

# DECRYPTING RANSOMWARE OPERATIONS

EXPLORING RANSOMWARE GANGS' VALUE ALLOCATION FOR EFFECTIVE DISRUPTION STRATEGIES

M.R.S. VAN LANGE



# Decrypting Ransomware Operations

Exploring Ransomware Gangs' Value Allocation for Effective Disruption Strategies

by

Marieke R.S. van Lange

A thesis submitted to the Delft University of Technology in partial fulfillment of the requirements for the degree of

**Master of Science**

in **Complex Systems Engineering and Management**

to be defended publicly on Monday, August 26, 2024.

Student number: 5854016

**Thesis committee**

Chair: Dr. R.S. van Wegberg

First Supervisor: Dr. R.S. van Wegberg

Second Supervisor: Prof. Dr. M.E. Warnier

FIOD Supervisor: J.E. van Rijs



## Executive Summary

Ransomware attacks, orchestrated by cybercriminal organizations, pose a global threat in our digital era by exploiting system vulnerabilities and demanding ransoms for seized and encrypted data. Conti, a Russian ransomware group, ceased to exist after a 2022 data leak, offering a unique opportunity to study their modus operandi. The leak includes chat transcripts containing indicators of value, like compensation agreements and digital transaction details. By using the value chain lens, these indicators can be used to determine how ransomware groups create and allocate value within their operations. This understanding is essential for law enforcement aiming to disrupt ransomware activities more effectively, as targeting the most valuable components of their operations can result in significant disruptions to the organization. This value attribution is currently unknown.

The central question of this thesis is: *How do ransomware groups allocate value within their operations, and how can this understanding support law enforcement in developing effective intervention strategies?* This question is explored by analyzing the leaked chat transcripts from the Conti ransomware group using a semi-structured keyword search approach. The research categorizes findings based on the phases of the ransomware value chain: Development, Distribution, Take-Over, and Cash-Out.

This research is significant both academically and practically. It addresses a crucial gap in cybersecurity literature by providing empirical data on the internal value creation and allocation processes within ransomware groups, specifically focusing on the Conti organization. Unlike previous studies that often rely on theoretical models, this thesis applies a value chain perspective to the actual operations of a ransomware group, offering tangible insights into their modus operandi. These findings may be beneficial for law enforcement as they highlight the most vulnerable and valuable aspects of ransomware operations, informing the development of more effective intervention strategies.

The key findings of this thesis reveal that the Development and Cash-Out phases of the ransomware value chain are the most critical for disrupting ransomware operations. In the Development phase, high value is placed on the creation of malicious software and the involvement of highly skilled, internally employed workers. Disrupting this phase by targeting these workers or impeding the funding for software development could have significant and long-lasting impacts on ransomware activities. The Cash-Out phase is equally critical, as it involves converting illicit gains into usable currency and obscuring financial trails. Successful disruption of this phase would severely hinder the group's ability to sustain its operations. The Distribution phase offers medium disruption potential, as the workers involved are often part of an affiliate scheme and can be easily replaced. Therefore, disrupting this phase may not significantly impact the group's overall operations. The Take-Over phase, involving negotiation

and extortion, presents the least disruption potential, as the roles and activities in this phase are undervalued and easily replaceable.

The findings of this research have significant implications for enhancing cybersecurity and combating ransomware. By revealing how ransomware groups like Conti operate and allocate value, the study provides critical insights into the vulnerabilities and dependencies within these criminal networks. This knowledge is invaluable for law enforcement agencies and investigative authorities, such as the FIOD, in developing targeted disruption strategies. By focusing on the most valuable components of ransomware operations, disruptive actions can be developed to be more effective. These informed strategies can more effectively mitigate the economic and social impacts of ransomware.

## Preface

Dearest reader,

When I started my Master's in Complex Systems Engineering and Management at TU Delft two years ago, I could never have imagined the journey it would take me on. But here we are, at the finish line, with you reading my research. This thesis marks the end of my journey at the TU Delft, which initially intimidated me but ultimately turned out to be an incredible experience. It brought me new friends, unique opportunities to gain relevant experience, and took me to the other side of this planet. This thesis concludes a nine-month internship at the FIOD, where I had the honor of writing this thesis. I am deeply grateful for the incredible opportunity this experience has provided. And finally, this thesis concludes my chapter as a student, which began six years ago at Utrecht University. Although it feels surreal to end this phase, I am so happy with how it has unfolded.

I would like to express my gratefulness to everyone who has supported me over the last few months. First of all, I'm grateful to my daily supervisor, Dr. Rolf van Wegberg, for catching a glimpse of interest in cybercrime and introducing me to the world of ransomware. I truly appreciate your unconditional trust, belief in my capabilities, and support during our weekly meetings. Next, I want to thank Jocelyn van Rijs for welcoming me to the FIOD, for taking me along on your fascinating investigations, and for taking the time to teach me all there is to know about Russian cybercriminals. I also want to thank my colleagues of team FACT for their help, gezelligheid, and 12:00 on the dot lunches. Thanks to my second supervisor, Prof. Dr. Martijn Warnier, for being part of my committee and for taking the time to provide me with constructive feedback. Finally, I want to thank my family, Luuk, and my friends for their endless support. It would have been a lot harder without all the tea dates and walks around the uni.

♥*WomenInSTEM*

*Marieke van Lange  
Den Haag, August 2024*

## Table of Contents

<b>Executive Summary</b>	<b>2</b>
<b>Preface</b>	<b>4</b>
<b>Table of Contents</b>	<b>5</b>
<b>List of Figures</b>	<b>6</b>
<b>List of Tables</b>	<b>6</b>
<b>1. Introduction &amp; Background</b>	<b>7</b>
1.1 Ransomware	7
1.2 Ransomware as Profit-Driven Cybercrime	7
1.2.1 Marketplaces	8
1.2.2 Division of Labor: Affiliate Business Model	8
1.2.3 Enterprise Organizational Structure	9
1.2.4 Ransomware Financials	9
1.3 Disruption Based on Value Chain Approach	11
1.3.1 Ransomware Value Chain	11
1.3.2 Conti	12
1.4 Research Gap	13
1.5 Research Questions	13
1.6 Thesis Structure	14
<b>2. Methods</b>	<b>15</b>
2.1 Research Objective	15
2.2 Research Approach RQ1: Conti Chat Data Collection	15
2.2.1 Collecting Data Points from Conti's Chat Transcripts	15
2.2.2 Sources	16
2.2.3 Keyword Search Method	17
2.2.3.1 Keyword Search Method Disadvantages	18
2.2.4 Value Chain Research Lens	19
2.2.5 Blockchain	19
2.2 Research Approach RQ2: Determining Value Attribution and Formal Charts	20
2.3 Research Approach RQ3: Confronting Literature	21
<b>3. Conti Chat Transcript Research</b>	<b>22</b>
3.1 Development	22
3.2 Distribution	25
3.3 Take-Over	28
3.4 Cash-Out	31
3.5 Governance	33
<b>4. Value Attributions and Interdependencies in Conti Group</b>	<b>35</b>
4.1 Development	35
4.2 Distribution	37
4.3 Take-Over	39
4.4 Cash-Out	41
4.5 Governance	43
<b>5. Reflection of Results in Scientific Literature</b>	<b>44</b>
<b>6. Discussion</b>	<b>49</b>
6.1 Interpretation of the Results	49
6.1.1 Development	49
6.1.2 Distribution	50
6.1.3 Take-Over	51
6.1.4 Cash-Out	52
6.1.5 Governance	53
6.2 Recommendations for Law Enforcement	53
6.3 Academic Relevance	54
6.4 Limitations	55
6.5 Future Research	56
<b>7. Conclusion</b>	<b>57</b>
<b>8. Bibliography</b>	<b>60</b>

<b>Appendix A</b>	<b>63</b>
<b>Appendix B</b>	<b>64</b>
<b>Appendix C</b>	<b>66</b>
C.1 Development Chat Findings	66
C.2 Distribution Chat Findings	71
C.3 Take-Over Chat Findings	78
C.4 Cash-Out Chat Findings	82
C.5 Governance Chat Findings	83
<b>Appendix D</b>	<b>87</b>
<b>Appendix E</b>	<b>88</b>

## List of Figures

Figure 1: Value Chain of ransomware groups.	12
Figure 2: Flow diagram for semi-structured keyword search of Conti chat transcripts.	17
Figure 3: Chronological timeline of Development activities.	24
Figure 4: Chronological timeline of Distribution activities.	27
Figure 5: Chronological timeline of Take-Over activities.	30
Figure 6: Chronological timeline of Cash-Out activities.	32
Figure 7: Chronological timeline of Governance activities.	34
Figure 8: Formal chart of the Development phase in ransomware cybercriminal activities.	35
Figure 9: Formal chart of the Distribution phase in ransomware cybercriminal activities.	37
Figure 10: Formal chart of the Take-Over phase in ransomware cybercriminal activities.	39
Figure 11: Formal chart of the Cash-Out phase in ransomware cybercriminal activities.	41
Figure 12: Formal chart of the Governance in ransomware cybercriminal activities.	43

## List of Tables

Table 1: Conti actors and chat log data.	63
Table 2: Keyword search terms for chat research. Not exhaustive.	64
Table 3: Conti output division data based on Ransomware.live data.	87
Table 4: Blockchain analysis cross-referencing overview.	88

## 1. Introduction & Background

### *1.1 Ransomware*

In our increasingly digitalized world, the persistent threat of ransomware attacks poses a challenge on a global scale. Ransomware has emerged as a pressing social and economic threat, posing significant challenges to individuals, businesses, and governments worldwide. Performed by cybercriminal hacker organizations, these attacks target computer system vulnerabilities, aiming to extort individuals or corporations by encrypting sensitive data (Irwin & Dawson, 2019). Ransomware has evolved into an exceptionally destructive form of malicious software, designed to lock data until a ransom, typically ranging from a hundred to millions of dollars, is paid (Irwin & Dawson, 2019; Wilner et al., 2019). In 2023, a record amount of ransom was paid by victims to cybercriminals, with a total value of over \$1 billion (Chainalysis, 2024). While the immediate consequences of an attack involve significant economic losses and digital system shutdowns, the full outcomes extend beyond the ransom costs, including lost productivity, business disruptions, reputation damage, and the loss of critical and personal data (Brewer, 2016).

The malicious attacks are orchestrated by highly sophisticated criminal organizations, posing a significant threat to enterprises and the economy. Disrupting these operations is important for the safety of individuals and enterprises. Cybercriminals hide themselves by operating fully anonymously (Brewer, 2016), making it difficult to disrupt the organization by arresting individuals. To effectively disrupt cybercriminal enterprises, it is essential to interrupt their illegal activities, scarce resources, or capital flows (Thomas et al., 2015). Identifying dependencies that allow the ransomware group to continue their operations and weak links susceptible to disruption is crucial (Thomas et al., 2015). Therefore, it is important to gain insights into these important dependencies to equip Dutch investigative authorities, such as the FIOD, with detailed insights into how ransomware groups allocate value and pinpoint their vulnerabilities. This knowledge enhances the ability to disrupt and dismantle cybercriminal networks.

### *1.2 Ransomware as Profit-Driven Cybercrime*

Ransomware represents a category of cybercrime that is primarily motivated by financial gain. As defined by Lusthaus (2018), this type of cybercrime operates similarly to legitimate businesses, featuring marketplaces, a division of labor, structured organizational hierarchies, and a well-organized financial system, all aimed at maximizing profitability. These elements facilitate the success of such operations and create a network of interdependencies among different components of the criminal organization. This network of dependencies is crucial because it reveals potential vulnerabilities that could be targeted for disruption. The structure that facilitates success also creates vulnerabilities; these criminal enterprises thrive on the same



interdependencies that can be their downfall (Lusthaus, 2018). This section will explore the specific characteristics of ransomware as profit-driven cybercrime and examine the interdependencies within each characteristic to identify potential points of disruption.

### 1.2.1 Marketplaces

One characteristic of profit-driven cybercrime, of which ransomware, is the dependency on marketplaces. Research done by Thomas et al. (2015) shows how cybercriminal groups are highly dependent on the underground economy, where specialists offer services and resources specifically designed to support cybercriminal activities. Criminal organizations exploit others' skills and resources distributed on the black market to create new criminal schemes, making the organizations quick to adapt to new developments. The black market allows cybercrime to outsource parts of their business (Thomas et al., 2015). However, this high dependency on the black market introduces dependencies, which are vulnerable to disruption. Any disruption to these dependencies can undermine entire operations. One of these interdependencies includes profit centers, which are actions within the cybercriminal ecosystem that funnel money from victims into the underground economy (Thomas et al., 2015). This movement of capital includes gangs committing financial fraud and victims paying ransom. Without victims paying their demanded ransom, cybercriminal groups are not able to make revenue and continue their operations. Another interdependency includes support centers. Support centers act as hubs that offer resources essential for cybercrime like exploit kits and human affiliates. These centers enable cybercriminals to outsource parts of their operations, offering solutions in areas where they lack expertise or resources. These centers are typically solely for illicit activities, offering no legitimate, non-criminal applications (Thomas et al., 2015).

### 1.2.2 Division of Labor: Affiliate Business Model

As mentioned in the previous section, support centers are essential for cybercriminal operations. Support centers are necessary to facilitate the ransomware affiliate business model. In this business model, the core of the cybercriminal organization, the operators, handle business in some niche criminal activity, like distributing ransomware (Thomas et al., 2015). However, affiliates support the core of the cybercriminal group by performing other essential activities. Affiliates are external workers who license and execute the malware, negotiate with victims on ransom payments, and in return earn a percentage of the ransom payments (Meland et al., 2020). Affiliates function as revenue generators, working as independent contractors. Most affiliates carry out the attacks without having any special skills but are instructed by the operators on how to run the ransomware and request ransom payments (Gómez Hernández et al., 2023). This division of labor acknowledges the value of specialization and the professionalization of ransomware operations. The affiliate business model has great advantages for management, as it mitigates the risk of poor-performing affiliates by paying commissions solely based on new revenue (Thomas et al., 2015). It accommodates affiliates by allowing them to switch between,

or work for multiple cybercriminal groups. This setup creates a workforce that can be quickly accessed, with low initial costs and no regulatory restrictions (Thomas et al., 2015). With ransomware groups operating with an affiliate business model, disrupting the interdependence between profit-driven cybercriminal groups and their affiliates would disrupt the workforce essential to the criminal group's revenue scheme.

### 1.2.3 Enterprise Organizational Structure

The structure of ransomware groups is similar to that of traditional firms, as concluded by Gray et al. (2022) through their examination of the Conti ransomware group. This finding is further supported by Ruellan et al. (2023), who state that Conti operates like a traditional organization by exhibiting diverse styles of management, and interactions and discussions among managers regarding business operations. Gray et al. (2022) research shows how operators form the core of the criminal organization. This core consists of all employees of the cybercriminal group, and their tasks include the recruitment of developers and affiliates, malware development and sales, and maintenance of the payment platform (Gray et al., 2022). These operators include full-time managers and team leaders and form a panel of control to manage ransomware attacks (Gómez Hernández et al., 2023). It is suspected that ransomware groups are formed like regular companies, and thus have a strict line of hierarchy. Through leaked reports, several researchers have concluded that organizations have upper-level managers, senior managers, administrators, and people responsible for negotiations and money laundering (Gray et al., 2022; Ruellan et al., 2023). Besides these tasks, cybercriminals prefer to hire third parties to do repetitious tasks instead of doing it themselves (Collier et al., 2020). These service providers also do a lot of regular administrative work, like running secure hosting, customer support, and managing malware (Collier et al., 2020).

This traditional enterprise structure brings interdependencies that are not only financial but also strategic. For example, the division of labor within these groups is highly specialized, where each unit depends on the functioning of the others to keep operations running and maximize profits. Cybercriminal organizations exhibit dependencies on external employees. A failure in this dependency can lead to significant operational delays and expose the group to high risks. Disruptions in any part of this operational structure can have a cascading effect on the group's overall capability. Disruption in the overall hierarchy and management effectiveness could impact profitability, level of management control, and continuation of operations.

### 1.2.4 Ransomware Financials

Ransomware groups function similarly to traditional organizations in that their operations depend on careful financial management and regulation. Payments connect the entire underground ecosystem (Thomas et al., 2015). Disrupting the flow of money from victims to

criminals, as well as between criminals themselves like salary pay-out, can result in a disruption of cybercriminal activities.

Regarding cryptocurrencies, Bitcoin stands out as the preferred currency for these transactions. Unlike traditional payment systems, Bitcoin operates without a centralized payment processor, which complicates efforts to disrupt financial transactions (Thomas et al., 2015). Instead, interventions often focus on the points of exchange from Bitcoin to regulated, fiat currencies (Thomas et al., 2015). This decentralized nature of Bitcoin appeals to cyber criminals because it enhances their ability to conduct transactions globally easily and minimizes detection risk (Oosthoek et al., 2023). Huang et al. (2018) argue how the use of Bitcoin as currency by ransomware groups allows for investigation into the financial structures of these organizations. All transactions are public and traceable due to their administration via blockchain technology. Tracking Bitcoin transactions on the blockchain allows for tracking revenue, affiliate schemes, and the overall infrastructure of the ransomware group (Huang et al., 2018).

Ransomware economics consists of inflowing and outflowing Bitcoin streams. The main source of inflowing Bitcoin is revenue generated from incoming victim payments (Huang et al., 2018). Negotiation and subsequent payment of ransom are what keep ransomware operations thriving and running (Laszka et al., 2017). Hernandez-Castro et al. (2020) have performed research on the influence of victims paying the demanded ransom and suspects an increase in the amount of ransom asked by the criminal group. The research shows how criminals active in ransomware prioritize profit and thus high-value victims over the number of victims. These profits are increased through price discrimination: the ransom demanded is adjusted to the victim enterprises or individuals' worth (Hernandez-Castro et al., 2020). The Bitcoin outflow of ransomware groups consists mostly of Bitcoin moving from wallets to a Bitcoin exchange, or from wallets to mixers (Huang et al., 2018). Mixers serve as services that collect Bitcoin from cybercriminals and combine these funds through multiple transactions, creating a complex trail that makes accurate tracking of Bitcoin complex (Oosthoek et al., 2023).

Research by Conti et al. (2018) on the identification of Bitcoin traces shows how clustering and investigation into historic transactions help in identifying ransomware transactions. The research shows how the pseudo-anonymity and irreversibility of Bitcoin make it an attractive currency for cybercriminal organizations. Bitcoin has since become the main method of payment for ransomware groups, as it allows criminals to commit untraceable fraud (Conti et al., 2018). Identification of ransomware payments with Bitcoin has further been researched by Turner et al. (2020), who found through a comparative study between using Bitcoin for illegitimate (ransomware) vs. legitimate (charity) payments that ransom payments are typical by uniformity. This is confirmed through research by Homayoun et al. (2020), who found that patterns are a useful tool for identifying ransomware payments and families. Besides uniformity, Turner et al. (2020) found that ransom payments are often either kept on hold until

the right moment to cash out or have their addresses “zeroed” after each day of operations. Frequent cash out is therefore a sign of ransomware (Turner et al., 2020).

The financial operations of ransomware groups form a complex network of interdependencies among various actors within the cybercriminal ecosystem and between the criminals and their victims. Primary interactions, such as ransom payments made in Bitcoin, fuel the ransomware business, enabling ongoing criminal operations and dependency on digital, hard-to-trace payment systems. Ransomware operations also rely on revenue sharing between operators. Disrupting any part of this financial structure, such as blocking payment channels or transactions can significantly impact ransomware operations. This disruption not only impacts the immediate cash flow but also the operational capabilities of ransomware groups, ultimately disturbing their effectiveness.

### *1.3 Disruption Based on Value Chain Approach*

Disruption is a necessary measure in combating cybercrime. To make disruptions the most impactful, it is necessary to target the most valuable, and thus vulnerable activities within the cybercriminal organization (Thomas et al., 2015). To do this effectively, according to Kraemer-Mbula et al. (2013), it is necessary to understand the roots of cybercrime. If one wants to gain insights into the groups’ most value-generating activities and understand where disruption is the most effective, one has to increase one’s understanding of the cybercriminal modus operandi, organization, and internal structures (Kraemer-Mbula et al., 2013). Thomas et al. (2015) further emphasize how disruption is most impactful when activities are targeted that include valuable actors, use scarce or highly sought-after resources and the flow of capital. Enhanced comprehension of the actions on the cybercriminal value chain directly correlates with the efficacy of countermeasures taken by authorities and helps them design more effective disruption strategies (Kraemer-Mbula et al., 2013).

#### *1.3.1 Ransomware Value Chain*

To evaluate the value of ransomware group activities and to organize this thesis, the ransomware value chain approach is used. Porter's value chain approach, introduced in 1985, views organizations as systems with interconnected activities that create value. It provides a framework for analyzing how these activities affect costs and profits, highlighting potential areas for optimization. The value chain framework offers valuable insights into how a business ecosystem operates (Kraemer-Mbula et al., 2013).

As ransomware groups are structured similarly to traditional businesses, the value chain approach is suitable to analyze these organizations and their activities. The value chain approach is used to identify the main players, and their ability to add or retract value from the operation (Rush & Mbula, 2014). It is used to identify strategies and how these change over

time. Additionally, value chain analysis enables one to understand the overall context of operations and provides perspective on individual and isolated data points (Rush & Mbula, 2014).

The ransomware value chain is a representation of the operations of a ransomware group, split up into four phases: development, distribution, take-over, and cash-out (van Wegberg et al., 2017). These phases consist of activities that contribute to the financial profitability of the ransomware group, and thus where value is created. It is in these phases that ransomware groups have to invest to generate revenue and grow as an organization.

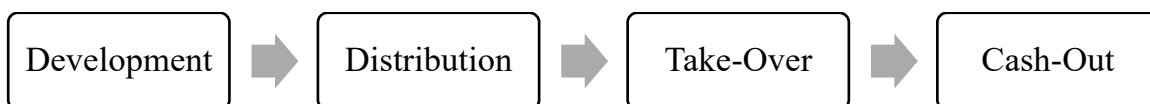


Figure 1: Value Chain of ransomware groups.

*Development* focuses on the creation and refinement of malicious ransomware code. It involves technical expertise not only in software development but also in understanding the security vulnerabilities of potential victims. *Distribution* covers the methods of distributing the ransomware, which starts with an initial access procedure that may include phishing emails, exploiting network vulnerabilities, or implementing social engineering tactics. Effective distribution is crucial as it directly affects the reach and impact of the attack. During the *Take-Over* phase, the ransomware activates and locks out the victim from their systems, encrypting data and demanding a ransom. This phase is critical as it represents the moment of attack and the initial engagement with the victim. Negotiations are done to make sure the ransom is paid. The final phase *Cash-Out* involves the laundering of the ransom payments. This stage is important for converting the illegally gained cryptocurrency into usable capital while attempting to avoid detection and capture.

### 1.3.2 Conti

Revenue-generating activities create value, and value creates opportunities for effective disruption. This thesis aims to provide insights into the value attribution of ransomware groups and thus to gain a better understanding of how ransomware groups can be disrupted in their operations. To do this, chat transcripts of the Conti ransomware group are used as a source. Conti was a Russian profit-driven ransomware organization whose activities were disrupted following a data leak in 2022 (Gray et al., 2022). This leak, primarily consisting of chat transcripts and blockchain addresses, presents a unique opportunity to investigate the group's operations and organizational structure. By gaining insights into how this ransomware group operates, authorities can pinpoint the primary and valuable activities of the ransomware group, enabling them to disrupt these operations and seize revenue streams, thus disrupting the entire organization.

