From Lamborghinis to Ladas: Empirical Analysis of LockBit's Business Operations

Ian Gray
New York University
New York, NY, USA
iwg210@nyu.edu

Dalyapraz Manatova
Indiana University Bloomington
Bloomington, IN, USA
dmanato@iu.edu

Kris Oosthoek
Delft University of Technology
Delft, The Netherlands
k.oosthoek@tudelft.nl

Damon McCoy
New York University
New York, NY, USA
mccoy@nyu.edu

***Abstract*—Since 2020, LockBit has operated as a ransomware-as-a-service (RaaS) platform, leasing their malware to affiliates who conducted attacks on their behalf. LockBit emerged as one of the most prolific ransomware groups globally. However, the operation faced significant law enforcement disruptions on February 20, 2024, and May 7, 2024, during Operation Cronos. On May 7, 2025, an affiliate panel database from LockBit 4.0 leaked, providing an opportunity to better understand the latest iteration of the ransomware operation. The leak occurred one year after the second phase of the law enforcement disruption, Operation Cronos, which included a seizure of servers and infrastructure from LockBit 3.0.**

In this paper, we present an empirical analysis of LockBit 4.0 business operations observed through the compromised affiliate panel data. Based on the leaked data, we construct an operational workflow of LockBit 4.0. Our financial analysis found that post-Cronos interventions LockBit 4.0 was operating in a degraded state. LockBit 3.0 affiliates achieved a 54% compromise-to-payment rate while LockBit 4.0 had an 11.5% rate, which represents a 4.7-fold decline.

The leaked LockBit 4.0 affiliate panel offers empirical insights into a major ransomware operation's post-disruption phase, highlighting both the effectiveness of coordinated law enforcement action and the challenges facing cybercriminal groups attempting to rebuild after takedown operations. Our analysis reveals that while LockBit appeared to resume their operations unabated, it was severely hampered by Operation Cronos. Given their downscaled operation, LockBit 4.0's affiliate recruitment slogan, "Want a Lamborghini" is more appropriately "Want a Lada," a cheaper Russian brand of Soviet-era automobiles.

***Index Terms*—Ransomware, Bitcoin, Cybercrime**

I. Introduction

The Ransomware-as-a-Service (RaaS) ecosystem has fundamentally transformed cybercrime from isolated attacks targeting singular users, to sophisticated criminal enterprises operating at scale [1]. Since the emergence of double-extortion tactics in 2019 by the Maze ransomware group, RaaS operations have evolved into complex business models that mirror legitimate technology platforms, complete with affiliate networks, customer support systems, and revenue-sharing arrangements [2]. Among these operations, LockBit emerged as one of the most prolific RaaS groups globally, consistently ranking among the top threat actors since launching their public-facing ransomware blog in 2020.

Public ransomware blogs serve to further extort victims by threatening to leak their data if a ransom is not paid within a set period of time. Victims are paying to both recover their encrypted data, and prevent further data from being leaked on a ransomware blog.

Ransomware blogs can provide insights on their victims and targeting, though our understanding of these criminal enterprises remains limited. Industry research has relied on external measurements from ransomware blogs, law enforcement indictments, and victim disclosures [3]–[5]. Academic research has relied on crowd-sourced cryptocurrency addresses used in ransomware payments, and leaked datasets and chat logs [1], [6]–[8]. These datasets provide fragmentary insights into the internal mechanics of a RaaS operation. There are continual questions on affiliate recruitment, operational efficiency, and sustainability of RaaS operations, particularly following a major law enforcement operation.

The February and May 2024 Operation Cronos law enforcement action against LockBit 3.0 serves as a litmus test of cybercrime resilience in the face of disruption. While these coordinated international operations disrupted LockBit's core infrastructure, arrested key personnel, and seized critical assets, the group's attempts to rebuild offer unprecedented insights into post-disruption adaptation strategies [9].

The compromise-to-payment conversion rate serves as a critical indicator of ransomware group effectiveness, measuring the percentage of successfully compromised victims who ultimately pay ransoms. According to NCA Operation Cronos disclosures, LockBit 3.0 achieved a 54.1% compromise-to-payment rate during its peak operational period from 2022 to 2024 3. In stark contrast, our analysis of the leaked LockBit 4.0 panel data reveals a dramatic collapse to just 11.5%, representing a 4.7-fold decline that illustrates the devastating impact of law enforcement disruption on the group's core monetization capabilities.

The leaked dataset enables us to examine two critical research questions:

- RQ1. What are the key components and revenue streams of the current ransomware-as-a-service business model?
- RQ2. How successful is this model in practice, as measured by recruitment rates, conversion rates, and affiliate payouts?

Subsequently, answering these questions, we can get a deeper understanding of:

978-1-6654-XXXX-X/25/$31.00 © 2025 IEEE

RQ3. How do law-enforcement disruptions (e.g., server take-downs, key arrests) impact the operational efficiency and force adaptations in ransomware-as-a-service illegal businesses?

This study contributes to our understanding of criminal enterprise adaptation, the economics of ransomware groups, and the effectiveness of law enforcement disruption. By analyzing ground-truth operational data during a critical transition period, we provide empirical evidence of how sophisticated criminal organizations restructure their business models to survive major disruptions while maintaining the appearance of operational continuity.

II. Background

LockBit ransomware first appeared in September 2019, initially known as "ABCD" ransomware due to the ".abcd" file extension it appended to encrypted files. By late 2019, the broader ransomware-as-a-service (RaaS) ecosystem was also taking shape, when Maze's high-profile extortion of Allied Universal (November 2019) introduced data-leak sites as a negotiating lever and set the stage for the RaaS model [1], [2]

Building on this shift, LockBit rapidly evolved through multiple technical variants: LockBit 1.0 (2020), LockBit 2.0 "Red" (2021), LockBit 3.0 "Black" (2022), LockBit Green (2023, incorporating leaked Conti code), and LockBit 4.0 (2024) [10].

Table I: LockBit Development Timeline

Date	Event
Sep 2019	ABCD ransomware first observed
Jan 2020	LockBit appears on Russian cybercrime forums
Jun 2021	LockBit 2.0 (LockBit Red) released
Aug-Sep 2021	LockBit interviews with "Russian OSINT" and "The Record"
Oct 2021	Linux-ESXi (ESXi) targets virtualized environments
Mar 2022	LockBit 3.0 (LockBit Black) released
Sep 2022	Builder leak enables widespread non-affiliate use; Tattoo contest and bug bounty launched
Jan 2023	LockBit Green (LBG) incorporates Conti code
Apr 2023	macOS encryptors identified
Feb 2024	**Operation Cronos disrupts infrastructure and arrests 2 affiliates.**
May 2024	LockBit administrator identified and sanctioned
Dec 2024	LockBit 4.0 announced
May 2025	**LockBit Lite Panel leaked**

Meanwhile, LockBit's administrator cultivated an unusually public persona online across multiple forums, Exploit, XSS, RAMP, and Telegram, using pseudonyms including "LockBit," "LockBitSupp," "putinkrab," and "Fox William Mulder" [11], [12]. Unlike other prominent ransomware groups that moved underground following the May 2021 Colonial Pipeline attack and subsequent forum restrictions, LockBit's administrator became increasingly outspoken, conducting media interviews and launching publicity campaigns including $1,000 payments for LockBit logo tattoos [13], [14].

This high-visibility strategy belied their stated commitment to "quality over quantity". In a January 2020 forum announcement, the admin insisted:

> "We're not chasing quantity of ads, we care about quality."

LockBit seemingly differentiated their operations by providing affiliates more control of the ransom payment process. [15], [16]. Unlike other ransomware operators that centrally control ransom disbursement, LockBit promised affiliates that they could set their own ransom amounts and receive payments directly. The admin claimed:

> "You set the ransom amount after talking with the victim. Payment is received in your wallets, in the currency of your choice."

In this model, affiliates receive the payments in their personal cryptocurrency wallets, while the administrator retains exclusive control over the decryption part of the extortion. The affiliate is unable to decrypt the victim's files until the commission is paid into a LockBit controlled address. The operator advertised "the first decryption is free as a test," positioning this as a quality assurance measure while ensuring affiliate dependence on operator-controlled infrastructure.

A. Operation Cronos and Infrastructure Disruption

On February 20, 2024, international law enforcement launched "Operation Cronos," targeting LockBit's infrastructure and personnel. The operation resulted in substantial seizures: 34 servers, 14,000 accounts, 200 cryptocurrency accounts, and 1,000 decryption keys. Two LockBit affiliates were arrested, and authorities took control of the ransomware blog to tease intelligence releases [17] [18] [19] (See Appendix for screenshots of releases X).

Just a few weeks later, on May 7, 2024, a second wave of actions publicly identified LockBit's administrator as Russian national Dmitry Yuryevich Khoroshev and imposed international sanctions against him [4]. A $10 million bounty was announced for his capture. These actions severely damaged LockBit's operational capacity and reputation, forcing the group to continue operating in a degraded state, posting recycled content and borrowed material from other RaaS groups on their ransomware blog [20].

On December 19, 2024, the LockBit admin rolled out a "LITE PANEL", accompanied by a recruitment pitch calling affiliates "pentesters":

> "Want a lamborghini, a ferrari and lots of titty girls? Sign up and start your pentester billionaire journey in 5 minutes with us."

On May 7, 2025, exactly one year after Khoroshev's public identification, attackers breached the affiliate panel with the message "Don't do crime CRIME IS BAD xoxo from Prague," releasing a SQL database of this new panel, spanning December 18, 2024, through April 29, 2025. The timing appeared intentionally symbolic, marking the anniversary of LockBit's most significant law enforcement disruption. And although LockBit's administrator downplayed the incident, insisting it impacted only the insignificant part ("lite panel"), the leak provides evidence of the success of LockBit's 4.0 operation.

The leaked dataset provides unprecedented insight into LockBit's post-disruption operations, revealing the internal mechanics of their business model during a critical transitional period.

In Table I, we summarize key events in the LockBit development history and in the next sections, we delve into the leaked database and the business model that we reconstructed from this information.

B. LockBit Affiliate Model and Technical Infrastructure

Ransomware-as-a-Service (RaaS) typically relies on a two-role ecosystem: the *ransomware operator*, who develops and maintains the malware, manages encryption/decryption, controls decryption key distribution and payment flows; and the *ransomware affiliate*, who serves as a distribution partner, focusing on targeting victims and deploying the operator-provided "builds" (customized ransomware variants). Affiliates receive commissions for successful infections and often handle ransom negotiations and collection [7].

