A Longitudinal Analysis of LockBit 3.0's Extortion Lifecycle and Response to Law Enforcement

***Abstract*—In this study, we present a 532-day longitudinal analysis of LockBit 3.0's leak site. We track 1,856 victims across multiple states—countdown, data publication, deletion, and relisting—and reconstruct a structured, three-stage extortion lifecycle: (1) pre-listing negotiation, (2) countdown negotiation, and (3) post-leak monetization. We find that 8.5% of countdown-state victims are deleted before their data is published, suggesting private settlements. In the post-leak phase, victims with price tags exhibit significantly more variable deletion timing compared to those without, despite sharing the same median exposure. This indicates that LockBit actively manages some listings after data publication, potentially extending monetization or negotiation efforts.**

We also measure the operational impact of law enforcement actions—including Operation Cronos and affiliate arrests—on LockBit's infrastructure and victim activity. While the group rapidly restored services after takedowns, we observe a sustained decline in new victim onboarding, reduced infrastructure redundancy, and delayed payment behavior, suggesting long-term weakening.

To our knowledge, this is the first empirical study to model a ransomware extortion lifecycle based on continuous monitoring of leak site behavior. Our findings provide actionable insights into ransomware monetization tactics, negotiation patterns, and post-takedown adaptation.

***Index Terms*—ransomware, LockBit 3.0, extortion lifecycle**

I. Introduction

LockBit 3.0, also known as LockBit Black, has emerged as one of the most dominant ransomware operations since its reappearance in 2022. Operating under a Ransomware-as-a-Service (RaaS) model, it enables affiliates to launch attacks across diverse sectors including healthcare, finance, and critical infrastructure [1]. By mid-2023, LockBit 3.0 was responsible for over 20% of all reported ransomware incidents [2], with more than 1,000 publicly listed victims [3]. Its extortion infrastructure—which includes a leak site ("blog"), a separate data hosting site, and a private negotiation portal—plays a central role in coercing victims and monetizing stolen data.

While prior research has examined LockBit's payloads, encryption schemes, and infection vectors [4], [5], much less is known about how the group systematically manages victims across different extortion stages, or how it adapts to disruptions such as law enforcement takedowns. Industry reports provide incident-specific snapshots [6]–[8], but longitudinal insights into its operational strategy and monetization lifecycle remain scarce.

In this paper, we present a 532-day longitudinal analysis of LockBit 3.0's darknet infrastructure, spanning from June 27, 2023 to December 10, 2024. We continuously monitor the group's leak site and collect structured data for 1,856 victims, including their status transitions (e.g., countdown, published, deleted, reposted), countdown timer changes, price-tagged listings, and chat log timestamps. This enables us to reverse-engineer LockBit's extortion logic and assess its resilience under external pressure.

Our study is guided by the following research questions:

• **RQ1: How does LockBit 3.0 manage victim transitions across extortion stages, and what do these transitions reveal about negotiation behavior and monetization strategies?** To answer this question, we analyze the movement of victims across three extortion stages: pre-listing negotiation, countdown negotiation, and post-leak monetization. We track deletion events, countdown timer adjustments, and price-tag usage to understand how LockBit maintains leverage at each phase. Our results show that 8.5% of countdown-state victims were deleted before data publication, suggesting possible private settlements. In the post-leak stage, victims with price tags—where a sample of data is shown alongside a monetization interface—exhibited significantly more variable deletion time distributions. This suggests LockBit may continue managing these listings individually, extending monetization opportunities well beyond initial exposure. In addition, we also identify three cases of pre-listing negotiation using chat log timestamps.

• **RQ2: How do law enforcement interventions impact LockBit 3.0's infrastructure, victim behavior, and monetization over time?** We assess the operational and economic impact of law enforcement actions—particularly Operation Cronos in February 2024 and subsequent arrests in October. We observe a decline in victim onboarding, weakened infrastructure redundancy, changes in payment timing, and disrupted monetization flows. These findings offer a rare empirical view of how ransomware groups respond to sustained external pressure.

Contributions.

- We propose a structured, three-stage lifecycle model of LockBit 3.0's extortion process, based on 532 days of leak site monitoring and analysis of victim transitions, ransom deadlines, and price-tags.
- We document the impact of law enforcement interventions on LockBit's infrastructure and extortion economy, revealing long-term degradation in its operational capacity.
- To support reproducibility, we provide an anonymized dataset of 1,856 victims with time-aligned metadata, made available to verified researchers upon request.

This paper provides the first end-to-end, empirically grounded view of LockBit 3.0's extortion lifecycle and its adaptation under pressure. Our findings highlight the value of continuous leak site monitoring as a window into ransomware operations and negotiation behavior.

II. Related Work

Existing research and industry reports have extensively analyzed ransomware operations, particularly the activities of the LockBit ransomware group. Academic studies have largely focused on the technical aspects of ransomware, including infection mechanisms, persistence strategies, and preventive measures. For example, Eliando et al. employed static and dynamic analysis to examine the infection vectors and persistence tactics of LockBit 2.0, proposing technical countermeasures to mitigate its impact [4]. Similarly, Tyagi explored the static, dynamic, and network footprints of LockBit Black ransomware, aiming to generate detection signatures for early identification [5].

Additional technical analyses have been conducted by security vendors. Cybereason's threat report provides a comprehensive analysis of LockBit 3.0's builder and DLL binaries, shedding light on its modular architecture and evasion techniques [9]. CISA's joint advisory with international partners offers a comprehensive threat overview, listing LockBit's TTPs, affiliate structure, and mitigation strategies [10]. These studies offer valuable insights into LockBit's technical execution, but they primarily capture short-term or event-specific snapshots, without addressing the longitudinal evolution of its extortion behavior.

Beyond technical analysis, some academic work has investigated the broader economic and organizational structure of ransomware groups. Gray et al. conducted a detailed business analysis of Conti's internal chat logs, revealing that modern ransomware groups operate like businesses, with dedicated HR systems, team roles, and profit-sharing models [11]. Meurs et al. explored deception and negotiation tactics in double extortion ransomware, shedding light on monetization strategies, but without a longitudinal or infrastructure-level view [12].

Industry reports have further supplemented these perspectives by highlighting high-profile LockBit incidents. Assured's 2024 ransomware report documented law enforcement efforts like Operation Cronos, which temporarily disrupted LockBit infrastructure [8]. However, such reports typically lack follow-up analyses of ransomware groups' adaptations or the long-term effectiveness of takedowns. Other sources, such as JDSupra and Ransomware.live, have analyzed tactics like countdown timers and chat publication as means to pressure victims [13], [14], yet they offer anecdotal rather than empirical insights.

