Money Over Morals: A Business Analysis of Conti Ransomware

Ian W. Gray, *New York University*
Jack Cable, *Independent Researcher*
Benjamin Brown, *University of Michigan*
Vlad Cuiujuclu, *Flashpoint*
Damon McCoy, *New York University*

***Abstract*—Ransomware operations have evolved from relatively unsophisticated threat actors into highly coordinated cybercrime syndicates that regularly extort millions of dollars in a single attack. Despite dominating headlines and crippling businesses across the globe, there is relatively little in-depth research into the modern structure and economics of ransomware operations.**

In this paper, we leverage leaked chat messages to provide an in-depth empirical analysis of Conti, one of the largest ransomware groups. By analyzing these chat messages, we construct a picture of Conti's operations as a highly-profitable business, from profit structures to employee recruitment and roles. We present novel methodologies to trace ransom payments, identifying over $80 million in likely ransom payments to Conti and its predecessor – over five times as much as in previous public datasets. As part of our work, we will publish a dataset of 666 labeled Bitcoin addresses related to Conti and an additional 75 Bitcoin addresses of likely ransom payments. Future work can leverage this case study to more effectively trace – and ultimately counteract – ransomware activity.

***Index Terms*—Ransomware, Conti, cybercrime**

I. Introduction

Ransomware is a type of malware that encrypts the files on a victim's computer, and charges an extortion fee for the decryption key. Ransomware attacks have significantly increased over the past years with the addition of more adversarial groups, new extortion tactics, and more targeted attacks. In 2021, ransomware payments exceeded $600 million USD, according to cryptocurrency analysis firm Chainalysis [1].

This has resulted in the emergence of large-scale Ransomware as a Service (RaaS) operations that have streamlined segments of their campaigns by dividing the work across different roles and responsibilities. This often encompasses affiliate models, where a core team responsible for developing malware leases it to others to deploy and infect potential victims. However, there has been little academically peer-reviewed analysis of modern ransomware operations. This lack of insight into backend information on RaaS campaigns has left the security industry inferring for years, on an anecdotal basis, how these threats operate.

In this paper, we perform an analysis of leaked chat messages and cryptocurrency addresses associated with Conti. Based on a report from Chainalysis, Conti is one of the most prolific ransomware groups and has attacked thousands of organizations [1]. Conti's victims include critical infrastructure entities such as hospitals and food providers [1]. Despite setbacks to the Conti ransomware collective, including self-proclaimed shutdowns and re-branding, they continually ranked in the top three ransomware groups for number of victims and volume of ransoms in 2020 and 2021 [2].

The chat data was leaked by a Ukrainian security researcher in February 2022 in response to the Russian invasion of Ukraine [3]. The leak included over 168,000 messages from Conti's internal chat logs. The chat logs contain information pertaining to the inner workings of the group, such as discussions of malware development and victim negotiations. These chats contain a wealth of data to aid in the understanding of Conti's inner operations, including associates' Bitcoin wallet addresses, employee recruitment processes, and delineation of roles and responsibilities.

Our analysis drives insights that can be leveraged by law enforcement and policymakers to aid in counteracting ransomware. For instance, just two exchanges – one unidentified exchange and Gemini – are responsible for over 90% of identified payments to Conti. Likewise, Conti exhibits poor operational security, with its associates sending a large amount of salary payments to exchanges like Gemini and Binance that enforce Know Your Customer (KYC) regulations. These centralized points provide opportunities to trace ransomware actors and seize funds.

In this paper, we make the following contributions:

Economic on-chain measurement. We manually annotate all 666 Bitcoin addresses present in the leak according to their function (e.g. salary or reimbursement) which we will publicly publish. After annotating, we then use on-chain transaction data to provide an analysis of Conti's bottom line, including estimated gross revenue, operating cost, salary per role, cash-out techniques, and relation to other cybercrime activity (like dark web marketplaces). As part of this analysis, we develop a methodology to identify ransom payments based on common proceed splitting behavior, which we use to identify $83.9 million in new likely payments.

Qualitative business structure analysis. The chat logs also contain qualitative information on different roles and responsibilities of Conti. Along with the Bitcoin address annotations, we identified the roles and responsibilities within the collective. We assessed team composition from the chats, as well as the primary users based upon interactions within the chat logs. We also provide an analysis of their employee recruitment process and challenges managers faced with employees that did not know the illicit nature of their employer.

II. Background

In this section, we describe the functional roles of the archetypal Ransomware as a Service operation. These roles are segmented into specialized tasks that fulfill different parts of the ransomware attack chain [4]. We explore how these roles execute the respective parts of the ransomware campaign, from malware delivery to cashing out [5], [6].

Ransomware operations require individuals to build, test, maintain, and deliver the malware, as well as maintain victim communications during the ransom. Once a victim pays a ransom in cryptocurrency, the attacker launders the funds through a variety of exchanges and third party services.

Since the introduction of the first public ransomware leak site in 2019, approximately 80 ransomware groups have created public leak sites, where they threaten to post victim data if victims fail to meets the terms of the extortion [7]. There are ransomware groups that do not maintain leak sites, and thus this number is not exhaustive. There is also overlap in these operations, including code re-use, and re-branding that typically occurs after a significant ransomware incident [8], [9].

At a macro-level, RaaS operations are generally divided between **Ransomware Operators** and **Ransomware Affiliates**. The operators are typically salaried workers that recruit new members, develop the malware, advertise and sell access to their ransomware, and maintain the victim payment portal and leak site post-compromise. Affiliates are typically commissioned workers that license the malware for a fee or a percentage of the ransom payment. Their role is to target and compromise new victims, deliver and execute the ransomware, and handle victim negotiations. Affiliates have also been associated with lateral movement, persistence, and data exfiltration in a victim's network [9], [10].

Management: RaaS operations can encompass hundreds of specialized workers. They have been likened to a gig economy for their on-demand services provided by their affiliate structure. Additionally, many phases of the attack chain are facilitated by human decision-making [9], [10]. The managers are responsible for the human effort, which includes human resources, hiring, finances, and payroll. Managers may also have cross-departmental responsibilities, and support the other lines of effort listed below.

Development and Infrastructure: Illicit economies are dependent upon administrative work and maintenance to ensure uninterrupted operations through development and infrastructure [11]. System administrators and software developers are salaried workers, essential to ensure uninterrupted RaaS operations. This may include acquiring or developing software, virtual machines, servers, proxies, antivirus (to test malware against), and a variety of other tools. These roles also offer IT support functions.

Access Operations: Access brokers may sell access to affiliates, who use the access to escalate privileges and move laterally within a victims network. Initial access brokers monetize access to victim's networks. RaaS collectives may have their own access brokers, or they may outsource to third parties for access-as-a-service. Initial access brokers employ a variety of tactics, techniques, and procedures to gain access to victims networks, including spear-phishing key members of an organization, compromised credentials or remote desktop protocols (RDP), and exploiting vulnerabilities [12]–[14]. Access operations may employ a variety of tools to deploy malware, including Emotet, IcedID, Trickbot, and BazarLoader.