However, despite authorities' efforts to disrupt these activities by targeting capital flow, there remains a gap in comprehensively understanding the value allocation of ransomware groups, along with their related operational structures. While it is generally believed that the most significant disruption power is situated at the top of the ransomware group's hierarchy, as this part involves the largest capital transactions, this has yet to be confirmed through an examination of the organization's value allocation. It is possible that seizing opportunities and disruption power lie elsewhere within operational activities, being those that generate the most revenue, use scarce resources, or sustain the organization.

### *1.4 Research Gap*

Literature exists on profit-driven cybercrime, with ransomware as an example of this type of crime. Previous research has extensively explored the activities, dependencies, infrastructure of capital flow, and the underground economy associated with cybercriminal operations. Ransomware group Conti serves as a significant source for various research purposes, as the leaked chat transcriptions offer lots of details about its operations. However, the elements of ransomware operations are mostly evaluated conceptually. There remains a gap in measuring the importance of the activities of ransomware operations, to determine effective disruption strategies. While value chains have been implemented conceptually to understand cybercriminal groups' operational strategies and revenue generation, there is a scarcity of studies that empirically measure the activities of the value chain. Moreover, there is a lack of application of the value chain analysis to ransomware groups, particularly with a focus on a single specific group.

This gap highlights the need for an in-depth investigation into the value creation and allocation strategies of the Conti ransomware group, using the publicly available Conti leaks as a source of indicators to guide the research. The gap presents an opportunity to better understand ransomware value allocation and elements vulnerable to disruption, to develop more effective countermeasures against ransomware crime.

### *1.5 Research Questions*

Based on the identified knowledge gap, this thesis aims to conduct exploratory research by analyzing the data leaks of the ransomware group Conti. The main research question has been formulated as follows:

*How do ransomware groups allocate value to the activities of the ransomware value chain, and how can this inform law enforcement in developing effective intervention strategies?*

To support the main research question, the following sub-questions are formulated:

*Sub-RQ 1:* To what extent, and how, can data on value attribution within the ransomware value chain be extracted from the Conti ransomware group leaks and blockchain data?

*Sub-RQ 2a:* To what extent is it possible to extract indicators of value creation and allocation from the Conti chat transcripts?

*Sub-RQ 2b:* How do value creation and allocation indicators extracted from chat transcript findings contribute to reconstructing the ransomware value chain and mapping the operational structure of the Conti ransomware group?

*Sub-RQ 3:* How do the insights from mapping value allocations within the ransomware value chain challenge state-of-the-art literature, and what new perspectives or findings can be derived from this comparison to enhance intervention strategies?

### *1.6 Thesis Structure*

Chapter 3 aims to answer the first sub-question by exploratively reviewing the Conti chat transcripts for data on value attribution within the ransomware operations. This is preceded by a methodology introduction in Chapter 2. Chapter 4 includes an examination of the data found by answering the first sub-question, utilizing this data to extract indicators of value allocation, and using these to design formal charts and reconstruct the value chain of the ransomware group. In Chapter 5, the findings are reflected in the state-of-the-art literature. Finally, the discussion includes the interpretation of the research results, and what recommendations for authorities can be taken from it on how to implement the findings in their disruption strategies. The conclusion finishes the thesis.



## 2. Methods

### *2.1 Research Objective*

The research objective is to exploratively analyze the value creation and allocation within ransomware operations. By examining publicly available data from the Conti ransomware group, this study aims to identify patterns and agreements that show how ransomware organizations attribute value to their operational activities. By gaining insights into how value is attributed to activities within ransomware operations, it can be determined which activities are the most impactful to disrupt the organization when disturbed. By enhancing the understanding of ransomware structures, this research seeks to inform Dutch investigative authorities with tools to develop specialized interventions targeting vulnerabilities and scarcities within these operations, crucial for effectively disrupting entire ransomware organizations.

### *2.2 Research Approach RQ1: Conti Chat Data Collection*

This study adopts an exploratory research approach to research the value creation and allocation of ransomware groups. An exploratory research approach is suitable for this thesis, as it focuses on a phenomenon that is known but relatively unexplored, necessitating a deeper understanding of the topic (Bhat, n.d.). In this context, the exploratory research method does not aim to provide definitive conclusions but rather seeks to establish a framework that explains value attribution by ransomware organizations (Bhat, n.d.).

To facilitate an in-depth investigation, the Conti ransomware group is chosen as a specific case for examination. This group is the primary focus due to the abundance of available data resulting from a large data leak. By analyzing public indicators within the Conti ransomware operations, we aim to evaluate the extent to which the organization values its activities and thus where vulnerabilities for disruption are located.

#### *2.2.1 Collecting Data Points from Conti's Chat Transcripts*

In the first sub-question, the Conti leaks messages are researched for any data points that might indicate how the ransomware group operates, interdependencies between actors and departments, and any indicators of value attribution. These potential indicators of value might include the percentual distribution of incoming capital flow, percentual division of salaries, and any type of agreement on monetary flow. All of these data points show how large a part of a certain capital someone receives, and therefore how much value is attributed to that individual or action.



By researching these features of value in the publicly available data, an overview of data points that give information on the value attribution per phase of the value chain of the Conti group is constructed. Simultaneously, an analysis of blockchain transactions associated with the Conti group is performed to validate and cross-reference the data points. The objective is not only to identify explicit mentions of transactions but also to uncover subtle cues and contextual clues indicative of any arrangements or patterns. Interdependencies among various actors and departments within the ransomware group are examined by searching for their capital transactions and agreements. This analysis will show the flows that support the operations of the ransomware group and demonstrate how funds are distributed throughout different value chain stages.

It is important to emphasize that this thesis exclusively considers data points that potentially signify value attribution. This approach is taken because a high value attributed to an activity may suggest a scarcity of resources or a weak link within the operations, thereby increasing the disruptive potential for authorities. It's important to note that indicators solely consisting of transaction amounts in fixed currencies, such as US Dollars, Russian Rubles, or Bitcoin, are not included in this research as much as division percentages or other relative indicators. This is because these static amounts do not reflect their proportionate significance within the overall financial context, and thus do not effectively indicate the value attached to these transactions.

### 2.2.2 Sources

In line with the exploratory research approach, this research relies primarily on secondary data sources. The main source of public data is the Conti leaks, consisting of leaked chat conversations of the Conti ransomware group. This transcript consists of 168,000+ chat messages between the ransomware group actors. Although these chat transcripts are publicly accessible on the internet, a version specifically provided by FIOD authorities is utilized for this thesis. The chat conversations, originally in Russian, have been translated into English using Google Translate, optimized for readability where possible, and organized in an Excel sheet for easy navigation and keyword searching. The primary chat source is the Jabber Chat, featuring direct messages between two Conti members. For an overview of the actors derived from the Jabber chats, as well as their incoming and outgoing messages, consult Appendix A.

Additionally, Rocket chats, containing group conversations, are researched, these have been downloaded pre-translated from the internet for this thesis. This source, however, has not contributed to this thesis with any usable data points. In addition to chat transcripts, scientific literature, and gray literature such as cybercrime reports serve as resources. It is important to note that this research exclusively analyzes existing data sources, no new or primary data is collected. By focusing on secondary data, the research ensures a comprehensive analysis of the delineated set of data, allowing for in-depth exploration and insights into the subject.

### 2.2.3 Keyword Search Method

The chat transcripts are researched for data points that might contain indicators of the value attribution of the ransomware group. The search methodology involves a semi-structured keyword search of the Conti chat transcripts. These keywords serve as the foundation for the search, aiming to identify data points including conversations that indicate patterns, or agreements within the ransomware group. For an overview of the used keywords and the order in which they were searched, consult Appendix B.

To effectively research a large chat transcript for indicators of value attribution, a systematic search process is adopted to mitigate risks and enhance the completeness of the findings. The steps involved are as follows:



Figure 2: Flow diagram for semi-structured keyword search of Conti chat transcripts.

#### **Initial Keyword Search**

The research attempt begins with an initial keyword search. As the search is aimed at finding patterns and agreements about compensation and value attribution, the keywords “%” and “percent(age)” are searched, since these terms often indicate a fixed division of capital or resources. Each keyword result (in this case over 700) is read in context to determine whether it indicates a compensation agreement, value creation or allocation, or an irrelevant topic like the percentage of a computer processor in use. Relevant indicators are filtered, noted, and used to get familiarized with the chats and used language.

#### **Contextual Familiarization**

The context of the identified indicators is analyzed thoroughly by reading entire chat transcript conversations. While this step helps in determining the relevance of the found indicator, this step also helps to build familiarity with the chats. Reading conversations between different actors discussing a variety of topics helps to get familiar with the actor roles within the ransomware group, their modus operandi, reoccurring themes, and topics and to gain a general understanding of the context related to the conversations. This familiarization aids the search process by recognizing recurring patterns in language, which helps identify potential search keywords. Additionally, it provides a deeper understanding of the chat context, making it easier to interpret indicators during the research process. In Appendix B, the order in which the keyword search has taken place and how familiarization and contextualization contributed to this keyword search can be found.

Finally, this phase helps the researcher become familiar with chats containing specific language, recurring code terms, and other typical words used by the ransomware group to describe their

operations. Code language is decrypted by reading numerous examples of key terms used in different contexts. Additionally, decoding code words is achieved by consulting FIOD experts who have previously read the chats and engaged with other cybercrime experts knowledgeable about the Conti leak transcripts. For example, through experience, it has been determined that messages including “sn” or “zp” often pertain to salary-related questions. Similarly, "kosh" frequently appears in salary discussions and is often related to the use of a digital wallet. These terms and their implications are noted wherever possible and utilized in the following steps to interpret indicators by understanding the context and language.

### **Keyword List Expansion**

The initial keyword list is supplemented with new terms discovered from the initial analyzed conversations and the familiarization phase. This snowballing technique ensures the keyword list becomes more comprehensive, including less obvious terms that might occur in the chats. Additionally, the list is expanded through literature reviews, suggestions from FIOD experts, and analysis of gray literature, such as cybercrime reports on ransomware activities. The presented keyword list is dynamic and continuously expanded through this iterative approach.

### **Expanded Keyword Search and Review**

A search using the expanded keyword list is conducted. The results, along with their context, are thoroughly reviewed to identify conversations that might indicate value attribution. This review process aims to uncover new information and indicators that may not include the initial keywords but still point to a pattern that might indicate value. As the expanded keyword search is performed, any new words or phrases indicating value attribution are added to the search list. This iterative process ensures that the keyword list remains dynamic and continually evolves to capture all relevant indicators within the chats. View Appendix B for the order in which the keywords are added to the search list.

### **Final Keyword List**

All the previous steps contribute to a comprehensive list of keyword search attempts. It is important to note that numerous key terms were used to explore the chats during the exploration phase, before implementing the semi-structured keyword search method. Therefore, the final keyword list may not fully represent all the search attempts that were performed.

#### **2.2.3.1 Keyword Search Method Disadvantages**

Using a keyword search approach to research chat messages presents several disadvantages, particularly concerning the completeness and accuracy of the found indicators.

Firstly, the chats were previously translated from Russian to English using an automated Google Translate approach, which can introduce translation errors. These errors can obscure key terms, making it difficult to perform effective keyword searches in English. Additionally, the chats contain a significant amount of code language. For example, terms like "cue balls" (Bitcoin),

and "cat" (often indicating a wallet or Bitcoin address) are used. Proper keyword searches require familiarity with these specific terms and code language. Relevant messages may be missed if these code words are not identified and used as search terms.

Moreover, there is the possibility of leetspeak within the chats, where words are written in an unconventional manner (e.g., using numbers or special characters to replace letters). This can lead to further translation errors and difficulties in identifying key terms during searches. Russian or criminal group-specific slang poses a similar problem. Such slang may not be accurately translated through automated translation, leading to important conversations about value attribution possibly being overlooked.

After accounting for translation and language challenges, human error is another significant factor. A researcher might misinterpret certain conversations, mistaking discussions about operational structures or agreements for unrelated topics. This misinterpretation can result in critical information being overlooked or misunderstood. To mitigate these issues, it is crucial to become familiar with the specific language, code terms, and slang used within the chats. A thorough understanding and careful review of context and language can enhance the accuracy and completeness of the keyword search.

### 2.2.4 Value Chain Research Lens

After the chat transcript research, the findings are structured according to the ransomware value chain. This provides a guide for organizing the results and analyzing them further. The ransomware value chain is a representation of the operations of a ransomware group, split up into four phases: development, distribution, take-over, and cash-out (van Wegberg et al., 2017). These phases consist of activities where value is created for ransomware groups, and thus where ransomware groups like Conti have to invest to generate revenue. By using the value chain as a guide for the categorization of indicators, this data serves as structured input for sub-question 2, where the data points are reviewed for their potential to indicate any value creation and allocation within the ransomware group. By using the value chain as a guide, the data provides insights into what activities within the ransomware operations are valued the most and how this is expressed.

### 2.2.5 Blockchain

To confirm and supplement the findings of sub-question 1, blockchain analysis is implemented using blockchain analysis tools, Chainalysis and Mempool Bitcoin Explorer. This analysis aims to validate and verify the indicators of value attribution gained from the chat transcript data. This analysis tests the verifiability of the leaked chat transcripts by using the public accessibility of blockchain tracing to test the addresses and hashes named in the chats. This confirmation increases the dataset's reliability and value for research purposes.

Reflecting on reproducibility and reliability, blockchain analysis provides a robust method for verifying the authenticity of the findings. Since blockchain transactions are immutable and publicly accessible, the findings can be reproduced and verified by other independent researchers using the same methods. This enhances the reliability of the conclusions drawn from the analysis. Reproducibility is further increased by using public and free blockchain analysis websites like the Mempool Bitcoin Explorer for tracing purposes. This is done as Chainalysis, an investigative tool used with the appropriate authorization of the FIOD, is not publicly accessible. Therefore, this tool is mainly used for visualization. The labeling of data points (attributing an actor to a transaction or wallet and clustering addresses that belong to the same actor) is performed by Chainalysis and is not universally accessible, and therefore used as least as possible.

In Appendix E, an overview of the blockchain analysis implementation is provided. It should be noted that while attempts were made to use blockchain analysis to uncover new information, these were largely unsuccessful. Nonetheless, the primary focus remains on verifying existing information rather than discovering new data.

### *2.2 Research Approach RQ2: Determining Value Attribution and Formal Charts*

In the first part of the thesis, the Conti chat transcripts are analyzed to identify data points that might include indicators of how ransomware groups create and allocate value, to determine which activities are crucial to their operations. In the second sub-question, the data gathered from sub-question 1 is analyzed for indicators of value creation or allocation, which is then used to determine the value allocation structure for each activity phase of the value chain.

For each phase, the actors involved in the operations are identified, as well as their (financial) interdependencies and cooperation. This information is summarized and visualized into a formal chart, a method of analyzing institutional contexts based on "Policy Analysis of Multi-Actor Systems" by Enserink et al. (2022). Formal charts depict important formal and informal relationships and interconnections between actors, as well as resource interdependencies. Following the formation of the formal chart, the findings from sub-question 1 are analyzed for value attribution. This analysis focuses on where value is created and allocated, and where prioritization occurs within the ransomware group. After analysis, this information is added to the formal chart to visualize where value is created within the activities, which includes anything that generates revenue for the ransomware group, as well as how this value creation is compensated and thus where value is allocated among the activities and actors involved. Using these insights, conclusions can be made regarding the modus operandi of the organization and where its critical points are situated.

### *2.3 Research Approach RQ3: Confronting Literature*

In this third sub-question, the objective is to reflect all the insights obtained from the Conti ransomware case within this thesis on existing scientific literature, exploring the empirical contribution of the thesis. After determining the value creation and allocation within ransomware operations in sub-question 2, these findings are confronted with other literature, which has been included in the literature review of the thesis introduction.

The purpose of mapping these findings against existing literature is to identify where new insights have been generated and where the findings align with previous, more conceptual research. This comparison helps determine the extent to which the thesis findings support or expand upon earlier concepts of profit-driven cybercrime and value chain applications. Additionally, this reflection aims to increase the generalizability of the report and assess its contribution to the available literature.

This chapter also includes a reflection on applying the value chain lens in a cybercriminal investigation. Employing the value chain lens as a tool to empirically attribute value and identify critical activities within a criminal group's operations is a novel approach. Consequently, the scientific contribution of this method is also examined.

### 3. Conti Chat Transcript Research

In this chapter, the first sub-question is investigated. The Conti chat transcripts are explored to identify any data points that might include indicators of value creation and value allocation within components of the Conti ransomware group. In the previous chapter, a method for data research using a keyword strategy is proposed. Using this method, the Conti leaks chat transcripts are researched as objectively as possible. This exploration is conducted through the lens of the value chain framework, categorizing and plotting all findings. The chats are examined for relevant data points with indicators of value, with supplementary blockchain analysis conducted to validate and supplement the findings. For the chat findings that form the foundation for this chapter, consult Appendix C.

The ransomware value chain comprises several phases: Development includes software and malware development, while Distribution involves gaining initial access and affiliate collaboration. Take-Over involves system seizure, negotiations, and victim extortion through blog posts, while Cash-Out focuses on money laundering and converting funds into fiat currencies. Governance stands as a distinct phase, with overseeing actors determining revenue allocation and the organization's modus operandi. All research findings are sorted by phase and presented chronologically, potentially revealing evolution or changes over time. Each phase concludes with a timeline of its findings.

#### *3.1 Development*

The chat transcripts of the Development phase reveal various compensation and revenue-sharing strategies within the cybercriminal group and show the structured approach to developer recruitment and software development.

The developmental phase within the value chain of ransomware cybercrime involves establishing the infrastructure necessary for executing attacks. This phase predominantly revolves around software development, where coders write the malware essential for ransomware operations. Malicious code writers, primarily motivated by financial gain according to Rush et al. (2009), drive this process.

Profit-driven cybercrime often involves a workforce that aids in the execution of criminal activities rather than managing or devising strategies (Paquet-Clouston & García, 2023). These workers undertake critical tasks such as coding, software development, and testing. Examples of such roles include coders, who write the malware; crypters, who encrypt and obfuscate malicious code; lockers, who manage access controls and encryption keys; and testers, who assess the effectiveness and functionality of the developed software (Check Point Research, 2022). For all of the activities in this phase of the value chain, a certain level of technical knowledge is required (Rush & Mbula, 2014).



### **Software developers' rate**

The recruitment of software developers within the Development phase involves various flexible compensation strategies, including fixed payments, revenue sharing, and deposits to attract and maintain talent despite challenges in hiring.

In one instance, Tom (affiliate, supplies networks) communicates with Stern (the boss) about hiring coders, offering them 10-20% monthly with variable deposits [Tom > Stern: *"10-20% per month plus or minus the increase in deposit suits me"*]. Tom further mentions he is struggling with recruiting these developers. This shows how the group does not have a fixed percentage of revenue available for developers but is flexible to vary the rate when scarcity is apparent. This is done to attract new developer talent, including providing these workers with a deposit to cover initial costs.

This finding is further substantiated by a discussion between Dino (developer) and Mango (technical manager). The negotiation of terms indicates that software developer talent has to be proven through fixed payments first, but that a percentage can be earned in the long run. [Mango > Dino: *"30 and 20 can be made, but not immediately, at least there the first payments 3 must be received"*]. This indicates how developers are compensated well but need to show their potential first in a trial run. A division of 20% or 30% of the initial ransom payment is a reoccurring percentage, as visible from the Conti ransom payment data of RansomwareLive.com (see Appendix D). Furthermore, this chat find confirms how coders and developers can receive a deposit. Dino receives around \$2000 worth of Bitcoin as a deposit, confirmed through blockchain data.

The chats show that testing the software is done by hired employees, often students, who are hired for \$1000-1200 per month. While this does seem like a large sum for the relatively easy job they are to do [Bentley > Stern: *"any student who is able to install Windows, virtual machine and vpn can handle it"*], as the salaries per month of the other employees are unknown, there is no way to attach a value to this allocation of salary.

### **Software rent and revenue sharing**

The chat transcripts reveal discussions on redistributing earnings, optimizing software and network usage, and preferring in-house software development to maximize value and efficiency.

The findings include a discussion regarding the redistribution of earnings from a locker called "Maze." Maze will take 25-30% [Kevin > Stern: *"how much maze will take 25-30%"*]. Kevin (coder) suggests that instead of an even split, the distribution should be based on involvement and contribution, allowing Stern, himself, and the Professor (hacking operations manager) to



share the remainder of the revenue [Kevin > Stern: “Well, either equally between you, me and the prof. I just don't know what arrangements you have there.”]. This shows how first, the locker operator takes his rightful share, after which the operators receive the remainder. Later in the chats, the group shows disinterest in locker rental, as they operate their lockers internally.

In another discussion about software usage, Stern and Bobby discuss the details of optimizing software and network usage rates and percentages. The aim is to cut costs. Stern argues that keeping the 20% network usage rate as a base for making an offer [Stern > Bobby: “for grids from others more than 20 percent, let's not offer”]. There is a focus on efficiency and cost reduction regarding software usage.

Software rent rates are further discussed between Stern and Bobby, where the current software rent rate of 16.5% is no longer suitable for the group. This indicates that developing software themselves is more profitable than renting it for 16.5%, valuing their in-house software development. He does tell Bobby that his “correspondence on experience” is worth 6.5%, indicating that a part of the revenue is reserved for experience.

**Conclusion**

Overall, the group's strategies illustrate how value is attributed to different roles and activities, with flexible compensation schemes for developers based on proven performance and involvement. The findings highlight the emphasis on internal development over renting, reflecting a strategic allocation of value to maximize profitability and efficiency within their operations.

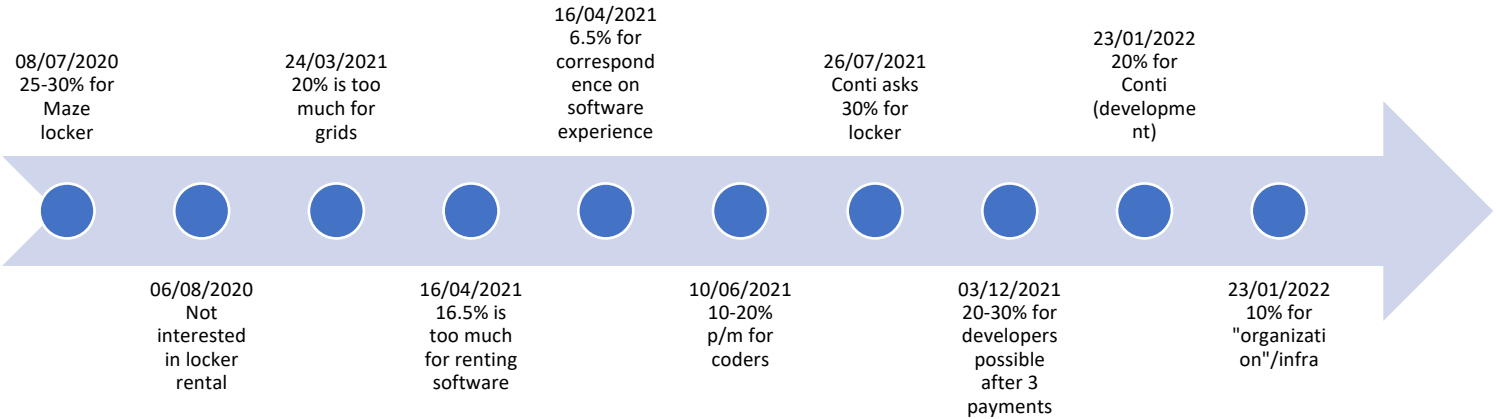


Figure 3: Chronological timeline of Development activities.

### 3.2 Distribution

The examination of chat transcripts reveals insights into the compensation strategies for operational workers, highlighting the flexible approach to rewarding affiliates and hackers based on their contributions and performance.