Under most RaaS schemes, victims transfer the ransom into operator-controlled wallets, and those funds are then further divided according to predetermined agreements. The standard split allocates 80% of the ransom payment to the *affiliate* and 20% to the *operator*, though percentages vary based on the ransomware group, victim revenue, and ransom payment amount. This arrangement can create tension between operators and affiliates since operators control the payment process. Multiple instances have occurred where disgruntled affiliates rebelled against operators by leaking sensitive group information. To attract and retain talent, some operators modify terms to create more favorable arrangements for their affiliates. LockBit, however, allows affiliates to receive the funds before sending the share to operators [21] (see Figure 1).

Affiliates access LockBit's web panel and builder tools by paying a registration fee (i.e., 777 USD in Bitcoin, often routed through mixers to obscure the transaction). Once inside, they generate custom executables or builds for the targets from the available LockBit variants: LBG (Green), LBB (Black), LBL (Linux), or ESXi. They also fill out information about the intended victim that the build was generated for, however this data is user-generated and potentially erroneous. When the victim visits the provided link and initiates a chat, the affiliate negotiates, provides their wallet address, and collects the ransom directly through the web platform.

Yet despite this apparent autonomy, affiliates remain dependent on the operator for decryption. Victim chats consistently show that LockBit's administrator must join negotiations to deliver the decryption tool, ensuring the operator's ongoing control over the payment stream and decryption process.

Figure 1 illustrates the end-to-end flow of a LockBit affiliate campaign, from panel registration and build creation through victim infection, negotiation, key delivery, and final payment. We describe each step and validate its mechanics in detail in Section V.

III. Data

The core data for this study comes from the complete SQL dump of LockBit's affiliate panel - `paneldb_dump`. The dataset originated from a breach of LockBit's affiliate administrative interface on May 7, 2025. This leak exposed every table from December 18, 2024 through April 29, 2025, providing an unprecedented window into LockBit's post-disruption operations. We have sanitized the leaked dataset from victims' identifiable information and made it public for future analysis[1].

In this section, we describe the structure and contents of the leaked affiliate panel database. The following sections then examine the resulting information flows, our methods of validation, and key findings derived from that dataset.

A. Ethical and Legal Framework

All analysis was conducted under appropriate institutional oversight and ethical guidelines for studying criminal infrastructure data. The research focuses exclusively on aggregate patterns and systemic analysis rather than individual victim identification or operational details that could enable further criminal activity. Personal identifying information has been anonymized or excluded from analysis to protect victim privacy while preserving analytical value.

B. Database Tables

The dataset comprises 20 database tables (including 5 empty tables) spanning 132 days (approximately 4.3 months) of post-disruption operations. This timeframe captures LockBit's transition period following Operation Cronos, providing unique insights into criminal enterprise adaptation strategies. The leaked database contains tables filled with the backend information from the affiliate web panel, which includes operational data across affiliate management, victim targeting, payment management, and technical capabilities.

Although the full database contains 20 tables, six contain structural headers but no data, and several others proved irrelevant to our analysis. Below is the complete list of tables, with those we ultimately focused on highlighted in bold: `api_history`, **`btc_addresses`**, **`builds`**, **`builds_configurations`**, **`chats`**, **`clients`**, `events`, `events_seen`, `faq`, **`files`**, **`invites`** , `jobs`, `migrations`, `news`, **`pkeys`**, `socket_messages`, `system_invalid_requests`, `testfiles`, **`users`**, **`visits`**.

Analyzing the records in the database and the relationships between tables, we arrive at the following high-level summaries:

- `btc_addresses`: LockBit admin-controlled addresses for commission payments.
- `builds` and `builds_configurations`: records of compiled ransomware builds with information including victim details, target specifications, configuration parameters, and affiliate comments.
- `chats`: chat messages with negotiations between affiliates and victims.
- `clients`: victim records (presumably server clients), containing encrypted file details, an associated build, ransom negotiation chat status, and payment tracking.
- `files`: file transfer and encryption operation logs.

[1] https://github.com/iwg210/lockbit-lamborghinis-to-ladas

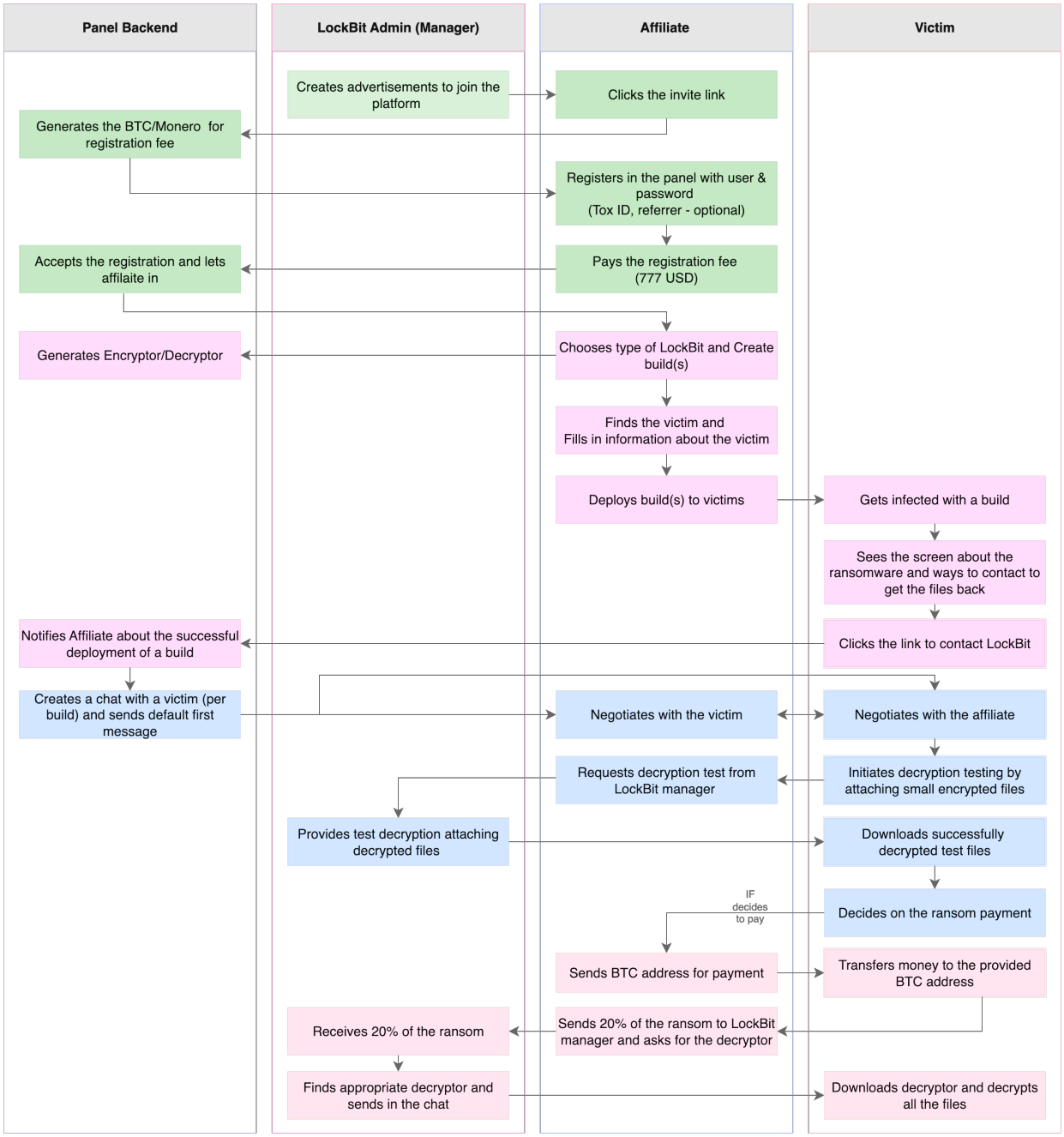

Figure 1: The Flow of the LockBit Affiliate Web Panel. The workflow breaks into four sequential stages: **Registration**, **Deployment**, **Victim Interaction**, and **Ransom Payment**.

- `invites`: invites with accompanying cryptocurrency wallet addresses for registration fee payment, transaction amounts (777 USD - based on cryptocurrency daily conversion rate), status indicators, and creation timestamps.
- `pkeys`: public keys used within the encryption process, including decryption identifiers, type classifications, status tracking, and temporal metadata.
- `users`: affiliate user accounts, including credentials, permission levels, and account tags.
- `visits`: victims' timestamped visits to the chat page.

C. Data Integrity Checks

Since we did not gather the information ourselves, we evaluated the completeness and accuracy of the data leak to ensure it had not been manipulated by either LockBit operators or the third party who compromised their affiliate panel. To validate data integrity, we conducted systematic external verification, internal consistency analysis, and cross-platform mapping using multiple independent data sources: blockchain transactions, law enforcement disclosures, cybercrime forums, and ransomware blogs.

Table II: LockBit Database: High-level data summary used for analysis

Category	Metric	Count
BTC Addresses	Ransomware Payments	18
	Commission Payments	18
	Paid Registrations	12
Users	Users	75
	Users Creating Builds	54
	Negotiating Users	35
	Paid Users	10
Builds	Unique builds	1,183
	Builds targeting companies	156
Clients	Total Clients	246
	Unique Clients	208

1) Data Accuracy: To ensure that our analysis is based on reliable data, we cross-validated key elements of the leaked dataset against multiple independent sources.

a) Blockchain Transaction Verification: We extracted all Bitcoin addresses referenced in victim negotiation chats (`chats`) and matched them on the transaction chain to commission payouts recorded in `btc_addresses`. In total, 18 addresses appeared in both sources. For each, we retrieved the corresponding on-chain transactions and confirmed that affiliate commission payments occurred within 24 hours of the victim's ransom payment, averaging approximately 20% of the total amount, which precisely matches LockBit's advertised revenue-share model. This on-chain verification validates both the timing and scale of financial flows documented in the leak.

b) Law Enforcement Correlation: The UK's National Crime Agency's public materials from Operation Cronos [22] provided additional ground truth and independent validation of our dataset structure. Screenshots and summary tables released by the NCA confirmed that victim company information requires manual input, build-type classifications (e.g., Windows, ESXi, Linux), and the distinct sequencing of build creation versus chat generation. These independent disclosures align with the schema and metadata captured in the leaked database. The materials useful for our analysis can be found in the Appendix X.

c) Dark Web Cross Reference: We compared the leak's recruitment messaging and technical timelines with archived posts on key underground forums (Exploit, XSS, RAMP) and the official LockBit blog. The December 2024 launch of "LockBit 4.0" and $777 registration fee are explicitly mentioned in multiple posts, matching the `invites` table's timestamps and payment records.

d) Victim Verification: To independently confirm that the entities in our dataset represent real-world victims rather than test or dummy entries, we employed two verification strategies. First, we cross-referenced the leak against LockBit's official ransomware blog. During our December 2024 – April 2025 window, the blog mentioned 39 distinct organizations. Of these, 29 have matching build records in the `builds` and `builds_configurations` tables, and 11 ultimately engaged in live chat negotiations. This demonstrates consistency between public disclosures and the leaked internal data.