Negotiations: Affiliates are typically responsible for managing negotiations post-compromise through an admin panel included with the ransomware. Large corporations may employ the use of ransomware negotiators, which deal directly with the ransomware affiliates to transfer cryptocurrencies through exchanges. RaaS operators manage the public leak site, where details of the victim are included if they fail to pay within a given time period. The operators also control the processing of ransomware payments.

III. Data

Our analysis in this study uses both leaked data, public blockchain data, and an annotated set of Bitcoin addresses from Crystal Blockchain, a commercial blockchain analysis platform [15]. Table I provides a brief description of these data sources. When using leaked data, there can arise both ethical and validity concerns. In this section, we provide an overview of the datasets, discuss how we validated the data, and talk about the ethical framework of our study.

A. Description

On February 27, 2022, the Twitter account @ContiLeaks began tweeting links to an anonymous file sharing service that contained information related to the Conti Ransomware collective. In addition to malware source code and other internal files, the account shared three files of chat logs: two files containing messages from Conti's Jabber server and one file containing messages from Conti's Rocket.Chat server.

The dataset that we used for our analysis only contained text (i.e., no images). The leaked chats cover the period from July 2020 to February 2022. The portion of the dataset we analyzed did not contain any Personally Identifiable Information (PII). We created a set of regular expressions to extract Bitcoin addresses and confirmed that they were valid addresses. Table II provides a summary of the the datasets that we analyzed.

B. Validation

The leaked datasets have been extensively validated by the security community, including the fact that gaps in the chat logs correlate with times when Conti was disrupted by law enforcement [16]. In our analysis, Bitcoin addresses included in the leak are consistent with previously-known Conti Bitcoin addresses, such as those in the Ransomwhere dataset [17], with addresses in the leak having received funds from both Conti payment addresses and Ryuk (another ransomware strain operated by the same threat group [18]). Furthermore, we do not observe any internal inconsistencies in the dataset.

Source	Information	Explanation
Leaked Chats	timestamps, message, participants	Leaked Chat logs from Conti Jabber server
Bitcoin Transactions	addresses, amount, timestamp	Public Bitcoin Blockchain Data
Crystal Blockchain	annotated Bitcoin addresses	Platform to investigate Bitcoin addresses

Table I: Summary of Datasets

Source	Time Period	Posts	Users	Addresses
Jabber	2020-06-21 - 2022-02-25	168,624	463	665
Rocket.Chat	2020-08-31 - 2022-02-26	88,110	248	1

Table II: Summary of Leaked Conti Chat Logs

C. Ethics

We reason about potentially harms of our study through the lens of the Menlo report [19]. We have two primary ethical questions. The first is a high-level question concerning whether the data being leaked should *prima facie* prohibit all subsequent uses of it. For example, should a researcher be prohibited from analyzing the Facebook leaks in understanding their policies? We believe that the potential benefits of our study to society outweigh the minimal increased risks of harm.

We observe that this data is already broadly available and the knowledge of its existence, its association with the Conti organization, and information, such as online handles and amount of Bitcoin transactions, have been publicly documented. Also, there is likely little if any Personally Identifiable Information (PII) in this leak and we did not find any during our analysis. This was a criminal service and the usernames are pseudonyms that are intentionally difficult to link to the actual persons. Thus, there is a minimal risk of us creating any new harm from our analysis.

To further manage any remaining harms we institute several safeguards. We did not attempt to deanonymize anyone in these leaks as part of our study. Also, we do not use the publicly-known real names of any Conti employees or affiliates.

IV. Methodology

A. Database Annotation

Jabber, the Extensible Messaging and Presence Protocol (XMPP), is a popular messaging application in the cybercrime underground. The open source instant messenger supports strong encryption, and independent federated servers that are located around the world [20]. Well-established cybercrime forums, like Exploit, run their own Jabber servers. The Conti collective also operated their own Jabber server: q3mcco35auwcstmt[.]onion.

Similar to other online messengers, the Conti Leaks often included short text that by itself was absent of any substantive content. The large number of users (n = 463) within the chats are often overlapping, and span different parts of the operation. Additionally, Russian cybercriminals often use specialized slang, dubbed Феня (Fenya), that is purposefully difficult for a layperson to understand as it provides shorthand, obfuscation, and signals group membership [21]. To better prepare the leaked messages for scientific analysis, we included a mixed method analysis that included quantitative and qualitative data analysis.

Our primary objective in analyzing the data is to conduct an economic on-chain analysis of the cryptocurrency addresses observed in the dataset. We conducted a regular expression search within the chat messages to identify all mentions of Bitcoin addresses. In total, we identified 665 Bitcoin addresses in the Jabber dataset and 1 Bitcoin address in the Rocket.Chat dataset. As a result, we primarily focused on the Jabber dataset for this analysis.

In order to provide context when annotating addresses, we included 10 messages in a conversation before and 10 messages after each mention of a Bitcoin address. Using this approach, we were able to augment machine-translated text with manual translations for Russian slang, label the context of the Bitcoin address to inform the follow-on economic and business analysis, and ascribe roles to the Conti ransomware operators through the context of the chat messages.

To better understand the context of the messages, including the Russian cybercrime slang, one of our annotators is a native Russian speaker and expert in the criminal underground. Three of the authors annotated the addresses, with one author annotating each address. We maintained a Russian slang dictionary that annotators could reference throughout our analysis.

When reviewing the Bitcoin addresses, we annotated the addresses according to the following labels:

Salary: The address is associated with a request for salary or payment. Associates in the chat will often request from a manager that a salary be transferred to a wallet.

Reimbursement: The address is associated with a request for reimbursement for a variety of services. Associates may directly or indirectly request through a manager that funds be transferred to a wallet for reimbursement of various tools.

Ransom Payment Address: The address is used to receive payment from a Conti ransomware victim.

Claimed Ownership: A member of the Conti collective claimed to own the address.

Services: Any services that we can identify being directly mentioned by the Conti collective.

Victim Name: The name of the victim who made the payment.

Inter-Annotator agreement: To ensure that our annotations were consistent across researchers, we randomly sampled 100 posts containing cryptocurrency addresses and conducted a blind annotation with 3 raters. We then measured Inter-Annotator Agreement (IAA) by computing Fleiss' Kappa

for all 3 raters, which yielded a score of 0.73, indicating substantial agreement [22].

B. Economic On-Chain Measurement

We obtained Bitcoin addresses from the Conti leaks as well as the Ransomwhere dataset [17]. Ransomwhere is a public, crowdsourced dataset of ransomware payment addresses, which we use to understand the blockchain techniques of Conti. We then performed on-chain blockchain analysis, detailed here, on these addresses.