Despite these contributions, prior work leaves key questions unaddressed. While these studies and reports provide valuable perspectives on LockBit's technical behavior and negotiation practices, they lack structured modeling of its extortion lifecycle and empirical tracking of its operations over time. Notably absent are analyses of how victim state transitions, monetization mechanisms (e.g., price-tags), and infrastructure recovery evolve across law enforcement events.

These limitations are not unique to LockBit-related research. Prior academic and industry work on ransomware has largely focused on static malware analysis, payment tracing, or isolated chat leaks—approaches that capture technical or economic aspects but offer limited insight into the behavioral evolution of public extortion strategies. In particular, they provide little visibility into how attacker-controlled leak sites are used to stage pressure, manipulate deadlines, or relist victims over time.

To address this gap, we focus on LockBit 3.0 for two main reasons. First, it was the most active ransomware group at the start of our data collection in 2023, consistently maintaining a high volume of victim disclosures and a stable leak site. Second, LockBit 3.0 uniquely exhibited a three-stage extortion lifecycle: pre-listing negotiation, countdown-based pressure, and post-leak monetization, including interactive options to extend payment deadlines, delete data, or enable downloads. While our analysis focuses on LockBit, our methodology is applicable to other groups that publicly stage victims over time. For example, RansomHub [15], PLAY [16], and Black Basta [17] implement countdown-based leak staging, and more recently, Medusa [18]—now a top ransomware group in 2025—has adopted a similar three-stage model, reflecting LockBit's influence on the broader ransomware ecosystem.

Our work addresses these gaps by conducting a 532-day longitudinal analysis of LockBit 3.0's leak site, negotiation behavior, and infrastructure resilience. We reverse-engineer a structured, three-stage extortion lifecycle and evaluate the group's monetization strategy before and after law enforcement disruptions. Our study provides a perspective on how LockBit 3.0 manages victims, sustains pressure, and adapts under external intervention.

III. Preliminaries

LockBit 3.0 operates through three distinct types of darknet websites, each serving a specific role within its ransomware ecosystem. These components include: (1) the leak site, which serves as the public face of extortion; (2) the data hosting platform, which facilitates the distribution of leaked files; and (3) the negotiation chat portal, used for direct communication with victims. Most of these services are hosted on the Tor network, though sample data is occasionally shared via clearnet file-sharing platforms or non-hidden service domains. Additionally, many of these sites have multiple darknet mirrors that replicate the original content to ensure availability and operational resilience.

A. *Leak Site (also known as blog site)*

LockBit 3.0's primary public infrastructure is its ransomware leak site—referred to internally as its "blog." This darknet site displays victim listings on the homepage and serves as a coercion tool to pressure payment. Victim entries fall into two categories: (1) victims currently in the countdown

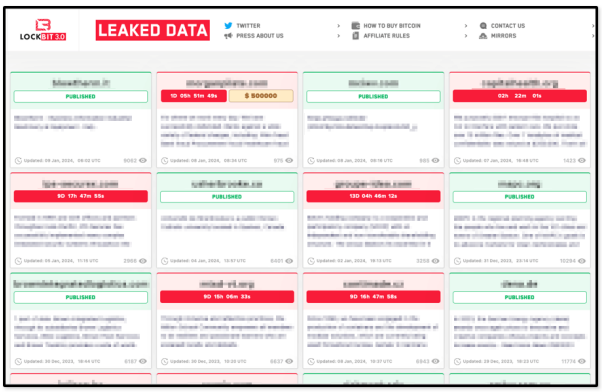

Fig. 1. Homepage of the LockBit 3.0 leak site, where victims are listed with countdown timers, published data, and negotiation outcomes.

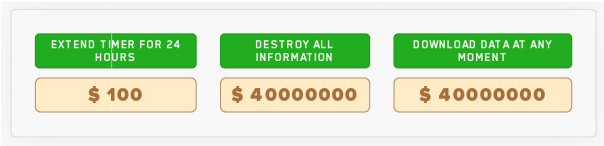

Fig. 2. Example of monetization options shown for leaked data, including buttons to purchase, delete, or extend the data listing—each with a corresponding price.

state, whose data may be published if ransom is not paid, and (2) victims whose data has already been made public.

Figure 1 shows a snapshot of the homepage, where each victim is listed with its current status and associated metadata (e.g., update timestamp, view count, countdown timer, and price-tag status). Among the published entries, some display price-tags offering the option to download, destroy, or extend the listing for a specified fee. These price-tags represent LockBit's attempt to monetize victim data even after initial negotiations have failed.

Figure 2 illustrates the interface for these monetization options, where three buttons—each labeled with a corresponding price—allow visitors to choose an action for the leaked data. Chat transcripts from failed negotiations are also often embedded in individual victim pages, providing additional pressure and public shaming.

B. *Leaked Data Hosting Website*

Separate from the blog, the data hosting website acts as the backend for file distribution. It features a simple interface listing victims' names as folder labels, each linking to the corresponding leaked data. While the blog serves primarily as an extortion threat and negotiation pressure tool, this platform operationalizes the delivery of stolen files to the public or to paying parties.

C. *Negotiation Chat Portal*

The negotiation chat portal is a dedicated portal for private communication between the ransomware operators and their victims. It is used for ransom negotiations, settlement discussions, and threat delivery prior to any public leak. Victims must enter a unique Chat ID, typically provided in the ransom note, to access their communication portal. This chat system plays a central role in LockBit's extortion lifecycle, particularly in the initial negotiation phase that precedes public victim listing (Stage 1). Logs of failed negotiations are sometimes made public and embedded into victim pages on the leak site.

D. *Victim Status Definitions*

Throughout our analysis, we categorize each victim based on their observed status on the leak site at a given point in time:

- **Countdown:** The victim is listed with an active ransom deadline. Data has not yet been made public.
- **Published:** The victim's data has been publicly released on the leak site. "Published state with a price tag" refers to cases where only a sample of the data is shared, as indicated by the accompanying descriptions on the site. LockBit's price-tag interface presents monetization options—such as "Download data at any moment," "Destroy all information," and "Extend timer for 24 hours"—each associated with a specific USD amount. These price-tags are not equivalent to initial ransom demands, but instead function as part of the post-leak monetization strategy. Based on textual cues on victim pages (e.g., "Some of the data from the "victim name" is available at this link for download"), we infer that victims with price-tags are often partially leaked, with the full dataset held back to incentivize further payment. Conversely, victims without price-tags are typically described with language suggesting the data is already fully published.
- **Deleted:** The victim is no longer visible on the leak site. This may reflect ransom payment, a negotiated resolution, or operational cleanup.
- **Relisted:** A previously deleted victim reappears on the leak site after at least one week. This may be an attempt to restore pressure or resume extortion.