Second, we subjected all unique victim domains in the `clients` table to a five-indicator audit: DNS resolution, WHOIS registration, HTTP/HTTPS connectivity, SSL certificate validation, and suspicious naming pattern detection. We additionally verified company profiles using a custom GPT model trained on online business registries (e.g., Crunchbase, LinkedIn, regional corporate registries). Given a domain, the model retrieved public metadata, such as industry classification, founding date, and headquarters location, which we manually checked against corporate filings or official websites. Of the 132 unique domains in our dataset, 101 were verified as genuine organizations through our multi-step validation process. An additional 17 domains, though not verifiable via public records, nonetheless exhibited clear victim behavior (chat-page visits and message exchanges). Together, these 118 confirmed cases form the victim base set for the analysis in this paper.

D. Data Completeness

Six database tables (`api_history`, `events`, `events_seen`, `faq`, `jobs`, `testfiles`) contained headers but no data or one entry, indicating either unused functionality or selective data retention. However, critical operational tables (i.e., `builds`, `clients`, `chats`) remained populated.

Some expected fields are empty. For instance, the `stealerid` column in `builds` table, which likely references an initial-access infostealer, has no entries despite its appearing in NCA-released screenshots. These gaps suggest either data sanitization or configuration differences between the "lite panel" and the full administrative interface. However, these gaps do not impede our financial and conversion analyses since all key transactional and communication fields are intact.

Cross-table primary key relationships examination reveals that, of the 281 expected total IDs in `clients` table, 35 are missing (ranging from 24 to 281). Likewise, 23 out of roughly 60,000 expected Bitcoin address records in the `btc_addresses` table are missing. These absent keys occur in contiguous clusters (for example, IDs 12001–12006), suggesting intentional operational cleanup rather than random data loss or corruption. Additionally, we observe a user missing in the `users` table with the ID of 60. There is a possibility that the missing data can be linked to this particular missing user, but we do not have any confirmation of that. Overall, just 14.2% of client IDs and 0.038% of BTC-address records are missing, and all essential transactional and communication fields are intact.

We also compared recorded registration and ransom payments against on-chain Bitcoin transactions. Although 43 affiliates appear in the `invites` table as having paid the $777 registration fee, only 12 corresponding blockchain transactions could be found, of which 10 clearly map to code (50) (registration-to-affiliate conversions). This discrepancy could

imply that some fees were either waived, deferred, or paid via alternative channels.

Although LockBit operators characterized the breached system as a "lite panel", the dataset contains sufficient transactional, operational, and communication data to support our analysis. When combined with our successful cross-validation against blockchain data, law-enforcement disclosures, and forum archives, these minor gaps point to post-disruption operational constraints rather than systematic manipulation. We therefore have high confidence in the dataset's suitability for characterizing LockBit 4.0's affiliate recruitment model and its economic dynamics.

IV. Methodology

Our analysis of the leaked LockBit dataset `paneldb_dump` employs multiple complementary methodological approaches to reconstruct the operational structure and economics of this affiliate panel for ransomware operations. Our methodology combines a relational analysis of leaked databases that we developed into an affiliate workflow, a transaction analysis of the bitcoin addresses observed within the database, and a conversion funnel analysis to measure the success of LockBit affiliates of converting builds into ransom payments.

To understand the operational workflow of LockBit 4.0, we mapped the end-to-end proces of an affiliate's interaction with the LockBit affiliate panel, including coordination with the LockBit administrator and engagement with victims. We reconstructured this workflow by analyzing database relationships, and the timing of events within the tables (user creation, build creation, client creation, etc.) to identify four sequential operational stages: Affiliate Registration, Ransomware Deploymentment, Victim Interaction, and Ransom Payment.

For each stage, we analyzed the specific database records generated, identified the actors involved (affiliate, administrator, victim), and validated our results through cross-table analysis. This reconstruction enabled us to understand the complete business process flow and identify key operational dependencies and bottlenecks. Following the process flow, we progressed to the financial analysis to understand how successful LockBit's affiliates were in achieving victim payments.

To assess the ransomware collective's revenue, we identified Bitcoin payments within the `invites` and `btc_addresses` table. Additionally, we analyzed the `chats` table for successful negotiations where a final ransom demand was established, and the corresponding Bitcoin address. All payments were verified on the blockchain for transaction amount and timing, and correlated with the tables ensuring it was consistent with affiliate registration, victim payment, and commission payment.

After we established these payment addresses, we identified additional addresses controlled by the group through the co-spending heuristic, a robust method for associating multiple addresses with a single entity. The co-spending heuristic identifies addresses that are spent together in a single transaction, suggesting they are controlled by the same actor due to the shared use of private keys. By analyzing transaction patterns, this approach enables the clustering of related addresses with high confidence. We utilized GraphSense, a blockchain analytics tool forked from BlockSci and maintained by researchers at the University of Vienna. For this study, we received complimentary API credits for their cloud-based platform. Furthermore, we queried Arkham Intel and Scorechain to obtain address labels in order to identify platforms used by affiliates to launder their proceeds.

Using GraphSense, we queried all addresses listed in the panel leak and a supplementary set of LockBit-affiliated addresses obtained from a proprietary source. A summary of the clustering dataset is presented in Table V. For the blockchain analysis, we excluded clusters containing more than five addresses or exceeding 100 incoming transactions. This is a conservative threshold which may omit some LockBit-related proceeds, but which ensures a cleaner dataset by minimizing the inclusion of exchange clusters and thus including funds not associated with LockBit.

The affiliate workflow and financial analysis inform our conversion funnel analysis. We define the ransomware conversion funnel as a five-stage process, from build creation to payment completion. Conversion rates were calculated as the proportion of entities that progressed from one stage to the next.

To account for sampling uncertainty in our conversion rate estimates, we calculated 95% confidence intervals using the Wilson score method. This approach was selected over standard normal approximation methods due to its superior performance with small sample sizes and extreme proportions, both of which characterize ransomware conversion data.

The Wilson score method adjusts for boundary effects that can produce impossible confidence intervals (e.g., negative percentages) when success rates are very low or very high. The method calculates confidence intervals using the formula:

$$\frac{\hat{p} + \frac{z^2}{2n} \pm z\sqrt{\frac{\hat{p}(1-\hat{p})}{n} + \frac{z^2}{4n^2}}}{1 + \frac{z^2}{n}}$$

where $\hat{p}$ represents the observed conversion rate, n is the sample size, and $z = 1.96$ for 95% confidence intervals.

For example, the build-to-compromise conversion rate of 13.2% (156 successes from 1,183 builds) produces a Wilson confidence interval of 11.3%–15.4%, indicating we can be 95% confident that the true conversion rate falls within this range. This method is particularly valuable for our analysis given the low overall success rates and varying sample sizes across conversion stages, providing more reliable uncertainty estimates than traditional approaches.

V. Process Flow Analysis

To fully understand the operational workflow of LockBit 4.0, we mapped the end-to-end process of an affiliate's interaction with the LockBit affiliate panel, including coordination with the LockBit administrator and subsequent engagement with the victim. As shown in Figure 1, this workflow is separated into four sequential stages: Affiliate Registration,

Ransomware Deployment, Victim Interaction, and Ransom Payment. In the paragraphs that follow, we describe each stage in turn, indicate who performs each action, and, where possible, provide validating evidence from the leaked panel database and external sources.

A. Affiliate Registration

The Affiliate Registration phase begins when the LockBit administrator publishes promotional posts and invitation links on underground forums and blog posts (see the example in Appendix 4). When a potential affiliate clicks the invite link, the panel backend generates a unique cryptocurrency address (Bitcoin or Monero) to collect the "entrance fee" (777 USD). We are convinced that this happens at this step, as in the database table `invites`, each user (affiliate) had a unique wallet address to pay the registration fee. The purpose of these addresses is evident from the observed transaction of 777 USD on the chain (10 affiliates had a transaction with the associated wallet in the invites table (Status Code: 50) and 2 additional addresses received payment but were not converted to affiliates (Status Code: 10)). After paying the registration fee to the provided address, the affiliate is approved with the registered credentials (username, password, optional referrer ID) to log in (see Appendix, Figure 8 for details). At that point, the affiliate's account is activated, granting them access to the LockBit control panel and its malware builder tools.

B. Ransomware Deployment

The Ransomware Deployment phase begins once the affiliate has registered and logged in. Using the panel's builder tools, the affiliate generates one or more customized ransomware binaries ("builds") tailored to their chosen target environment (Windows, Linux, or ESXi). During this process, the affiliate manually enters details such as the victim's website, estimated revenue, and any free-form comments (for details see Appendix, Figure 10). When the affiliate finalizes a build, the panel backend produces the corresponding encryptor and decryptor.

While the information within the build is user-generated, we have observed victims matching the company website from within the `builds` table on LockBit's ransomware blog, indicating that these builds are being used to infect users in the wild. Once the affiliate infects a client, the victim's machine displays a ransom note with a link to contact the criminals via chat. We infer that clicking this link both creates a new chat record in the `chats` table and logs a visit in the `visits` table, notifying the affiliate (and the administrator) that the victim has arrived in the chat interface. In the database, the time between build creation and client record creation in the `clients` table ranges from 1.7 seconds to 98 days, and the interval from client record creation to the first chat message spans from 1 sec to 13 min. Each newly created chat is prepopulated with LockBit's default opening message, at which point the affiliate begins direct ransom negotiations with the victim. In Table III, we computed the observed delays in the database between these stages: user creation, first build creation, build converging to a client record, and the first chat message sent to the client.