To enrich our data, we fetched incoming and outgoing transaction data for all addresses from the blockchain.com API [23]. We then calculated dollar values for transactions by multiplying the amount of Bitcoin transacted by the closing Bitcoin to USD exchange rate the date the transaction was made from the CoinDesk API [24]. While we cannot know the exact amount the ransomware actors sold the Bitcoin for, this serves as an approximation and is consistent with previous work [6], [25].

Additionally, to understand the types of wallets the addresses have interacted with, we utilized Crystal Blockchain [15]. Crystal Blockchain is a blockchain analytics tool that offers insight into the ownership of Bitcoin addresses based on a variety of public sources [26]. We fetched the source and destination entities for all addresses in the dataset.

In order to gain insight into the proceeds of Conti, we performed analysis to identify potential ransom payment addresses. Based on confirmed Conti ransom payment addresses from Ransomwhere and those labeled in our dataset, we found 17 of 32 addresses to exhibit payment splitting, where the proceeds are immediately split to two wallets according to an exact percentage. This is likely due to the affiliate structure of Conti, where affiliates and the Conti core developers split proceeds. We found that for the 17 split addresses, split percentages ranged from 5% to 40%, with the most common (9 addresses) being 20%. An example of a split payment is shown in Figure 1. Note that when we refer to split percentages, the percentage is the portion of the payment that the Conti collective keeps, with the remaining portion going to the affiliate.

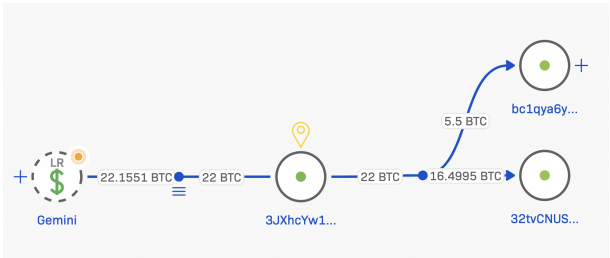

Figure 1: An example of splitting. This address received 22 Bitcoin from the US-based Gemini exchange, and split into 25% and 75%. 1 Bitcoin from this address would eventually be sent to an address in the leak. Other funds were transferred to other illicit entities, such as the sanctioned exchange Garantex.

In addition to low-risk exchanges such as Gemini, a large portion of these ransom payments to Conti originate from an unlabeled cluster of Bitcoin addresses. It is possible that this cluster belongs to an Over The Counter (OTC) desk, which many exchanges operate as a way for customers to exchange cryptocurrency outside of private markets. Given the significant portion of known Conti ransom payments originating from this cluster, it is possible that it is used by a common ransomware negotiator or incident response firm working with multiple victims. We consider this cluster in further analysis as a potential origin of Conti payments. Future work may attempt to identify the owner of this cluster.

We also analyzed 41 ransom payment addresses belonging to Ryuk from the Ransomwhere dataset. Ryuk is widely believed to be the predecessor to Conti, and both Conti and Ryuk have been attributed by Crowdstrike to be operated by the Wizard Spider group [27]. Of these 41 addresses, 17 exhibited splitting. Split percents ranged from 10% to 50%, with the most common (6 addresses) being 35%.

To discover other likely ransom payment addresses, we considered addresses that: (1) sent money (directly or indirectly) to an address in the leaked dataset, (2) exhibited splitting according to an exact percent that was a multiple of 5 (e.g. 20%, 25%) and (3) had received more than 99% of its funds from a low risk exchange (e.g. Gemini) or the identified unlabeled cluster. Results of this analysis are detailed in Section V.

While we are able to designate these addresses as likely ransom payment addresses, the distinction between whether they are Conti or Ryuk is less clear. Through the course of the analysis, we observed previously known Ryuk addresses being used to fund addresses in the leaked Conti dataset, further suggesting that Conti and Ryuk are operated by the same actor. As Wizard Spider (an organized cybercrime group that has been attributed to Conti, Ryuk, TrickBot, and BazarLoader) paused operating Ryuk in March 2020, which coincided with the emergence of Conti, we label a likely ransom payment address as Ryuk if the address was first used before March 2020, and Conti otherwise [18].

C. Qualitative Business Analysis

We extracted the unique aliases (463) from the Conti Leaks, and created a separate annotation document. We then read through the full dataset of the Conti Leaks (168,624 messages) and attempted to categorize the user roles based upon the content of their conversations. We found that a small number of individuals comprise a large number of the chats, so we sorted the aliases by degree centrality to understand who sent and received the most messages. We then decided to focus on the top 50 aliases, as most were also observed in our prior annotation of the cryptocurrency addresses. We maintained a full list of users, however we chose to focus annotations on the top 50.

We made the following categories to understand their roles within the organizations: **Role**, **Direct Report**, **Working Relationships**, **Alternative Aliases**, and **Tasks**. While certain

Source	Amount	Addresses
Ransom payments in leaked dataset	$3.4M	5
Ransom payments (Ransomwhere)	$17.1M	28
Likely ransom payments (Conti)	$57.4M	41
Likely ransom payments (Ryuk)	$26.5M	34
Total income	**$104.4M**	**107**
Salary	$21.9M	419
Reimbursement/Salary	$5.4M	15
Reimbursement	$3.8M	227
Total expenses	**$31.2M**	**661**

Table III: Conti income and expenses based on annotated Bitcoin addresses, Ransomwhere data, and inferred payments.

information regarding their respective roles could be gleaned from the chats, we had to otherwise infer based upon the context of the discussions, or their working relationships.

V. Economic Analysis

As with any business, Conti has income and expenses. The bigger the profit margin, the more its operators can walk away with. To begin our economic analysis, we utilize the labeled addresses to understand which addresses represent a business expense for Conti and which represent income. We consider reimbursements and salary to be expenses, while ransom payments are income.

Table III shows the total income and expenses for Conti. Of the addresses in the leaked dataset, salaries represent the most in number (419) and the highest dollar value at $21.9 million. Addresses that are used for both salary and reimbursements are relatively low in number but represent $5.4 million in payments. Reimbursements, while lower in dollar value at $3.8 million, have 227 addresses, suggesting that less money goes to reimbursement wallets on average than salary addresses.

Based on addresses in the leaks alone (the first row of Table III), expenses exceed income. This is to be expected, as Conti primarily used its administrator portal to communicate with victims, while the leaked chat logs appear to be the primary forum for requesting salary payment and reimbursement. As a result, ransom payment addresses surface in the chat logs only incidentally, while salaries and reimbursements are expected.