IV. Dataset

We collect data from the LockBit 3.0 leak site, leaked data hosting pages, and negotiation chat portals. The following section explains the details of our data collection process.

Leak Site: We systematically monitored the LockBit 3.0 leak site every six hours from **June 27, 2023** to **December 10, 2024**, resulting in a longitudinal dataset of **1,856 victim entries**. Each entry represents a victim organization listed on the leak site and captures both static attributes (e.g., victim name) and dynamic attributes (e.g., update time, countdown). The data was collected by periodically parsing the leak site's HTML content and extracting structured information for each listed victim.

Each victim entry is stored as a JSON object with the following fields:

- `name`: The victim's domain name or organization name as displayed on the leak site (e.g., `"abc.org"`).

- `note`: A descriptive text provided by LockBit about the victim. This often includes a summary of the victim's business or justification for the attack.
- `timelimit`: A structured countdown indicating the remaining time before the victim's data is (or was) scheduled to be published. It includes `days`, `hours`, `minutes`, and `seconds`.
- `price`: The ransom demand, if displayed. It consists of a `value` (which may be `null` if not shown) and a `unit` (typically `"$"`).
- `update`: A timestamp in the format `YYYY-MM-DD HH:MM:SS` showing the last time the leak site updated the status of this victim.
- `views`: The number of views the victim's post received on the leak site.
- `link`: A hyperlink to the victim's dedicated leak post on the LockBit 3.0 site.

We also collected and archived 41 publicly available negotiation chat logs, comprising a total of 1,886 messages. These transcripts, often published after failed negotiations, provided insights into extortion tactics and their timing relative to victim listing events.

Leaked Data Hosting Website: We monitored LockBit 3.0's leaked data hosting site from October 24, 2023 to December 10, 2024 (413 days total). Every 12 hours, we checked the site's availability and recorded the number of listed victims. To ensure ethical compliance, we did not download any leaked files and focused only on site accessibility and listing counts.

Negotiation Chat Portal: We accessed the negotiation chat portal on two specific occasions: (1) February 24, 2024, shortly after LockBit resumed operations following a takedown on February 19, and (2) October 6, 2024, following the arrest of four LockBit affiliates on October 1 [19]. These snapshots allowed us to document structural and design changes in the negotiation interface during periods of operational disruption.

Summary of Observation Periods: Our monitoring covered three components of LockBit 3.0's infrastructure:

- **Leak site (blog website):** June 27, 2023 – December 10, 2024 (532 days)
- **Leaked data hosting site:** October 24, 2023 – December 10, 2024 (413 days)
- **Negotiation chat portal:** Snapshot observations on February 24, 2024 and October 6, 2024

A. *Data Collection Method*

To collect victim and infrastructure data from the LockBit 3.0 leak site, we developed a custom scraping method that operated over the Tor network. Our primary system used Selenium WebDriver [20] in headless mode to load LockBit's .onion domain through a local SOCKS5 proxy, which was served by a Dockerized Tor proxy container [21]. The scraper randomized user-agent strings across 16 commonly observed browser profiles and adjusted viewport sizes (i.e., the visible area of the web page, which influences layout rendering) to mimic diverse real-user environments. We enforced full JavaScript rendering by combining explicit element waits with fixed delays. Once the page was fully loaded, its HTML source was parsed with BeautifulSoup [22] to extract victim metadata and site structure. All components were containerized for reproducibility, and Slack alerts were integrated to notify us of scraping failures, URL changes, or unexpected behavior in real time.

During a brief period when LockBit introduced a CAPTCHA mechanism for site access, we deployed a fallback workflow based on robotic process automation (RPA). This system launched the Tor Browser in GUI mode and used PyAutoGUI [23] to automate navigation, keystrokes, and mouse interactions. CAPTCHA images were captured from the screen, encoded in base64, and sent to OpenAI's GPT-4o model [24], which returned decoded answers in structured JSON format. To increase reliability, we allowed up to five attempts per CAPTCHA, refreshing the image as needed between retries. Once LockBit reverted to a CAPTCHA-free setup, we resumed use of the Selenium-based pipeline.

We used Plotly [25] to create interactive visualizations and Streamlit [26] to present them through a user-friendly web interface for data analysis.

V. Methodology

Our methodology is designed to answer the following research questions:

- **RQ1:** How does LockBit 3.0 manage victim transitions across extortion stages, and what do these transitions reveal about negotiation behavior and monetization strategies?
- **RQ2:** How do law enforcement interventions impact LockBit 3.0's infrastructure, victim behavior, and monetization over time?

A. *Modeling LockBit 3.0's Extortion Lifecycle (RQ1)*

To address RQ1, we group all victims observed on the leak site into two categories—those in the countdown state and those in the published state— and conduct three complementary analyses to model LockBit 3.0's extortion process. Victims were identified using the unique displayed domain name.

*1) **Countdown-Stage Negotiation**:* Group 1 consists of victims listed with an active ransom countdown. We refer to this as the *countdown state*. For these victims, we examine: (a) how many transition from countdown to data publication without deletion, and (b) how many are deleted before the countdown expires. From (a), we estimate the proportion of victims who likely refused to negotiate. From (b), we infer possible negotiation or payment activity during the countdown phase. We also analyze how the countdown timer changes over time, as deadline extensions may signal ongoing negotiations.

*2) **Post-Leak Monetization**:* Group 2 includes victims whose data has already been published, or after transitioning from the countdown state. We refer to this as the *published state*. For this group, we compare the timing of their removal, focusing on differences in deletion time distributions rather than median exposure. This analysis helps us understand how

LockBit treats victims after the sample data is published. In addition, we also studied the distribution and value of price-tagged victims.

To support consistent lifecycle modeling, we apply four key rules in handling victim state transitions, price-tag evaluation, and lifecycle segmentation.

(1) State Transition Rule: Victim status is encoded as a binary sequence, where `0` indicates the countdown state and `1` indicates the published state. Most victims follow a typical transition such as `0, 1`, but some display irregular patterns like `1, 0, 1`. We consider any instance of a `0` → `1` transition during a victim's observed timeline as evidence of a transition from Stage 2 (countdown negotiation) to Stage 3 (post-leak monetization).