The distribution phase within the value chain of ransomware operations involves spreading the developed malware to victims. This process includes activities such as gaining initial access to targeted systems. Initial access is often gained through spamming or phishing, utilizing emails or botnet spammers (Rush et al., 2009). Initial access tasks are commonly outsourced to affiliates, who provide this service to ransomware groups for a share of the ransom payment (Thomas et al., 2015). Affiliates vary in skill level, ranging from script kiddies or unskilled hackers to more experienced individuals. They may utilize Ransomware-as-a-Service (RAAS) packages sold by ransomware groups, which often do not require any special skills.

Additionally, botnet operators, spammers, and hackers play significant roles in this phase. Botnet operators manage networks of seized devices used for spamming or launching attacks (Rush & Mbula, 2014). Spammers send out phishing emails or other malicious communications to gain access to systems. Hackers utilize their skills to exploit vulnerabilities and gain entry to targeted networks (Check Point Research, 2022). These operational workers contribute to the deployment and management of the malware within targeted systems.

#### Compensation for Operational Roles

The data points show how affiliates in the distribution phase are compensated for simple tasks with a set percentage of the ransom, how initial payments are low but can increase based on performance and experience, and how value is attributed through proven success and negotiation.

In the distribution phase, outsourcing work to affiliates is done for simple, repetitive tasks. Their payments are mentioned in the chat transcripts, where for example for operational roles like enabling VPN access, spammers are compensated with 20% of the initial ransom payment. This percentage is confirmed by both the Professor (hacking operations manager) and Stern (the boss) [Stern > Professor: *“for the entrance I usually give 20 percent”*]. This division, confirmed through blockchain analysis, shows how affiliates are valued for their entrance services. The remaining 80% of the ransom payment is, as it turns out from the labeling by Chainalysis, divided among highly ranked actors like Stern, Target, and the Professor, to be kept or to be further distributed to those entitled to a share.

As an affiliate working for Conti, initial payments are low, but hard work pays off. The group shows reluctance in compensating affiliates, with initial rates starting at 15% for each target

[Tramp > Mango: “*max 15 at the start I will give him*”] and potentially increasing to 30% based on the affiliate's success. This reluctance at the beginning of the affiliate’s career reflects how value needs to be gained through experience and success. This is confirmed by a chat find where recruits are promised a fixed amount per successful attack, before receiving a percentage for their work. This also counts for reverse engineers, who are offered a low salary but where the operators are “ready to raise the salary to what the candidate wants, if he can CONvincingly prove that he is worth the money” [Buza > Salamandra].

### **Adjustments in Hacker Payments**

The data points reveal issues with financial arrangements, including discrepancies in promised versus received compensation, the high value placed on target acquisition, and a strategic shift from using external hackers to training internal talent for cost efficiency.

Not all financial arrangements proceed smoothly. One noticeable case is the case of Netwalker, who was promised 70% for his hacking contributions but received only 40%. This shows how the value attributed to a certain action can shift quickly, and how this can lead to dissatisfaction for the worker. Cybergangster (manager of Conti locker & hacker) later admitted to paying only 40%, suggesting a discussion of the worth of hackers, indicating a possible decline in their perceived value [Cybergangster > Demon: “*I promised him 70%, but in fact I barely gave 40%*”].

Netwalker's situation also underscores the high value placed on target acquisition. He is initially offered 45% for his targets, but he does not receive this offer and later even complains about how his targets were spied on and stolen. The new agreement of 20% extra for targets is also not paid. This shows the importance and value of securing and owning credits for targets, and how financially powerless the hackers are in comparison to the higher-ranked actors of the group.

A significant shift in the group's strategy was observed in February 2022, in their transition from using externally trained hackers to training internal talent. Previously, external hackers would receive a rate of 35% of ransom payments. However, with the shift to training hackers internally, this rate has been reduced to 20%. This new model reflects Conti's capability to train hackers in-house, presenting a long-term cost-cutting strategy. This is confirmed by a chat find where operators discuss how they should invest in high-quality hackers, for example by growing their compensations over time.

**Profit Share Models**

The data discusses Logan's proposal for a profit-sharing model to enhance efficiency and reduce risks, and the importance of maintaining reputation and security as indicated by Reverse's compensation.

In 2020, Logan insists on a 50% profit share from his affiliates and assures that his level of control ensures superior work quality and reduces operational risks. He suggests that Stern should adopt a similar strategy, working with affiliates exclusively recruited through him. This would provide Stern with better-quality work for less money and fewer responsibilities, as Logan would handle part of the management. It is uncertain whether this new management style is adopted, although Stern seems eager as he only has “one person left to work”.

Reverse (hacking operations manager) is given a 10% compensation for maintaining the reputation and security of a locker. This might indicate how besides operational work, maintaining reputation is also important during this phase.

**Conclusion**

The findings illustrate how value is attributed within the cybercriminal group, with compensation varying according to the role, experience, and success of individuals. Affiliates start with lower rates but can earn more through proven performance, while high-level actors receive a larger share of the profits. The shift to training internal talent and adjusting hacker payments further reflects the group's strategic emphasis on efficiency and long-term value optimization.

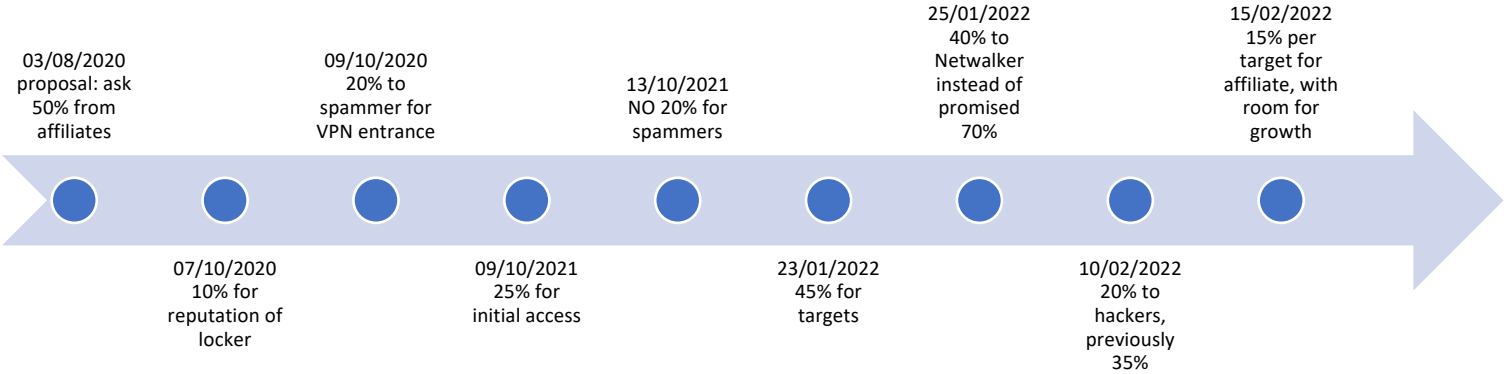


Figure 4: Chronological timeline of Distribution activities.

### *3.3 Take-Over*

The chat transcripts reveal the compensation dynamics for OSINT operators and bloggers during the take-over phase, highlighting the discrepancies in pay rates and the impact of individual performance and role on financial rewards.

In the take-over phase of the ransomware value chain, the targeted system is infected, and the victim's data is encrypted, often containing sensitive personal information, valuable company reports, or financial details. To obtain the decryption key, victims must pay a ransom. However, negotiation with the ransomware group can sometimes lead to a reduction in the ransom amount. To facilitate negotiations, cybercriminal groups employ negotiation staff who assist in tasks such as communication and translation (Paquet-Clouston & García, 2023). These individuals are integral members of the criminal organization's workforce. Additionally, ransomware groups may operate blog websites to pressure victims into paying by threatening to release stolen data. Ransomware groups employ blog operators to manage these platforms and post content aimed at forcing victims into compliance.

#### **Compensation for Chat Take-Over**

During the take-over phase, OSINTs (Open-Source Intelligence operators) play a critical role in taking over chats. They contribute by utilizing open-source intelligence to aid in the extortion of victims. They earn 1% for these efforts, a rate they are happy with. This compensation typically ranges from 5-10K, reflecting the value and importance of their work within the group's operations.

#### **Bio the Blogger**

The chat transcripts reveal Bio's struggles with compensation and working conditions, highlighting his dissatisfaction with a 0.5% payment rate, and attempts to negotiate a higher rate.

Between November 2021 and February 2022, Bio, who is the blog operator for Conti and does negotiations as well, extensively discusses his payment structure and frustrations with colleague Skippy. Skippy is also a negotiation employee of Conti.

First, Bio and Skippy discuss the challenging working conditions under Tramp (Take-Over team leader). They express frustration over working overtime on weekends, for which they do not receive any additional payment. The men receive 0.5% of the ransom payment for their jobs. Due to feeling undervalued for their overtime on the weekend, Bio and Skippy consider quitting. However, Bio hesitates due to family responsibilities.

Bio again verbalizes his frustrations to Skippy about being undervalued with his 0.5% compensation rate [Bio > Skippy: *"I want them to just appreciate me and consider me a full-fledged in the team, and not half 0.5))"*]. Skippy then reveals that Decoy, another operator, provides his team with 3%, suggesting that other teams or ransomware families may offer better financial incentives. Additionally, bloggers in Decoy's team receive a fixed salary, indicating a more stable payment structure compared to the percentage-based compensation in Bio's case.

Bio requests Tramp for an increase from 0.5% to 1%, but Tramp rejects this, promising that Bio already receives 1% when he receives bonuses [Tramp > Bio: *"you already get 1% with my bonuses"*]. Despite these assurances, Bio remains dissatisfied, feeling overworked and underappreciated. Tramp emphasizes that Bio's total compensation, including bonuses, is comparable to his colleague Skippy's earnings.

One day after the negotiation chat, Tramp awarded Bio a 1% bonus, amounting to approximately \$7000, confirmed by a transaction of 0.1194 BTC. This bonus highlights the occasional financial rewards given to operatives, though the structure and frequency of such bonuses seem inconsistent.

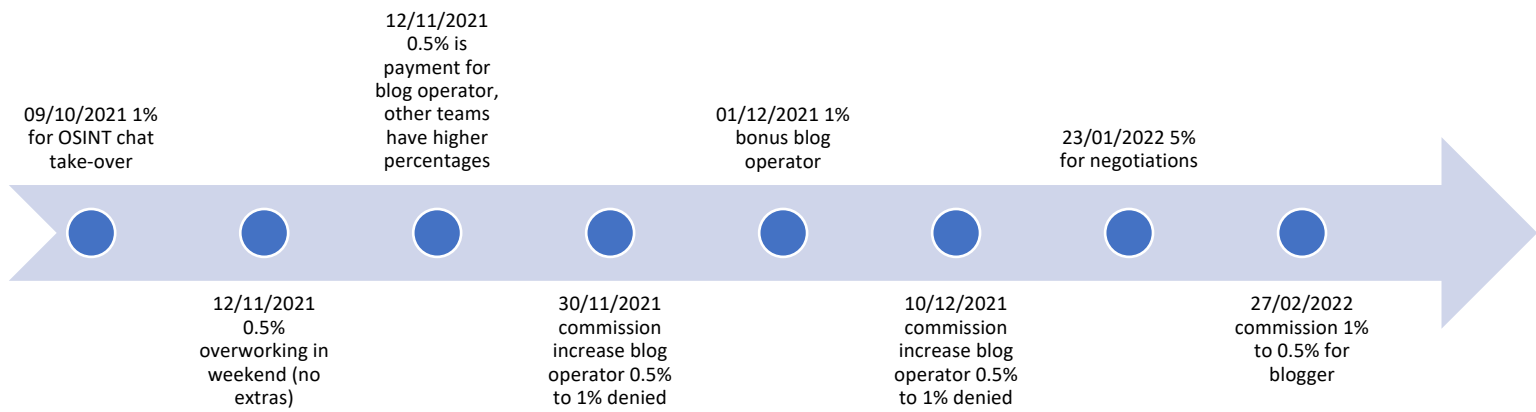
Only 10 days after the initial request, Bio's second request for a salary increase to 1% is again denied. Tramp promises to reconsider the rate after the New Year but maintains the current rate of 0.5%, supplemented by potential bonuses. Bio voices his dissatisfaction, comparing his extensive workload to that of an external known as "the Indian," who receives the same 0.5%. Bio feels that his multiple responsibilities, including data analysis, blog writing, and negotiation management, should receive higher compensation.

About three months later, Bio has changed his name to Pumba. Pumba experiences a reduction in his compensation rate from 1% to 0.5%. This means that in the gap of three months, Bio has convinced Tramp to increase his salary to 1%. Tramp, citing mistakes made by Pumba, decides to cut the rate, suggesting that blogging is a lower-value task that can be managed internally and one that the boss can even do himself. After the reduction, Pumba receives a payment of 0.746645 BTC, approximately \$29,000, which aligns with the reduced 0.5% rate based on the ransom amount discussed. Pumba requests to leave Tramp's team.

### **Conclusion**

The data reveals how value is attributed to different roles within the group. OSINT operators receive modest but satisfactory compensation for critical tasks, while bloggers experience significant dissatisfaction due to perceived undervaluation and inconsistent pay increases. The shifting compensation rates and bonuses show how both role importance and individual performance influence financial rewards.

## Decrypting Ransomware Operations



*Figure 5: Chronological timeline of Take-Over activities.*

### *3.4 Cash-Out*

The chat transcripts discuss the challenges and considerations associated with money laundering and exchange commissions, including the varying rates for laundering services and the search for more cost-effective exchange options.

Cash-Out represents the phase in the value chain where cybercriminals convert their illegal gains into cash. This involves various tactics, including money laundering, where cryptocurrencies are exchanged for traditional fiat currencies through crypto exchange services, typically for a commission fee. This phase also includes crypto mixing, where mixer services process Bitcoin from cybercriminals through multiple transactions, creating a blockchain trail that is harder or impossible to trace (Oosthoek et al., 2023). This phase is where detection and the risk of arrest increase (Rush & Mbula, 2014). It is a phase that implicates high risk, though requires less technical capabilities (Rush & Mbula, 2014).

Other activities contributing to Cash-Out include reinvesting in the cybercriminal organization by for example purchasing new software or other advancements. Additionally, paying salaries to internal employees is categorized under cashing out the earned ransom.

#### **Money Laundering and Exchange Commissions**

Money laundering and exchanges are discussed in the chats, but the commissions are not mentioned very frequently. In one instance, Mango, the technical manager, requires assistance with converting and laundering funds. He needs to change \$12,500 into dollars and launder another \$12,500. Zulas offers to help Mango. Mango seems willing to accept a laundering commission of 30%, highlighting the high cost and complexity of such services.

In the context of converting Bitcoin (referred to as "cue balls") to fiat currency, Zulas mentions that a 30% commission is quite substantial. He suggests that while this rate might be on the higher side, it is not entirely uncommon in the context of money laundering operations.

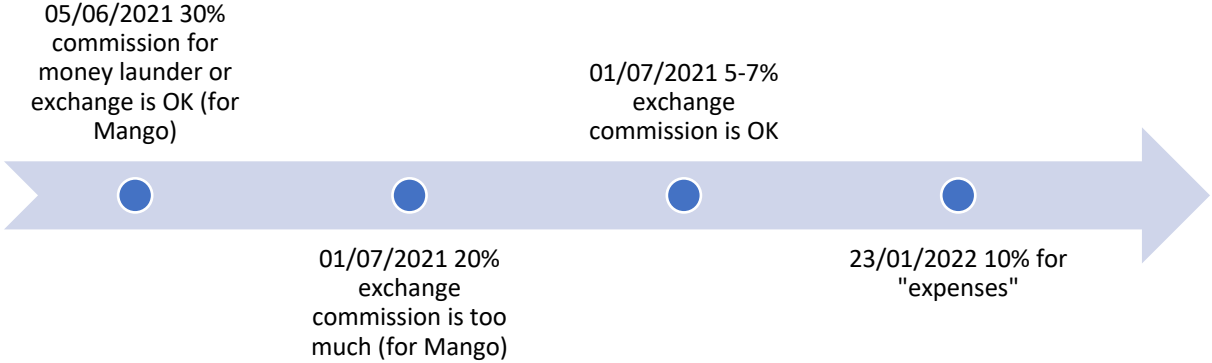
#### **Exploring Lower Exchange Commissions**

In another conversation one month later, Mango expresses concern over high exchange commissions. He finds a 20% exchange commission excessively high and seeks more economical alternatives, aiming for a commission rate of 5-7%. This dialogue shows the importance of finding cost-effective methods for converting Bitcoin to fiat cash, a critical aspect of their financial operations.



**Conclusion**

The chat transcripts illustrate how value is attributed to financial operations, where high commission rates reflect the complexity and risk of money laundering services, while the search for lower exchange commissions underscores the group's focus on minimizing costs in their financial transaction.



*Figure 6: Chronological timeline of Cash-Out activities.*

### 3.5 Governance

This section includes findings that indicate the governance regarding the value chain. In the value chain, those who govern the organization have the power to determine who is involved in the value chain (Rush & Mbula, 2014). These operators determine the modus operandi, price, type, and quality of products, and are largely responsible for the distribution of profits along the value chain (Rush & Mbula, 2014). In the case of this research, governance is mostly centered around the division of ransom among those placed in the higher tiers of the organization.

#### **Bosses**

In a conversation about payment distribution, Target (HR manager) seeks Stern's (the boss) instructions on how to allocate the received ransom payment. Stern decides he wants to receive 30% of the total payment, amounting to 22.5 BTC from a 75 BTC payout. This transaction took place on October 9, 2020, and is confirmed by blockchain data. The remaining 70% is divided by Target into two separate internal transfers to be further distributed. There is a structured approach to financial distribution within the group.

With another ransom payment, after allocating a discussed 30% to Stern and 20% to the spammer, the remaining 50% of the funds are designated for the hackers, Target, and the Professor. This means that out of a balance of \$400,000, \$200,000 goes to Target and \$200,000 to the Professor. These transactions are confirmed on the blockchain, indicating fixed dollar amounts rather than percentages for these transfers. The amount left over, approximately \$22,600, is not possible to track. The hackers may be paid by either Target, the Professor, or with the transfer of \$22,600.

Further discussions between Professor (hacking operations manager) and Stern reveal discrepancies in the reported percentages. Stern claims he took only 20% when he took 30%. This conversation shows how the upper-level actors still mislead each other with false information for their benefit. The Professor indicates that if Stern owned both the software and the botnet, he would be entitled to 50%, but since the botnet belongs to the spammer, the spammer rightly receives 20%.

Conti receives 74 BTC in another instance, and Kevin (coder) confirms that 40% of this amount is allocated to Stern. Although the initial transaction of 74 BTC isn't found, subsequent transfers include Stern sending 20% to Kevin and another 20% split between two other addresses. Additionally, Stern transfers 52.5 BTC to an exchange, approximately 70% of the initial 74 BTC. This situation suggests a complex and potentially overlapping series of transactions where Stern might be exchanging his share (40%) immediately, paying Kevin 20%, and distributing another 20% to others, indicating intricate financial maneuvers.

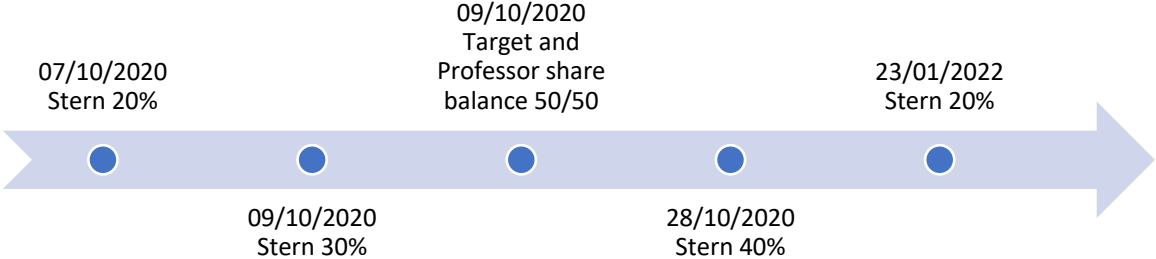


Figure 7: Chronological timeline of Governance activities.

## 4. Value Attributions and Interdependencies in Conti Group

In this chapter, the second sub-question is answered. The chat transcript findings of the previous chapters are analyzed and sought for value indicators to help dissect the operational structure of the ransomware group Conti. To answer the research question, a formal chart is created for each phase of the value chain to visualize the key financial actors within a ransomware organization and their relationships and interdependencies. It will also show how value is created within the organization and how this value creation is compensated.

### 4.1 Development

During the Development phase, most value is created by coders and developers of malicious software. Their work is allocated and valued at a percentage that varies by function and depends on their experience and efficiency. The organization values these workers, as these highly technically skilled developers are scarce and difficult to recruit.

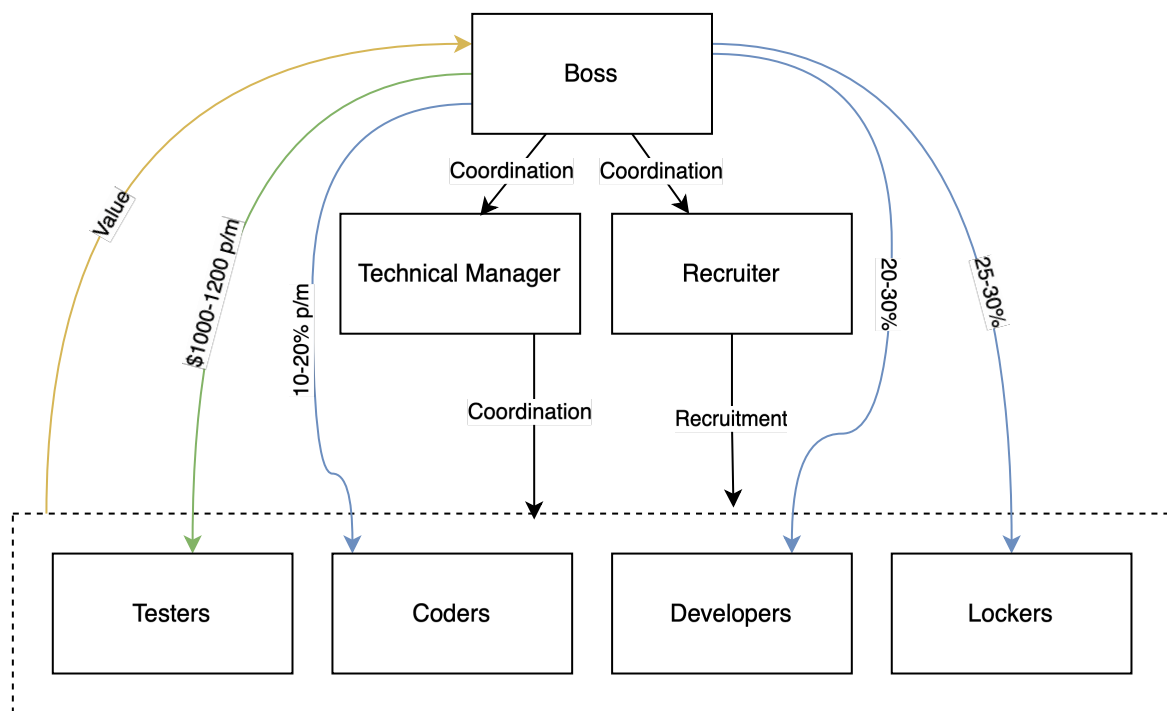


Figure 8: Formal chart of the Development phase in ransomware cybercriminal activities.

Single-sided arrows indicate a hierarchical relationship, two-sided arrows indicate other relationships. Yellow arrows indicate where value is generated for the organization, and blue arrows indicate the compensation for this value creation. The green arrow indicates value compensation in a fixed sum.

