛ 1к: {Bookkeeping | Accounting} {company|firm} is {looking for|seeking} a {Finance|Accounting} {Clerk|Assistant} to {perform|maintain} daily {accounting|bookkeeping} {operations|procedures}. {This|The} {position|job} is {focused|targeted} on {developing|improving} {company's|firm's}{projects|annual plans}. {Duties|Responsibilities}: - {Assistance|Taking part} in the {preparation|calculation} of monthly financial {reports|schedules}; - {Reconcile|Examine|Study} {invoices|reports|ledgers} and {identify|point out|determine} {discrepancies|deviations|differences}; - {Verify|Track} accounts {receivable|payable}; - {Maintaining|Updating} the {market|business} {research|spreadsheets}; - {Other|Additional} {related|associated} {duties|tasks} as {assigned|required}. {JOB REQUIREMENTS|REQUIRED QUALIFICATIONS} College degree/School diploma or equivalent experience; {Proficiency|Excellent} in the use of {computer|office applications}; Knowledge of {accounting|bookkeeping} {principles|basis}; {Strong|High} {communication|analytic} skills; {Salary|Wage}: $2,500 + {monthly bonuses|percentage} Accounting firm is seeking Financial Clerks who will carry out financial analysis tasks, including costing and presentation of financial data by managing their daily schedule and undertaking general administration tasks to ensure the effective running of the finance team and to assist the Director of Finance in overseeing and directing all aspects and operations with regards to the processing and distribution of payroll and the accounting operations of the organization. The main duties include: - Create and update Excel spreadsheets; - Monitor bank balances on a daily basis; - Verify and post accounts payable and receivable to ledgers; - Notifying customers of insufficient and due payments; - Assist with preparation of payroll reports; - Assist senior accountants as needed; - Other duties as assigned. Required Skills and Qualifications: School diploma/Bachelors degree; Good verbal, written, and telephone communication skills; Proficient in	Vacancy description mentions monetary bonuses

	Word, Outlook, and knowledge of Excel. Compensation: $2,500 + bonuses.	
57784	Bookkeeping | Accounting} {company|firm} is {looking for|seeking} a {Finance|Accounting} {Clerk|Assistant} to {perform|maintain} daily {accounting|bookkeeping} {operations|procedures}. {This|The} {position|job} is {focused|targeted} on {developing|improving} {company's|firm's}{projects|annual plans}. {Duties|Responsibilities}: - {Assistance|Taking part} in the {preparation|calculation} of monthly financial {reports|schedules}; - {Reconcile|Examine|Study} {invoices|reports|ledgers} and {identify|point out|determine} {discrepancies|deviations|differences}; - {Verify|Track} accounts {receivable|payable}; - {Maintaining|Updating} the {market|business} {research|spreadsheets}; - {Other|Additional} {related|associated} {duties|tasks} as {assigned|required}. {JOB REQUIREMENTS|REQUIRED QUALIFICATIONS} College degree/School diploma or equivalent experience; {Proficiency|Excellent} in the use of {computer|office applications}; Knowledge of {accounting|bookkeeping} {principles|basis}; {Strong|High} {communication|analytic} skills; {Salary|Wage}: $2,500 + {monthly bonuses|percentage} If you are interested, please, {do not hesitate|feel free} to leave {a call-back|the best} number and one of our HR-managers will get in touch with you. Accounting firm is seeking Financial Clerks who will carry out financial analysis tasks, including costing and presentation of financial data by managing their daily schedule and undertaking general administration tasks to ensure the effective running of the finance team and to assist the Director of Finance in overseeing and directing all aspects and operations with regards to the processing and distribution of payroll and the accounting operations of the organization. The main duties include: - Create and update Excel spreadsheets; - Monitor bank balances on a daily basis; - Verify and post accounts payable and receivable to ledgers; - Notifying customers of insufficient and due payments; - Assist with preparation of payroll reports; - Assist senior accountants as needed; - Other duties as assigned. Required Skills and Qualifications: School diploma/Bachelors degree; Good verbal, written, and telephone communication skills; Proficient in Word, Outlook, and knowledge of Excel. Compensation: $2,500 + bonuses. If you are interested, please, do not hesitate to leave a call-back number and one of our HR-managers will get in touch with you.	Vacancy description mentions monetary bonuses
71086	i give bonuses	Target seems to be in charge of handing out bonuses
100790	15k with bonuses	mention of a bonus (15k rubles), for setting up an AV system
106104	[13:46:29]<Stern> Hello, I'm ready to give you a management bonus [13:46:33]<Stern> create a payment for 140k	Specific 'management' bonus of 140k rubles (around 1,400 usd)
112523	Hello, I am writing to you off. Our old case was resumed, the investigator said why it was resumed, the Americans officially requested information about Russian hackers, not only about us, but in general who was caught in the country. Actually, they are interested in the trickbot, and some other viruses. On the following Tuesday, the investigator called us for a conversation, but for the time being, like as witnesses. But for now we will be at 51. Even as the investigator said, the case was extended until the end of October in order to have a conversation with us. Since if the case is suspended, they cannot interrogate us in any way, and, as a matter of fact, because of this, they resumed it. We have already contacted our lawyers. Question: Would it be possible to get a salary? What would I do to extend my lawyer right now and go on vacation until the end of October? To destroy all this bullshit. The only thing I will go to issuing routers every day. I give them to thunder and defu.	Conti appears to have lawyers that stand by their employees if necessary (most messages sent around the same time are encrypted, making it difficult to determine whether Conti fully pays for these lawyers)
133185	and do not thank)) the best gratitude is a bonus from you for the holidays))	Holiday bonus