(2) Price-Tag Classification Rule: Price-tag presence is also encoded as a binary sequence, where `1` indicates that a monetization interface was present and `0` indicates it was not. A victim is classified as having a price-tag if any part of its observed sequence includes a `1`—e.g., sequences such as `0, 1, 0, 1, 0, 0`, or `0, 0, 1` are all marked as price-tagged. This rule is used for transition and monetization prevalence statistics.

(3) Victim Lifecycle Rule: If a victim disappears and is later relisted, we analyze only its first appearance window for deletion time analysis. For example, if a victim is listed from April 1 to 12 and again from June 5 to 10, only the April 1–12 period is used to compute deletion timing. Deletion time refers to the number of days a victim remains listed on the leak site, measured from its first appearance to its last observed presence, excluding the relisted period.

(4) Post-Leak Price-Tag Rule (for Deletion Analysis): For inclusion in our deletion time analysis, a victim must be in the published state at the time of deletion and must have an active price-tag in its final observed entry. Victims with unstable or missing tag visibility in their final state are excluded from this statistical comparison to avoid misclassification.

*3) **Pre-Listing Negotiation**:* Some victims have chat messages published alongside their leak. By comparing the timestamps of these chats with the first appearance of the victim in the countdown state, we identify cases where negotiation occurred *prior* to listing. If chat timestamps predate the listing, we interpret this as evidence of failed or ongoing negotiations before public exposure.

Together, these analyses allow us to reconstruct LockBit 3.0's extortion lifecycle as a structured, three-stage model:

- **Stage 1: Pre-Listing Negotiation** – Victims engage in private negotiation with LockBit prior to any public exposure. If ransom demands are not met, they may be listed on the leak site.
- **Stage 2: Countdown Negotiation** – Victims appear on the leak site with an active ransom deadline. Public exposure is threatened but not yet executed. We refer to this temporal phase as a *stage*, while their leak-site label (e.g., countdown) is referred to as a *state*.
- **Stage 3: Post-Leak Monetization** – Victims' data is published. Some entries include price-tags offering options for purchase, deletion, or extension. This reflects continued monetization attempts beyond the initial extortion.

In this paper, we use the term *stages* to represent the attacker's intended phases in the extortion lifecycle, while *states* refer to our empirical classification of a victim's condition at a point in time on the leak site (e.g., countdown state, published state).

B. Assessing Law Enforcement Impact (RQ2)

To answer RQ2, we assess how external pressure—especially law enforcement actions—affects LockBit 3.0's operational behavior and monetization outcomes. Our analysis focuses on four key dimensions that reflect the group's resilience, adaptability, and economic fragility.

*1) **Victim Listing Dynamics**:* To analyze victim listing dynamics, we visualize the LockBit leak site data collected every six hours, categorizing each victim by their stage at the time of each crawl—either in the *countdown* state (listed with an active ransom deadline) or the *published* state (data has been leaked). We also track whether victims were deleted from the site and later re-listed. We define such cases as *relists*, where a victim is considered relisted if it was deleted and reappeared on the site at least one week later.

*2) **Infrastructure Resilience**:* By analyzing the changes of the leak site domain migrations, and access restrictions (e.g., CAPTCHA, passwords), we evaluate how quickly LockBit can recover and restore critical services.

*3) **Victim Payment Behavior**:* We analyze timing patterns of victim removals—particularly those occurring before countdown expiration—to infer shifts in perceived credibility or coercive power.

*4) **Economic Disruption**:* We measure the impact of takedowns on LockBit's monetization potential by examining the fate of price-tagged victims (e.g., whether they are deleted, relisted, or leaked for free).

Together, these dimensions help us evaluate not just short-term disruptions but long-term weakening in LockBit's extortion economy. To support consistency in our measurement, we applied operational definitions to detect deletion, relisting, and duplication in Section III-D.

VI. Results

A. RQ1 Results: Victim Management Across Extortion Stages

Based on the following analyses, we reconstruct a three-stage extortion model of LockBit3.0, as illustrated in Figure 3. This model captures the progression of victims through distinct stages: (1) pre-listing negotiation, where LockBit may attempt to settle privately before public exposure; (2) countdown negotiation, where a visible deadline pressures victims into payment; and (3) post-leak monetization, where leaked data is assigned price-tags for sale or deletion. Figure 3 visualizes these stages alongside potential outcomes—such as victim removal at each stage—and highlights the structured nature of LockBit's extortion process.

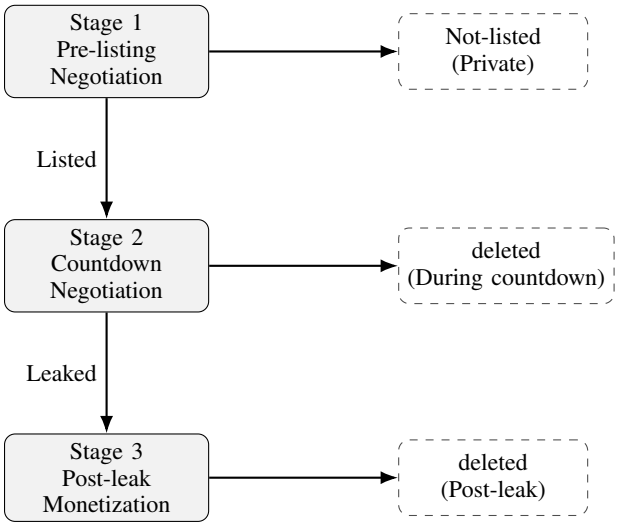

Fig. 3. Figure 3. LockBit 3.0's three-stage extortion lifecycle. Each stage reflects an attacker-driven phase: (1) pre-listing negotiation, (2) countdown negotiation, and (3) post-leak monetization. Arrows represent possible transitions between states on the leak site (e.g., countdown, published, deleted, relisted), and gray boxes indicate possible removal points.

1) ***Results of Countdown-Stage Negotiation****:* Out of the 1,856 victims collected from the LockBit 3.0 leak site, 981 were initially observed in the countdown state. These constitute Group 1 in our analysis. Among these, 853 victims (86.9%) progressed from countdown to data publication, suggesting no apparent interruption in the extortion process. The remaining 128 victims (13.0%) were deleted during the countdown state. Of these, 45 were deleted immediately after the law enforcement Operation Cronos. Excluding these, 83 victims (8.5% of the countdown-stage group) were deleted during the countdown phase under normal conditions. This suggests that while most victims remain listed until publication, a small but significant fraction may resolve the extortion privately. While payment is one plausible explanation, alternative possibilities include attackers deeming the data non-valuable or removing entries for operational reasons.