Coders and developers are crucial during the development phase, as they generate value for the ransomware group by creating malicious software. Their work directly impacts the quality of the software, and thus the efficiency of ransomware attacks. If coders lack skills, effort, or motivation, it can negatively affect the business operation. Therefore, these workers are offered a percentage of the ransom payments after demonstrating their potential with three fixed

payments. For developers, this ranges between 20-30% per successful attack, while for coders a long-term percentage of 10-20% per month is mentioned. This revenue-sharing tactic indicates that management recognizes developers' power to disrupt the organization through poor-quality work, and thus provides them with a hopeful future perspective of a percentage of the ransom payment to maintain their motivation. This tactic further protects the organization from investing in incompetent developers. By relating compensation to performance, the organization ensures that only those who generate value through their skills are rewarded.

The fixed percentage with potential for growth in times of scarcity therefore indicates a value allocated to these workers by the organization. This value is supplemented with chat messages confirming how recruiting developers is difficult. This can be explained as the job entails a high level of technical knowledge, which is a rare qualification. This further suggests how these workers are high in value to the Conti ransomware gang.

The value placed on experience is confirmed by a 6.5% bonus awarded for "correspondence on experience," meaning that workers with relevant experience receive this bonus when they use their expertise for the benefit of the group.

Lockers, who generate value by managing controls and encryption keys, are able to take 25-30% of the ransom payment. With this percentage being comparable to or higher than that of coders and developers, it can be concluded that these lockers are of high value to the Conti ransomware gang. This is confirmed by the disinterest in renting external lockers: Conti values them high enough to have them internally.

Finally, financial considerations such as software prices, renting rates, and development costs are mentioned in this phase. Internal software development is prioritized over renting software externally when the price is higher than what the internal development is perceived as. This is done to maximize profitability and avoid dependency on external partners. For example, a 16.5% rent rate for software is considered too high, indicating that internal development is perceived as more valuable. Similarly, discussions revealed that a 20% network usage rate is seen as too much, which emphasizes the organization's focus on maintaining value through efficient resource allocation.

The development phase demonstrates how the ransomware group aligns compensation with value creation by offering coders and developers a percentage of ransom payments based on their performance, thus ensuring high-quality work and protecting against underperformance. The significant share of ransom payments allocated to lockers and the preference for internal software development further illustrate the group's emphasis on maximizing value and cost-efficiency. These practices highlight the group's focus on incentivizing valuable contributions and maintaining control over critical resources to enhance overall operational effectiveness.

## 4.2 Distribution

During the Distribution phase, Conti's affiliates and internal hackers generate the most value by gaining initial access to systems and exploiting them for ransom. Their work is valued at 15-35% of the ransom, influenced by experience, training, and success rate. Despite this, cost cuts are pursued through in-house training and underpayment of hackers.

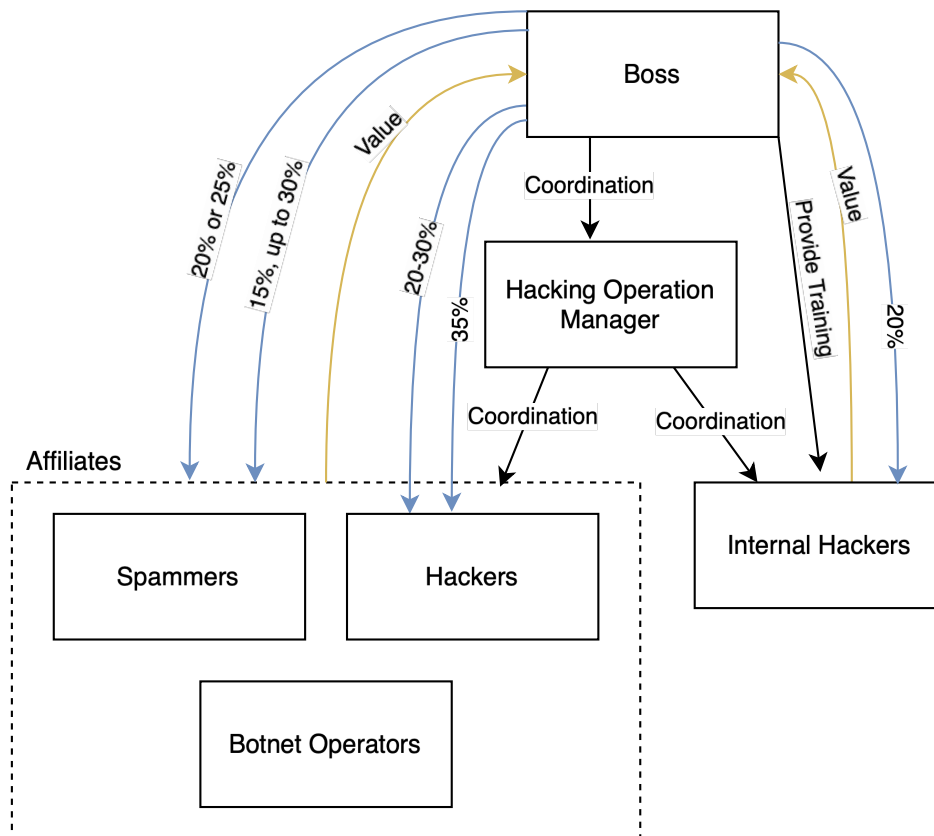


Figure 9: Formal chart of the Distribution phase in ransomware cybercriminal activities. Single-sided arrows indicate a hierarchical relationship. Yellow arrows indicate where value is generated for the organization and blue arrows indicate the compensation for this value creation.

During the Distribution phase, both affiliates and internal employees play a crucial role by accessing vulnerable systems to extort ransom, thereby creating value for Conti. Affiliates are allocated value by receiving a percentage of ransom payments based on their success and prior experience, with initial rates starting at 15% for new affiliates and potentially increasing to 30% with good performance. Those providing VPN access typically earn 20-25%, with potential growth if they deliver high value. This performance-based compensation incentivizes high-quality work, as each successful attack directly increases their income. Efficient operation enhances their value and thus compensation, motivating them further and leading to greater profitability for the ransomware group.

Hackers generally receive 20-30% for their work, with internal hackers receiving specialized training to exploit victim systems and generate value for the ransomware group. To optimize costs, the group is shifting from hiring external hackers to internally training them. Internally trained hackers receive 20%, while external ones get 35%. Although this program requires an initial investment, it aims to reduce long-term expenses by paying lower rates to internal hackers. Training in a controlled environment ensures high-quality instruction, resulting in skilled hackers working for less. This cost-efficient approach saves on payroll, enhances efficiency, and reflects the group's priority on reducing expenses by investing in internal training over hiring potentially less skilled external hackers.

However, there are instances where workers feel undervalued, as seen with Netwalker, who was promised 70% of the ransom payment for this contribution but received only 40% for his work. The actual payment not aligning with the promised compensation shows an undervaluation for a specific actor in this instance.

In terms of value creation, the chats indicate how targets (potential victims) are sold for 45%. However, there have been instances where targets were spied on and stolen, which indicates that owning (the credits of) targets is a high-value thing.

In the Distribution phase, Conti strategically allocates compensation based on performance, with affiliates and hackers earning percentages of ransom payments that incentivize high-quality work and align with their contributions. The shift from external to internal hacker training shows a cost-efficient approach to maximizing value and reducing long-term expenses.

### 4.3 Take-Over

During the Take-Over phase, the Blog Operators and Negotiators are generally undervalued for their work, which takes place under high pressure and unsupportive working conditions. The workers create value for the organization by handling the negotiation process and exerting the pressure necessary to make the victims pay their demanded ransom. Undervaluation for these workers might indicate that the performed job is not as essential or complicated as that of others.

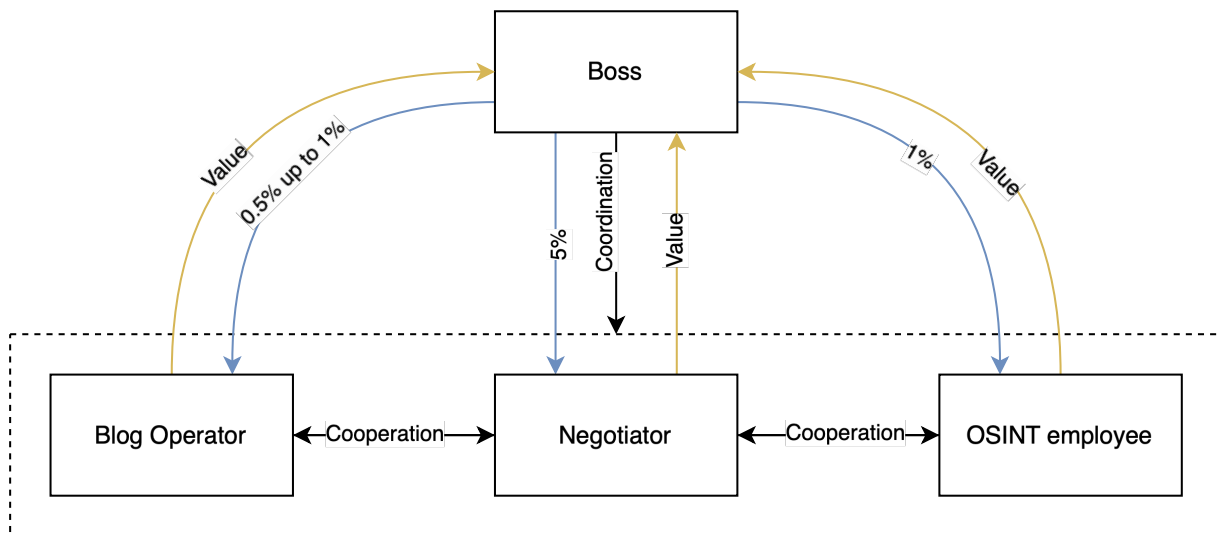


Figure 10: Formal chart of the Take-Over phase in ransomware cybercriminal activities.

Single-sided arrows indicate a hierarchical relationship, two-sided arrows indicate other relationships. Yellow arrows indicate where value is generated for the organization, and blue arrows indicate the compensation for this value creation.

Blog Operators are compensated based on their effectiveness in pressuring victims. This is achieved by extorting victims through posting or threatening to post their data on the blog. The chats indicate that the base rate is 0.5% of the ransom payment, which can be raised to 1% based on good performance. Receiving this increase in compensation is not easy, as the Blog Operator shows by asking his boss multiple times for two months and being denied. This indicates that the Blog Operator job is valued enough by the organization for a fixed percentage but is not essential enough to be rewarded with a salary increase that satisfies the worker. That compensation rates are dependent on job performance shows when the percentage is readjusted based on poor performance, as seen with the Blog Operators' rate reduction, where he first earned 1% and is reduced to 0.5%. In this instance, the Boss even mentions that he can do the work himself. This means that Blog Operators' job is deemed low effort and easily replaceable, and only valued when their work is adequate. Lack of quality work has a salary reduction as a consequence.

The minor value placed on the Blog Operator and potentially even negotiation employees is reflected in a conversation between the Blog Operator and a Negotiator, who both work very hard, receive barely any vacation, and are expected to work on weekends while maintaining a



family, all for their base rate. Due to the top-down control of the bosses, the workers feel undervalued and overworked despite their crucial role in the ransomware attack. These high-pressure working conditions in combination with the reluctance to increase salary to a suitable rate illustrate how these workers are generally undervalued by the organization.

The Negotiator offers value by negotiating with the victim on a ransom amount, ensuring that this amount is paid to the correct address, and confirming that the money enters the organization. The compensation for the Negotiator is not mentioned explicitly, though in one instance, 5% of the budget is set aside for it.

OSINT operators contribute by utilizing open-source intelligence to aid in extortion, making the ransom payment more likely to succeed. They receive 1% of the ransom payment for chat takeovers. They are satisfied with this compensation and feel appreciated and valued for their work. This means that the organization recognizes the importance and value of the OSINT operators' activities to provide them with adequate compensation.

Blog Operators and Negotiators are essential to the ransomware operation but often feel undervalued due to low and unadjusted compensation rates, which shows their replaceability and the high-pressure conditions they, therefore, go through.

#### 4.4 Cash-Out

In the Cash-Out phase, the primary goal is to convert illegally obtained cryptocurrency into usable currencies. This service involves a commission fee. Minimizing this commission is crucial for maximizing transaction efficiency, allowing the organization to reinvest as much as possible back into its operations.

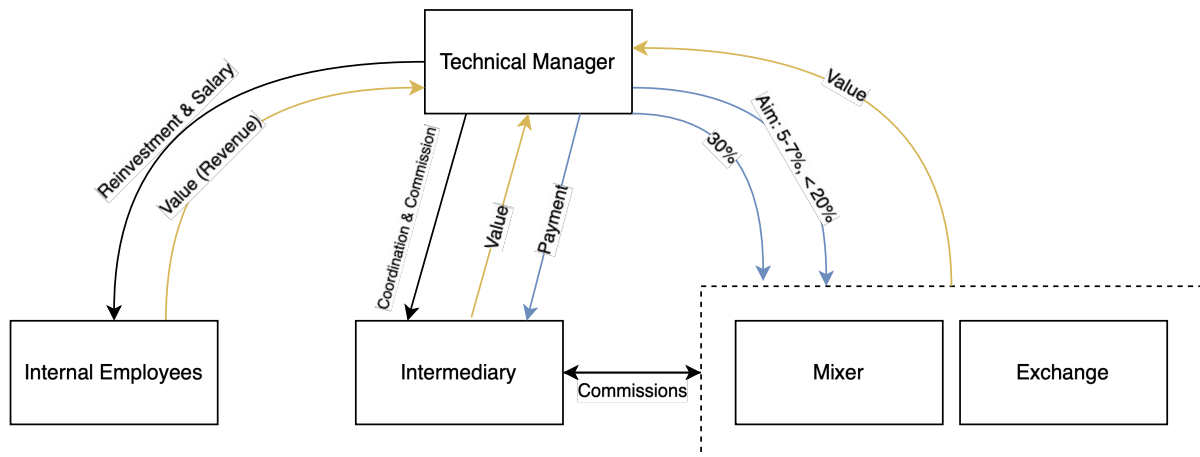


Figure 11: Formal chart of the Cash-Out phase in ransomware cybercriminal activities.

Single-sided arrows indicate a hierarchical relationship, two-sided arrows indicate other relationships. Yellow arrows indicate where value is generated for the organization, and blue arrows indicate the compensation for this value creation.

Crypto Mixers and Exchange Services process the Bitcoin of the ransomware group through multiple transactions to hide trails and convert the Bitcoin into common or fiat currency respectively. These services provide laundering and exchange functions but charge a substantial commission fee for their operations. The chat transcripts reveal that commission fees for money laundering and exchanges can be substantial. In one instance, the Technical Manager accepts a 30% commission for laundering funds. An Intermediary acknowledges that while 30% is high, it is not uncommon for laundering operations. However, as paying commissions to exchanges lowers the value that is gained through the exchange process, the pursuit of lower commission rates is a recurring theme. The Technical Manager later aims for commissions as low as 5-7%, while indicating that a 20% commission is too much. This aim for a lower commission rate highlights the importance of minimizing expenses in the Cash-Out phase, to retain as much value as possible of the gained ransom payments.

The Intermediary responsible for money laundering offers significant value by converting illegal money into usable currencies, which can be reinvested into the organization for growth or maintaining operations. No specific compensation is mentioned, apart from that there will be a payment.

Beyond converting illicit gains into cash, the cash-out phase also includes reinvesting in the organization. Cashed-out funds are reinvested in the organization through salary payments and other expenses to maintain operations. This includes illegal activities such as renting or buying

software and paying employees, as well as regular business-related activities like renting office buildings and purchasing materials.

Internal Employees provide value to the organization by generating revenue through performing ransomware attacks and ensuring victims comply with ransom demands. They receive compensation for their work, derived from the ransom payments. The incoming flows of ransom capital are reinvested in the organization by investing in software (see chapter Development), training programs (see chapter Distribution), and by paying Internal Employees their salaries or commissions. The organization depends on the Internal Employees to generate revenue, while the Internal Employees depend on the financial aspect of the ransomware organization for their cash-out and commission payments.

Crypto mixers and exchange services are essential for laundering and converting Bitcoin, but their substantial commission fees drive a continual search for lower rates to maximize value. In the cash-out phase, the reinvestment of funds into the organization for operations and salaries underscores the interdependence between internal employees who drive revenue and the financial mechanisms that support their compensation and ongoing operational costs.

4.5 Governance

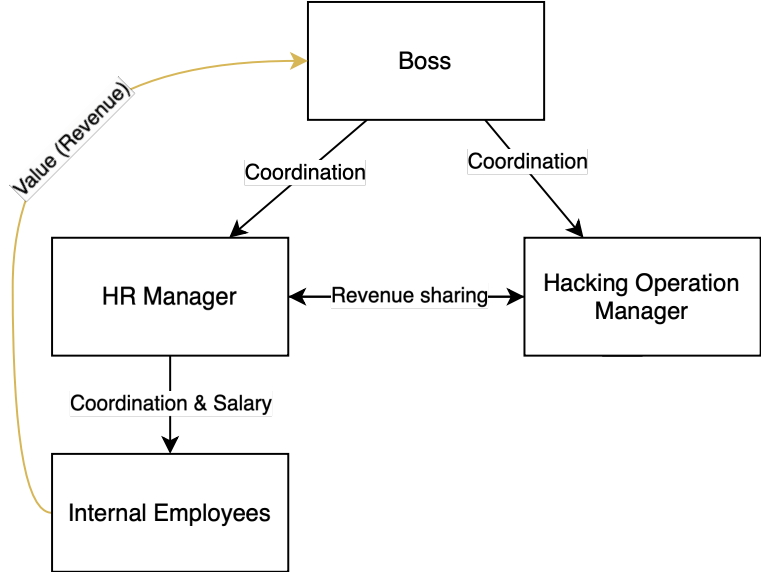


Figure 12: Formal chart of the Governance in ransomware cybercriminal activities. Single-sided arrows indicate a hierarchical relationship, two-sided arrows indicate other relationships. Yellow arrows indicate where value is generated.

Within the Governance part of the ransom activities, no real value is generated for the organization directly. Governance is responsible for keeping the organization running and coordinating the employees that generate revenue and value.

The value attributed to the actors of the Governance part of the organization is centralized around key figures who determine the allocation of ransom payments. The Boss manages overall operations and is compensated with a percentage of the ransom payments per attack. He decides how the received ransom payments are to be distributed. In different instances, the Boss decides to take 20, 30, or 40% of the ransom payments for himself. This decision is often followed by the HR manager who then divides the remaining percentage through internal transfers for further distribution, dividing the ransom payment among those entitled to a share.

## 5. Reflection of Results in Scientific Literature

In this chapter, the findings of this thesis are mapped against existing scientific literature to identify their contributions to the field of cybercrime research. This confrontation with the state-of-the-art literature aims to determine how the findings align with or extend existing theoretical frameworks, particularly those related to profit-driven cybercrime and value chain applications. The comparison will focus on seminal works, including “Framing Dependencies Introduced by Underground Commoditization” by Thomas et al. (2015) and “Cybercrime: A Value Chain Approach” by Rush & Mbula (2014). These papers were chosen for this confrontation as they are foundational in the study of value attribution and value chain approaches in cybercrime. These papers are significant as they represent the pioneering efforts in conceptualizing and framing value chains and dependencies within the cybercrime research topic. They provide a comprehensive and theoretically grounded understanding of the subject, making them ideal benchmarks for evaluating how the findings of this thesis contribute to and extend existing knowledge. Other papers, while valuable, may not offer the same level of foundational insight or may focus on different aspects of cybercrime that are less directly relevant to the value chain approach used in this research.

Following the literature confrontation, this chapter provides a review of the scientific contribution achieved by applying the value chain perspective through an empirical method, contrasting it with its traditional conceptual use as demonstrated in the cited papers. This review emphasizes the significance of transitioning from a purely theoretical framework to an evidence-based approach, wherein the value chain is not merely a conceptual model but a practical tool for data analysis and interpretation.

### **Thomas et al. (2015)**

Confrontation with this paper shows how the Conti ransomware group operationalizes the value chain by emphasizing the high value placed on technical skills in hacking and performance-based compensation, while undervaluing negotiation and payment procedures, expanding on the theoretical interdependencies outlined by Thomas et al. (2015).

Thomas et al. (2015) state that the most important interdependencies for ransomware organizations are the profit centers and the support centers. The profit centers, which are the actions that funnel money from victims into the underground economy, are in the case of ransomware cybercriminal activities defined by the victims paying their ransom to the organization. To achieve this, the ransomware group needs to attack the victim system in the Distribution phase of the Value Chain. The hackers responsible for this task are valued by the Conti ransomware group, as their work is rewarded with a fixed percentage of the successful ransom payment, ranging between 20 to 35%. Their compensation rate is, however, based on their experience and efficiency, which incentivizes hard work and successful attacks. Hacking

into systems requires a high level of technical skill. Their expertise in defeating defenses and maintaining access is critical to the success of the operation, justifying higher compensation. The ransomware group, however, is saved from incapable workers by compensating per achievement and not having to pay for any unsuccessful attacks.

The final step to getting the victims to pay their ransom demand, the negotiation and payment procedure, is slightly undervalued by the ransomware group Conti in the Take-Over phase of the Value Chain. The compensation for these workers is minimal (0,5-1%) and working long hours and sacrificing their personal lives are not compensated at all. Hacking the victim system and holding their data for ransom is valued a lot higher than the process of exerting the ransom payment, which is reflected in the compensation percentage. This may be because the negotiation process is not technically complicated, and because the underground economy values technical skills higher because it is rarer and more difficult to acquire than negotiation skills. The scarcity of skilled hackers increases their value within the organization. Finally, since after taking over the victim system, the ransom group holds great power over the stolen data and the victim's reputation, the ransom demand might after negotiation be accepted out of desperation by the victim and no extensive negotiation skills are necessary to achieve this outcome.

Support centers are the resources essential for cybercrime, including the software necessary to perform attacks and human affiliates (Thomas et al., 2015). Affiliates are mostly present for Conti in the Distribution phase of the Value Chain as spammers and hackers. The valuation for these affiliates is reflected in the Conti ransomware group by affiliates being compensated a percentage for their successful attacks, which increases based on their performance from 15 to 30%. As Thomas et al. (2015) state, this outsourcing affiliate business model has great advantages for management, as it mitigates the risk of poor-performing affiliates by paying commissions solely based on new revenue, and thus when no successful attack is done, no compensation needs to be paid. This pay-for-performance model aligns costs directly with revenue generation, enhancing the organization's overall cost efficiency and ensuring that funds are only allocated to activities that generate revenue.

This thesis expands upon Thomas et al. (2015) by providing a detailed examination of how the Conti ransomware group operationalizes the value chain concept, particularly in terms of compensation structures and performance incentives. Unlike the foundational work of Thomas et al., which outlines theoretical interdependencies, this study offers empirical insights into how these dynamics are applied in practice, revealing the differential valuation of technical skills over negotiation abilities and the strategic use of performance-based compensation to optimize cost efficiency.

### **Rush & Mbula (2014)**

The value chain stages identified by Rush & Mbula (2014) are compared with the operational practices of the Conti ransomware group, highlighting how Conti's phases of Development, Distribution, Take-Over, and Cash-Out correspond with and diverge from Rush & Mbula's theoretical framework.

Rush & Mbula (2014) identify their own cybercrime value chain, where each activity achieves financial gain. The phases of the value chain include detecting vulnerabilities, the distribution and infection phase, and the exploitation phase.

In the “detecting vulnerabilities” phase, the main roles are dedicated to malicious code writers and hackers. Here, hackers refer to the developers of malware kits. This phase requires technical skills such as programming and computer knowledge to develop the software necessary for the attack. This phase can be compared best to the Development phase of this thesis, as it involves the preparatory steps needed for a ransomware attack and does not yet have any relation to the victim. Rush & Mbula (2014) state that skilled workers for this phase are rare yet essential to the operations of a cybercriminal group. This is reflected in the Conti chats, where workers in the Development phase are found to be difficult to recruit and are rewarded with a fixed percentage for their work after proving their worth. This scarcity and regulated compensation indicate the high value placed on these workers for their successful contributions.