7.5 Appendix E

Index	Message (English)	Memo
1722	and then the office itself will fly forward + they will start recruiting new ones and the professional will be able to do whatever he wants	Mention of new recruitment (no mention of how)
2962	before vacation, I will prepare training manuals and approve and supplement the scheme	Mention of training manuals within Conti
2894	did our HR immediately throw off the admins for you or did they prepare them somehow? tell me, I talked superficially with them, I didn't have time to delve into it, I was talking about the viper and the salamander, they knocked me that they were responsible for the admins and introduced me to the course	Target asks Revers if HR prepared new admins before they were sent to them
2898	asking stupid questions	Potential new employees are being asked questions to test their knowledge on certain subjects
2915	I thought you had sets of 10-30 people there	Target thought HR had managed to recruit between 10-30 new employees
2916	from him I have 2 works in total	Revers tells Target he only has two new team members instead of the expected 10 to 30
2966	for training manual and funnel	Revers is in charge of training of new employees
2992	that I need to understand the whole scheme from beginning to end to understand the pitfalls + - to understand the funnel of actions - the whole stem divided into groups, stages, time costs, the level of complexity to understand the training system and the work system from A to Z + the time costs of the desired qualification of people is will be thoroughly reported to the security officer and the responsible office how they will understand all the actions and the funnel of actions, stages, "how they understand the whole process" in practice - they will recruit 20-30 people a week in the office for 1-2 test days of work, you will drive them through the funnel above we will invite the most gifted to work and talk with them about their safety, I don't think that you can write a scheme, a funnel, pitfalls, + a training system in an hour, thesis, even this can take a day of thinking, I can appear a couple of times a month in the office, but responsible my security guard and office administrator will be behind the office	Description of how new employees enter the organization
10682	Good afternoon. I am a new employee. Please instruct me.	New employee is asking for instructions (might be worth looking into further)
10683	Yes, new. I told Sergey Ivanov - salamander that I work for free, a beginner programmer. I need a mentor first. In the future, as I get involved, I am ready to become a full-fledged member of your team. There is no stack, I studied C ++ to classes. But I don't know how to apply them. Please take me to your team.	(follow-up) new employee (programmer) mentioning he will start working for free during training
12327	now 8 are working, this is who the prof and dooms are happy with, the rest were removed at the end of 50 - 3 offices in anticipation of the prof and recruiting a new set at the end of the month, the prof asked to slow down a little ph a week is 140,000 dirty rubles excluding office, cleaning, administration	
14548	C++/C# programmer IT, internet, telecom • Programming, Development Employment: part-time, full-time Work schedule: shift method, remote work, flexible schedule, full-time, shift schedule Desirable travel time to work: doesn't matter 70 000 rub. Work experience —11 years 10 months August 2017 — October 2017 3 months Forest, OOO Beloretsk, www.for-est.ru Developer of information systems Development of information systems for automating business processes September 2014 — July 2017 2 years 11 months OOO Uralmetindustriya Beloretsk Engineer-APCS programmer Building automatic weighing systems, implementation,	CV of a developer the organization is interested in