Nonetheless, we can identify likely ransom payment addresses. Given that Conti's income comes from ransom payments, and due to the traceable nature of Bitcoin, we can trace back payments visible in the leaked dataset to the ransom payments where the funds originate. Using the criteria established in Section IV, we identify 75 likely ransom payment addresses representing $83.9 million in payments. Of this, based on the dates Ryuk and Conti were active, we label $26.5 million as Ryuk payments and $57.4 million as Conti payments. The largest discovered likely payment of $9.5M is shown in Figure 2.

Given this perspective, income begins to dwarf expenses. In addition to leftover money from Ryuk used to fund the Conti operation, the total Conti income ($77.9 million) is more than double total expenses ($31.2 million). A significant portion

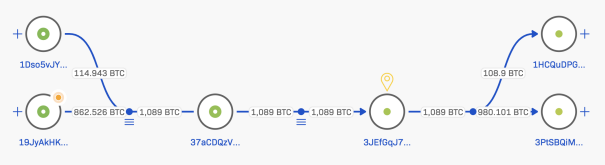

Figure 2: The largest discovered likely payment, of $9.5M in March 2020. The funds originated from the unlabeled cluster discussed in Section IV.

Exchange	Confirmed Payments	Likely Payments	Total
Unlabeled Cluster	$8.6M	$64.8M	$73.4M
Gemini	$5.9M	$17.4M	$23.1M
Kraken	$1.0M	$0.2M	$1.2M
Coinbase	$0.4M	$0.6M	$1.1M
Binance	$0.6M	$0.0M	$0.6M

Table IV: Top exchanges from which Conti ransom payments originate. Note that "Unlabeled Cluster" represents the unlabaled cluster of bitcoin addresses, discussed in Section IV.

of the proceeds go directly to the hands of affiliates. Our numbers are likely incomplete – Chainalysis identified $180 million in proceeds from Conti in 2021 alone [1]. However, unlike Chainalysis, we have provided our methodology for identifying ransom payment and we will publicly publish the addresses.

Table IV shows the most common origins of confirmed and likely Conti ransom payments. The unlabeled cluster discussed in Section IV represents a majority of payments – almost 70%. Following that, Gemini composes a significant share at $23.1 million. The fact that just two exchanges represent the vast majority of identified payments to Conti suggests strong intervention points.

We have published the derived likely ransom payment addresses on GitHub. [1] Notably, the release of these addresses increases the amount of publicly known Conti payments more than fivefold – from Ransomwhere's $17.1 million to $104.4 million.

Next, we consider the sources and funds of funds from wallets in the leaked dataset, shown in Figure 3. We use money laundering risk levels provided by Crystal Blockchain to group exchanges into three categories of low, medium, and high risk. Consistent with the hypothesis that most money originates from victim payments, most money originates either from low risk exchanges or the unlabeled cluster. Moderate-high risk exchanges, sanctioned exchanges, illegal services, and mixers represent smaller amounts – suggesting that some Conti actors might take steps to conceal their funds, though this practice is not systematized across the group. The receiving profile varies by type of address – ransom payment funds come almost exclusively from low risk exchanges or the unlabeled cluster, while salaries and reimbursements represent a more diverse portfolio. We speculate that some salaries and reimbursements

[1] See https://github.com/cablej/conti-payments

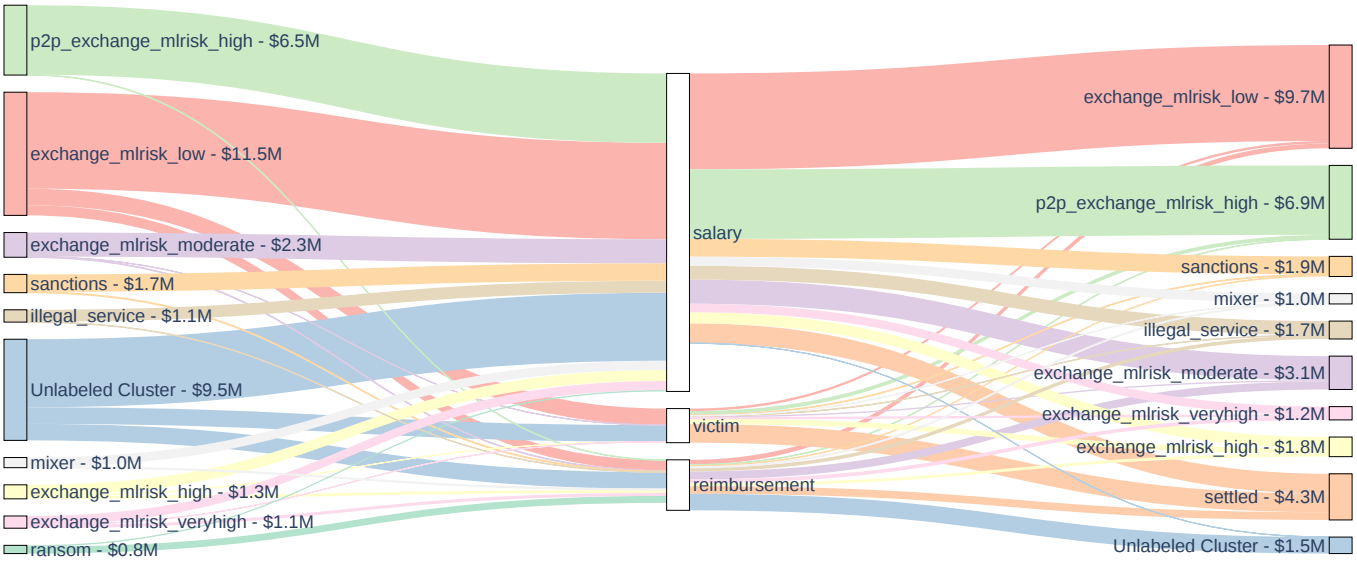

Figure 3: Labelled origins and destinations of wallet funds occurring in the Conti leaks dataset. Note that unknown addresses are excluded. “mlrisk” stands for money laundering risk. Further, note that as there are few ransom payment addresses in the Conti leaks dataset, the "victim" section in this chart only represents a fraction of all victim ransom payments to Conti.

are paid from a slush fund belonging to the core operators, and thus have a variety of sources.

A large portion of wallet transactions, somewhat surprisingly, are to low risk exchanges – exchanges most likely to abide by Know Your Customer (KYC) regulations. Gemini and Binance account for a large portion of these funds – $4.3 million and $2.9 million, respectively. Given Gemini’s position particularly as a regulated, U.S.-based exchange, Conti actors may have jeopardized their operational security by trading there. Other funds wind up in a variety of illicit destinations, such as $6.8M in Ren Exchange, a peer-to-peer cross-blockchain exchange that can be used to launder funds, $2.8M in the Seychelles-based exchange Huobi, and $1.4M in the now-sanctioned Hydra marketplace.