In the “distribution and infection” phase, the main roles are for the spammers, botnet masters, and script kiddies. These actors implement the software developed in the previous activity and therefore do not need special skills. However, in the case of this thesis, the comparable phase is the Distribution phase, for which skills are a definite must. This is reflected in Conti’s efforts to compensate their workers in this phase generously, with rates between 15 and 35% of the ransom payments. Additionally, Conti has set up a program to train their hackers themselves for more controlled and cost-efficient attacks on victims. This approach ensures a higher quality of work and greater efficiency in operations.

In the “exploitation” phase identified by Rush & Mbula (2014), the most important actors are the gangs themselves. The stolen data is turned into cash. While Rush & Mbula (2014) describe this as selling the data, in the case of Conti, this Take-Over phase involves negotiations and extortion. This activity is valued low, at 0.5-1% of the ransom payment, and is deemed a replaceable job requiring little skill. The exploitation phase of Rush & Mbula (2014) also includes the Cash-Out process described in this thesis. They explain that converting the data into cash requires a commission. In the case of Conti, the goal is to secure the lowest possible commission rate for the exchange into usable funds, typically 5-7%, but aiming to keep it below 20%. However, Rush & Mbula (2014) also confirm that this phase involves significant risk, as this is where detection and arrest are most likely. Consequently, Conti sometimes cannot avoid

commission rates of about 30%, as intermediaries are used and paid to ensure that the transaction is conducted discreetly and without danger to the ransomware group.

Rush & Mbula (2014) further emphasize the role of governance within the value chain, as it structures the power balances within the group. The governance department decides who gets to contribute to or benefit from the value chain, thereby having the power to determine the distribution of revenue (Rush & Mbula, 2014). This is reflected in the chats, where higher-tier actors decide who receives what portion of the ransom payment, allocating themselves a significant share ranging from 20% to 40%. While this is a substantial part of the payment, the upper-level bosses and managers bear full responsibility for their employees and the continuation of their cybercriminal organization.

This thesis builds on Rush & Mbula's (2014) value chain by providing empirical insights into the specific compensation structures and operational strategies used by the Conti ransomware group. While Rush & Mbula offer a theoretical model of cybercrime value chains, this study reveals practical applications, such as the higher valuation of technical skills and the nuanced approach to minimizing commission rates in cash-out processes, enriching the understanding of how cybercriminal organizations manage and optimize their value chains.

### **Value Chain Approach as an Empirical Method**

In contrast to the traditional conceptual applications of the value chain, this research utilizes empirical data, specifically chat transcripts from the Conti ransomware group, to construct and analyze a real-world value chain. This approach allows for an understanding of how value is created, allocated, and optimized within the operational framework of a ransomware organization. By mapping out the value chain in detail and examining the empirical data, this study reveals specific insights into the operational dynamics of cybercriminal enterprises, highlighting areas of high value and potential vulnerabilities.

The empirical application of the value chain perspective offers several key scientific contributions. Firstly, it provides a concrete methodology for assessing value creation and resource allocation within complex systems, grounded in actual operational data rather than theoretical assumptions. This shift from concept to practice enhances the ability to identify critical elements and weak points within the value chain, which offers the opportunity to assess where improvement of the business, or, in the case of cybercriminal research, intervention is the most efficient. Key elements for successfully applying this empirical value chain perspective include ensuring that all measured units are comparable to determine relative value accurately. This research uses percentages and agreed-upon divisions to represent parts of a larger whole, allowing for an effective assessment of the importance of each activity and distribution of resources.



Secondly, this research demonstrates the practical utility of the value chain lens in understanding and addressing real-world (cyber)crime scenarios. By applying an empirical approach, the study offers actionable insights that can inform strategies for combating ransomware and optimizing organizational operations. This methodology extends the value chain concept's applicability beyond theoretical models, providing a framework for scientific investigation. Furthermore, careful documentation of data sources and extraction methods ensures that the constructed value chain accurately reflects real-world situations, managing potential biases and enhancing reproducibility.

In conclusion, the empirical application of the value chain perspective represents an opportunity in the field of cybercrime research. It bridges the gap between theoretical frameworks and real-world data, offering valuable insights into the operations of cybercriminal organizations and enhancing the ability to make informed, data-driven decisions. This approach not only enriches the scientific understanding of value chains in cybercrime but also provides a practical tool for researchers and authorities seeking to understand crime-related complex issues.

## 6. Discussion

In this chapter, the results of this thesis are interpreted and discussed, to generalize and determine the level of value allocated to each phase of activities in the value chain. After this, recommendations for law enforcement authorities are provided, as well as an explanation of the academic relevance of this thesis. The chapter concludes with a reflection on the limitations of this thesis, as well as suggestions for future research.

### *6.1 Interpretation of the Results*

In this subchapter, the findings of this thesis are interpreted and generalized. The foundation of this value allocation interpretation, which is not solely done conceptually but based on empirical evidence, consists of chat transcript findings and the financial indicators derived from them.

This initial data interpretation is informed by hours of chat transcript read-throughs and analysis, the reading of literature related to Conti and other ransomware groups, cybersecurity reports, experience gained from cybercriminal investigations at FIOD, and discussions with cybercriminal investigation experts. The interpretation is structured according to each phase of activities along the value chain, where each phase is concluded with a list of elements that play the most important role in value creation and allocation.

#### 6.1.1 Development

In this phase of the value chain, high levels of value are allocated to those generating significant contributions for the ransomware group. During the development activities, substantial value is placed on the processes of malicious software development and the people who facilitate these activities. The malicious software forms the foundation of the ransomware attack, as, without it, all other steps would be impossible to initiate. High-quality software is essential for overcoming the security systems of potential victims and requires a high level of skill in its development.

The chats reveal that highly skilled workers are scarce and difficult to source for the ransomware group. This scarcity, which inherently creates value, makes these workers highly valued. Their compensation reflects this value, with a high percentage of the ransomware payment allocated to them and opportunities to increase this percentage through good performance. Specialization is also of high value to the ransomware group. Specialized skills are scarce, further increasing their value. As potential victims continuously improve their security measures, continuous innovation and staying on top of the latest developments are essential skills of valuable workers in this phase. Experience is another significant factor contributing to value. The chats indicate that both prior experience before joining the ransomware group and accumulated experience within the group, demonstrated by consistent

high-quality work, increase a worker's compensation and, consequently, their value to the group.

Finally, the development of malicious software in-house is crucial for the ransomware group. In-house development ensures the quality, innovation level, and efficiency of the software, thereby improving the group's chances of success. Therefore, substantial value is placed on internal software development, with no value allocated to renting software externally.

In conclusion, within the development phase of the ransomware value chain, high levels of value are tied to the skill, specialization, and experience of the workers, as well as the in-house production of malicious software. These elements are critical for the group's success, and their scarcity and effectiveness hold great value to the group.

- High-quality malicious software creates value
- Scarcity in high-level skills creates value
- Specialized skills create value
- Experience creates value
- Producing in-house instead of renting externally creates value

### 6.1.2 Distribution

During the distribution phase of the ransomware value chain, varying but mostly medium levels of value are allocated to those generating value for the ransomware group. Value is allocated primarily to those who contribute to the group's successes. Many processes in this phase are outsourced to affiliates, who only receive compensation for successful work. Consequently, no value is placed on affiliates with unsuccessful work. The workers themselves are not highly valued; they receive no employment benefits or fixed salaries from the ransomware group. Nevertheless, their successful work is valued at a percentage.

Chats reveal that there is sometimes a shortage of employees for certain tasks. This scarcity immediately increases the value of these workers, as an unfulfillment of an essential job is needed to keep the operations going. When shortages arise, their compensation is increased without hesitation. This scenario demonstrates that scarcity creates value in this context.

Where necessary, a scarcity of highly skilled workers is solved by developing an internal training program. The quality of work of these hackers is valued enough to invest in them through the internal training procedure. It decreases their salary, which increases the overall gains for the operators. This shows how the group invests in quality and saving on long-term costs, both value-generating elements for the ransomware group.

Another valuable asset within the distribution phase is the ownership of credits for a target. This is evident from people offering a percentage to take over targets from another colleague or stealing target credentials. Such actions show that the reputation among actors within the ransomware group is highly valued. Additional chats indicate that maintaining the reputation of a locker is crucial, as a high reputation increases the locker's value when rented out or used for value creation within the ransomware group.

However, in this phase of the value chain, value is fragile, and holding onto value is challenging. The value allocated to affiliates increases when shortages appear but decreases quickly when the shortage is resolved, sometimes this value even decreases for no apparent reason. Workers in this phase are seen as replaceable, as there is a large market of affiliates with various specialized skills or knowledge. This is confirmed by the finding that agreements between affiliates and higher-level operators are not strict. There is a significant power imbalance between operators and affiliates, which shows up with operators easily canceling or undoing agreements that have been made with affiliates when it suits them. This shows that workers are valued only when needed and only if they are successful.

- Success creates value
- Target ownership creates value
- Locker reputation creates value
- Shortages of people creates value
- Training internally creates value
- Saving on salary creates value

However

- Value of employees decreases quickly and suddenly
- Value of affiliates decreases through power imbalance

### 6.1.3 Take-Over

In the Take-Over phase of the value chain, low levels of value are placed on the workers who generate value for the organization. While OSINT workers receive satisfactory compensation, negotiators and blog operators are undervalued and underpaid. These workers are treated poorly: they are required to work overtime and on weekends without extra compensation, have very few days off, and experience pressure to work, leading to stress, dissatisfaction, and difficulty maintaining a work-life balance while supporting their families.

The operators make it clear that these workers do not require specialized skills, as their jobs are easily replaceable and could even be taken over by the operators if necessary. Although this might be more of a threat than a realistic scenario, it sets the expectation that these workers should work without complaining. Their compensation is performance-based, with successful extortion resulting in a percentage of the ransom and occasional bonuses. Consistently good

work can lead to increased compensation, but underperformance is immediately punished by reducing any salary increase.

The undervaluation of these workers is likely due to the relatively simple and non-specialized elements of their jobs, as well as the high level of power the ransomware group has over its victims. The group holds control over the victims' data and potential reputation damage, and although the full ransom demand is not always met, many victims pay a significant amount to save their data and avoid reputation or repair issues.

- Working overtime creates value
- Working consistently hard for a low wage creates value

However

- Value decreases when workers are replaceable
- Value decreases when little specialization is necessary to work
- Value decreases when workers underperform
- Value decreases when the ransomware group holds all the power over the victims

### 6.1.4 Cash-Out

In the final phase of activities that make up the value chain, medium to high levels of value are placed on converting illegally gained funds into usable currencies or making blockchain trails untraceable through a mixing service. In this phase, the ransomware group seeks the lowest commission as a cost-saving measure but prioritizes methods that ensure successful fund transfers. Intermediaries are sought and paid to assist in the money transformation process. Since ransomware groups are often rejected by service providers due to the illegal nature of their Bitcoin, the group compensates those who can guide them through this process well, indicating the high value placed on this assistance.

The Cash-Out phase also includes reinvestment within the organization. The ransomware group consistently spends money on improving its software, developing training programs, and hiring specialized employees. This indicates their commitment to staying relevant and maintaining high standards. As anti-ransomware efforts of potential victims innovate, the ransomware group is forced to innovate as well, developing new specialized techniques and methods for successful attacks. This phase also involves paying the workers who generate revenue for the group. Although the amount varies based on role, success, and other factors, salary payments are made consistently, highly controlled, and following agreements and standards. Those who generate revenue are highly valued and unmissable for the group's operations and success.

- Successful mixing/exchanging creates value
- Help in arranging exchange creates value

- Innovation creates value

### 6.1.5 Governance

The operators who oversee the governance activities of the ransomware value chain do not directly generate value. Instead, the organization's value, primarily expressed in revenue, is generated by the workers under the operators' management. The operators ensure that these value generators work to high standards, receive adequate training, are compensated fairly, and are managed effectively to maximize successful and efficient value creation. The operators, consisting of bosses and higher-tier managers, give themselves a significant portion of the ransomware revenue as compensation for maintaining the organization's operations. Without the governance department, value generation would not be possible, making the operators an essential part of the organization.

- Successful management creates value generation

## 6.2 Recommendations for Law Enforcement

To effectively disrupt cybercriminal enterprises, it is essential to interrupt their illegal activities, scarce resources, or capital flows by targeting the most valuable and vulnerable activities within the organization. Identifying what activities on the value chain allow ransomware groups to continue their operations contributes to developing the most successful disruption strategy.

The most effective disruption potential occurs during the Development phase. The development of software and the involvement of internally employed highly skilled workers are crucial to sustaining the operations of ransomware groups. While software can be rented, high prioritization is placed on developing high-quality, innovative, and highly effective software in-house. Disrupting either the specialized workers or the fundings that go towards software development would have long-lasting impacts on the ransomware group's activities.

Another phase with significant potential for successful disruption is the Cash-Out phase. Cash-Out is vital for the group to convert their gains into spendable money and to obscure their trails, and doing this procedure successfully is valuable to the group. Disrupting this exchange or mixing process would severely impact the group's ability to sustain their spending, such as rent, investment in physical computers, and hiring lawyers, and therefore impact the sustaining of the ransomware activities.

The Distribution phase offers medium levels of successful disruption potential. While this phase shows the value being gained by the activities of workers and the importance placed on those doing the work, it also indicates that outsourced workers can be easily replaced due to the

affiliate scheme strategy. Disrupting this phase would not impact the operations of the ransomware group.

The least potential for successful disruption is during the Take-Over phase. Little value is placed on the workers and processes of negotiation and extortion during this phase. Disrupting this phase would not impact the operations of the ransomware group over an extended period.

Disrupting the largest transactions handled by operators and those placed in the higher tiers of the operations is not the most effective way to disrupt the entire organization. Operators receive substantial payments from each successful attack and are unlikely to be financially destabilized or significantly affected by individual disruptions. The ransomware group's revenue streams are so substantial that any single disruption would not complicate their ongoing activities or the functioning of their departments. It is only through disrupting the entire Governance department as a whole that the continuation of the ransomware group could be influenced.

### *6.3 Academic Relevance*

This thesis contributes to scientific research by addressing a research gap: there is a lack of research investigating the value creation and allocation of ransomware operations and the related financial or economic structures of ransomware groups like Conti. Unlike previous research that primarily focuses on theoretical frameworks, this study expands upon state-of-the-art literature by providing empirical insights into how the value chain concept can be applied to ransomware organizations. It systematically maps and measures how value is created and allocated across each phase of the Conti ransomware group's operations, revealing practical applications of theoretical models.

The societal relevance of this research lies in its contribution to understanding and combating the threat of ransomware attacks, which have escalated into a major global challenge. By examining how ransomware groups, such as Conti, operate and allocate value, the research provides insights into their operational structures. This knowledge aids in identifying vulnerabilities and dependencies within these criminal networks, which is essential for effectively disrupting their activities. By equipping investigative authorities like the FIOD with detailed empirical data on ransomware operations, the research supports efforts to mitigate the economic and social impacts of ransomware, including significant financial losses, business disruptions, and data breaches, thus enhancing overall cybersecurity and protecting individuals and enterprises.

Furthermore, this thesis has already made contributions to cybercriminal investigations conducted by the FIOD. Through collaboration with cybercriminal experts and the sharing of preliminary chat transcript findings, this research has directly supported the development of police reports (proces verbaal) used in legal proceedings against cybercriminal activities.

This thesis aligns with the CoSEM Masters' program by addressing the complex issue of investigating strategies to disrupt ransomware groups effectively. It explores specific ransomware operations through a value chain perspective to identify optimal points for intervention by authorities. Given the complexity of disrupting ransomware activities, which involves unpredictable human behavior, business operations, and strategies, this research addresses a complex issue essential for combating cybercrime effectively. The investigated ransomware group forms a complex system of actors, relationships, interdependencies, and activities. Investigating the value creation and allocation within this complex system puts this thesis in alignment with the goals of the CoSEM program. The thesis aims to offer valuable insights guiding the Dutch authorities' future decision-making processes, as it is grounded in scientific literature and empirical data. The ability to effectively cooperate and communicate with cybercriminal investigation experts underscores the relevance of this project to the CoSEM program, further emphasizing its alignment with the program's goals and requirements.

### *6.4 Limitations*

Several factors limit this research. Firstly, the research relies solely on the Conti chat logs as a data source. Conti is the only ransomware group studied for this thesis, which may lead to a very focused and potentially one-sided perspective and consequently, conclusions. Secondly, the thesis relies solely on desk research, which necessitates adapting to the limitations of the available data. The dataset itself is constrained as the chat messages and conversations are incomplete, there is frequent use of code language and often lacks context, making interpretation of conversations difficult. This risk is mitigated by extensive familiarization with the chat logs, making the process of interpretation easier. More limitations and disadvantages related to the keyword search methods are elaborated upon in Chapter 2.2.3.1.

There are several limitations to this thesis concerning the use of blockchain analysis, which affects the reproducibility of the study. One significant challenge is the reliance on Chainalysis, a blockchain tool that labels transactions based on chat data and informant information. Chainalysis is not available for scientific use, and while it was used with proper authorization from the FIOD, its restricted accessibility complicates the replication of the results by other researchers. To mitigate this, Chainalysis was primarily employed as a visualization tool rather than the core basis of the research. Instead, publicly available blockchain analysis websites were utilized to investigate the addresses and transactions mentioned in the chats, working with the transparency of blockchain tracing. Chainalysis was used sparingly to obtain additional labeling information. However, given its lack of public accessibility, it served only as a supplementary resource. Another limitation involves the potential complexity and redundancy of data sources. Chainalysis applies labels to blockchain data using information from various sources, including the Conti chats. This double usage could lead to data duplication and potential biases, as the same source might be used for both labeling and confirming data.



To mitigate the risk of considering criminal data, only public sources of data are used for the analysis, which is based on a cybercriminal organization that is not active anymore. Finally, any ethical risk regarding Personally Identifiable Information in the data set is debunked in the research of Gray et al. (2022), as they found the chat logs contained mainly pseudonyms as usernames and very few personal details of the involved Conti members.

### *6.5 Future Research*

Future research is crucial for deepening our understanding of the financial structures and behaviors of ransomware groups.

It might be interesting to research how external factors influence the financial structures of ransomware groups, like political conflicts, job market saturation, or Bitcoin value fluctuations. As Bitcoin is a common currency for ransom payments, its value fluctuation might influence the strategies and timing of ransomware attacks. Future studies could explore whether there is a correlation between Bitcoin price changes and the financial strategy of the ransomware group. Investigating whether ransomware groups alter their operations in response to external factors could reveal strategies aimed at exploiting vulnerabilities and disrupting these ransomware groups more effectively.

Moreover, the current study focuses on a single ransomware group, which limits the generalizability of the findings. Future research should include a broader range of ransomware groups to validate the conclusions drawn. Comparative analyses of different ransomware groups could identify common and differentiating strategies, which contributes to a better understanding of the ransomware ecosystem.

Addressing these research areas will not only enhance our understanding of the financial structures of ransomware groups but also support the development of more effective countermeasures to combat cybercrime.

## 7. Conclusion

In this thesis, the leaked chat transcripts of the ransomware gang Conti were analyzed to uncover indicators of value creation by various employees and departments, and value allocation to these workers. This analysis was conducted through a value chain lens to gain insights into the ransomware group's most value-generating activities and to identify where law enforcement can most effectively disrupt their operations. The research was structured with a main research question, and 3 sub-questions, which will be answered in this chapter.

*Sub-RQ 1: To what extent, and how, can data on value attribution within the ransomware value chain be extracted from the Conti ransomware group leaks and blockchain data?*

The Conti ransomware group chat transcripts were researched using a structured keyword approach. This method was supplemented with blockchain research. This combination of methods reveals data points giving insights into value attribution within the group. Data on compensation structures shows that value is assigned based on role, experience, and performance, with developers and high-level actors receiving higher shares of profits. Internal development is preferred over outsourcing, reflecting a focus on long-term efficiency. Financial data highlights the group's strategic emphasis on minimizing costs and managing risks in money laundering operations. Overall, the data points illustrate how value is created, allocated, and managed across different roles and activities within the ransomware value chain.

*Sub-RQ 2a: To what extent is it possible to extract indicators of value creation and allocation from the Conti chat transcripts?*

The Conti chat transcript found data points provide indicators of value creation and allocation within the ransomware group. They reveal how coders and developers primarily create value during the Development phase, whose compensation is directly tied to their performance and the resulting ransom payments. The transcripts also show how value is allocated in the Distribution phase, where affiliates and internal hackers are rewarded based on their success in exploiting systems. In the Take-Over phase, the undervaluation of Blog Operators and Negotiators highlights the disparity in perceived value despite their critical role. Finally, the data on Cash-Out activities underscores the group's focus on minimizing commission fees to maximize financial efficiency.

*Sub-RQ 2b: How do value creation and allocation indicators extracted from chat transcript findings contribute to reconstructing the ransomware value chain and mapping the operational structure of the Conti ransomware group?*

Indicators from the chat transcripts contribute to reconstructing the ransomware value chain and mapping the operational structure of the Conti group. This is done by reconstructing the

formal charts of each specific phase of activities on the ransomware value chain. These charts illustrate how value is strategically created and allocated across different phases.

The compensation structures and role-specific performance discussions provide insights into how the group gives priority to internal development, incentivizes high-quality performance, and manages costs. The undervaluation of certain operational roles and the strategic search for lower commission rates show how the group's operational focus is on efficiency and profitability. These indicators collectively offer a view of the group's value generation and allocation strategies.

*Sub-RQ 3: How do the insights from mapping value allocations within the ransomware value chain challenge state-of-the-art literature, and what new perspectives or findings can be derived from this comparison to enhance intervention strategies?*

This thesis confronts existing literature by showing how the Conti ransomware group operationalizes the value chain in practice, diverging from traditional theoretical models by Thomas et al. (2015) and Rush & Mbula (2014). Unlike these conceptual frameworks, this study uses empirical data to reveal specific insights on value attribution, such as the high valuation of technical skills and performance-based compensation, and the undervaluation of negotiation processes.

The empirical approach provides a concrete methodology for analyzing value creation and allocation, offering actionable insights into ransomware operations. This shift from theory to practice helps identify critical elements and vulnerabilities in the ransomware value chain, enhancing intervention strategies by focusing on real-world data rather than theoretical assumptions. The study enriches understanding and provides practical tools for researchers and authorities to address cybercrime more effectively.

Through answering the previous sub-questions, the main research question can be answered: *How do ransomware groups allocate value within their operations, and how can this understanding support law enforcement in determining the most effective disruption strategy?*

Value is allocated based on the level of skill, specialization, scarcity, and replaceability of workers. Disruption is most effective where these elements are the most apparent.

In the Development phase of the ransomware value chain, high value is placed on the creation of high-quality malicious software, the scarcity and specialization of highly skilled workers, and their experience, as these elements are critical for the group's success. During the Distribution phase of the ransomware value chain, value is allocated to successful affiliates, ownership of targets, addressing workforce shortages, and internal training, but the allocated value is fragile and decreases quickly due to the replaceability of workers. In the Take-Over

phase of the ransomware value chain, workers such as negotiators and blog operators receive low value and compensation despite working overtime and under pressure, reflecting their replaceability and the ransomware group's dominating position over victims' data and compliance. In the final Cash-Out phase of the ransomware value chain, medium to high value is placed on successfully converting illegal Bitcoin, using mixing services, innovating to stay ahead of anti-ransomware efforts, and investing in software development, training, and specialized personnel crucial for the group's ongoing operations and success.