Table III: Time Lags Between Operational Phases in the Database

Phase	Mean	Median	Min-Max	Size
Invite to User Creation	44.4 hrs	0.6 hrs	18 sec – 841.1 hrs	73 users
User Creation to First Build	45.7 days	0.3 days	83 sec – 1051.9 days	54 users
Build to Client Record	11.8 days	3.7 days	1.7 sec - 98.8 days	246 records
Client Record to First Message	11.2 sec	5 sec	1 sec - 13.9 min	208 records

C. Victim Interaction

Once an affiliate's build infects a victim's system, the victim is presented with encrypted files and an embedded ransom note (see the example in Appendix, Figure 5). Clicking this link automatically opens a pre-created chat thread (logged in the visits and chats tables), where the affiliate presents an initial ransom demand, fields the victim's questions (or pushback), encourages a test decryption, and outlines the next steps (see Appendix, Figure 6 for details). Affiliates typically create multiple builds with different build types for clients to improve their success rates. Since the chat is created only once the client opens the link, it is possible to have builds that never progress to the victim interaction phase.

If the victim requests a test decryption, the affiliate uploads a small selection of encrypted files directly into the chat. The affiliate then relays this request to the LockBit administrator, who returns a decrypted sample in the same chat, often after a several-hour delay or, if the admin is offline, the next day. We infer this handoff because decrypted files consistently appear in the chat hours after the victim's request, and some affiliates explicitly tell victims that only the "boss" or "admin" can perform the decryption.

Once the test decryption is successful, negotiations progress to a final ransom demand. If the victim agrees to pay, the affiliate supplies their own Bitcoin address for the transfer. We can be confident this address belongs to the affiliate because it never overlaps with the operator addresses stored in the `btc_addresses` table.

D. Ransom Payment

In the final stage, the victim transfers the agreed ransom to the affiliate's Bitcoin address. Once the affiliate confirms receipt, they remit 20% of the payment to the LockBit administrator's wallet, which is exactly as advertised in the affiliate rules [21] . Although this handoff does not appear directly in the leaked database, we have evidence from blockchain analysis: the payments into affiliate addresses are followed, within 24 hours, by corresponding 20% commission payments into operator addresses recorded in the database and connected to the corresponding victim and affiliate.

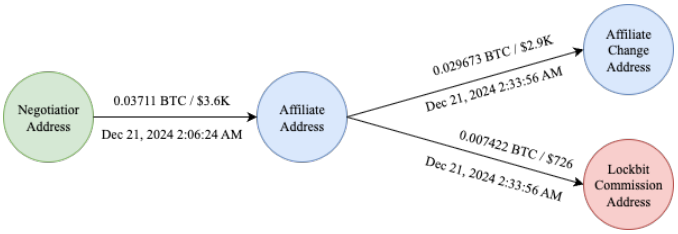

Figure 2: An example of a LockBit payment transferred from a victim to an affiliate, and splitting between a LockBit address and an affiliate change address

After sending the operator's share, the affiliate requests the full decryptor tool from the LockBit operator. As evident from the chats, affiliates do not have access to the decryptor. Instead, they have to wait for the LockBit "boss" or "admin" to join the chat and deliver the dedicated decryptor tool to the victim. The administrator then locates the appropriate decryptor (presumably matching the original build's key pair) and delivers it via the chat, enabling the recovery of all encrypted files. For the Linux-based decryptor, additional instructions accompany the decryptor tool, as it requires extra steps compared to the Windows version of the build.

VI. Financial Analysis

In the following subsections, we delve into the financial analysis of the operator and affiliates, mainly relying on the blockchain analysis of transactions and closely related clusters on-chain. We begin by investigating registration fees from within the `invites` table. We then progress to the commission payments within the `btc_addresses` table. Finally, we review the available affiliate addresses shared within the `chats` table as part of the negotiation. Finally, we assess the ransomware collective's revenue, we performed a blockchain analysis to uncover additional addresses controlled by the group.

A. Registration Fees

The `invites` table records paid registrations for the affiliates. The table containing 3,693 entries, with 2,338 Bitcoin addresses (63.3%) and 1,355 Monero addresses (36.7%).

Status codes revealed a systematic progression through the payment process, with 93.4% of entries in status (0), .32% in status (10), 1.95% in status (50), and 4.3% in status (100). We are confident that status (50) refers to paid registrations, since all 72 users with that code have corresponding affiliate accounts. We are not confident in status (10), since only one registered affiliate has this status.

Of the registered affiliates, 43 paid in Bitcoin and 29 in Monero. We are only able to observe payments transacted on the Bitcoin blockchain. Of those 43 Bitcoin addresses, only 10 wallets paid registration fee. This may indicate that some of the fees are waived or deferred. The Bitcoin amounts tied to these registration payments generally matched the $777 fee disclosed by LockBit panel users, and conversion confirmed with historical BTC/USD rates.

Four of the registration fees were transferred out of the wallets, however the funds within the remaining addresses remain parked. The total observed payments to invite addresses is $9,449. This sum is much less than the expected total income from registration of $56,721, granting each affiliate pays the $777 fee. This indicates that registration fees are not a substantial source of income for the operation.

B. Commission Payments

Ransomware builds are equipped with LockBit admin-controlled BTC addresses. Affiliates will receive the decryption key for the victim's data once the commission is paid. These addresses, recorded in the `btc_addresses` table are primarily unused, as only 18 affiliates were successful in completing a ransom payment and receiving an extortion.

The prevalence of unused addresses in the `btc_addresses` table (59,816 out of 59,975 records) can be attributed to the use of a hierarchical-deterministic (HD) wallet (*BIP-32/44*). HD wallet clients maintain a cache with look-ahead keys, which are fresh deposit addresses, enabling the back-end system to instantly provide an address when an affiliate requests a payment address [23]. Consequently, at any given time, thousands of these addresses remain unused. By tracing on-chain activity, we matched actual commission payments to specific addresses in this pool, roughly accounting for 20% of each final negotiated ransom with the victim. This alignment confirms that these pre-generated addresses are indeed controlled by the LockBit operator and serve as the destination for affiliates' 20% commissions.

1) Revenue from Ransom Payments: IV includes the calculated collective revenue from the ransom payments, and individual revenue per each affiliate from the ransom paid. To identify the revenue from ransom payments, we analyzed the `chats` table for successful ransomware transactions. These chats are identified through a negotiation, which culminates in sharing a cryptocurrency address and then a decryptor. We started with a list of 118 companies that we consider successfully deployed builds. The list of companies were de-duplicated to remove identical targeted company websites, as well as test builds. Of those 118, only 81 victims engaged in negotiations, where an initial ransom demand was proposed by the affiliate. We identified 18 addresses from the 81 negotiations that had corresponding payments.

We cross-referenced the `invites` and `btcaddresses` table, confirming there is no overlap or reuse. We then investigated the transactions on the blockchain, confirming that the incoming transactions to that address and transaction amount were consistent with the chat message date. To confirm this, we extracted data from successful chat negotiations and joined it with the `btc_addresses` table based on `target_id/client_id`. The short time gap in address creation - often within one day of each other - supports the hypothesis that the `btc_addresses` table is used exclusively for commission tracking, with affiliates retaining control over the ransom payment addresses.

Six of these addresses appeared to have clear splitting with an address appearing in the `btcaddresses` table, whereas the approximately 20% of the ransom payment was transferred to a LockBit controlled addresss from the table 2. The other ransom payments appear to be consolidated by the affiliate, where small amounts are transferred from one address to another, possibly collecting the funds into a central wallet for redistribution.

Table IV: LockBit Ransomware Operations: High-level data summary

Category	Metric	Count
BTC Addresses	Registrations	73
	Registrations with code "50"	72
	Observed Paid Registrations	12
Payments	Expected Paid Registrations (USD)	56,721
	Observed Paid Registrations (USD)	9,449
BTC Addresses	Ransomware Payments	18
	Commission Payments	18
Payments	Observed Paid Ransoms (USD)	2,455,578
	Observed Paid Commissions (USD)	466,143
Victims	Total Victims	118
	Victims Engaged in Negotiations	81
	Paying Victims	18

The observed paid ransoms from within IV are observed on the blockchain. However, at least one of the negotiations appears to have been truncated due to the database leak, as the timestamp of the chat corresponds to the date of the breach, April 29, 2025. The commission payment address (`bc1qjl6t3wsx6e5cx93q37cg938ypux6zzahpue4k4`) was identified in the `btc_addresses` table and verified on the blockchain, confirming a 20% commission. Through an analysis of addresses with exposure to LockBit, corresponding to the date of the breach +1 day, date of the commission, and a projected amount of the ransom based upon the chat and the commission ($2 million), we were able to identify the address. Subsequently, this payment was the largest ransom payment observed for LockBit 4.0, and changed our understanding of the operation.

2) Revenue Over Time: To assess the ransomware collective's total revenue outside of our observations within the database, we performed a blockchain analysis to uncover additional addresses controlled by LockBit. This analysis leveraged the co-spending heuristic, a robust method for associating multiple addresses with a single entity. The co-spending heuristic identifies addresses that are spent together in a single transaction, suggesting they are controlled by the same actor due to the shared use of private keys [24]. By analyzing transaction patterns, this approach enables the clustering of related addresses with high confidence. We utilized GraphSense, a blockchain analytics tool forked from BlockSci and maintained by researchers at the University of Vienna. For this study, we received complimentary API credits for their cloud-based platform.

Using GraphSense, we queried all addresses listed in the panel leak. A summary of the dataset is presented in Table V.

Table V: Summary of Ransom Payments

Metric	Count
Total Transactions	45
Total Value (USD)	877,162.09
Mean Value (USD)	19,492.49
Median Value (USD)	3,058.76
Min Value (USD)	1.94
Max Value (USD)	401,135.34
Outlier Count	5
Outlier Mean (USD)	131,246.37
Outlier Min (USD)	41,277.58
Outlier Max (USD)	401,135.34

The panel leak dataset includes only addresses from the database dump, covering solely the operation of LockBit 4.0. We also obtained addresses from a proprietary source, which span the entire duration of LockBit's activities and which we used to build Figure 3, to show the decline of LockBit after Operation Cronos.