Of the expanded set of ransom payments, the destination of funds includes a variety of services used to launder money. $14.4M is sent to Ren Exchange, $17.9M to Huobi, and $12.6M to Binance. While both Huobi and Binance enforce KYC, certain illicit exchanges such as the now-sanctioned Suex have operated "nested exchanges" within both exchanges, providing an opportunity to launder funds through otherwise-regulated exchanges [28].

The leaks also offer insight into the individual salaries of Conti associates. Based on addresses where a Conti associate appeared to have claimed ownership of the address – most often a salary address – we compute the highest-grossing associates to be tramp ($1.2M), mango ($470K), baget ($400K), bullet ($280K), and andy ($98K). We note that this is an incomplete view into the proceeds of these associates.

We also observe evidence of co-spending among some associates. Co-spending occurs when two Bitcoin addresses are used as input to the same transaction, suggesting that the same entity controls both addresses. We observe two clusters of associates – viper, jumbo, ganesh and sonar, and sticks, stakan, elvira, and bekeeper. It is likely that these two clusters use a shared Bitcoin wallet to manage their funds, or otherwise share ownership of funds.

VI. Business Analysis

A. Overlap and Re-branding

Conti is assessed to be the successor of the Ryuk RaaS collective, which largely down-scaled their operations in March 2020 [18]. This is evidenced from the leftover revenue that we identified that was likely used to fund Conti. Ryuk and Conti shared multiple features, most notably the use of Trickbot for initial infection.

It is well documented that Trickbot and Conti are both technically and operationally interconnected [29]. This overlap is significant to understand some of the roles and structures within Conti, because there are shared group members duties. Trickbot provided the initial infection and facilitated the installation of the Conti ransomware on a victim’s machine, similar to Ryuk [30]. An arrest warrant for a member of the Trickbot collective, max, indicates that a large number of Trickbot’s members had also collaborate on the Dyre Trojan, a precursor to Trickbot. The remaining members of the Dyre collective transitioned to Trickbot following Dyre’s takedown in 2015 [30]. max’s alias was identified within the Conti Leaks, also indicating overlap with Trickbot and Conti. Further, the Conti Leaks Twitter account leaked information from both Trickbot and Conti, including Trickbot’s wider membership, indicating that there is approximately 18% overlap with those Trickbot aliases within Conti’s Jabber.

The indictment of Trickbot malware developers max and follow-on indictment of ffx provided further details into the

Trickbot organization, which also helped inform our understanding of Conti. Some of the same roles and responsibilities that were observed within the Trickbot organization were also observed within Conti, indicating that it was likely a rebranding as opposed to a reorganization. Trickbot and Conti also shared similarities in their roles, responsibilities, and recruiting methods [30], [31].

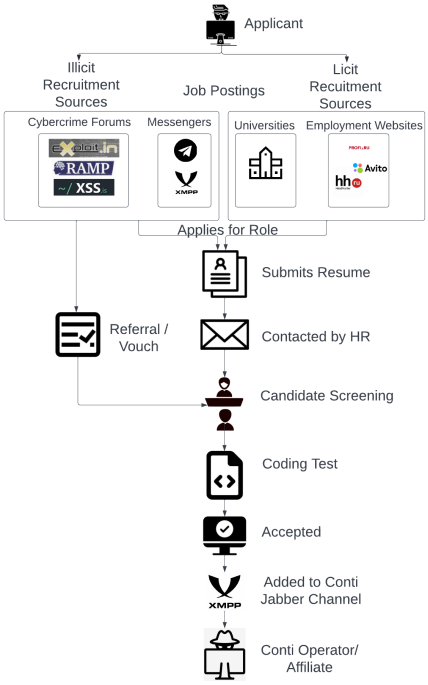

Figure 4: A flow chart demonstrating the recruitment sources of a RaaS affiliate

B. RaaS Roles, Responsibilities, and Recruiting

Similar to RaaS collectives, Trickbot relied upon a network of specialized workers to facilitate different functions. For example, the unnamed defendants in the Trickbot indictment included the following roles:

- **Malware Manager:** Recruiting, hiring, testing malware, and procuring infrastructure
- **Malware Developer:** Oversaw functionality within the development of the malware
- **Crypters:** Encrypted the malware to prevent detection from anti-virus
- **Spammers:** Deployed the malware through targeted and broad-based phishing campaigns

According to the indictment, Trickbot advertised these roles on legitimate job posting websites, like LinkedIn and Indeed, as well as Russia-based freelance websites. After completion of a programming test, users were added to a private Jabber OTR communication server where they collaborated on "development, maintenance, and deployment of Trickbot." This is consistent with our observations of the recruiting methods used by Conti, which included recruiting for licit roles on job posting website like Avito, HeadHunter, and Profi[.]ru. Conti utilized similar recruiting methods, as observed in their Jabber, and select threads on underground forums.

On August 5, 2021, a disgruntled Conti affiliate m1Geelka leaked internal training materials, and IP addresses of their Cobalt Strike servers on XSS, a top tier underground forum. m1Geelka also commented on an IT recruitment thread from a user IT_Work, stating that it was an advertisement to work with Conti. Between June 10, 2021 and September 6, 2021, IT_Work had posted multiple offerings on underground Russian language forums, like XSS and Exploit, advertising seemingly legitimate job roles to support large IT projects. In our research, we assessed that these advertisements for licit roles were in concert with job postings on Russian-based freelance websites.

- **C++ Programmer** (with reverse engineering skills)
- **Full-stack web developer for PHP, NodeJS**
- **Windows System Administrator**
- **Data Analyst**
- **Business Analyst**
- **UI/UX Designer**
- **HTML Designer**
- **Pentester**

IT_Work's posts demonstrate that while RaaS collectives are commonly associated with illicit tasks, like malware management and development, they also rely on technical talent to maintain infrastructure. These seemingly licit advertisements, albeit on underground forums, allowed Conti to recruit witting and unwitting tech workers to support the infrastructure of their operation.

Following the Colonial Pipeline ransomware incident on May 6, 2021, President Biden threatened action against "ransomware networks [32]." As a result, XSS, Exploit, and Raid Forums banned ransomware advertisements. The leader of the former Babuk ransomware collective then started their own dedicated ransomware forum in May 2021, originally dubbed Payload.bin. The site changed its name to RAMP (Ransom Anon Market Place). While originally a closed forum composed of reputable threat actors, RAMP became public in August 2021 following an extortion attempt. Ransomware advertisements continued to be available on Telegram and Jabber [33].