	commissioning March 2012 — September 2014 2 years 7 months complex Developed software for tibbo controllers January 2008 — January 2010 2 years 1 month Magnitogorsk Iron and Steel Works, OAO Magnitogorsk, mmk.ru/ Leading Programmer Engineer Development of 1st and 2nd level process control system software, communication interfaces, TP visualization systems. Maintenance of industrial networks and Ethernet networks Commissioning of mill 5000 January 1999 — January 2003 4 years 1 month Beloretsk Iron and Steel Works, OAO engineer programmer Development of software for process control systems of the 1st level, industrial communication interfaces Reconstruction of mill 150 Education Higher 1993 Ufa State Aviation Technical University, Ufa Faculty Aviation instrumentation, Information-measuring equipment and technologies Key skills Knowledge of languages Russian — Native English — A1 — Beginner Skills Knowledge of scada systems and basic protocols Knowledge of tibbo controllers Knowledge of C# Knowledge of C++ Software development of tibbo controllers Development environment Visual Studio 2010 Additional information About me Specific knowledge: features of construction of systems and visualization systems for process control systems of any level, industrial controllers, microcontrollers. Complete knowledge of Windows OS families. UNIX and related software. Complete knowledge of PC repair and maintenance. Ability to learn: Able to develop automation systems and software from scratch. We easily teach materials related to directly ongoing developments.	
20809	[19:44:20]<target> Now they are compiling lists of those who wish from the IT departments of two universities, so far there are 17 people, there will be 40-50 people in a week, 50-70 people will be recruited in a couple of weeks, we will choose 20-30 suitable ones after testing, there will be specifics on numbers	Recruitment process
41157	we have 2 options, these are specialized universities, and as a backup option, I wanted a dozen people to be recruited from xx, but this is all offline	Mention of a 'specialized university' that they are recruiting from
50408	of the cool personal ones out of 5, three are on vacation))) and I plan to pick up one from the online group and in the future, as a team leader, put it on the second group of office workers when we recruit, he wants, and he is a mega-responsible dude, a good specialist in network analysis, namely data collection and clogging	Description of a potential new employee
64367	professional reverse dooms - full control over the entire process online and are responsible for hackers booze - scripts, automation, srm, funnel - waiting for tasks, selects people or we give him priority 1 these tasks i - offline, recruitment, execution control, organization process for our tasks with you, scaling, indirect participation with booze and hackers to build processes	Vacancy description
114172	here it's like 14 days for free, I made an acc https://privnote.com/RuJQzlbb#FfJKWxkaz At work, people are starting to unsubscribe, so soon there will be new employees. dayey wrote, it seems like builds will take this week	Usage of Privnote (platform that deletes messages after time) by new employees
144697	there it would be necessary for people to give out salaries, newcomers fall off, I recruited them with such difficulty	Difficulties during recruitment process
144859	[06.05.2021 12:10:57]<buza> c++ I am talking with swift, web mavemat, admins - green [06.05.2021 12:11:38]<buza> [12:11:27]<buza> there will be a couple more very specific vacancies a little later, related to the crypto exchange [12:11:31]<buza> I haven't written them yet [05/06/2021 12:11:49]<buza> the same vacancies were given to salamander [05/06/2021 12:12:06]<buza> work in cooperation [06.05.2021 12:12:35]<buza> stern considers this a priority, recruiting people	Recruiting new employees seems to be a priotity
163994	right now we are looking for new people on the hack forums. in the announcement, a salary of 2k is indicated, there are a lot of comments that we are recruiting galley slaves) of course, how can we dispute that they say those who work and bear results get more, etc., etc. 10k earn .. in short, it's difficult to negotiate with them all	Salary they offer is critized on forums
165929	do not slow down with the recruitment of people and interviews	Urge to keep on recruiting

7.6 Appendix F

- Import the data

```
import pandas as pd
df_2020 = pd.read_csv('https://github.com/NorthwaveSecurity/complete_translation_leaked_chats_conti_ransomware/blob/main/jabber_chat_2020_translated.csv?raw=true',index_col=0)
df_2021 = pd.read_csv('https://github.com/NorthwaveSecurity/complete_translation_leaked_chats_conti_ransomware/blob/main/jabber_chat_2021_2022_translated.csv?raw=true',index_col=0)
df = pd.concat([df_2020,df_2021]).reset_index(drop=True)
```

- Create a dataframe focusing on a specific word in a message (this code retrieves all messages containing 'salary', but this can be substituted for another word)

```
df_salary = df[df['body_en'].str.contains('salary', case=False, na=False)]
```

- Create a dataframe focusing on all messages sent from and to a specific user (this code retrieves all messages sent from and to 'salamandra@q3mcco35auwcstmt.onion', but this can be substituted for another adress)

```
df_salamandra = df[df['from'].str.contains('salamandra@q3mcco35auwcstmt.onion', case=False, na=False) |
                   df['to'].str.contains('salamandra@q3mcco35auwcstmt.onion', case=False, na=False)]
```

- Create a dataframe consisting of specific rows (this code retrieves all messages with index number 60000 up to, but not including, 70001. These numbers can be substituted for other index numbers)

```
selected_rows = df.iloc[60000:70001]
```

- Compute high level statistics of dataframe to give an overview of the analyzed data

```
def compute_statistics(df):
    stats = {
        'Column Name': [],
        'Data Type': [],
        'Description': [],
        'Unique Values': [],
        'Missing Values': []
    }

    for column in df.columns:
        stats['Column Name'].append(column)
        stats['Data Type'].append(df[column].dtype)
        stats['Description'].append('')
        stats['Unique Values'].append(df[column].nunique())
        stats['Missing Values'].append(df[column].isnull().sum())

    return pd.DataFrame(stats)

# Compute and display the statistics
statistics_df = compute_statistics(df)
statistics_df
```