Deadline Adjustments: Table I details how LockBit 3.0 altered ransom deadlines for 304 victims of a total of 981 victims of the countdown state. While most extensions were brief, the presence of 83 shortenings suggests strategic use of countdowns to escalate urgency or penalize negotiation failure.

2) ***Results of Post-Leak Negotiation****:* The published-state group, corresponding to Group 2 in our analysis, consists of 1,728 victims. This includes 853 victims who transitioned from the countdown state to the published state during our monitoring period, and 875 victims who were observed in the published stage from the outset. We excluded 875 victims from the post-leak deletion time analysis for the following reasons. Of these, 789 victims were already in the published state at the very start of our monitoring period (Day 0), meaning their prior transitions through the countdown phase were unobservable. The remaining 86 victims first appeared after the start of our monitoring but were already in the published state upon first observation, making it impossible to observe their transition from countdown negotiation to post-leak monetization. Because our analysis aims to model victim transitions across extortion stages, including timing from initial listing to deletion, we excluded these 875 cases due to the lack of observable transition history.

TABLE I
FREQUENCY OF RANSOM DEADLINE MODIFICATIONS ACROSS 304 VICTIMS. MOST ADJUSTMENTS INVOLVED SHORT EXTENSIONS (UNDER 12 HOURS), BUT 83 VICTIMS SAW SHORTENED DEADLINES—LIKELY AS PRESSURE TACTICS OR TO PUNISH NEGOTIATION DELAYS.

Adjustment Duration	Number of Cases
Deadline shortened	83
Up to 12 hours	92
12h–1 day	5
1–3 days	44
3–7 days	30
1–2 weeks	25
2–4 weeks	16
More than 1 month	9

Out of the 853 victims, we excluded 409 that disappeared immediately after the Operation Cronos takedown, assuming their removal was due to the enforcement action. The remaining 444 victims were retained for deletion time analysis. In the post-leak phase, deletion time reflects how long a victim remains listed after data publication. It serves as a proxy for LockBit's monetization strategy, where shorter durations may imply resolution or abandonment, while longer durations—especially for price-tagged victims—may reflect ongoing extortion attempts.

Among 444 published victims analyzed for deletion timing, 427 had no price tag, while 8 displayed monetization interfaces. The remaining 9 victims exhibited erratic or intermittent price-tag behavior—such as fluctuating tag presence or changing monetization buttons—and were excluded from the statistical comparison to maintain consistency.

To evaluate whether the presence of a ransom demand (i.e., a "price tag") was associated with differences in the duration of data exposure on leak sites, we compared the time to deletion between two groups: victims with a price tag and victims without one. We used the Mann–Whitney U test to assess statistical differences between the two groups, as the data were non-normally distributed.

Although the median deletion time was the same for both groups (7 days), the distribution of deletion times was significantly different ($U = 216.0$, $p = 0.0019$). Victims without price tags were typically removed in a predictable window, with an interquartile range (IQR) of 8.00 days and a standard deviation of 14.19 days [27]. In contrast, price-tagged victims—though fewer in number—exhibited greater relative variation, with an IQR of 6.25 days and a standard deviation of 22.58 days. Some price-tagged listings persisted for up to 69 days. This suggests that the presence of a price tag does not necessarily shorten or extend the median exposure time, but it affects the distribution, potentially increasing variability.

Figure 4 revealed that while victims without price tags

tended to be deleted in a more consistent timeframe, victims with price tags showed greater variation in deletion time compared to those without, despite sharing the same median exposure (7 days). This indicates that LockBit does not treat all published victims uniformly, but likely tailors in its handling based on monetization potential. Some victims may face prolonged exposure as LockBit attempts to extract late-stage payments, while others may be quickly removed if negotiations resume. This challenges the conventional assumption that data publication ends the extortion cycle. Instead, it suggests that LockBit continues to manage victim pressure even after leaks, reinforcing the need for post-leak response protocols and ongoing threat monitoring from defenders.

This may reflect different extortion or negotiation strategies employed by attackers when a ransom value is explicitly attached.

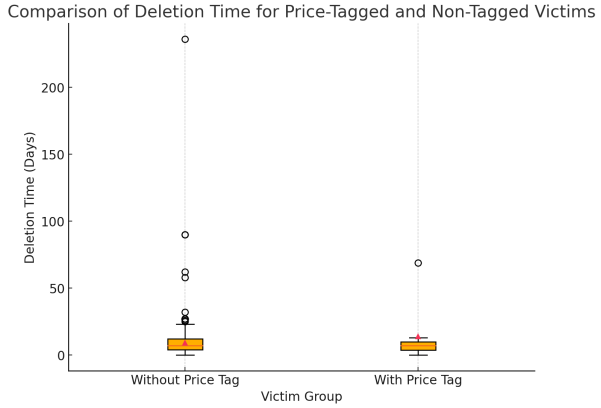

Fig. 4. Boxplot comparing the time to deletion for victims with and without price tags. Each box represents the distribution of deletion durations (in days) for two groups of victims listed on the ransomware leak site. While both groups share the same median deletion time of 7 days, the distribution differs significantly ($p = 0.0019$, Mann–Whitney U test). Victims with price tags exhibit greater variability, suggesting differing extortion or negotiation dynamics.

Price-Tags Analysis Results: These offer options for data deletion or purchase. As shown in Figure 5, LockBit 3.0 assigns widely varying price-tags to leaked data, ranging from $14,000 to nearly $40 million. These figures may reflect the group's valuation of victim importance or expected willingness to pay.

*3) **Results of Pre-Listing Negotiation**:* By comparing the timestamps of negotiation chat logs with the first appearance of victims in the countdown state, we identify three cases where LockBit engaged in private negotiations prior to public exposure. Although LockBit3.0 has published only 41 negotiation transcripts in total—limiting the scope of this analysis—we were still able to find three clear instances of pre-listing negotiation. As illustrated in Figure 6, chat logs for these victims began up to 10 days before they were listed on the leak site. This provides concrete evidence of LockBit's attempts to negotiate privately before initiating public extortion.