Conti suffered a minor disruption in November 2021 after details of their infrastructure were reported on by a security firm [34]. Shortly thereafter, a user JordanConti surfaced on RAMP highlighting that they were undeterred by the disruption, which included "peripheral IPs and wallets." JordanConti began openly recruiting for illicit roles required for their ransomware operation on RAMP, listing the Russian language as a requirement. The following roles were advertised on RAMP:

- **Pentesters:** "Top networkers who know how to bypass problematic AVs like Sentinel, work with RMM (Remote Monitoring Management) and EDR and backups"

- **Bot herders:** "Ideally, people with their own botnet, with a sufficient number of corp bots, especially in the US."
- **Targeted Spammers:** "who could beautifully send letters for "individual recipients" - the priority is USA."

From the Conti Leaks, we were able to ascertain that their HR specialists were also continuing to recruit on Russian-language freelance job posting websites and specialized universities. According to the Jabber chat logs, details of the roles varied. In a conversation between viper, a hiring representative, and bourbon, a developer, the reasoning varied from "we do pentesting for big clients," to more vague responses like "the work is remote, communication via messenger, the nature of the work is specific. That's all I know about conditions." viper then specified, "We do pen testing, write hacker software - exploits, grabbers, spam bots and more."

The legitimacy of the work was often questioned throughout the Conti leaks, as workers wondered why they had to be paid in cryptocurrencies, only communicated through encrypted messenger, and were unaware of the name or actual function of their employer. It does not appear that Conti used front companies to obscure their operations, but relied upon their managers to convey the appropriate messaging of the work. This meant deceiving their employees, or providing indirect answers to describe the true nature of their work.

C. Team Composition

From the chats, it appears that Conti is divided into several sub-teams. These teams are generally divided into functional areas, including management, development and infrastructure, access operations, and negotiations. These roles are consistent with the ransomware team structure outlined in the background.

In a chat from mango, a manager that oversees development and infrastructure, to stern, the organizational leader, mango shares details of the structure of his team, along with budgeted salaries:

> the main team - $97,447; 52 people
> new team - $4,000; 3 people, one has not started yet
> reverse engineering - $23,347; 16 people
> research team - $12,500; 6 people
> osint intelligence team - $9,000; 4 people

mango's team does not appear to encompass the whole Conti operation, however one functional area. The total monthly salary for their team is assessed to be $146,294.

Other references to a team structure appeared throughout the chat. For example, in a conversation between target and poll, target asks if poll needs individuals to attack logistics and manufacturing. poll highlights that they have a team that only "locks defense/military companies." In this regard, it appears that the sector specific targeting is divided between sub-divisions. However, some sector targeting like healthcare appeared to be off-limits.

Among RaaS operations as a whole, operators have informally agreed not to target healthcare. Following the DarkSide attack on Colonial Pipeline, REvil announced several new self-imposed restrictions for its operators and their affiliates. These announced restrictions included not targeting social sectors (such as healthcare and education) or any government entities, as well as requiring ransomware affiliates to get REvil operators' approval for any future targets. In an interview, LockBit claimed that they have a, "negative attitude towards those who encrypt medical and educational institutions." In an exchange between reshaev, one of Conti's main developers, and pin, who is possibly an affiliate, pin defends their reasoning for targeting a sports treatment center, claiming that it has no resuscitation unit and they have over 3K in insurance. reshaev emphasizes that they have a policy prohibiting ransoming healthcare, and recommends that pin "goes around them now." Despite this assertion, Conti had ransomed the healthcare sector through their operation including Ireland's Health Service Executive (HSE) and Department of Health (DoH), presumably choosing money over morals.

In the Conti leaks, there are abstract references to specific teams. For example, mango introduces themselves as "support C, manager for general issues of the team trick locker, now I'm looking for access to work for the gang." buza, a team lead of coders, in an exchange with hof, a technical manager, makes abstract reference to "rocket" and "A," likely meaning Rocket.Chat and team "A" (one of three teams). The Rocket.Chat messages, though not included in our primary research, did include details of the team composition of the access operations. The user alter briefly described the structure and responsibilities of teams A, B, and C. alter did not mention the size of the groups, however there were 54 unique aliases in that server.

> The current composition is divided into groups, each group is assigned a team leader (one or two depending on the size of the group).

D. Primary Actors

To further understand the main actors within the Conti leaks Jabber, we sorted the aliases by degree centrality. The top five individuals within the chats, defender, stern, buza, mango, and bentley, are Conti managers controlling payments, operations, developers, and malware builds. These managers also fulfilled HR functions, often sending bulk messages to users with comments, queries, and reminders to share cryptocurrency addresses for payments. Users that had a lower degree centrality were likely affiliates or developers. The limited number of chat messages made their roles much more difficult to identify. Managers like buza identified their developers by role in bulk messages that included requests to continue working on a bug tracker.

Defender also sent bulk messages, not identifying recipients by role, requesting for alternative forms of communication. This likely indicates that the leaked Jabber was likely a

centralized communication channel, and other communication channels may have been used for more specialized operations, like the Rocket.chat and Trickbot Forum, which included details on using the Trojan.

The managers have power of the purse. The top five users by centrality are assessed to be some of the primary leadership, since their role also included communications with the channel. Requests for funds typically occurred in the Conti leaks Jabber, with team leads requesting salaries and reimbursement from managers on the behalf of the individuals on their teams. This information helped inform us on the hierarchy of the roles, relationship between aliases, and an understanding of the team structure.

However, unlike previous cybercrime research that described the importance of cybercrime cultural capital within communities, the allure of experience and experimentation, it appears that RaaS operations center around mundane tasks of operating infrastructure [11], [35]–[37]. The most important members of the Conti operation appear to be the managers overseeing the collective work, administering salaries, and approving expenses for reimbursement.

E. Rewards for Justice

On May 6, 2022, the Department of State offered a $10 million reward for information leading to the identification or location of the members of Conti collective as part of the Rewards for Justice program. On August 11, 2022, they requested specific information on five individuals:

- dandis: manager, crypters
- professor (aka alter): ransomware negotiator
- reshaev: manager, ransomware builds
- target: manager, access operations
- tramp: manager, operations

From our research, we identified these individuals as being highly technical managers concerned with crypters, ransomware builds and development, access operations, and victim negotiations. Most of these aliases also appears within the Trickbot leaks, indicating that this may have overlap with the aforementioned Trickbot investigation. These individuals were most likely selected based upon the value that they provide the Conti collective in achieving a competitive advantage in the RaaS landscape [38].

On February 9, 2023 (following the initial publication of this paper), the United States and United Kingdom sanctioned several members of the Trickbot collective for their role in cybercrime and ransomware operations [39]. These individuals also appeared in the Conti Leaks, through the primary aliases shared in the sanction, or alternative aliases that helped us identify their membership in the collective. The following individuals were included in the sanction:

- bentley (aka ben): senior manager
- baget: developer
- globus: developer
- tropa (aka kerasid): money laundering
- iseldor: malicious injects
- mushroom: manager
- strix: administrator

These sanctions demonstrate a continued focus on cybercrime and ransomware operations. While the Rewards for Justice identified many of the lead members of Conti by alias, the sanctions listed the seven individuals by name. These measures underscore the importance of human capital in building and maintaining modern ransomware operations.