Figure 3 visualizes the monthly distribution of payments, derived from positive (incoming) transactions to all LockBit address clusters, over time as a boxplot. Each box represents the spread of transaction values for a given month, showing the median, interquartile range (IQR), and overall range (excluding outliers). The X-axis displays months in chronological order, while the Y-axis shows transaction values in thousands of USD. Outliers are hidden for clarity. The plot highlights how the typical transaction size and variability change from month to month, allowing for easy comparison of transaction patterns and the identification of periods with unusually high or low transaction values. The dashed lines highlight specific events in the history of the LockBit affiliates, such as updates to their ransomware strain as well as Operation Cronos.

The plot demonstrates a significant decline in LockBit's revenue following Operation Cronos. The introduction of the panel in December 2024 had minimal impact on increasing revenue, whether from ransoms or affiliate income. The peak in transaction activity observed in April 2025 is caused by outflow of pre-existing cryptocurrency reserves, collected prior to the launch of LockBit 4.0 and predating the panel's operation.

3) Money Laundering: The limited revenue from the LockBit 4.0 panel provides minimal evidence for investigating money laundering activities. However, in April 2025, some affiliates transferred pre-LockBit 4.0 ransom reserves, offering some insight into their financial operations. They utilized several platforms to launder their illicit proceeds. Although most recipient endpoints remain unidentified by our sources, specific affiliates have been linked to transactions involving various exchanges. Affiliate *Christopher* has transferred funds to WhiteBit ($64,182), KuCoin ($99,019), MEXC ($43,512), and HTX ($58,744). Affiliate *JamesCraig* has directed funds to OMG!OMG! ($101), a Russia-based darknet marketplace specializing in narcotics. Similarly, *btcdrugdealer* has been observed sending funds to ByBit ($464), MEXC ($325) and Bridgers ($40), a decentralized swap and bridge platform.

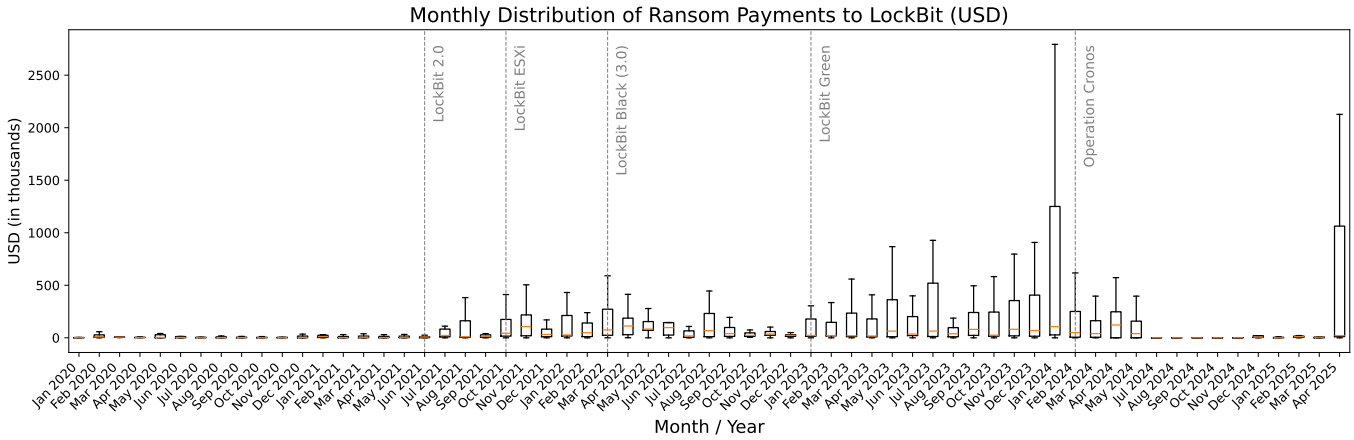

Figure 3: Monthly Ransom Payments to LockBit

Additionally, *Swan* has employed Binance ($8,868), Rapira (a high-risk Russian exchange $242), and FixedFloat (a non-custodial exchange, $117) to launder fragments of the proceeds derived from a single victim.

C. Conversion Analysis

Understanding the operational efficiency of RaaS operations requires systematic analysis of the affiliate workflow, which we established in the first part of the analysis 1. RaaS affiliates must navigate a multi-stage conversion process where each transition point represents operational overhead for client builds and potential revenue loss for failed victim negotiations. The leaked LockBit 4.0 dataset provides visibility into this conversion process, enabling quantitative analysis of performance across the complete affiliate lifecycle.

This section examines the ransomware conversion funnel through a structured framework that we developed, a five-stage process based upon the affiliate workflow 1. By analyzing conversion rates, we attempt to identify the bottlenecks that constrain ransomware revenue generation. These findings have direct implications for understanding ransomware economics, predicting affiliate behavior patterns, and identifying potential intervention points for disruption strategies.

We define the ransomware conversion funnel as a five-stage process:

1) **Build Creation**: Initial compilation of ransomware executable by an affiliate through the LockBit 4.0 builder panel, captured as a record in the `builds` table.
2) **Deployment Success**: The ransomware successfully infects a victim's system, creating a record in the `clients` table. The malware has executed and can communicate back to LockBit's servers.
3) **Communication Establishment**: The victim contacts the attackers after discovering the encryption, shown by the first message for that client in the `chats` table. The victim has found the ransom note and reaches out.
4) **Negotiation**: Active ransom discussions begin. The affiliate presents payment demands, and the victim engages in back-and-forth communication about amounts and timelines.
5) **Payment Completion**: The victim pays the ransom, verified through blockchain transactions and commission records in the LockBit dataset.

To assess the success of the ransomware affiliates, we looked at several metrics:

- **Build-to-Negotiation**: Percentage of ransomware builds that successfully progress to active ransom negotiations with victims. This rate is 75.6% (118 negotiating victims out of 156 successful builds).
- **Communication-to-Payment**: Percentage of victims who initiated communication with an affiliate and ultimately paid the ransom. This rate is 15.3% (18 paying victims out of 118 total victims).
- **User-to-Active Affiliate**: Percentage of registered users who become operational by creating at least one ransomware build. This rate is 72.0% (54 active affiliates out of 75 total users).
- **Payment Concentration**: Percentage of affiliates who successfully received ransom payments out of all registered affiliates. This rate is 13.3% (10 successful affiliates out of 75 total affiliates).
- **Success per Build**: Average number of paying victims generated per ransomware build created. This rate is 0.115 (18 paying victims divided by 156 successful builds).
- **Victims per Affiliate**: Average number of successfully compromised victims per affiliate. This rate is 1.57 (118 total victims divided by 75 active affiliates).
- **Payments per Affiliate**: Average number of paying victims per affiliate. This rate is 0.24 (18 paying victims divided by 75 total affiliates).

While the affilates maintains relatively high user activation rates, massive attrition occurs during the technical deployment phase, with 86.8% of builds failing to achieve successful victim compromise. The most critical bottleneck emerges in the final monetization stage, where the vast majority of suc-

cessfully compromised victims refuse to pay ransoms despite engaging in negotiations.

1) Comparative Analysis with LockBit 3.0: To contextualize the conversion funnel research, we begin with a comparative analysis of the data snapshot published by NCA following the Operation Cronos law enforcement disruption (for details see Appendix, Figure 9). This published data included success metrics of LockBit affiliates from 2022 to 2024 (i.e., LockBit 3.0), which was arguably LockBit's most successful period of operation, as demonstrated through blockchain analysis and review of a scrape of their public ransomware blog from 2020 to the present (see Figure 3).

In our comparative analysis, we compute the same measures and provide the results in Table VI. We have listed the numbers of victim engagement, affiliate success rates, and conversion metrics corresponding to the LockBit 3.0 (data reported by NCA) and the LockBit 4.0 (recent database leak). This comparison between LockBit 3.0 and LockBit 4.0 reveals fundamental differences that impact conversion efficiency metrics and provides critical context for interpreting our funnel analysis results.

Table VI: Comparative Analysis: NCA Operation Cronos published affiliate statistics vs. analysis of LockBit 4.0 leaked dataset

Metric	LockBit 3.0	LockBit 4.0	Difference
Operational Scale			
Total Affiliates	194	75	-119
Total Builds/Attacks	148	156	+8
Builds per Affiliate	0.76	2.08	+1.32
Victim Engagement			
Ransomware Blog Victims	1,876	51	-1,825
Compromised Victims	1,876 + UNK	118	-1,758 + UNK
Communicated Victims	119	118	-1
Paying Victims	80	18	-62
Conversion Rates			
Build-to-Negotiation	80.41%	75.6%	-4.81pp
Comm.-to-Payment	67.23%	15.3%	-51.93pp
Affiliate Performance			
Affiliate Activation Rate	76.3%†	72.0%	-4.3pp
Affiliates with Payments	80	10	-70
Payment Concentration	41.24%	13.33%	-27.91pp
Operational Efficiency			
Success per Build	0.54	0.115	-0.425
Victims per Affiliate	0.76	1.57	+0.81
Payments per Affiliate	0.41	0.24	-0.17

† LockBit 3.0 activation assumes each build → unique affiliate.
pp = percentage-point difference; UNK = unknown; Comm. = Communication.
Negative values indicate declines from 3.0 → 4.0.

LockBit 3.0 deployed 194 affiliates to execute 148 targeted attacks (0.76 builds per affiliate). Conversely, the LockBit 4.0 operation concentrated activity among 75 affiliates who generated 156 builds (2.08 builds per affiliate), indicating a high-volume approach to victim targeting, which was contrasted with lower success rates.

This resource allocation difference correlates with only modest differences in negotiation rates: 80.4% of LockBit 3.0 attacks progressed to victim negotiation compared to 75.6% of LockBit 4.0 attacks. The LockBit 3.0 model's 4.8 percentage point advantage in negotiation conversion suggests that while selective targeting provides some benefit in victim engagement, the difference is relatively small compared to the dramatic disparities observed in later conversion stages.

The comparative analysis reveals divergent affiliate compensation patterns that could be due to underlying business model differences. The LockBit 3.0 operation achieved a 41.2% affiliate success rate, with 80 affiliates receiving compensation from their attacks. In contrast, the LockBit 4.0 operation demonstrated extreme payment concentration, with only 13.3% of affiliates (10 individuals) receiving compensation from 18 paying victims out of 118 compromised victims.

2) Conversion Funnel Performance: Table VII presents the complete conversion funnel metrics for the LockBit 4.0 operation, while Table VIII shows how many affiliates end up converting to a successful ransom payment through the LockBit 4.0 panel.