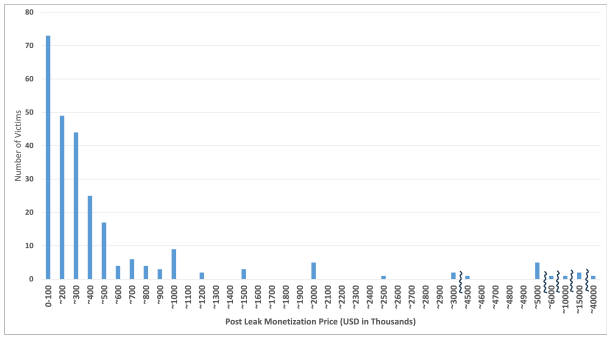

Fig. 5. Histogram of price-tags assigned to published victims by LockBit 3.0. The x-axis represents the ransom amount (USD in thousands), and the y-axis indicates the number of victims offered at each price point. Prices range from $14,000 to nearly $40 million, with a concentration around $1 million. This variation reflects LockBit's internal valuation of victims, likely based on perceived organizational value, industry sensitivity, or negotiation leverage. Such pricing patterns suggest active monetization strategies in the post-leak phase.

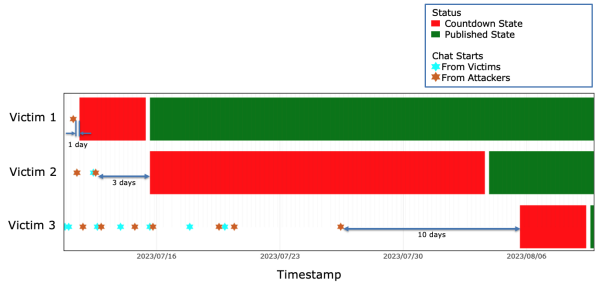

Fig. 6. Timeline of chat activity for three victims whose ransom negotiations began prior to their appearance on the leak site. Colored bars represent blog states (red = countdown, green = post-leak), and stars indicate message timestamps from attackers (orange) or victims (cyan). This confirms the presence of Stage 1 (pre-listing negotiation).

B. RQ2 Results: Impact of Law Enforcement Interventions

To understand how LockBit 3.0 responds to external pressure, we analyzed changes in victim listing dynamics, infrastructure resilience, victim payment behavior and economic disruption.

*1) **Victim Listing Dynamics**:* Figure 7 provides a longitudinal view of victim state transitions. Immediately after the February 2024 takedown, LockBit's leak site went offline for several days. Victim listings dropped sharply during this period, especially in the countdown state (red bars), which represents active ransom deadlines.

Following the takedown, LockBit gradually restored its infrastructure and reinitiated victim postings. On May 10, 2024, we observed a surge in new countdown victims and relisted victims, including both countdown (dark red) and published (dark green) entries. This suggests a recovery strategy aimed at reasserting control and applying pressure on previously targeted victims.

Later in the year, coordinated law enforcement activity led to the arrests of several LockBit affiliates. Following the August 2024 arrests [28], we observed a plateau in new victim activity. A more pronounced impact followed the October 1

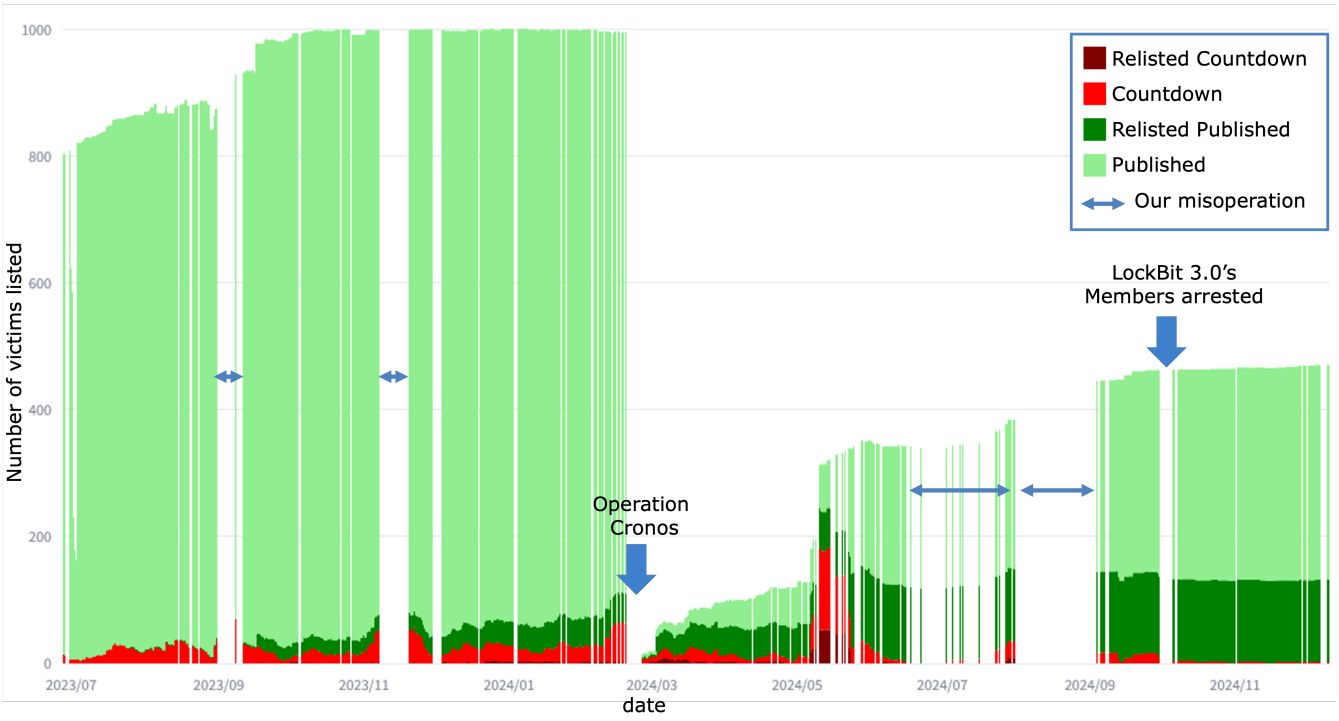

Fig. 7. Longitudinal breakdown of victim activity on LockBit 3.0's leak site over 532 days. Countdown-stage listings (red) dominate early activity, followed by spikes in relisting (dark red/green) and a sharp post-takedown decline. This figure illustrates LockBit's listing strategy and recovery attempts.

arrests [19], [29], after which the number of newly listed countdown victims declined sharply and continued to fall.