VII. Related Work

In order to conduct our analysis of the Conti ransomware operation, we use and extend methodologies from cyptocurrency tracking, leaked cybercrime data, and ransomware analysis.

A. Cryptocurrency Tracking

Prior work has shown that Bitcoin wallets and transactions are often linkable to the same entity using several heuristics [40]–[43]. These Bitcoin tracing heuristics have been implemented into a number of commercial cryptocurrency forensic analysis tools which also use techniques to label the owner of account clusters, such as Chainalysis, TRM Labs, Elliptic, and Crystal Blockchain. We use Crystal Blockchain's cryptocurrency forensic tools to perform analysis of Bitcoin accounts that we identify in the leaked Conti chat data.

Huang et al. conducted a two year end-to-end measurement of ransomare operations, tracing bitcoin from acquisition to ransomware payment. In this analysis, known-victim payments were identified through seed addresses, and were clustered with previously unknown-victims. The authors identified ransomware revenue exceeding $16 million USD, and infrastructure that was used to cashout illicit proceeds [6]. Paquet-Clouston et al. identify $13 million USD in ransomware payments between 2013 and 2017 [44].

B. Ransomware as a Service

Oosthoek et al. analyze over $100 million in ransom payments through a crowd-sourced dataset of ransomware addresses [25]. The authors characterized the shift from commodity ransomware to RaaS. Along with increased profits came a growing sophistication evidenced by faster time to launder funds and increased operational security practices. We build on this work by conducting an in-depth analysis of a single ransomware groups, which allows us to map over five times the amount of payments to Conti, in addition to operating costs which were not previously analyzed.

Previous work has also documented the practice of Ransomware as a Service groups "splitting" payments between the ransomware group and affiliates. Cong et al. document DarkSide's split percentage, which varies based on the size of the ransom payment [45]. Regarding Conti, Elliptic noted a 22.5% split for several Conti ransom payment addresses [46].

C. Conti

To date, relatively little academic work has analyzed the Conti leaks. Cong et al. investigate the cryptocurrency activities of several notable ransomware groups, including Conti [45]. The authors compile data from a variety of sources, including public and proprietary data. As part of their work, the authors discuss Conti's activity at a high level, including analyzing Conti's posting of victim data on leak sites. Our work builds on this paper by performing in-depth analysis of Conti's economic and business practices, including extracting and analyzing 666 Bitcoin addresses, compared to the 239 addresses the authors extracted.

Other industry groups have analyzed primarily the business aspects of the Conti leaks, including ForeScout, Secureworks, and Check Point [47]–[49].

VIII. Conclusion

Our study of Conti presents a vignette into the structure of a modern Ransomware as a Service group. This is the first comprehensive crypto-economic analysis of the Conti leaks, based on our annotation of cryptocurrency addresses present in the leaks, on-chain analysis of cryptocurrency payments, and qualitative business assessment based upon user conversations.

Through our analysis, we developed a methodology to identify ransom payments based on common splitting behavior. We use this methodology to identify $83.9 million in new likely payments and can help to better inform ransomware-affiliated payments through exchanges. Identifying these payments may assist cryptocurrency exchanges in blocking these payments, putting additional pressure on ransomware operators.

We find significant leverage points in both economic and business areas. The fact that a significant portion of funds both are received from and sent to low-risk exchanges presents an opportunity to monitor and seize funds. Further, targeting the organizational leadership responsible for the recruiting, hiring, training, and administering the various business units and infrastructure can also have an impact on their ability to function. The affiliate structure additionally provides opportunities to disrupt the more technical operators of the ransomware, thereby preventing affiliates' ability to lease the malware or receive operational support.

Acknowledgment

We thank the anonymous reviewers for their insightful and constructive suggestions and feedback, and Crystal Blockchain for providing access to their platform. Funding for this work was provided in part by National Science Foundation grants 1844753 and 2039693.

References

[1] Chainalysis, *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict*, en-US, Feb. 2022. [Online]. Available: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/ (visited on 09/18/2022).

[2] Trend Micro, *LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022 - Security News*, en. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022 (visited on 09/23/2022).

[3] S. Lyngaas, "I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang", Mar. 2022. [Online]. Available: https://www.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html.

[4] A. Hutchings and R. Clayton, "Configuring Zeus: A case study of online crime target selection and knowledge transmission", in *2017 APWG Symposium on Electronic Crime Research (eCrime)*, ISSN: 2159-1245, Apr. 2017, pp. 33–40. DOI: 10.1109/ECRIME.2017.7945052.

[5] K. Thomas, D. Y. Huang, D. Wang, *et al.*, "Framing Dependencies Introduced by Underground Commoditization", en, p. 24,

[6] D. Y. Huang, M. M. Aliapoulios, V. G. Li, *et al.*, "Tracking Ransomware End-to-end", en, in *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA: IEEE, May 2018, pp. 618–631, ISBN: 978-1-5386-4353-2. DOI: 10.1109/SP.2018.00047. [Online]. Available: https://ieeexplore.ieee.org/document/8418627/ (visited on 07/12/2022).

[7] L. Abrams, *Allied Universal Breached by Maze Ransomware, Stolen Data Leaked*, en-us, Nov. 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ (visited on 08/24/2022).

[8] L. Abrams, *Ryuk successor Conti Ransomware releases data leak site*, en-us, Aug. 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/ryuk-successor-conti-ransomware-releases-data-leak-site/ (visited on 08/28/2022).

[9] K. Baker, *Ransomware as a Service (RaaS) Explained | CrowdStrike*, en, Feb. 2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (visited on 09/22/2022).

[10] Microsoft, *Human-operated ransomware attacks: A preventable disaster*, en-US, Mar. 2020. [Online]. Available: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (visited on 09/21/2022).

[11] B. Collier, R. Clayton, A. Hutchings, and D. R. Thomas, "Cybercrime is (often) boring: Maintaining the infrastructure of cybercrime economies", en, p. 25,

[12] E. David, *The Secret Life of an Initial Access Broker*, en-US, Aug. 2020. [Online]. Available: https://kela.local/the-secret-life-of-an-initial-access-broker/ (visited on 09/05/2022).

[13] P.-M. Bureau, *Initial access broker repurposing techniques in targeted attacks against Ukraine*, en-us, Sep. 2022. [Online]. Available: https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/ (visited on 09/08/2022).

[14] V. Stolyarov and B. Sevens, *Exposing initial access broker with ties to Conti*, en-us, Mar. 2022. [Online]. Available: https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/ (visited on 08/19/2022).

[15] "Crystal Blockchain", [Online]. Available: https://crystalblockchain.com/.