Table VII: LockBit 4.0 Ransomware Conversion Funnel Analysis

Conversion Stage	Input	Output	Conversion Rate (%)
Build → Compromise (in builds)	1,183	156	13.2 (11.3–15.4)
Compromise → Comm. (in builds)	156	156	100.0 (97.9–100.0)
Comm. → Negotiation (in victims)	118	81	68.6 (58.8–76.4)
Negotiation → Payment (in victims)	81	18	22.2 (14.2–32.8)
End-to-End Conversion	**1,183**	**18**	**1.5 (0.9–2.4)**
Compromise-to-Payment	**156**	**18**	**11.5 (7.2–17.7)**

Note: Values in parentheses represent 95% confidence intervals using the Wilson score method.
Comm. = Communication
Compromise → Commu. assumes all compromised victims were contacted.

The analysis reveals significant attrition at multiple stages, with the most substantial losses occurring during initial deployment (86.8% failure rate) and negotiation-to-payment conversion (77.8% failure rate).

Table VIII: Affiliates' Success Conversion

Metric	Count
Total Users (Dec 18+ registrations)	73
Users with Invite Records	73
Users who Created Builds	54
Users who Received Commissions (Actual Ransoms)	10
Conversion: Invite → Build	54/73 (74.0%)
Conversion: Build → Ransom	10/54 (18.5%)
Overall Success Rate	10/73 (4.1%)

VII. Discussion

Evaluating ransomware intervention effectiveness typically relies on external observables, such as victim leak page activ-

ity, public announcements [25]. However, such metrics cannot distinguish between functional continuation and *degraded continuation*, where groups maintain visible activity despite catastrophic effectiveness collapse. Our internal operational data reveals that LockBit 4.0 appeared active externally (73 affiliates, 1,183 builds, 118 negotiations) yet achieved only 1.5% end-to-end conversion, representing a 4.7-fold decline from LockBit 3.0's 54.1% rate.

Our workflow reconstruction identifies where degradation concentrates. Successful ransom payment requires coordination between affiliates, the administrator, and victims. Affiliates cannot complete negotiations independently—they depend on the administrator to join chats and provide decryption tools. This centralized bottleneck makes the operation vulnerable: disrupting administrator availability disables monetization. While 72% of users create builds (automated, low-skill), only 13.2% successfully compromise victims (requiring technical expertise), revealing a talent pool bottleneck.

Total payments of $2.46M demonstrate extreme concentration: a single $2.1M payment represents 86% of revenue, with 86.7% of affiliates receiving zero compensation. This power law distribution [26], [27] suggests a novel intervention mechanism: *degrading the talent pool* through reputational damage prevents recruitment of sophisticated affiliates. Operation Cronos damaged LockBit's reputation across all dimensions, infrastructure vulnerability, administrator exposure, decryptor releases, creating persistent effectiveness collapse invisible to external observers.

This explains observed patterns in prior work: Meurs et al. found limited displacement post-intervention [25], groups experiencing severe disruption lose organizational capacity to execute attacks regardless of targeting strategy. With 1.5% conversion and 86.7% affiliate failure, the business model appears economically nonviable, demonstrating that intervention effectiveness may be measured by *monetization capability* rather than *visible activity*.

VIII. Related Work

A. Evolution of the Ransomware Ecosystem

The ransomware landscape has undergone significant transformations from commodity malware to sophisticated service-oriented models. Through a crowd-sourced dataset of Bitcoin transactions, this evolution has been traced through an analysis of ransomware payment economies, demonstrating how the ecosystem has shifted from individual operators to organized affiliate networks. This transition fundamentally altered the economics and operational structures of ransomware groups, creating specialized roles and revenue-sharing arrangements that mirror legitimate business models [1], [8].

These business models have been further traced on the blockchain, providing empirical evidence of the transformation by analyzing leaked chat logs and operational data, revealing the internal mechanics of modern RaaS operations and their business processes. Our work extends this understanding by providing detailed conversion funnel analysis of how these affiliate models perform in practice, particularly during periods of operational stress following a law enforcement disruption [6].

B. Blockchain Analysis and Payment Flows

Understanding ransomware financial flows has become critical for both threat assessment and intervention strategies. Through an initial analysis of the Conti ransomware group, extending out to a cluster of addresses likely controlled by a ransomware negotiation, there are identifiable methods to characterize payments across multiple ransomware groups demonstrating how blockchain analysis can reveal operational paterns and affiliate compensation structures [6], [7].

Specialized work has focused specifically on LockBit's payment mechanisms, developing techniques to identify transaction splitting patterns and trace commission payments between operators and affiliates [28]. These methodologies form the foundation of our blockchain analysis, which validates our leaked dataset against on-chain payments evidence and reveals the financial mechanics of LockBit 4.0's degraded operations.

C. Affiliate Networks and Revenue Models

The study of affiliate-based cybercrime has revealed common patterns across different enterprises. For example, deceptive affiliate marketing networks, revealing how criminal organizations recruit and compensate distributors through tiered commission structures. [29]

Understanding the spam value chain through end-to-end analysis how demonstrated how affiliate models enable criminal enterprises to scale operations while distributing risk. These studies establish that affiliate models create inherent tensions between operators and distributors, particularly around payment transparency and performance attribution. Our analysis builds on these insights by quantifying conversion rates and payment concentration patterns within a major ransomware affiliate program, revealing extreme inequality in success distribution that exceeds patterns observed in other criminal affiliate networks [30].

D. Sales Funnel in Criminal Contexts

The application of business analytics to criminal operations provides insights into operational efficiency and resource allocation [31]

The development of frameworks for analyzing and forecasting sales funnels in legitimate contexts establishes methodologies for measuring conversion rates and identifying optimization opportunities. While limited work has applied these techniques to criminal enterprises, the underlying principles of conversion analysis, measuring progression through operational states and identifying failure points, translates directly to understanding cybercrime effectiveness.

Our study represents the first comprehensive application of conversion funnel analysis to a major ransomware operation, revealing systematic inefficiencies and concentration patterns that challenge assumptions about ransomware profitability and operational sophistication.

IX. Conclusion

Our analysis indicates a ransomware operation in decline. The low affiliate entry fee may have strategically been designed to attract less experienced affiliates, as Operation Cronos inflicted reputational damage, prompting the departure of high-profile affiliates. By eliminating vetting requirements and enabling immediate attack capabilities, the LockBit 4.0 program lowered barriers to entry, suggesting LockBit sought to mitigate diminished ransom revenues by expanding its affiliate base. However, the limited adoption panel underscores the constrained potential for revenue generation from signup fees alone.

Acknowledgment

We thank the anonymous reviewers for their insightful and constructive suggestions and feedback. Funding for this work was provided in part by National Science Foundation grants 1844753 and 2039693. AI-assisted coding tools (i.e., GitHub Copilot) were used to generate initial code implementations for data analysis. The authors verified all code correctness and take full responsibility for the final implementation.

References

[1] K. Oosthoek, J. Cable, and G. Smaragdakis, *A tale of two markets: Investigating the ransomware payments economy*, 2022. arXiv: 2205.05028 [cs.CR].

[2] *Allied Universal Breached by Maze Ransomware, Stolen Data Leaked*, en-us. [Online]. Available: https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ (visited on 05/24/2025).

[3] Flashpoint Intelligence Team, "Flashpoint 2025 global threat intelligence report", Flashpoint, Tech. Rep., May 2025, Accessed: 2025-07-24. [Online]. Available: https://flashpoint.io/resources/report/flashpoint-2025-global-threat-intelligence-gtir/.

[4] *United States Sanctions Senior Leader of the LockBit Ransomware Group*, en, Feb. 2025. [Online]. Available: https://home.treasury.gov/news/press-releases/jy2326 (visited on 05/24/2025).

[5] Logix Infosecurity. "Lockbit ransomware attack: Everything you need to know". Accessed: 2025-07-24. (Jun. 2023), [Online]. Available: https://logix.in/blog/lockbit-ransomware-attack/.

[6] I. W. Gray, J. Cable, B. Brown, V. Cuiujuclu, and D. McCoy, "Money Over Morals: A Business Analysis of Conti Ransomware", *2022 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:258298293.

[7] J. Cable, I. W. Gray, and D. McCoy, "Showing the Receipts: Understanding the Modern Ransomware Ecosystem", en,

[8] D. Manatova, C. McGrath, and L. J. Camp, "The Organizational Anatomy of Cybercrime: A Multilayer Framework for Modeling Resilience", *In Review*, 2025.

[9] *The LockBit takedown: Law enforcement 'trolls' ransomware gang*, en. [Online]. Available: https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/ (visited on 05/24/2025).

[10] *Understanding Ransomware Threat Actors: LockBit | CISA*, en, Jun. 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (visited on 05/24/2025).

[11] *Ransomware ads now also banned on Exploit cybercrime forum*, en-us. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-ads-now-also-banned-on-exploit-cybercrime-forum/ (visited on 05/24/2025).

[12] *The moral underground? Ransomware operators retreat after Colonial...* en. [Online]. Available: https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime (visited on 05/24/2025).

[13] A. Sawhney, *10 people gets a LockBit ransomware logo tattooed for $10,000*, en-US, Sep. 2022. [Online]. Available: https://www.thetechoutlook.com/news/security/10-people-gets-a-lockbit-ransomware-logo-tattooed-for-10000/ (visited on 05/24/2025).

[14] C. Cimpanu, "Popular hacking forum bans ransomware ads", *The Record (from Recorded Future)*, May 2021, Accessed on 2025-07-27. [Online]. Available: https://therecord.media/popular-hacking-forum-bans-ransomware-ads.

[15] [LockBit], *[lockbit ransomware]*, Exploit.in Forum, [January 2020]. [Online]. Available: https://forum.exploit.in/topic/166914 (visited on 05/29/2025).

[16] [LockBit], *[lockbit ransomware]*, XSS Forum, [January 2020]. [Online]. Available: http://xsstorweb56srs3a.onion/threads/34426/unread (visited on 05/29/2025).

[17] cms-user26, *International investigation disrupts the world's most harmful cyber crime group*, en-GB. [Online]. Available: https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group (visited on 05/24/2025).

[18] *Office of Public Affairs | Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group | United States Department of Justice*, en, Jul. 2024. [Online]. Available: https://www.justice.gov/archives/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group (visited on 05/24/2025).