These trends suggest that while LockBit showed resilience in the short term, sustained law enforcement pressure contributed to long-term operational degradation.

*2) **Infrastructure Resilience**:* LockBit 3.0 maintained three core darknet services: a leak site, a leaked data hosting website, and a private chat portal. Each operated with multiple mirror URLs. Operation Cronos successfully took down the blog and chat servers on February 19, 2024, but the data hosting server remained online.

Leak Site: During our 532-day monitoring period, LockBit 3.0 changed the domain pattern of its leak site five times and adjusted the number of mirrors in response to operational disruptions and law enforcement pressure. From June 27, 2023, until the February 19, 2024 takedown, the site operated under the domain prefix http://lockbitapt* with 9 mirrors. After the takedown, the group relaunched on February 24 using http://lockbit[#]* with 7 mirrors. In August 2024, this was replaced with http://lbb*, which expanded to 20 mirrors—its largest mirror set—possibly reflecting an effort to strengthen redundancy.

On October 1, 2024, following the arrest of key LockBit members, the group again changed domains to http://ll* with a reduced mirror set of 10. Just a few days later, on October 7, it reverted back to http://lockbit[#]*, maintaining 7 mirrors until the end of our monitoring on December 10, 2024. This cyclical return to a previous domain suggests that LockBit maintains fallback infrastructure and is capable of restoring earlier server configurations when needed.

Importantly, all mirror sites hosted identical content. This indicates that the mirrors are not independent servers but rather synchronized replicas, designed to ensure continuous accessibility even if individual URLs are taken offline.

LockBit also introduced access restrictions after the takedown. In June 28 2024, CAPTCHA and password protection were added to the blog site to deter scraping and surveillance. The password (a private key) was shared via the vx-underground Twitter account [30]. These protections were later removed in October, likely to improve usability for affiliates and buyers.

Leaked Data Hosting Website: Throughout the 413-day (from October 24, 2023, to December 10, 2024) monitoring period of LockBit 3.0's leaked data hosting website, the number of victims remained nearly constant at around 708. This behavior confirms that the data hosting site serves as a static archive, separate from daily extortion and negotiation workflows, and plays a symbolic as well as functional role. Notably, this hosting site was not targeted during Operation Cronos.

Negotiation Chat Portal: We captured snapshots of the negotiation chat portal on two key occasions: first on February 24, 2024, when LockBit 3.0 resumed operations following the takedown, and again in October 2024 after the arrest of four LockBit affiliates. The chat portal and its mirror infrastructure were fully rebuilt after the February disruption, initially launching with 7 new mirrors. By October, this number had expanded significantly to 27, reflecting LockBit 3.0's

continued investment in redundancy and operational recovery.

*3) **Changes in Victim Payment Behavior**:* Law enforcement pressure not only disrupted infrastructure but also affected victim decision-making. Figure 8 shows the distribution of ransom payments (as inferred from victim removals before countdown expiration) relative to the deadline. Before the takedown, payments occurred across a broad time window, including many early payments (more than 10 days before the deadline). After the takedown (Figure 9), this pattern changed: payments became concentrated within the final five days, with almost no early payments. This shift suggests that victims perceived LockBit's threats as less credible and delayed payments, adopting a "wait-and-see" approach.

We confirmed this behavioral shift using the Mann–Whitney U test, which found a statistically significant difference in removal timing distributions between the pre- and post-takedown periods (U = 3210.5, p = 0.00189). This result supports the hypothesis that law enforcement action diminished LockBit's coercive influence on victims.

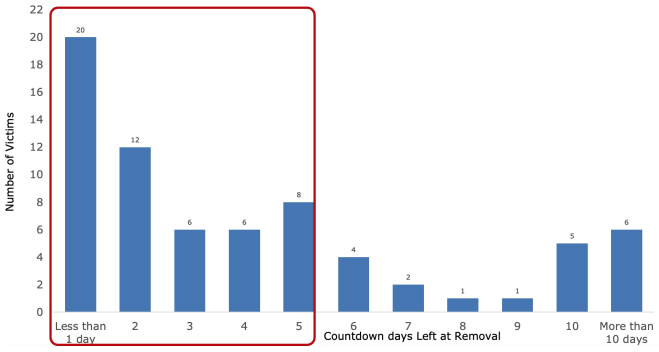

Fig. 8. Distribution of victim removals before Operation Cronos. Payments are spread across a wide time range, with many occurring more than 10 days before the countdown expired.

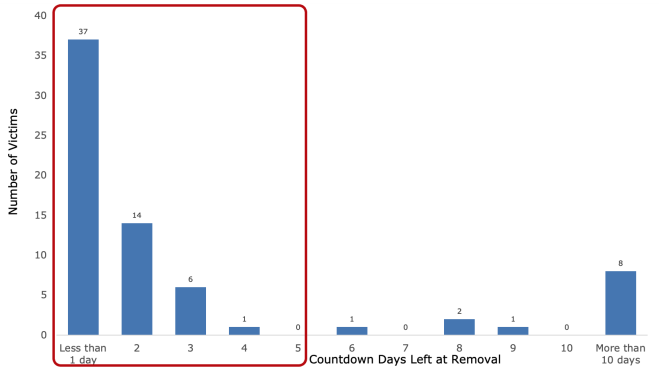

Fig. 9. Distribution of victim removals after Operation Cronos. Payments cluster tightly within the final 5 days of countdowns, suggesting increased victim hesitation and reduced perceived pressure.

*4) **Economic Disruption**:* To assess the financial impact of Operation Cronos, we analyzed how price-tagged victims were affected. Prior to the February 2024 takedown, 83 victims were listed with price-tags, representing ongoing monetization attempts. These price-tags ranged widely in value, with an average demand of approximately $905,000.

Of these 83 victims, 77 were not relisted after the takedown. This suggests that the intervention may have spared them from further exposure or delayed extortion. However, 6 victims—labeled A through F in Table II—were re-listed on the blog without price-tags. In these cases, their data was likely published freely, indicating a shift from monetization to punitive exposure. We also found a case G for which victim was newly assigned a price-tag post-takedown, despite not having one prior. The reason for this remains unclear.

This pattern highlights a nuanced consequence of law enforcement intervention: while the takedown successfully disrupted a majority of LockBit's monetization attempts, it may have unintentionally increased the severity of data exposure for a small subset of victims. The removal of price-tags suggests a loss of economic leverage over these victims, leading the attackers to leak the data publicly without financial gain. These cases underscore that although takedowns can reduce ransomware revenue, they may also result in uneven outcomes across victim populations.