To effectively disrupt ransomware groups, focusing on the Development and Cash-Out phases of their value chain shows the highest potential for impact. Somehow disrupting the development of in-house software with specialized skills, and the conversion of illegal Bitcoin into usable currency would severely hinder their operational capabilities. In contrast to the Distribution and Take-Over phases, which offer lower disruption potential due to their replaceable workforce and lower value allocation. Disrupting the Governance of the ransomware group is only truly effective when it impacts the entire continuation of operations.

## 8. Bibliography

- Bhat, A. (n.d.). *Exploratory research: Definition, Types, and Methodologies* | QuestionPro. Retrieved March 17, 2024, from <https://www.questionpro.com/blog/exploratory-research/>
- Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, 2016(9), 5–9. [https://doi.org/10.1016/S1353-4858\(16\)30086-1](https://doi.org/10.1016/S1353-4858(16)30086-1)
- Chainalysis. (2024, February 7). *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*. <https://www.chainalysis.com/blog/ransomware-2024/#:~:text=Ransomware%20Payments%20Exceed%20%241%20Billion,Record%20High%20After%202022%20Decline>
- Check Point Research. (2022, March 10). *LEAKS OF CONTI RANSOMWARE GROUP PAINT PICTURE OF A SURPRISINGLY NORMAL TECH START-UP... SORT OF*. LEAKS OF CONTI RANSOMWARE GROUP PAINT PICTURE OF A SURPRISINGLY NORMAL TECH START-UP... SORT OF
- Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2020). *Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies*. <https://api.repository.cam.ac.uk/server/api/core/bitstreams/f7773556-1402-4808-a01b-e0600378b02f/content>
- Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security*, 79, 162–189. <https://doi.org/10.1016/j.cose.2018.08.008>
- Enserink, B., Bots, P., van Daalen, E., Hermans, L., Koppenjan, J., Kortmann, R., Kwakkel, J., Slinger, J., Ruijgh van der Ploeg, T., & Thissen, W. (2022). *Policy Analysis of Multi-Actor Systems*. TU Delft Open. <https://doi.org/10.5074/T.2022.004>
- Gómez Hernández, J. A., García Teodoro, P., Magán Carrión, R., & Rodríguez Gómez, R. (2023). Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges. *Electronics*, 12(21), 4494. <https://doi.org/10.3390/electronics12214494>
- Gray, I. W., Cable, J., Brown, B., Cuijuclu, V., & McCoy, D. (2022). Money Over Morals: A Business Analysis of Conti Ransomware. *2022 APWG Symposium on Electronic Crime Research (ECrime)*, 1–12. <https://doi.org/10.1109/eCrime57793.2022.10142119>
- Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. *Royal Society Open Science*, 7(3), 190023. <https://doi.org/10.1098/rsos.190023>

- Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., & Khayami, R. (2020). Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. *IEEE Transactions on Emerging Topics in Computing*, 8(2), 341–351. <https://doi.org/10.1109/TETC.2017.2756908>
- Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., & McCoy, D. (2018). Tracking Ransomware End-to-end. *2018 IEEE Symposium on Security and Privacy (SP)*, 618–631. <https://doi.org/10.1109/SP.2018.00047>
- Irwin, A. S. M., & Dawson, C. (2019). Following the cyber money trail. *Journal of Money Laundering Control*, 22(1), 110–131. <https://doi.org/10.1108/JMLC-08-2017-0041>
- Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), 541–555. <https://doi.org/10.1016/J.TECHFORE.2012.07.002>
- Laszka, A., Farhang, S., & Grossklags, J. (2017). *On the Economics of Ransomware*.
- Lusthaus, J. (2018). *Industry of Anonymity*. Harvard University Press. <https://doi.org/10.2307/j.ctv24trdtf>
- Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, 92, 101762. <https://doi.org/10.1016/J.COSE.2020.101762>
- Oosthoek, K., Cable, J., & Smaragdakis, G. (2023). A Tale of Two Markets: Investigating the Ransomware Payments Economy. *Communications of the ACM*, 66(8), 74–83. <https://doi.org/10.1145/3582489>
- Paquet-Clouston, M., & García, S. (2023). On the Dynamics behind Profit-Driven Cybercrime: From Contextual Factors to Perceived Group Structures, and the Workforce at the Periphery. *Global Crime*, 24(2), 122–144. <https://doi.org/10.1080/17440572.2023.2211521>
- Ruellan, E., Paquet-Clouston, M., & Garcia, S. (2023). *Conti Inc.: Understanding the Internal Discussions of a large Ransomware-as-a-Service Operator with Machine Learning*. <https://arxiv.org/pdf/2308.16061.pdf>
- Rush, H., & Mbula, E. K. (2014). Cybercrime: a value chain approach. *International Journal of Value Chain Management*, 7(2), 134. <https://doi.org/10.1504/IJVCM.2014.062898>
- Rush, H., Smith, C., Kraemer, E., & Tang, P. (2009). *Crime Online: Cybercrime and illegal innovation*.

- Thomas, K., Huang Yuxing, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., Mccoy, D., Savage, S., Vigna, G., & University, G. M. (2015). Framing Dependencies Introduced by Underground Commoditization. *Workshop on the Economics of Information Security*.
- Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Discerning payment patterns in Bitcoin from ransomware attacks. *Journal of Money Laundering Control*, 23(3), 545–589. <https://doi.org/10.1108/JMLC-02-2020-0012>
- van Wegberg, R. S., Klievink, A. J., & van Eeten, M. J. G. (2017). Discerning Novel Value Chains in Financial Malware. *European Journal on Criminal Policy and Research*, 23(4), 575–594. <https://doi.org/10.1007/s10610-017-9336-3>

## Appendix A

The table below shows the Conti actors that are discussed in this thesis. It is guessed that about 350 people worked for the Conti ransomware group. The table shows the suggested role/function of the actor, as well as data on their sent and received messages. This is provided to give insights into the size of the chat transcripts and how the group is formed. The table is based on the Jabber chats, and data analysis done by Check Point Research (2022).

*Table 1: Conti actors and chat log data.*

Code Username	Role	Sent	Received	Most Interactions
Stern	The Boss	11947	16634	All top layer actors
Tramp	Take-Over team leader	1629	2222	Bio/Pumba, Skippy
Mango	Technical manager	4118	3437	Stern, Target, Bentley
Professor	Hacking operations manager	2251	4314	Stern, Target
Target	HR manager	26770	9878	Stern, Bentley, Professor (and more)
Kevin	Coder	304	195	Stern
Boby	Responsible for (spam) software	196	582	Target
Dino	Developer	54	184	Mango
Tom	Affiliate, network supplier	437	131	Stern, Dollar
Logan	Unclear. Assumed: advisor	741	308	Stern
Ghost	Spammer	1169	711	Hof, Mango
Cybergangster/ Resheav	Manager of Conti locker, hacker, decrypts data for victims	1985	1880	Stern, Professor, Bio
Netwalker	Locker operator	279	247	Bentley
The Dollar	Affiliate Hacker	684	365	Mango
Demon	Unclear. Assumed: manager of locker operators	266	412	Mango, Cybergangster
Bio (later Pumba)	Blog operator and negotiator	4111	2657	Tramp, Skippy
Skippy	Negotiator	1607	2060	Tramp, Bio
Zulas	Cash-Out intermediary, backend developer	719	1581	Defender
Elvira	Cash-Out intermediary	144	121	Mango



## Appendix B

The table below lists the keywords used for the chat transcript search and the order in which the groups of keywords were searched. As detailed in the "Methods" chapter, this list is not exhaustive. Numerous keywords were employed to initially explore the chat transcripts, utilizing snowballing techniques to uncover more relevant results from initial successful searches.

Table 2: Keyword search terms for chat research. Not exhaustive.

Keywords	Hits
<b>First search attempt</b>	
"%"	666
"percent"	110
"percentage"	46 of 110 "percent"
<b>Second search attempt after familiarization</b>	
"commission"	30
"agree"	321
"split"	14
"divide"	60
"priority"	59
<b>Third search attempt after contextualization</b>	
"affiliate"	7
"exchange"	482, most of which are a repeated spam message
"negotiation"	47
"invest"	44
"wash"	31
"mixer"	19
"credit"	79
"advance"	149
"hacker"	342
"spammer"	75
"invest"	44
"rate"	654, most of which are a repeated spam message
"agreement"	33 of 321 "agree", mostly about negotiations with victims and no internal agreements
"entrance"	30, No usable results
"initial access"	0, No results
"system access"	
"distribution"	20, No usable results
"division"	12, No usable results
"gift" "gift card"	35, No usable results
"mule"	0, No results
"reinvest"	0, No results
"pay" "paid"	No new results
"dnb"	30, No relevant results

## Decrypting Ransomware Operations

"rubles"	57, Salary questions
"salary"	327, Salary questions
"salaries"	33, Salary questions
lope sn (_sn_), (_sn), (sn_)	±250, Salary questions
"kosh"	187, Salary questions
"cue ball"	231, Salary questions

## Appendix C

This Appendix includes the Conti chat transcript research results, categorized by value chain phase. It contains only the processed results used for this thesis, excluding the full list of findings irrelevant to the research question.

### C.1 Development Chat Findings

#### 25-30% to Maze locker

The group invests in different types of software. Professor (hacking operations manager) took in another locker, Maze. Maze the locker will take 25-30%. But Kevin (coder) proposes not to divide the remainders in half but divide it equally over Stern (the boss), Kevin, and Professor.

2020-07-08 17:17:20	Kevin	Stern	Hello man. Proff took another locker, as I understand it. hike maze. ran in at night says.
2020-07-08 17:17:20	Kevin	Stern	Well, I told him that you should negotiate anyway, you have experience, and it's calmer like that.
2020-07-08 17:17:20	Kevin	Stern	[08.07.2020 12:15:54]<Kevin> how did stern react to the transition to another software, is that normal? [07/08/2020 12:16:23]<proff> xs haven't talked to him yet [07/08/2020 12:16:52]<proff> he wrote on the network was kind of read / no I don't know [07/08/2020 12:17:02]<Kevin> well, it is unlikely to be happy [07/08/2020 12:17:23]<proff> xs [07/08/2020 12:37:44]<Kevin> well, probably the admin panel should be given to the stern so that he negotiates, he has experience. [07/08/2020 12:37:59]<Kevin> by the way, I wouldn't refuse the admin panel either, the process is interesting [07/08/2020 12:38:50]<proff> let's figure it out
2020-07-08 17:17:20	Kevin	Stern	something like this.
2020-07-08 17:17:20	Kevin	Stern	how much <b>maze will take 25-30%</b>
2020-07-08 17:17:20	Kevin	Stern	I propose to divide these figures in half. that is, we will not receive 12.5-15% of both.
2020-07-08 17:17:20	Kevin	Stern	Well, either equally between you, me and the prof. I just don't know what arrangements you have there.
2020-07-08 17:17:20	Kevin	Stern	Stone would rather return. that's where everything is clear and clear.

#### Not interested in locker rental

Mango (technical manager) asks Stern (the boss) whether they are interested in the rent of a locker. But they are not, as they have their own.

2020-08-06 20:23:50	Mango	Stern	maze or bug, as I understand it, lockers right?
2020-08-06 20:28:32	Stern	Mango	Yes
2020-08-06 20:28:53	Mango	Stern	Are we not interested in them?
2020-08-06 20:28:57	Stern	Mango	No
2020-08-06 20:28:59	Stern	Mango	we have our own lockers
2020-08-06 20:29:02	Mango	Stern	understood

**20%+ is too much for grids**

Stern (the boss) and Bobby (responsible for (spam) software) discuss how 20% for a grid (network) is not worth it.

*The definition of the word “grid” was unclear as its use in sentences varies. Therefore, it was translated using the original Russian chat transcripts cemku to the neutral word “network”.*

2021-02-01 16:46:58	Boby	Stern	Hi
2021-02-01 16:46:58	Boby	Stern	proplatil tipy spam sednya.. vrode ne propal, gotovitsya... nadeus srastetsya...  Translation - "paid for types of spam today.. it doesn't seem to have disappeared, it's getting ready... I hope it will grow together..."
2021-02-18 09:21:45	Stern	Boby	here?
			[***]
2021-03-24 14:07:53	Stern	Boby	for grids from others <b>more than 20 percent</b> , let's not offer
2021-03-24 14:07:55	Stern	Boby	to have enough for everyone
2021-03-24 14:08:02	Stern	Boby	them and 20 percent of the norms

**16.5% is too much for software rent**

Stern (the boss) tells Bobby (responsible for (spam) software) that renting software or a locker is no longer worth it at a rent rate of 16.5%. Bobby will receive 6.5% for the correspondence about his experience.

2021-04-16 07:52:41	Stern	Boby	Hey
2021-04-16 07:52:51	Stern	Boby	wanted to talk to you about the fact that it might not make sense to rent software anymore
2021-04-16 07:53:13	Stern	Boby	locker
2021-04-16 07:54:1	Stern	Boby	<b>for 16.5 percent.</b> in fact. and <b>6.5 to you</b> for correspondence on experience. Something is missing from them.

**10-20% for developers**

Tom needs coders and asks Stern (the boss). He will pay them 10-20% per month plus or minus an increase in deposit. Tom mentions that it is hard to find coders. The concept of a deposit is mentioned more often in the transcripts: workers receive an amount of money to make a start with their work.

2021-06-10 14:41:16	Tom	Stern	How are you ? How is work in general?
2021-06-10 14:41:16	Tom	Stern	Well, I'm still into trading
2021-06-10 14:41:16	Tom	Stern	<b>10-20% per month</b> plus or minus the increase in deposit suits me
2021-06-10 14:41:16	Tom	Stern	I am looking for coders for writing a large project .. where to get them in my heart I don't fuck

2021-06-10 15:40:48	Tom	Stern	if you tell me how
2021-06-10 15:40:49	Tom	Stern	then I'm ready

### Conti asks 30% for their locker

Mango (technical manager) is in contact with a new cryptolocker partner. Mango offers the locker but asks for (that Conti receives) 30%. He emphasizes how they should "clamp down" their partner and steal from them. Crylock indicates that 30% for Conti's locker doesn't work, he had large teams that worked for him at a lower percentage, and he still has to get something out of it. He asks for a more interesting % for a collaboration. 25% is the new offer (for 5 lockers).

2021-07-26 20:09:14	Mango	Stern	I pulled up a team of arbitrageurs, they make traffic globally from fb and google, they have their own loader, but they deal with the crypto theme in general, suggested that they try to work on grids, I say you do traffic, we track networks ourselves, if we share something, and the logs on the crypt and others that arrive - all to them. Should launch next week. Tom also seems to be starting from PND, we provided him with everything he needed. I got an offer from supposedly competitors, crylock partner - they say they broke down there, they have pentesters, targets, they only need a locker. I say ok, <b>we will give for 30%</b> , they rested, they say a lot. We need to clamp them down and try to steal adverbs and pentesters from them, I think how to do it))) &quot; akonitborec@thesecure.biz In general, I am the admin of another cryptolocker, not so popular - crylock. And now we have a hitch there and we will rewrite it &quot;It's a long time. So in order to keep my work alive, I'm looking for a new locker partner. I have several teams of pentesters, several independent pentesters and my own targets, all kinds. I only need a locker, but in fact 30% will not suit me. Because big teams worked for me for a smaller percentage, and I still have to earn something on administration. Your locker fell into my hands from intermediaries and I tested it, it's not bad, so I wrote. If you have a more interesting suggestion for%, then I'm ready to consider it. &quot;We brought the pentesters to Khorsa there, found a few more coders this week, the recruitment is slowly moving forward. I collected all the reports on the modules and bugs of the trick, while we have the main problem with importdll and superbrowser, everything else works fine, everything has been cleaned/updated. With vnc is not yet understood, but everything is in the process
2021-07-26 20:09:14	Mango	Stern	By the way, we also have a loader with an admin panel in the torus. Just like arbitrators. Only written, was not in battle, and is launched with an OV sert bypassing the smartscreen. If you suddenly need under what topics ..
2021-07-26 20:09:14	Mango	Stern	Question from a subscriber (admin panel coder): Listen, do you happen to know why the corporate section is needed in the admin panel? There it accumulates domains that pass through us and collects titles like title, description on them. Is it currently used in work?
2021-07-26 20:12:00	Stern	Mango	ask for <b>25 percent of them 5</b> you will
2021-07-26 20:25:06	Stern	Mango	test several grids directly grand@ this is a man dollar@

### 20-30% for developers





Dino (developer) asks how much he can earn. Mango (technical manager) promises to give him a deposit and transfers \$2000. Mango indicates to Dino that he can earn a percentage in the

longer term, but he must first receive 3 fixed payments. Furthermore, more can be earned for nets with “hell” than for nets without “hell”.

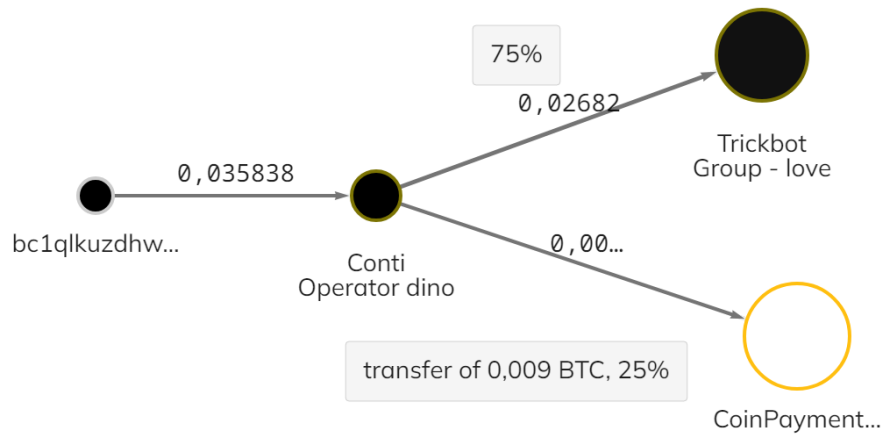
*Context: Cat = Bitcoin wallet*

2021-12-03 15:44:33	Dino	Mango	if I will do the grid you what% can I get?
2021-12-03 15:46:32	Mango	Dino	leave the cat I will send a little cabbage so that you are calm, Verona pliz maximum attention, I will pay for all the inconveniences if only he would be happy :)
2021-12-03 15:47:06	Mango	Dino	for nets, usually 25 for nets with hell and 15 for nets without hell, provided that we do everything
2021-12-03 15:47:22	Mango	Dino	date, lock, negotiations, osint, etc., etc.
2021-12-03 15:47:52	Mango	Dino	but if you are with us for a long time, of course we will <b>give you something by a percentage</b>
2021-12-03 15:48:26	Mango	Dino	<b>30 and 20 can be made</b> , but not immediately, at least there the <b>first payments 3</b> must be received
2021-12-03 15:48:57	Mango	Dino	when locking, we give an ID and access to the chat according to your user, you can watch the dialogues, whether the grid is connected or not
2021-12-03 15:49:14	Mango	Dino	but you don't need to write anything, trained people are sitting there, they know what they are doing
2021-12-03 15:49:28	Mango	Dino	I can just rent a locker if I have my own hackers
2021-12-03 15:50:10	Dino	Mango	it's not easier for me to work with you, I just if there are nets I will give
2021-12-03 15:50:39	Dino	Mango	bc1qdvmllyvaq46e53r8y6e4cyj4pq8cdf8fukj82x0
2021-12-03 15:50:50	Mango	Dino	yes, okay, write either to me or I will give a team lead from some hackers - they can directly

The wallet number bc1qdvmllyvaq46e53r8y6e4cyj4pq8cdf8fukj82x0 is researched via blockchain tool Mempool. The wallet receives a transaction on 03-12-2021 17:11 of 0,035 BTC, which amounts to approximately \$2000.

55f3a2a9cebb4e1c3973ae6a95e9046fd354bfecd72491968a21f8db4ab66338		2021-12-03 17:11	
 bc1qdvmllyvaq46e53r8y6e4cy... fukj82x0	0,03583818 BTC	3GhjKsKdzVH49v6HYQx9jUNkKWbqbudgYA	0,00900000 BTC 
		bc1qxwzu0s4xa7pmwyy4amd3p... 9xmr6phf	0,01052000 BTC 
		bc1q7w5n4z90det32cvz8zkk... mm88hyjp	0,01630000 BTC 
10,6 sat/vB - 1.818 sat US\$ 0,92		135336 bevestigingen	-0,03583818 BTC

After confirmation using blockchain tool Mempool, the transaction is researched using Chainalysis. The wallet belongs to the cluster of Dino. 20 minutes after the receiving of 0,035 BTC, Dino transfers 25% of the amount to a payment processor, and 75% to the Trickbot cluster labeled as “Love”.



**Salary indicator: Testers are needed and receive a salary of \$1200**

2020-09-15T19:51:48	Stern	Mango	I still need testers
2020-09-15T19:52:04	Stern	Mango	3-4 testers
2020-09-15T19:52:05	Stern	Mango	for salary
2020-09-15T19:52:12.	Stern	Mango	<b>\$1200</b>

**Salary indicator: students receive \$1000-1200 per month for software testing**

Mango (technical manager) shows how they are looking for students to cover an easy job: testing the software. The requirements are low, the pay is done monthly.

2020-09-21T11:29:57	Bentley	Target	<p>&lt;mango&gt;In connection with the expansion of the team, we need 2-3 testing specialists Required skills - the ability to identify and describe a problem in the software - Discipline, responsibility Responsibilities - testing internal products Conditions - working day 9:00-18:00 Moscow time, flexible schedule is possible by agreement - remote work The work is not dusty, <b>any student who is able to install Windows, virtual machine and vpn can handle it.</b> You need to test the exe assembly and describe the bugs, if any. <b>Paying \$1000-1200 per month.</b> Send toads in the PM, I will issue a test task.</p> <p>[18:29:22]&lt;bentley&gt; Fine! Is there a link? [18:29:33]&lt;mango&gt; <a href="https://xss.is/threads/42181/#post-260469">https://xss.is/threads/42181/#post-260469</a></p>
---------------------	---------	--------	---

## C.2 Distribution Chat Findings

**Logan asks 50% from its affiliates**

Logan explains to Stern (the boss) how Logan asks for 50% of the profit from its people and that due to Logan's control, the quality of work is higher. Logan remarks how Stern has its botnet open to everyone, and that Stern asks for much less turnover in return from its employees (probably affiliates). That's why Logan suggests to Stern to only work with affiliates through him, for various reasons. It would give Stern better quality for less money, and fewer responsibilities because Logan takes over some of this, with better-processed material and for a lot of money. Stern says here that he had little income because only 1 person was left to work.

2020-08-03 17:10:20	Logan	Stern	throughout this whole story, <b>I ask people for 50% of the profits</b> , someone will fuck someone up - but at least I can control the situation there. any account and no one complains about valid
2020-08-03 17:10:50	Logan	Stern	i.e. the chances of quality work are HIGHER at times. and the chances of naeb are reduced tenfold.
2020-08-03 17:11:00	Logan	Stern	but - I ran into two things
2020-08-03 17:11:39	Logan	Stern	1) that access to your botnet is not only for some people, but stupidly for everyone. 2) everyone says that I ask for a lot of money, because they pay you much less
2020-08-03 17:15:23	Logan	Stern	Well, from here the question arises - maybe it would be interesting for you to work only through me? 1) I issue a limited number of accounts if a person does not show results, he goes through the forest. 2) have their own drops - and here, too, you can earn an extra penny. 3) less chance to fuck employees 4) access only to limited content, i.e. people will not be able to look for something else there. 5) actually solving issues at the request of the client - a technical issue (I'm talking about that - that I have a connection with the right coders from my team, some of them are ready to work with pleasure) the list goes on. I don't see any downside at all.
2020-08-03 17:15:27	Logan	Stern	cons
2020-08-03 17:17:30	Logan	Stern	in a nutshell it looks like this. those who work well - they all have access to your panel and squeeze it out of poor quality - and for less money. you can do the same thing, with less load on you through my panel - with better processing of the material, and for big money
2020-08-03 17:17:47	Stern	Logan	[18:11:40]<logan> 1) that access to your botnet is not only for some people, but stupidly for everyone. 2) everyone says that I ask for a lot of money, because they pay you much less now there is no one, there was only one person left to work who always worked sandman

**20-30% for hacker**

Stern (the boss) tells Professor (hacking operations manager) here that if he were to work with Reverse (team leader/hacker/manager), he'd give him 20-30% (to Reverse) and keep the rest for himself. Stern (the boss) allows himself 20% (see sub-chapter "Governance"). Reverse earns around 150K and works for Conti internally.