[19] S. Hostetler, *Operation Cronos*, en-US, Feb. 2024. [Online]. Available: https://arcticwolf.com/resources/blog/operation-cronos-the-takedown-of-lockbit-ransomware-group/ (visited on 05/24/2025).

[20] T. Reitano. "The lockbit takedown: Law enforcement trolls ransomware gang". Accessed: 2025-07-24, Global Initiative Against Transnational Organized Crime. (Feb. 2024), [Online]. Available: https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/.

[21] [. 3.0], *[affiliate rules]*, LockBit 3.0 Ransomware Blog, [May 2025]. [Online]. Available: http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/rules (visited on 05/29/2025).

[22] *UK's NCA, U.S. DOJ, FBI and Europol Disrupt Lockbit Ransomware Group | TRM Blog*, en. [Online]. Available: https://www.trmlabs.com/resources/blog/nca-doj-fbi-europol-takedown-lockbit-ransomware (visited on 05/24/2025).

[23] T. Thomas, T. Edwards, and I. Baggili, "Blockquery: Toward forensically sound cryptocurrency investigation", *Forensic Science International: Digital Investigation*, vol. 40, p. 301 340, 2022, ISSN: 2666-2817. DOI: 10.1016/j.fsidi.2022.301340. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281722000099.

[24] S. Meiklejohn, M. Pomarole, G. Jordan, *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names", in *Proceedings of the 2013 Conference on Internet Measurement Conference*, Barcelona Spain: ACM, Oct. 2013, pp. 127–140, ISBN: 978-1-4503-1953-9. DOI: 10.1145/2504730.2504747. (visited on 09/17/2022).

[25] T. Meurs, R. Hoheisel, M. Junger, A. Abhishta, and D. McCoy, "What to do against ransomware? evaluating law enforcement interventions", in *2024 APWG Symposium on Electronic Crime Research (eCrime)*, 2024, pp. 76–93. DOI: 10.1109/eCrime66200.2024.00012.

[26] I. Pete, J. Hughes, Y. T. Chua, and M. Bada, "A social network analysis and comparison of six dark web forums", in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2020, pp. 484–493. DOI: 10.1109/EuroSPW51379.2020.00071.

[27] D. Manatova, D. Sharma, S. Samtani, and L. J. Camp, "Building and testing a network of social trust in an underground forum: Robust connections and overlapping criminal domains", in *2022 APWG Symposium on Electronic Crime Research (eCrime)*, 2022, pp. 1–12. DOI: 10.1109/eCrime57793.2022.10142120.

[28] A. Gautschi, "Finding and Analyzing Lockbit Split Transactions on the Bitcoin Blockchain", en,

[29] V. Le Pochat, C. Ballard, L. Desmet, W. Joosen, D. McCoy, and T. Lauinger, "Partnërka in crime: Characterizing deceptive affiliate marketing offers", in *Passive and Active Measurement: 26th International Conference, PAM 2025, Virtual Event, March 10–12, 2025, Proceedings*, ser. Lecture Notes in Computer Science, vol. 15567, Springer, 2025. DOI: 10.1007/978-3-031-85960-1_17. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-85960-1_17.

[30] K. Levchenko, A. Pitsillidis, N. Chachra, *et al.*, "Click trajectories: End-to-end analysis of the spam value chain", in *2011 IEEE Symposium on Security and Privacy*, IEEE, 2011, pp. 431–446.

[31] E. Griva, I. Butorina, A. Sidorov, and P. Senchenko, "Analysis and forecasting of sales funnels", *Mathematics*, vol. 11, no. 1, p. 105, 2023. DOI: 10.3390/math11010105.

X. Appendix

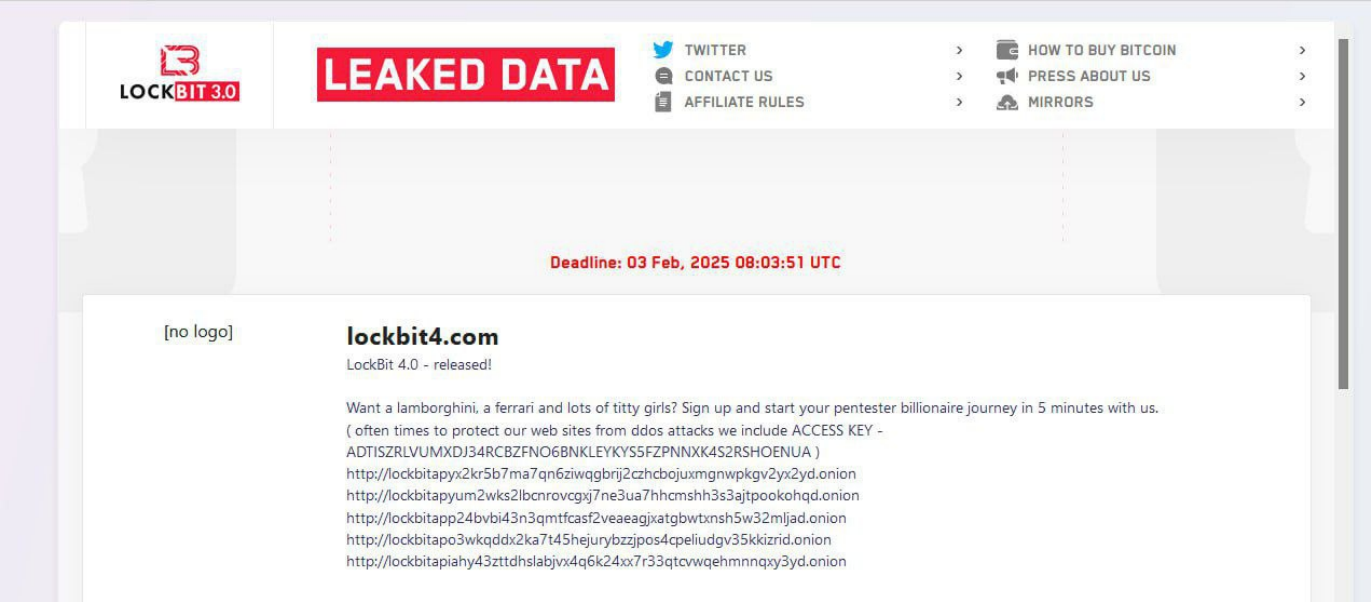

Figure 4: A screenshot of the LockBit 4.0 advertisement from LockBit's ransomware blog

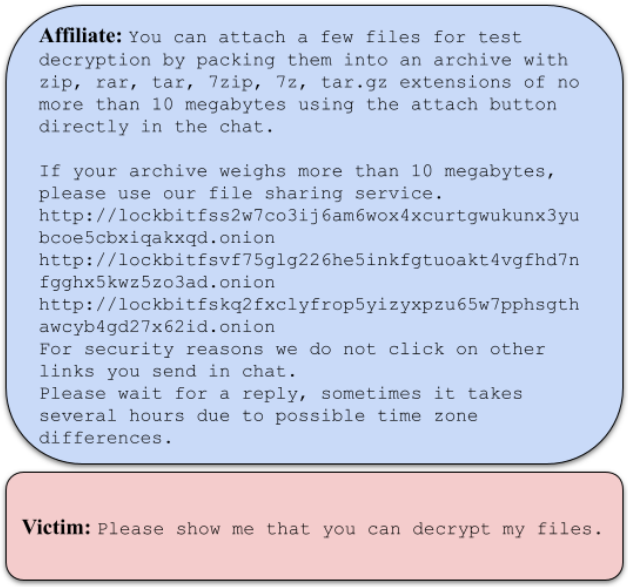

Figure 5: An example of an initial negotiation message created by an affiliate through the build

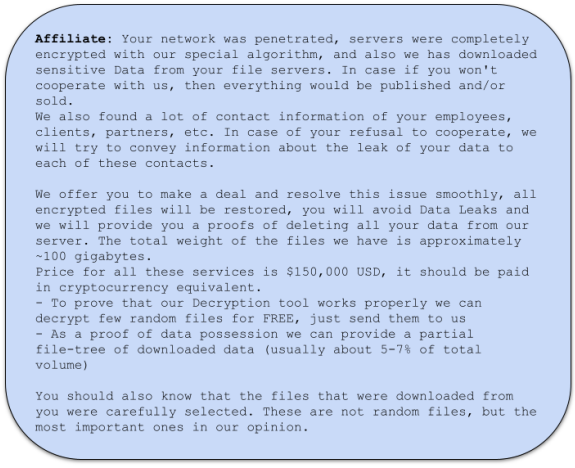

Figure 6: An example of a custom followup message created by an affiliate.