[16] B. Krebs, "Conti ransomware group diaries, part i: Evasion", Mar. 2022. [Online]. Available: https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/.

[17] J. Cable, *Ransomwhere: A Crowdsourced Ransomware Payment Dataset*, version 1.0.1, Zenodo, May 2022. DOI: 10.5281/zenodo.6562484. [Online]. Available: https://doi.org/10.5281/zenodo.6562484.

[18] CrowdStrike, "WIZARD SPIDER Update: Resilient, Reactive and Resolute", Oct. 2020. [Online]. Available: https://www.crowdstrike.com/blog/wizard-spider-adversary-update/.

[19] D. Dittrich and E. Kenneally, "The menlo report: Ethical principles guiding information and communication technology research", Accessed: 2022-9-20.

[20] P. Howell O'Neill, *Why Jabber reigns across the Russian cybercrime underground*, en, Apr. 2017. [Online]. Available: https://www.cyberscoop.com/jabber-xmpp-cybercrime-russia-encrypted-chat/ (visited on 08/12/2022).

[21] R. Faithfull, *Russian prison culture and slang on cybercriminal forums: Can you cram on the hairdryer? | Digital Shadows*, en-US, May 2022. [Online]. Available: https://www.digitalshadows.com/blog-and-research/russian-prison-culture-and-slang-on-cybercriminal-forums-can-you-cram-on-the-hairdryer/ (visited on 08/12/2022).

[22] J. L. Fleiss, "Measuring agreement between two judges on the presence or absence of a trait", *Biometrics*, vol. 31, no. 3, pp. 651–659, 1975, ISSN: 0006341X, 15410420. [Online]. Available: http://www.jstor.org/stable/2529549 (visited on 09/01/2022).

[23] Blockchain.com, *Blockchain Data API*, en. [Online]. Available: https://www.blockchain.com/api/blockchain_api (visited on 09/07/2022).

[24] CoinDesk, "Coindesk API", [Online]. Available: https://api.coindesk.com/v1/bpi/historical/close.json.

[25] K. Oosthoek, J. Cable, and G. Smaragdakis, *A Tale of Two Markets: Investigating the Ransomware Payments Economy*, en, arXiv:2205.05028 [cs], May 2022. [Online]. Available: http://arxiv.org/abs/2205.05028 (visited on 07/12/2022).

[26] Crystal Blockchain, "Frequently asked questions", [Online]. Available: https://crystalblockchain.com/frequently-asked-questions/.

[27] CrowdStrike, "Wizard spider", [Online]. Available: https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/.

[28] A. Baydakova, "Here's what we know about suex, the first crypto firm sanctioned by us", Oct. 2021. [Online]. Available: https://www.coindesk.com/business/2021/10/05/heres-what-we-know-about-suex-the-first-crypto-firm-sanctioned-by-us/.

[29] TRM Labs, *TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider | TRM Insights*, en, Apr. 2022. [Online]. Available: https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider (visited on 08/28/2022).

[30] *Latvian National Charged for Alleged Role in Transnational Cybercrime Organization*, en, Jun. 2021. [Online]. Available: https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization (visited on 09/23/2022).

[31] U.S. Department of Justice, *Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization*, en, Oct. 2021. [Online]. Available: https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal (visited on 08/23/2022).

[32] The White House, *Remarks by President Biden on the Colonial Pipeline Incident*, en-US, May 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/ (visited on 08/30/2022).

[33] Flashpoint, *After Ransomware Ads Are Banned On Cybercrime Forums, Alternative Platforms Being Used to Advertise and Recruit*, Jul. 2021. [Online]. Available: https://flashpoint.io/blog/avoslocker-ransomware-advertise-and-recruit/ (visited on 08/30/2022).

[34] MalwareHunterTeam [@malwrhunterteam], *Malwarehunterteam on Twitter*, en, Tweet, Nov. 2021. [Online]. Available: https://twitter.com/malwrhunterteam/status/1461450607311605766 (visited on 08/30/2022).

[35] T. J. Holt, R. Brewer, and A. Goldsmith, "Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime", en, 2019, Accepted: 2019-06-11T01:47:37Z ISBN: 9780030114939 Publisher: Taylor & Francis, ISSN: 0163-9625. [Online]. Available: https://digital.library.adelaide.edu.au/dspace/handle/2440/119431 (visited on 09/23/2022).

[36] R. Leukfeldt and T. J. Holt, Eds., *The Human Factor of Cybercrime*, English. Taylor & Francis, 2019, Accepted: 2019-12-09 13:48:21. [Online]. Available: https://library.oapen.org/handle/20.500.12657/23615 (visited on 09/23/2022).

[37] A. Goldsmith and D. S. Wall, "The seductions of cybercrime: Adolescence and the thrills of digital transgression", en, *European Journal of Criminology*, vol. 19, no. 1, pp. 98–117, Jan. 2022, Publisher: SAGE Publications, ISSN: 1477-3708. DOI: 10.1177/1477370819887305. [Online]. Available: https://doi.org/10.1177/1477370819887305 (visited on 09/23/2022).

[38] *Conti – Rewards For Justice*, en-US. [Online]. Available: https://rewardsforjustice.net/rewards/conti/ (visited on 08/19/2022).

[39] *United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang*, en, Jan. 2023. [Online]. Available: https://home.treasury.gov/news/press-releases/jy1256 (visited on 02/09/2023).

[40] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system", in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, 2011, pp. 1318–1326. DOI: 10.1109/PASSAT/SocialCom.2011.79.

[41] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin", in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 34–51, ISBN: 978-3-642-39884-1.

[42] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph", in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 6–24.

[43] S. Meiklejohn, M. Pomarole, G. Jordan, *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names", *Commun. ACM*, vol. 59, no. 4, pp. 86–93, Mar. 2016, ISSN: 0001-0782. DOI: 10.1145/2896384. [Online]. Available: https://doi.org/10.1145/2896384.

[44] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem", *CoRR*, vol. abs/1804.04080, 2018. arXiv: 1804.04080. [Online]. Available: http://arxiv.org/abs/1804.04080.

[45] L. Cong, C. R. Harvey, D. Rabetti, and Z.-Y. Wu, "An anatomy of crypto-enabled cybercrimes", 2022. [Online]. Available: https://ssrn.com/abstract=4188661.

[46] Elliptic, "Conti Ransomware Nets at Least $25.5 Million in Four Months", Nov. 2021. [Online]. Available: https://www.elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months.

[47] Forescout, "Analysis of conti leaks", Mar. 2022. [Online]. Available: https://www.forescout.com/resources/analysis-of-conti-leaks/.

[48] Secure Works, "GOLD ULRICK Leaks Reveal Organizational Structure and Relationships", Mar. 2022. [Online]. Available: https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships.

[49] Check Point, "Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of", Mar. 2022. [Online]. Available: https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/.