2020-10-07 17:10:37	Stern	Professor	if I directly worked with reverse
2020-10-07 17:10:45	Stern	Professor	<b>I would pay him 20-30 percent</b> and take the rest for myself
2020-10-07 17:10:46	Stern	Professor	for example
2020-10-07 17:10:50	Stern	Professor	and such
2020-10-07 17:10:51	Stern	Professor	and yes
2020-10-07 17:10:53	Stern	Professor	he is your man
2020-10-07 17:10:56	Stern	Professor	I take my <b>20 percent</b>
2020-10-07 17:11:04	Professor	Stern	Well, he was with us for all the time he got somewhere around 150k

The conversation continues. Stern and the Professor discuss what to pay Reverse. Reverse thinks he deserves a percentage for the reputation of a locker. Stern agrees with this, Professor does not. Reverse gets 10% for his efforts for the locker and the reputation. Furthermore, Stern says that after Reverse gets 10%, Professor and Bobi will be paid "equally." Furthermore, no one is allowed to make money from this, including Stern himself.

2020-10-07 17:14:17	Professor	Stern	he sees so that I say he owes him <b>for life a percentage</b> of some kind of what he receives reverse I dick knows what and finally without a clue where he got it from
2020-10-07 17:14:43	Professor	Stern	a person writes that for the reputation of a locker, I have to unfasten him
2020-10-07 17:14:44	Stern	Professor	))))))
2020-10-07 17:14:48	Professor	Stern	what is there to talk about
2020-10-07 17:15:06	Stern	Professor	well, the locker is the percentage of the solution
2020-10-07 17:15:16	Stern	Professor	so if u have to pay for reputation
2020-10-07 17:15:17	Professor	Stern	yes, the author
2020-10-07 17:15:18	Stern	Professor	then deciding
2020-10-07 17:15:28	Stern	Professor	we pay him <b>10 percent</b>
2020-10-07 17:15:33	Stern	Professor	and you and bobo
2020-10-07 17:15:36	Stern	Professor	equally
2020-10-07 17:15:43	Stern	Professor	neither am I
2020-10-07 17:15:45	Stern	Professor	nobody else
2020-10-07 17:15:47	Stern	Professor	takes nothing from this
2020-10-07 17:16:49	Professor	Stern	yes, I understand, I just don't fucking understand how in someone's head a percentage for the reputation of a locker was finally born

### 20% for spammer

Professor (hacking operations manager) and Stern (the boss) discuss that a spammer should receive 20% for VPN entrance. See the next transcript for transfer information.

2020-10-09 17:25:50	Stern	Professor	and tell me whose it was
2020-10-09 17:25:56	Stern	Professor	who is the spammer

2020-10-09 17:26:00	Profesor	Stern	no one, from vpn entrance
2020-10-09 17:26:00	Stern	Professor	so that I give him his percentage
2020-10-09 17:26:00	Stern	Professor	and further
2020-10-09 17:26:02	Stern	Professor	by target
2020-10-09 17:26:18	Stern	Professor	he was also paid
2020-10-09 17:26:21	Profesor	Stern	I agreed for <b>20 for the entrance</b> , I'll transfer it to him

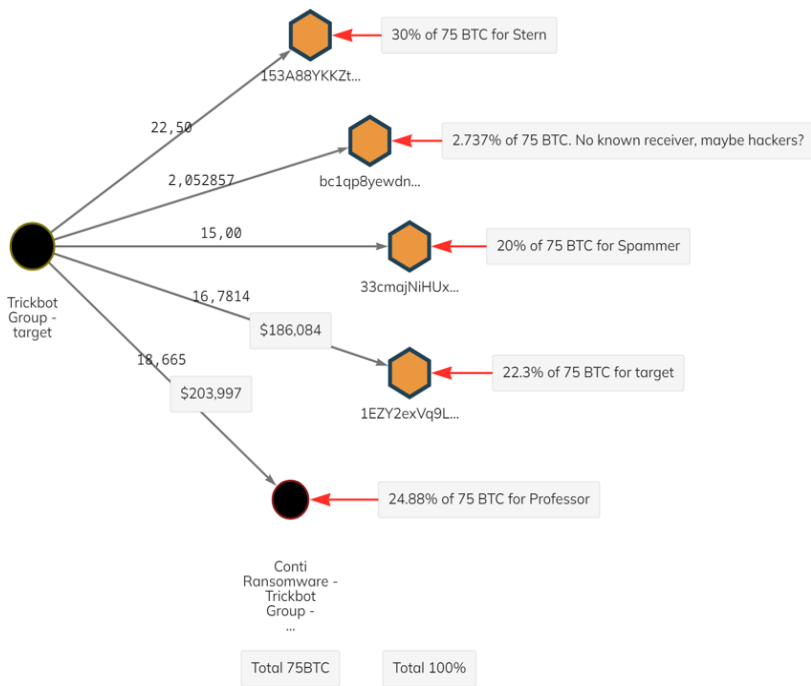
### 20% for entrance

Continuation of previous transcript. Spammer is paid 20% (15 BTC) of initial ransom payment of 75 BTC for entrance/initial access.

2020-10-09 17:31:04	Stern	Target	this is a bot of the spammer's chela, for which he was paid, he must be given money too. for the entrance I usually give <b>20 percent</b>
2020-10-09 17:31:13	Stern	Target	this is what the pro told me
2020-10-09 17:31:34	Stern	Target	33cmajNiHUxgUYY7EWS16P3BUnvFMf8MbG - here is his cat
2020-10-09 17:31:47	Target	Stern	Send 20%?

The wallet number 33cmajNiHUxgUYY7EWS16P3BUnvFMf8MbG is confirmed through blockchain tool Mempool. Here, the wallet receives 15 BTC on 09/10/2020 at 19:56. This is 20% of the initial 75BTC ransom payment.

The payment is researched through blockchain tool Chainalysis. The ransom amount of 75 BTC is divided as agreed upon in the chat, after it has been transferred fully to Target: 20% is given to the spammer (15 BTC). The other 60 BTC is divided over Stern, Target, Professor, and an unknown receiver. The payment division to Stern, Target and Professor is discussed in subsection “Governance”.



**25% for access**

25% of the success is what Mango (technical manager) promises Ghost for initial access. No transfer is found on Chainalysis indicating that this transaction took place.

2021-10-09 02:35:48	Mango	Ghost	and there it will fly from one grid to 2-3k and <b>25% of the success</b> just for the fact that you gave access
---------------------	-------	-------	--

**Spammers do not receive 20%**

Dylon indicates that his spammer is offended "because the rest received 20% of everything" but this is nonsense. There is no chat to be found between Dylon and another person where this is discussed. There is also no chat to be found where Dylon and Kaktus discuss this.

2021-10-13 16:06:59	Stern	Buza	[16:55:46]<dylon> spamer moi obidelsya tk oststyk 20% vsego... ny eto realno po syti erunda... uje 2 nedeli kajdiy den pishy ob etom kaktusu nikakih dvijeniya sovsem net  Translation: <Dylon> My spammer was offended because the rest is 20% of everything... but this is really essentially nonsense... I've been writing about this cactus every day for 2 weeks now, no movement at all
---------------------	-------	------	---

**40% instead of 70% for Netwalker****45% for targets**

One-sided contact between Netwalker and Demon. "They" (Cybergangster/Resheav – see Distribution messages 25/01/2022) gave Netwalker 40% instead of the promised 70% and offered him 45% for his targets. There is no transfer to the cluster of Netwalker somewhere around 23/01/2022 to be found on the blockchain platform Chainalysis.

The deal reflected on value chain: Conti (development) = 20%. Negotiations (take-over) = 5%. Organization (development/infrastructure) = 10%. Expenses (cash-out/reinvest) = 10%. Stern (boss/upper-level payment) = 20%. Consumables (unclear) = 10% = a total of 75%

2022-01-23 15:38:44	Netwalker	Demon	Instead of 70, they threw me 40% and they say everything is ok. and <b>offer max 45% for my targets.</b>
2022-01-23 15:38:53	Netwalker	Demon	we had a different deal.
2022-01-23 15:46:09	Netwalker	Demon	tent Admin 11:27 AM <b>20% conti 5% negotiations 10% organization 10% expenses 20% stern 10% consumables</b> , because they could earn more, but in the end they took what they gave
2022-01-23 15:46:29	Netwalker	Demon	It was he who painted so much why so little in our direction

Netwalker is upset that everyone received the same amount and not 20% extra. Furthermore, "he" spied so many targets -- possibly indicating that this person stole the credit for initial access to some target computers. This might indicate that receiving credit for targets is valuable.

2022-01-25 17:46:01	Netwalker	Demon	Father, he threw us all the same.
2022-01-25 17:46:10	Netwalker	Demon	Did not pay us <b>20% extra</b> (
2022-01-25 17:46:16	Netwalker	Demon	And he spied so many targets.
2022-01-25 17:46:32	Netwalker	Demon	Please write as you please. I look ugly in front of a spammer right now

**40% instead of 70% for Netwalker**

Cybergang / Resheav (manager of Conti locker, hacker, decrypts data for victims) explains to Demon (see earlier conversations with Netwalker) that he promised 70% but only gave 40% for throwing a Netwalker.

*Context: Threw/throw = transfer BTC*

2022-01-25 01:25:51	Demon	Cybergangster	hi come on
2022-01-25 08:20:32	Cybergangster	Demon	And there the moment happened so far xs, but apparently he threw a netwalker for money
2022-01-25 08:20:52	Cybergangster	Demon	I <b>promised him 70%</b> , but in fact I barely <b>gave 40%</b>
2022-01-26 06:33:57	Cybergangster	Demon	I'll figure it out

**20% is the new rate for internally trained hackers**

Intermediary The Dollar (hacker) introduced himself as Conti and faultily said they have a rate of 35%. But 35% is the previous rate and thus incorrect, as now Conti trains their hackers internally and offers them 20%.

2022-02-02 07:33:21	Cybergangster	Demon	Hey
2022-02-05 11:27:40	Cybergangster	Demon	work with a netwalker or not, what do you think?
2022-02-05 11:27:40	Cybergangster	Demon	netwalker asks fuck to text him
2022-02-05 11:28:16	Demon	Cybergangster	I don't think it will work)
2022-02-09 14:55:45	Cybergangster	Demon	We don't kick out the dollar in short. He again breaks the rules. He introduces himself on behalf of the conti and says we have a <b>rate of 35%</b> ahahah
2022-02-09 14:56:19	Cybergangster	Demon	Fuck us these intermediaries
2022-02-09 15:25:37	Cybergangster	Demon	About 20% of you pussy?
			[***]
2022-02-10 15:02:36	Demon	Cybergangster	Hey
2022-02-10 15:03:01	Demon	Cybergangster	dollar intermediary
2022-02-10 15:03:57	Demon	Cybergangster	no not bullshit
2022-02-10 15:04:17	Demon	Cybergangster	before when we ourselves trained our hackers
2022-02-10 15:04:37	Demon	Cybergangster	there was such a rate, now I left, and only remained in conti, <b>now the rate is 20</b>

**15% start compensation for affiliate**

Tramp (Take-Over team leader) tells Mango (technical manager) that he contacted "him" but that they did not think the same about the percentage. Affiliates working for Conti can increase their percentage commission, in this case from 15 to possibly 30% in the future.

2022-02-14 19:25:26	Mango	Tramp	hi, are you working?
2022-02-15 12:08:19	Tramp	Mango	I contacted him
2022-02-15 12:08:25	Tramp	Mango	but did not agree on the percentage
2022-02-15 12:08:33	Tramp	Mango	he wants <b>30% from each target</b>
2022-02-15 12:08:35	Tramp	Mango	I am not ready
2022-02-15 12:08:43	Tramp	Mango	<b>max 15</b> at the start I will give him

**Salary indicator: 1500 + bonuses, but after that a % can be earned.**

Rozetka (presumably a team leader) asks Mango (technical manager) how he must pay his recruits. Mango confirms a starting salary, and that a percentage can be earned in the long run.

2021-10-11 15:27:32	Rozetka	Mango	should I pay myself?
2021-10-11 15:27:41	Mango	Rozetka	if you agree with C, of course I can
2021-10-11 15:27:50	Mango	Rozetka	there part we pay part they pay
2021-10-11 15:27:55	Mango	Rozetka	depending on who brought whom
2021-10-11 15:27:57	Rozetka	Mango	what is their zp?
2021-10-11 15:27:58	Rozetka	Mango	1500 ?
2021-10-11 15:28:16	Rozetka	Mango	+ bonuses, as I understand it, I want to recruit 10 people somewhere
2021-10-11 15:28:37	Mango	Rozetka	the first time we pay 1.5k yes
2021-10-11 15:28:43	Mango	Rozetka	then they, in theory, <b>should go to%</b>
...			
2021-10-11 15:29:11	Mango	Rozetka	I will say that you need 10 people salary for us for the first time until they are at a percentage

### Salary indicator: Hackers earn salary and percentage

Stern (boss) shows Leo a conversation where he tells him how hackers earn a salary on top of their fixed percentage.

2021-06-26T15:15:21	Stern	Leo	[16:12:59]<Stern> I wanted to say that this 10k is the last one this year that I donated to your fund [16:13:02]<Stern> the rest from the profit only [16:13:35]<Stern> I'm not a topic, I don't need to earn money. I have here hundreds of K expenses every month. one crypter 8 people [16:13:47]<Stern> let's earn together with profits [16:14:32]<Stern> <b>hackers also get salary in addition to the percentage</b> ) so I can throw 1-2k and take some expenses from you, it's not on me. so these were donations to your foundation [16:15:09]<Stern> more with such a question about asking for money do not come any more please. there will always be rejection and negativity. [16:15:11]<Stern> thanks for understanding
---------------------	-------	-----	---

Bentley tells Azot how they invest in hackers by giving them more percentage over time

2020-09-30T17:59:44	Bentley	Azot	and that's why hackers grow in price over time))
2020-09-30T18:00:05	Azot	Bentley	investment in the future

### Salary indicator: Reverse engineers can raise their 150K salary by performing well.

Salamandra notices on the vacancy platform that Conti uses that reverse engineers are critical about the salaries that are offered. Buza then indicates that Stern (the boss) can raise these salaries if the reverse engineer can prove they are worth the money.

2021-04-20T11:59:23	Salamandra	Stern	denounced to the booze, he redirected to you: reversers do not agree to 2k sn. who says that it costs 5k who 7k. what will we change in the vacancy?
...			

2021-05-03T08:38:54	Salamandra	Stern	stern tells me where the results are and what can I do if they don't want to work for 150k [01:21:56]<buzza> so it's not me who raises [01:22:03]<buzza> sn stern and raises [01:22:08]<buzza> so tell him [01:22:33]<buzza> my position is this: <b>we are ready to raise the salary to what the candidate wants, if he can CONVincingly prove that he is worth the money</b> [01:22:39]<salamandra> I write to him about the salary, he will get it. and now I put the question point-blank where are the results, otherwise I'll fire you [01:22:58]<buzza> let him not fire [01:23:07]<salamandra> pissing) [01:23:21]<buzza> well, quote me to him, and give him statistics on how many resumes you had and how many of them were rejected because of salary [01:23:53]<buzza> the problem is that I have no idea how he can convincingly prove his worth [01:24:20]<buzza> if you do something difficult, he will solve it for a long time [01:24:28]<buzza> and some will refuse altogether [01:24:39]<buzza> so he must show some of his past merits [01:24:43]<buzza> like, I found such and such a CVE [01:25:23]<buzza> in general, these are the problems of the candidate - I think that if a person wants 5-7k, and he REALLY deserves them, then he has baggage behind him that he can show
---------------------	------------	-------	--

### C.3 Take-Over Chat Findings

#### 1% (5-10K) for chat take-over

OSINTs earn 1% for taking over chats. They are happy with this percentage.

2021-10-09 02:37:16	Mango	Ghost	Osints help us do a lot of things, they took over the chats and all this is <b>1%</b> . but they are also happy with the percentage) there for 5-10k they arrive from the grid
------------------------	-------	-------	--

#### 0.5% for overworking on the weekend

Bio (negotiations and blog operator) and Skippy (negotiations) discuss here that Tramp (Take-Over team leader) is "impossible", and they talk about working overtime on the weekend for which they receive 0.5%. After this, the men discuss that they would like to quit work, but that they are afraid of the consequences because Bio has a family.

2021-11-12 18:51:07	Skippy	Bio	and say that fucking boys is impossible
2021-11-12 18:51:22	Bio	Skippy	while even asking for the weekend
2021-11-12 18:51:29	Bio	Skippy	damn fuck))
2021-11-12 18:51:47	Bio	Skippy	and for <b>0.5%</b> thank God
2021-11-12 18:52:26	Bio	Skippy	so when you say write - bro is not a problem at all, but not as beautiful as you, but I can. but it's just stupid to delve even there is no time.

**0.5% for negotiator / Conti blogger operator**

Bio (negotiations and blog operator) feels undervalued and not completely part of the team, for 0,5%. Skippy (negotiations) tells him the secret that Decoy gives 3% to his team, indicating that other teams/ransomware families (unclear) are valued higher. The blogger in Decoy's team receives a fixed salary and not a percentage, indicating a steadier payment.

2021-11-12 19:07:17	Bio	Skippy	yes i don't give a fuck
2021-11-12 19:07:26	Skippy	Bio	it will lead to nothing but depression and fucked up)
2021-11-12 19:07:48	Bio	Skippy	I want them to just appreciate me and consider me a full-fledged in the team, <b>and not half 0.5))</b> )
2021-11-12 19:08:03	Skippy	Bio	05 because just greedy)
2021-11-12 19:08:06	Skippy	Bio	between us
2021-11-12 19:08:13	Skippy	Bio	decoy gives <b>3</b> to the team
2021-11-12 19:08:18	Skippy	Bio	call me a lawyer
2021-11-12 19:08:24	Skippy	Bio	and salary for the blogger
2021-11-12 19:08:43	Bio	Skippy	yeah i dont know them

**0.5% for blog operator, but bonuses promised**

Bio (negotiation, blog operator) is asking Tramp (Take-Over team leader) for a salary increase from 0.5 to 1%. This is rejected, and Tramp tells Bio he gets 1% bonuses and that he does not receive any less than his colleague Skippy (negotiations).

2021-11-30 07:44:10	Bio	Tramp	Well, great, maybe you will raise me there by 1%)
2021-11-30 07:45:33	Tramp	Bio	you already get 1% with my bonuses
2021-11-30 07:45:35	Tramp	Bio	is not it so ?
2021-11-30 07:45:41	Tramp	Bio	then all bonuses will be canceled immediately)
2021-11-30 07:45:49	Bio	Tramp	Yes! with your bonuses bro
2021-11-30 07:45:52	Bio	Tramp	thank you for this
2021-11-30 07:46:16	Bio	Tramp	Skippy needs to be warned
2021-11-30 07:46:18	Tramp	Bio	your <b>1% comes out</b> and so
2021-11-30 07:46:20	Bio	Tramp	and then he will overtake them
2021-11-30 07:46:25	Tramp	Bio	you get no less skippy don't worry

**1% bonus**

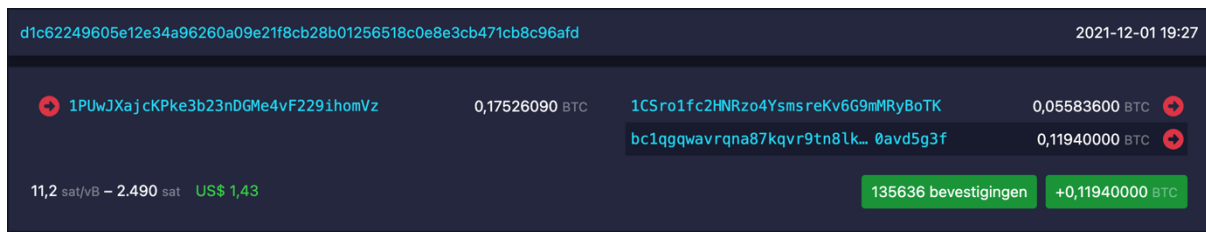
Bio (negotiations and blog operator) receives a 1% bonus, approximately \$7000, from Tramp (Take-Over team leader). Bio receives a bonus of 0,1194 BTC, or 1%. Simultaneously, there is another transaction of 0,055836 BTC to another deposit address belonging to Tramp, not indicating that anyone else received the bonus at the same time.

2021-12-01 18:16:57	Tramp	Bio	root@91.193.181.22 port: 1021 : xYnf0rTqweZ72on2021! Tramp @ 21:02 put it there 21:02 tree 21:02 throw off the hki text how we hacked them 21:05 I'm talking about the standard text 21:05 and I'll send you a purse bonus
2021-12-01 18:17:50	Bio	Tramp	accepted
2021-12-01 18:18:07	Bio	Tramp	bc1qgqwavvrqna87kqvr9tn8lk0w4uhudhp0avd5g3f

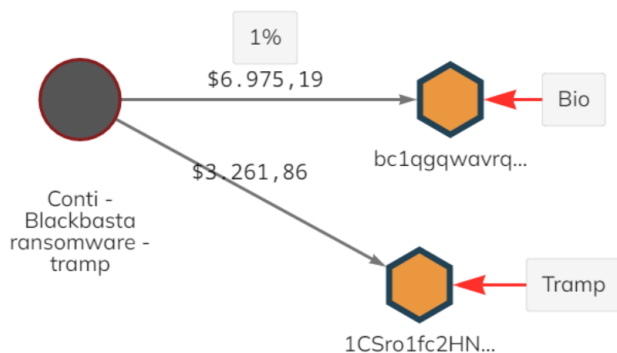
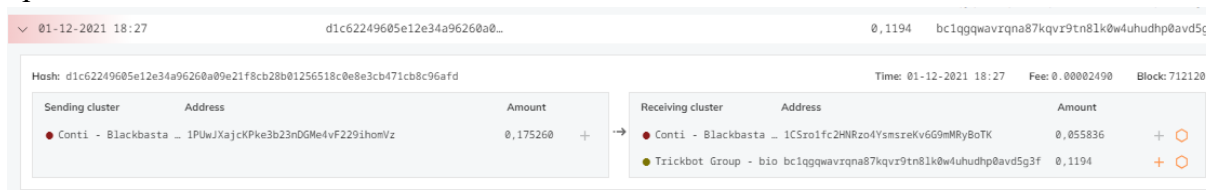


2021-12-01 18:18:10	Bio	Tramp	thanks
2021-12-01 18:20:38	Tramp	Bio	d1c62249605e12e34a96260a09e21f8cb28b01256518c0e8e3cb471cb8c96afd 0,1194
2021-12-01 18:20:47	Tramp	Bio	the same number of decisions must be sent
2021-12-01 18:20:54	Tramp	Bio	<b>will be your 1%</b>
2021-12-01 18:21:09	Bio	Tramp	Cool!!! Thanks, Trumpych

The transfer is confirmed using public blockchain tool Mempool. Bio receives 0,1194 BTC on 01-12-2021 at 19:27.