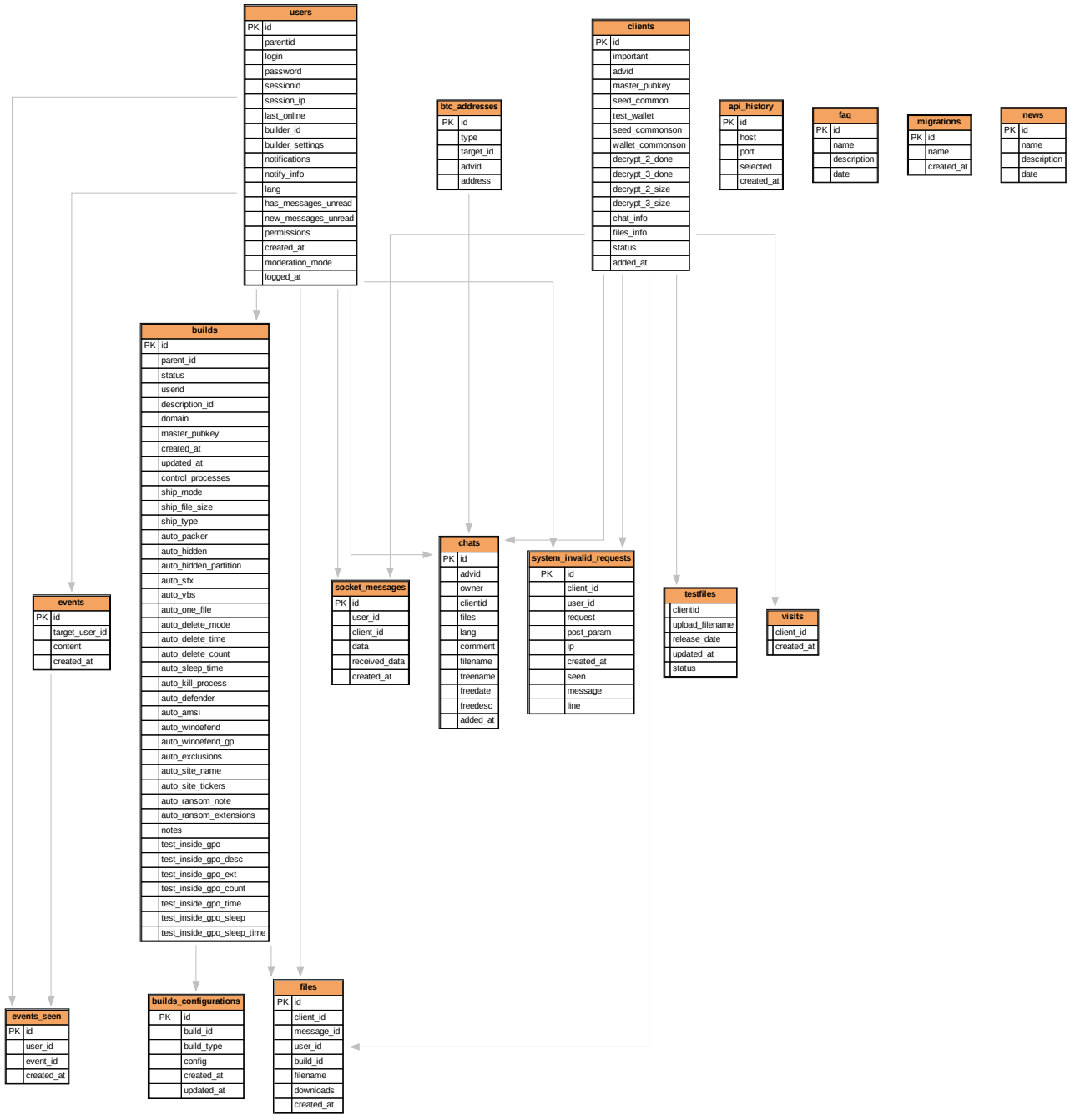

Figure 7: Complete LockBit affiliate panel database entity-relationship diagram. This is a version of the graphic shared by NCA, upscaled and reproduced for readability. The table names are consistent with LockBit 4.0, however some of the field names are different.

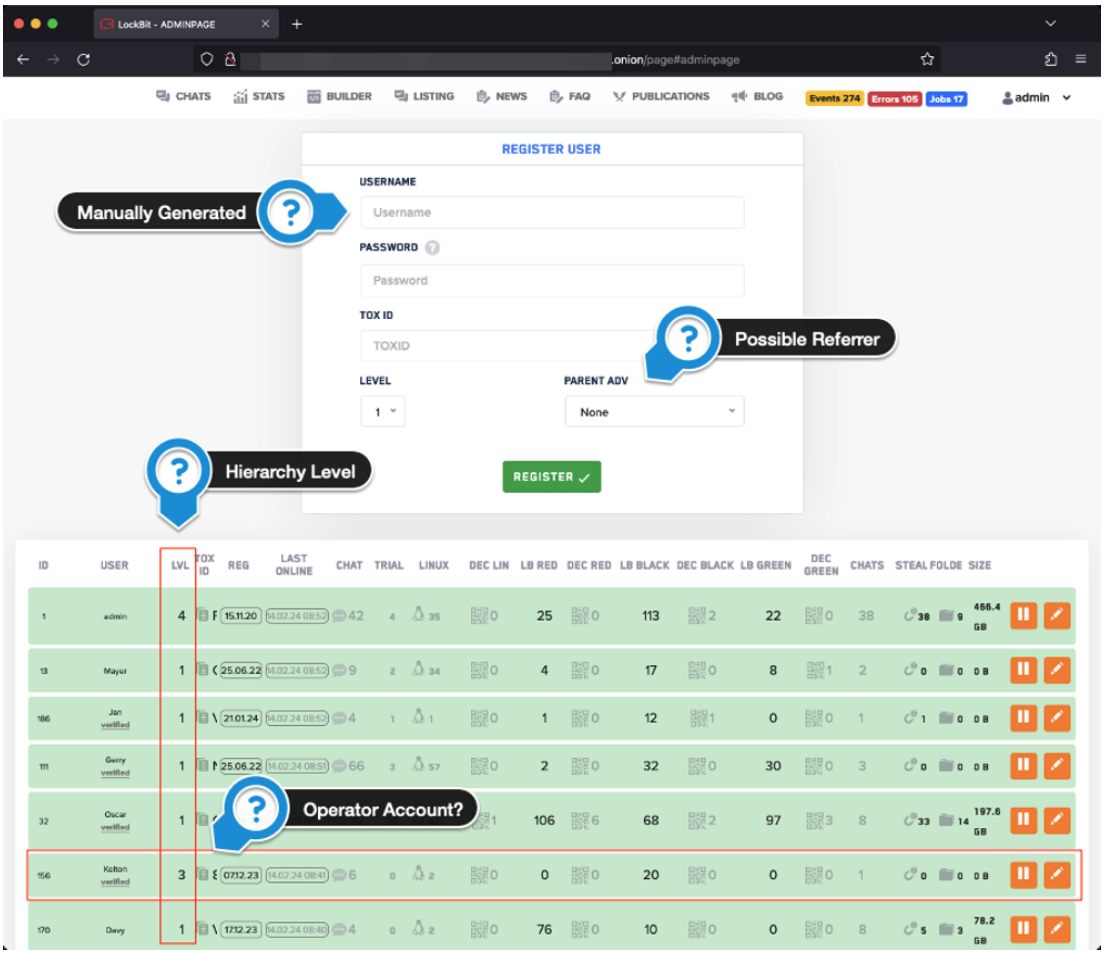

Figure 8: The admin page of LockBit's affiliate panel from LockBit 3.0. NCA posed similar questions about the information input into the panel. The available information validates our current understanding of LockBit the information input into the affiliate panel.

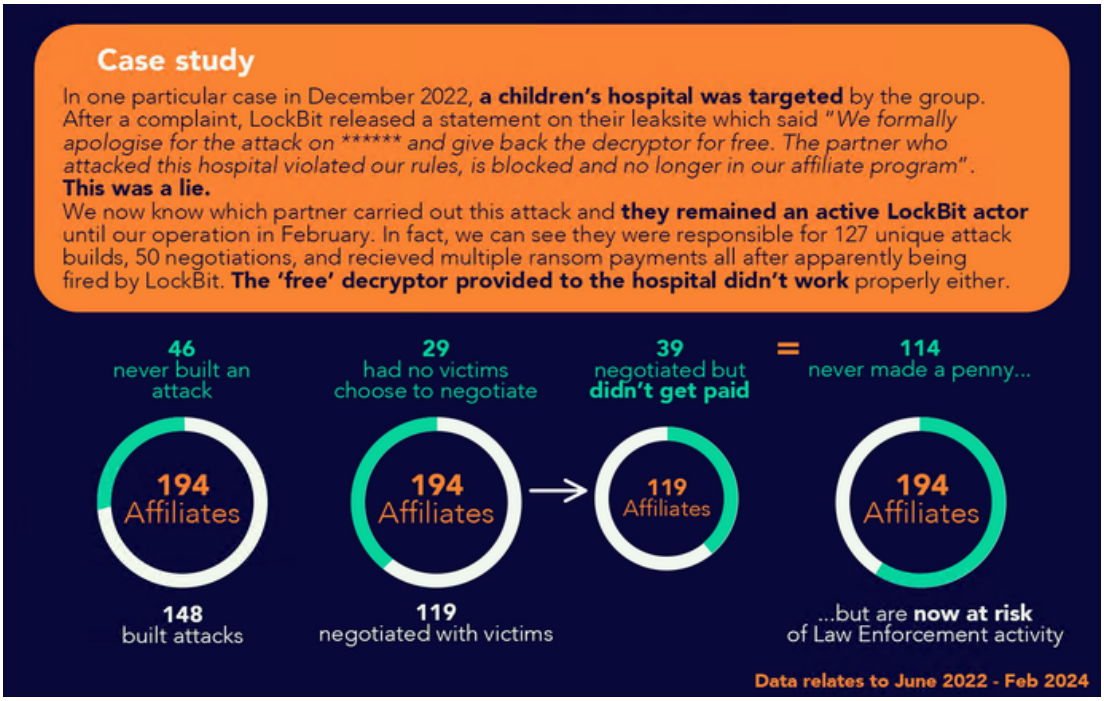

Figure 9: Though NCA only shared this snapshot of the data from LockBit 3.0, the information helped inform our current understanding of LockBit 4.0.

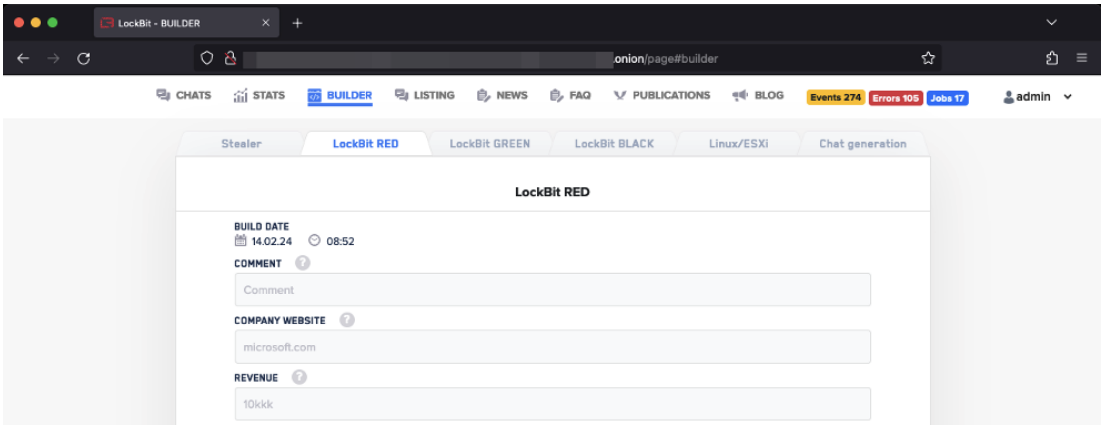

Figure 10: The data from this screenshot verifies that information about the client is input by the affiliate, and potentially prone to error. The various malware variants (ie. build type) can be seen on top of the text box. Additionally, it appears that affiliates have the option to generate the chat separately from build creation.