The transfer is researched using the blockchain tool Chainalysis, where it is confirmed that the cluster of bio receives 0,1194 or \$7000 from the cluster of Tramp. Tramp simultaneously transfers an amount to another address belonging to himself. No preceding transfer that makes up the 119,4 BTC which accounts for the 1% bonus is found.



**0.5% for blog operator, but bonuses promised**

Tramp (Take-Over team leader) rejects Bio’s (negotiations and blog operator) request for a salary increase but promises the prospect of bonuses.

2021-12-10 12:38:32	Tramp	Bio	it's too early to <b>raise salary to 1%</b>
2021-12-10 12:38:37	Tramp	Bio	<b>0.5%</b> but there will be bonuses
2021-12-10 12:38:44	Tramp	Bio	after ng we will reconsider
2021-12-10 12:39:09	Bio	Tramp	sorry, but as it is

2021-12-10 12:40:17	Tramp	Bio	It's not a pity, but it's right and fair!
---------------------	-------	-----	---

### 0.5% for blogger, no salary increases

Skippy and Bio (negotiations and blog operator) whine about how they are very busy, get little sleep, etc. Then Bio says that "he" told Trump/Tramp (Take-Over team leader) that Bio has been working for Conti for 1.5 months and that it is time for a salary increase to 1%. Trump would discuss that with Reshaev (manager of Conti locker, hacker). This was rejected and it remains at 0.5%, and Bio is dissatisfied with this because he works very hard.

2021-12-10 17:16:07	Bio	Skippy	by the way, today he told trump that I have been working with him for 1.5 months, isn't it time to <b>raise it to 1%</b>
2021-12-10 17:16:22	Bio	Skippy	he replied that he would talk with Reshaev
2021-12-10 17:16:27	Bio	Skippy	And what do you think they decided?
2021-12-10 17:17:03	Skippy	Bio	ahah
2021-12-10 17:17:07	Skippy	Bio	didn't fucking decide
2021-12-10 17:17:11	Skippy	Bio	05 left
2021-12-10 17:17:14	Bio	Skippy	Yes

### 0.5% for blog operator, same as "Indian"

Bio has a lot of work to do: data analysis, writing blogs for companies, managing negotiation. Bio has to do a lot of work even compared to "the Indian" for the same amount of 0,5% and thinks this is unfair. Takeover is possibly underappreciated by Tramp and of lower value, as it can be partially outsourced to "the Indian".

2021-12-10 17:20:35	Bio	Skippy	so I'm not quite happy here, of course, how the Indian is used
2021-12-10 17:23:19	Bio	Skippy	Well, I really started to freak out. I simultaneously poke around in terabytes of data, I have to make blogs for all companies at the same time, I post gigabytes of information on sites for those who have not paid, and I also have to have time to answer in all panels)))
2021-12-10 17:23:27	Bio	Skippy	<b>also for 0.5%</b>
2021-12-10 17:23:40	Bio	Skippy	they probably neighing there fucked up, they found an Indian
2021-12-10 17:28:18	Skippy	Bio	damn, we have separate people doing this
2021-12-10 17:28:41	Bio	Skippy	well, then fuck some people if there is an Indian

### From 1% to 0.5% for blogger

Pumba (former Bio, blogger) was given only 0.5% for his blogs, while promised 1% by Tramp (Take-Over team leader), and requests cybergangster / Resheav (manager of Conti locker, hacker) to be put in another team. The rate for blogs goes down from 1% to 0,5%. Tramp offers to do blogs themselves as Pumba had screwed up a couple of times.

On 27-2-2022 at 20:55:00 1F2wLzBwKBFrxDX3EGxfXmUsqDa3Mh9Y4J transferred 0.746645 BTC to Pumba, which amounts up to \$29,000. With the discussed ransom of 4,850,000 (brought down from 5 million by 150K) this is indeed approximately 0.5%.

2022-02-27 20:52:25	Pumba	Resheav	You once said that you have a lot of teams working. do they have a need for people, operator or blogs to do?
2022-02-27 20:58:10	Pumba	Resheav	broke up with trump, if you are interested, you can read the correspondence, there is not much
2022-02-27 20:58:27	Pumba	Resheav	[23:43:40]<pumba> well, not the whole amount [23:43:49]<pumba> half only [23:44:15]<pumba> trump, I thought you were an honest man [23:44:25]<tramp> - 0.746645 [23:44:30]<pumba> for what? [23:44:35]<tramp> yes, but there will be no more 1% [23:44:46]<tramp> <b>will be 0.5 for blogs</b> [23:44:55]<pumba> but not if it doesn't, then let's start with new companies [23:44:57]<tramp> trump, I thought you were an honest man - what is this? [23:44:58]<pumba> and these I led [23:45:07]<pumba> together with you [23:45:30]<tramp> no, as you entered I don't like [23:45:37]<tramp> therefore I made a decision like this [23:45:44]<tramp> do you want to discuss it? [23:46:08]<pumba> you are wrong trump. you kicked me out just before paying for these two companies [23:46:26]<pumba> and in the latter it was I who agreed on the amount of 4850 [23:46:30]<tramp> you learned how to blog normally, and keep doing it. [23:46:52]<pumba> be honest trump. pay at least the last one for this company [23:47:02]<pumba> and then we will work for 0.5 [23:47:10]<tramp> and in the latter it was I who agreed on the amount of 4850 - well, who asked you to give them such discounts? they would have taken more from them [23:47:24]<pumba> you put x3 [23:47:29]<pumba> it was 5kk [23:47:35]<pumba> I dropped 150k [23:47:41]<pumba> as we decided with you [23:47:49]<tramp> friend stop now [23:47:57]<tramp> or stop all work now [23:48:08]<tramp> I can do blogs myself [23:48:19]<tramp> you screwed up there a couple of times, so I made a decision 0.5 [23:48:24]<tramp> it's not up for discussion [23:48:46]<tramp> in general, another word and all expenses. better not go on like this [23:55:08]<tramp> a39395a368e87783498ccfd9460ecca6ed39f2d376b2af63a0b50a8b23c8a24 [23:55:18]<pumba> why? [23:55:23]<tramp> 1% [23:55:29]<tramp> consumption after that [23:55:42]<pumba> how do you plant [23:55:56]<tramp> this is where we finish the job.
2022-02-27 21:00:10	Pumba	Resheav	Well, in general, you understand the whole point. I will be grateful to you if you attach me to another team. thanks.

#### C.4 Cash-Out Chat Findings

##### 30% commission money laundering

Mango (technical manager) needs to change 12500 into dollars and to launder (“wash”) another 12500. He has not laundered or exchanged in a long while. Zulas will help Mango and prefers a payment that is not in Bitcoin. Mango seemingly does not mind an exchange or launder commission of 30%.

*Context: Cue Balls = Bitcoin*

2021-06-05 17:27:30	Mango	Zulas	but they want a commission of <b>20 30 percent</b>
2021-06-05 17:27:34	Mango	Zulas	I haven't done it in such a long time
2021-06-05 17:27:40	Zulas	Mango	then don't be a dick
2021-06-05 17:27:47	Zulas	Mango	30 dohuya)
2021-06-05 17:27:48	Mango	Zulas	let him send 12500 and I'll give cue balls)))
2021-06-05 17:27:57	Mango	Zulas	I need to wash 12500 in yus too ..
2021-06-05 17:28:33	Zulas	Mango	I don't need cue balls) you can't spread them on bread

2021-06-05 17:28:55	Mango	Zulas	we will send you a lope on the card through the money changer)
2021-06-05 17:29:15	Zulas	Mango	Well, yes ... and then what about the <b>30% commission?</b>
2021-06-05 17:30:09	Mango	Zulas	do you have a ru card? I have money changers who will throw a card on ru, but I need to pay 12.5k to the US lawyer. Can't your people help us there?

### 20% exchange commission is too much

### 5-7% exchange is more acceptable

Different exchanges to change Bitcoin into fiat cash are explored; a low commission is sought.

2021-07-01 13:44:04	Mango	Elvira	hell there commissions
2021-07-01 13:44:21	Mango	Elvira	look for some other withdrawal options <b>20% is bold</b>
2021-07-01 13:44:42	Elvira	Mango	I don't know, if you tell me where else you can easily exchange for cash?
2021-07-01 13:45:49	Mango	Elvira	I won't tell
2021-07-01 13:45:53	Mango	Elvira	why don't you put it on the map?
2021-07-01 13:46:02	Mango	Elvira	there are commissions of <b>5-7 percent</b>
2021-07-01 13:46:56	Elvira	Mango	on the card they are now monitoring the receipts from the unemployed, it seems like, so I thought cash
2021-07-01 13:47:52	Elvira	Mango	sometime next time I will try another exchanger with cash, I just used it

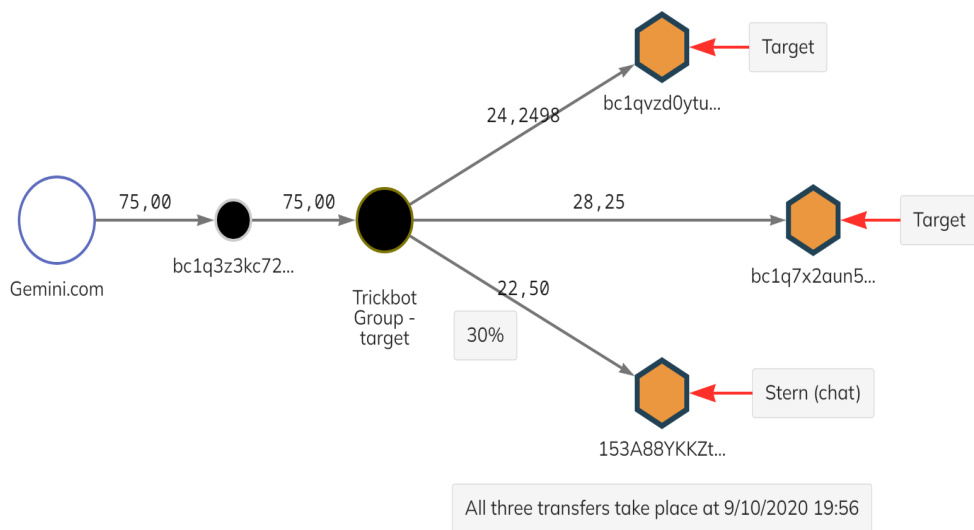
## C.5 Governance Chat Findings

### 30% to Stern

Target (HR manager) asks Stern (the boss) for instructions on how to divide the payment. Target asks Stern what % he'd like to receive.

2020-10-09 17:07:17	Target	Stern	<b>75 bts</b> paid out
2020-10-09 17:07:17	Target	Stern	prof, as always, is indignant and dissatisfied, but it works)))))) it is necessary to swing it, and well done of course
2020-10-09 17:07:17	Target	Stern	give me a basket
2020-10-09 17:07:17	Target	Stern	to whom how much to transfer
2020-10-09 17:07:17	Target	Stern	decide your not on%
2020-10-09 17:07:17	Target	Stern	decide everything
2020-10-09 17:18:42	Stern	Target	153A88YKKZtQTABAcBvvWVq1JDJLYCsgpQ 30%, this is my decision

Stern decides he wants to receive 30% of the money (=22.5 BTC). This transfer took place on 09/10/2020 at 19:56 and is confirmed with blockchain data using blockchain tool Chainalysis. The other 70% has been internally transferred by Target to Target (two separate wallets).



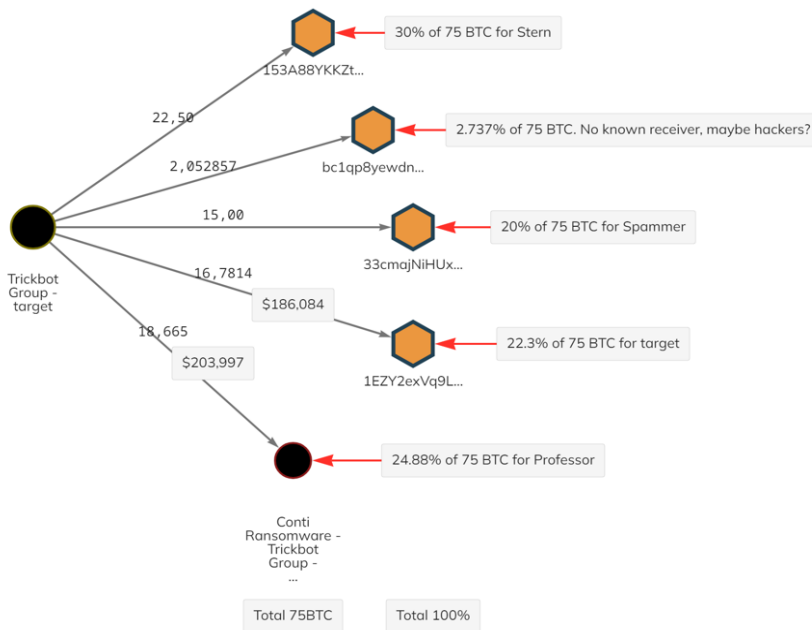
Date (UTC)	Tx Hash	153A88YKKZtQTABAcBvvWV...	Amount	Trickbot Group - target
09-10-2020 17:56	5e27c1595de84ee2dc9d0f0d...	153A88YKKZtQTABAcBvvWVq1...	22,50	

Sending cluster		Address	Amount		Receiving cluster		Address	Amount	
Trickbot Group - t...		bc1qufacuquaudvnn1zdg2y0hnnafsg0utqv5nxc6m	75,00	+	Trickbot Group Adm...		153A88YKKZtQTABAcBvvWVq1JDJLYCsgpQ	22,50	+
					Trickbot Group - t...		bc1qvzd0ytup14c64yxgmy7nuw8fx3fz7i3v2279v	24,2498	+
					Trickbot Group - t...		bc1q7x2aun5usrt4x4rtsm0vm1hxry46t93qhg0ru1	28,25	+

Continuation of previous transcript. The remaining 50% (100% minus Stern (30%) and the spammer (20%)) are for the hackers, Target, and the Professor. After this it is confirmed that of the 400K, 200K will go to Target and 200K to the Professor. These transactions are confirmed on the Blockchain: it indicates that the Professor and Target received a fixed amount in Dollars instead of a percentage. The amount transferred to the hackers (supposedly) seems random. The transfer to the hackers is around \$22,600.

2020-10-09 18:41:12	Target	Stern	the rest where
2020-10-09 18:41:32	Stern	Target	the rest <b>50 percent</b> is for hackers, yours and professional
2020-10-09 18:42:01	Target	Stern	I'm here more than you
2020-10-09 18:42:13	Target	Stern	balance 400k
2020-10-09 18:42:17	Target	Stern	<b>200k prof</b>
2020-10-09 18:42:19	Target	Stern	<b>and me 200k</b>
2020-10-09 18:42:34	Target	Stern	let's do you or pay for an office with hackers and devops from them
2020-10-09 18:42:36	Target	Stern	decide for yourself
2020-10-09 18:42:43	Stern	Target	we are all about the same



Conversation between Professor and Stern, follows from the previous transcripts. Stern lies how he took 20%, as he took 30%. Stern told “him” (= Target) to divide the rest between Target and the Professor. Professor indicates how Stern should have taken 50% if it were his software & bot, but it was a spammers’ bot (who received 20% as agreed). Indicates that ownership of bot gives right for 20%, and both software/locker & bot gives right for 50%.

2020-10-09 18:52:05	Professor	Stern	and how was it divided in the end?
2020-10-09 18:52:40	Professor	Stern	I will give a thought from mine by itself
2020-10-09 19:01:12	Stern	Professor	I do not know
2020-10-09 19:01:16	Stern	Professor	I took <b>20 percent</b> for myself
2020-10-09 19:01:18	Stern	Professor	and all
2020-10-09 19:01:23	Stern	Professor	money at the target
2020-10-09 19:01:34	Stern	Professor	I told him that the rest is yours with him
2020-10-09 19:01:43	Stern	Professor	he should give you
2020-10-09 19:01:46	Stern	Professor	shcha will probably take the cat
2020-10-09 19:04:06	Professor	Stern	damn, you confused me, did you take 20 for both the bot and the locker or what?
2020-10-09 19:05:39	Professor	Stern	logically there should be 50 of yours, soft + bot
2020-10-09 19:06:29	Stern	Professor	this is his bot
2020-10-09 19:06:31	Stern	Professor	<b>he gave him 20</b>
2020-10-09 19:06:34	Stern	Professor	10 solutions
2020-10-09 19:06:36	Stern	Professor	<b>and 20 I took</b>
2020-10-09 19:06:41	Professor	Stern	ok
2020-10-09 19:06:47	Professor	Stern	got it
2020-10-09 19:07:34	Professor	Stern	Well, he knows that it was not his bot that was the input, right?
2020-10-09 19:07:44	Stern	Professor	yes he knows

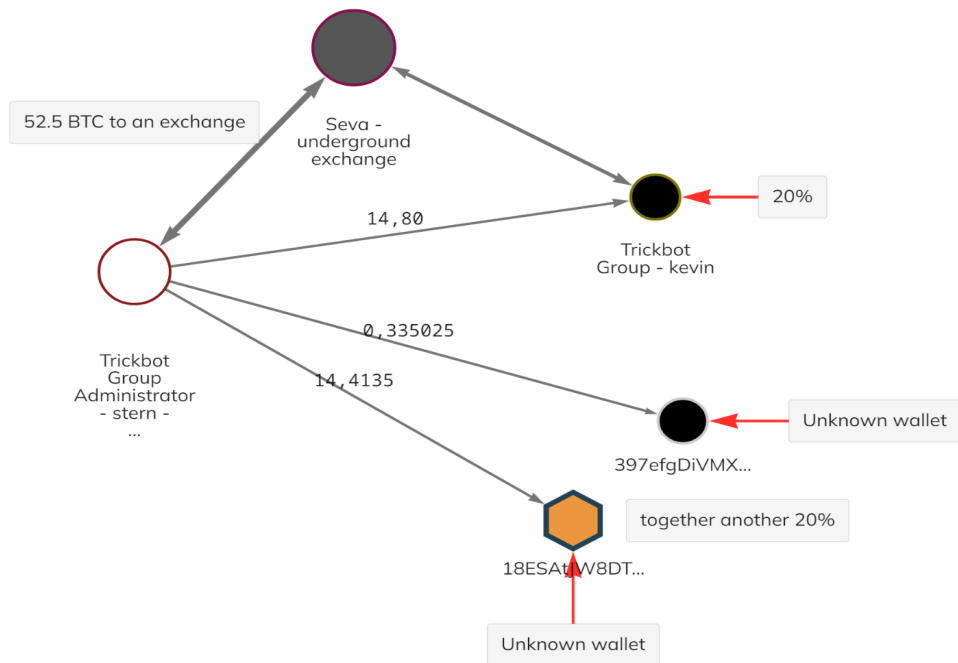
**40% to Stern**

Conti receives 74BTC of which Kevin (coder) says 40% is for Stern (the boss). Kevin asks for 20% of the payment.

2020-10-28 17:47:21	Kevin	Stern	hello old man
2020-10-28 17:47:28	Kevin	Stern	there from the floor the payment came. 74btc
2020-10-28 17:47:34	Kevin	Stern	<b>40%</b> of ours are with you.
2020-10-28 17:48:16	Kevin	Stern	<b>20%</b> - 14.8 bts. bc1qwy1aqmq041lfggxe9x7syxzm4kwrslr4yrffxa plz throw a purse on him

The initial transaction of 74BTC is not to be found on the blockchain platform Chainalysis. Stern transfers Kevin 20%, and another 20% (divided in 2 parts) to other addresses. At the same time, Stern transfers 52.5 BTC (fae0c65d8bdfa59f14201fb879a82ee1b24e4cc29b9341c691c05213cbf521cd) to an exchange. This is approximately 70% of 74 BTC. It is unclear how these transactions are interrelated, as this adds up to 110%. It is suspected that Stern exchanges his part of the deal (40%) immediately, pays Kevin 20%, and pays the other 20% to another person.

Sending cluster		Address	Amount	Receiving cluster	Address	Amount
Trickbot Group Admini...	1BGBMoW4asV24yGpqrLZkzhck9M8khYnFq		29,2144	18ESATJW8DT95cJUKF5ys...	18ESATJW8DT95cJUKF5ysw5sFKUCp5QNJP	14,4135
				Trickbot Group - kevin	bc1qwy1aqmq041lfggxe9x7syxzm4kwrslr4yrffxa	14,80



## Appendix D

The table below presents the initial division of Conti ransomware payments, as reported to Ransomware.live. This data, downloaded from the Ransomware.live API, was pre-processed by a FIOD expert to specifically reflect the initial divisions within the Conti ransomware group. This data is used to validate the divisions found in chat transcripts and to confirm the actual occurrence of these initial division percentages.

Table 3: Conti output division data based on Ransomware.live data.

Conti Output Division	Hits (total: 122)
['Output 0: 10.0', 'Output 1: 90.0']	26
['Output 0: 35.0', 'Output 1: 65.0']	24
['Output 0: 20.0', 'Output 1: 80.0']	13
['Output 0: 25.0', 'Output 1: 75.0']	10
['Output 0: 30.0', 'Output 1: 70.0']	7
['Output 0: 75.0', 'Output 1: 25.0']	5
['Output 0: 5.0', 'Output 1: 95.0']	4
['Output 0: 40.0', 'Output 1: 60.0']	4
['Output 0: 15.0', 'Output 1: 85.0']	4
['Output 0: 22.0', 'Output 1: 78.0']	3
['Output 0: 20.0', 'Output 1: 40.0', 'Output 2: 40.0']	3
['Output 0: 48.0', 'Output 1: 52.0']	2
['Output 0: 11.0', 'Output 1: 89.0']	2
['Output 0: 50.0', 'Output 1: 50.0']	2
['Output 0: 32.0', 'Output 1: 68.0']	2
['Output 0: 100.0']	2
['Output 0: 46.0', 'Output 1: 54.0']	1
['Output 0: 1.0', 'Output 1: 99.0']	1
['Output 0: 80.0', 'Output 1: 20.0']	1
['Output 0: 41.0', 'Output 1: 59.0']	1
['Output 0: 30.0', 'Output 1: 32.0', 'Output 2: 38.0']	1
['Output 0: 43.0', 'Output 1: 57.0']	1
['Output 0: 37.0', 'Output 1: 63.0']	1
['Output 0: 2.0', 'Output 1: 98.0']	1
['Output 0: 14.0', 'Output 1: 86.0']	1



## Appendix E

The table below outlines the methods and tools used for cross-referencing blockchain data referenced in the chat transcript findings.

Table 4: Blockchain analysis cross-referencing overview.

Address researched	Tools & Use	Result
bc1qdvmllyvaq46e53r8y6e4cyj4ppq8cdf8fukj82x0	Mempool for confirmation and Chainalysis for proceeding division	Recipient receives a fixed amount, as discussed in chat. Transfers it in 75/25 division to payment processor & different actor.
33cmajNiHUxgUY7EWS16P3BUvFMf8MbG	Mempool for confirmation, Chainalysis for preceding division, and search for preceding payment	Recipient receives the agreed upon 20% of 75BTC.
d1c62249605e12e34a96260a09e21f8cb28b01256518c0e8e3cb471cb8c96afd	Mempool for confirmation, Chainalysis for preceding division	Recipient receives the agreed upon 1% bonus.
153A88YKKZtQTABAcBvvWVq1JDJLYCsgpQ	Chainalysis for preceding division and confirmation	Recipient receives the agreed upon 30%, the other 70% division is mapped.
bc1qwylaqmQ04llfggxe9x7syxzm4kwrsr4yrffxa	Chainalysis for search for preceding payment and preceding division.	Recipient receives the agreed upon 20%, and the division is mapped.
fae0c65d8bdfa59f14201fb879a82ee1b24e4cc29b9341c691c05213cbf521cd	Chainalysis for finding this transfer to supplement data	
	Chainalysis for search through cluster transfer data, to confirm payments and agreements in the chats mentioned without address or hash	