TABLE II
LIST OF VICTIMS ORIGINALLY POSTED WITH PRICE-TAGS BEFORE THE FEBRUARY 2024 TAKEDOWN AND LATER RE-LISTED WITHOUT PRICE-TAGS. THIS SUGGESTS THAT LOCKBIT 3.0 MAY HAVE SHIFTED FROM MONETIZATION TO PUNITIVE EXPOSURE FOR THESE VICTIMS.

Victim	Price before takedown	Price after takedown
A	$800 000	–
B	$59 999	–
C	$2 000 000	–
D	$2 500 000	–
E	$1 500 000	–
F	$4 999 999	–
G	–	$300 000

VII. CASE STUDY: ANALYSIS OF VICTIM GEOGRAPHY AND INDUSTRY

To explore whether certain organizational characteristics are associated with a victim's likelihood of being removed from LockBit's leak site during the ransom countdown phase, we analyzed two structural attributes: geographic location and industry sector. This section outlines the data collection and labeling process, summarizes observed trends, and highlights limitations.

A. *Data Collection and Labeling*

We began with 981 victim domains from our longitudinal monitoring dataset, including 853 victims whose data were eventually published and 128 who were removed during the countdown phase and never reappeared. To enrich this dataset with metadata on industry and location, we used two complementary approaches:

- **Apollo.io API:** For each domain, we queried the Apollo.io platform to retrieve company-level metadata, including industry and country information. This process yielded usable results for 776 out of 981 victims [31].

- **GPT-4 Inference:** For the 205 victims lacking metadata from Apollo.io, we used OpenAI GPT-4o [24] to infer each organization's industry and country. The model was provided with the descriptive `note` field (see Section IV) extracted from the LockBit leak site and instructed to select the most appropriate industry from a predefined list of 112 categories derived from the Apollo results. The prompt was explicitly structured to request a JSON-formatted output to facilitate parsing. A temperature of 0.2 was used to reduce generation variability. The model was called programmatically using the OpenAI API. Figure 10 shows the prompt format used for each classification.

```
Choose the most appropriate industry
from the list below and infer the
country of the company from the note.
Industry List: {industry list}
Company Note:
""" {note} """
Output in JSON format:
{ "industry": "...", "country": "..." }
```

Fig. 10. Prompt used to infer industry and country from LockBit victim note using GPT-4o.

This approach enabled consistent classification while addressing missing values in a structured manner. We manually reviewed a subset of the model's outputs to ensure plausibility and semantic alignment.

Evaluation of Inference Accuracy: To assess the reliability of these labels, we randomly sampled 50 victim entries (40 Apollo-labeled, 10 GPT-4-labeled) and manually validated their industry and country assignments using external sources such as LinkedIn and company websites. For country, all 50 entries were accurate. For industry, 47 out of 50 were correct: two GPT-4-labeled entries and one Apollo-labeled entry were found to be inaccurate. These results indicate high reliability, though not perfect, and suggest GPT-4 inference is broadly suitable for supplementing structured data gaps when guided by constraints.

B. *Location-Based Trends*

Figure 11 presents the percentage of victims removed during the countdown period by country, limited to countries with at least five victims in our dataset. Countries such as South Africa (30%), the United Arab Emirates (29%), and China (22%) exhibit relatively high proportions of deletions, whereas others such as Japan, Singapore, and Germany showed no removals in our data.

These patterns may reflect regional differences in negotiation behavior, regulatory context, or victim response policies. However, the underlying reasons for deletions remain opaque, and no causal claims are made. It is also worth noting that countries showing a 0% removal rate may not necessarily indicate a lack of negotiation activity. One possible interpretation is that some victims from these regions could have engaged

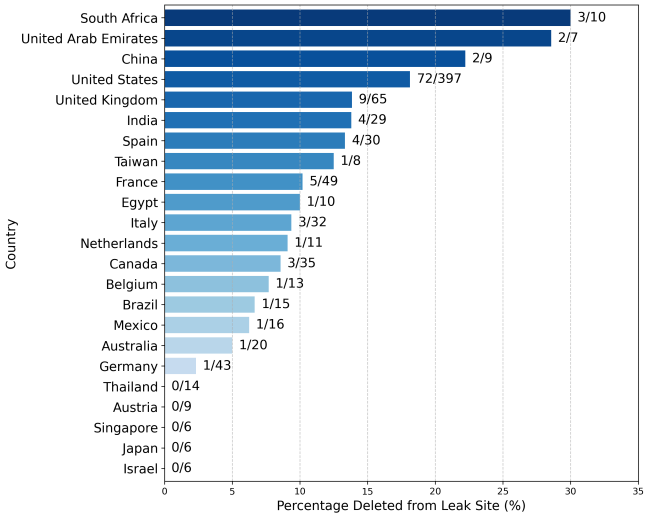

Fig. 11. Percentage of victims deleted during the countdown period, grouped by country. Only countries with at least five victims are shown.

in successful negotiations or payments prior to being publicly listed (i.e., prelisting), thereby avoiding appearance in the countdown phase altogether. While this remains speculative, it highlights the importance of recognizing that the leak site data reflects only a subset of the full extortion lifecycle.

C. *Industry-Based Trends (Raw Categories)*

Figure 12 shows the deletion rates for raw industry labels with five or more victims. These categories are based on either Apollo metadata or GPT-4 inference using a shared label list of 112 industry names. Examples with higher deletion rates include *financial services*, *farming*, and *airlines/aviation*.

While informative, these raw categories can be overly granular or inconsistently defined, complicating interpretation across sectors.

To enhance clarity, we grouped the 112 raw industry labels into 20 broader sectoral clusters (e.g., *machinery*, *construction*, and *semiconductors* were grouped into *Manufacturing & Industrial*). This consolidation was designed to retain semantic alignment while improving interpretability.

Figure 13 presents the deletion rates by grouped industry category. Sectors such as *Finance* (23%), *Automotive & Transportation* (22%), and *Real Estate* (17%) show higher proportions of countdown deletions, potentially indicating greater willingness or capacity to negotiate prior to publication. By contrast, some sectors such as *Security* or *Marketing & Advertising* had no observed deletions in our dataset.

D. *Interpretation and Limitations*

These analyses provide a descriptive view of how organizational context may relate to extortion outcomes. However, several limitations apply:

- **Label Reliability:** Although most metadata labels were accurate, both Apollo and GPT-4 inference may contain

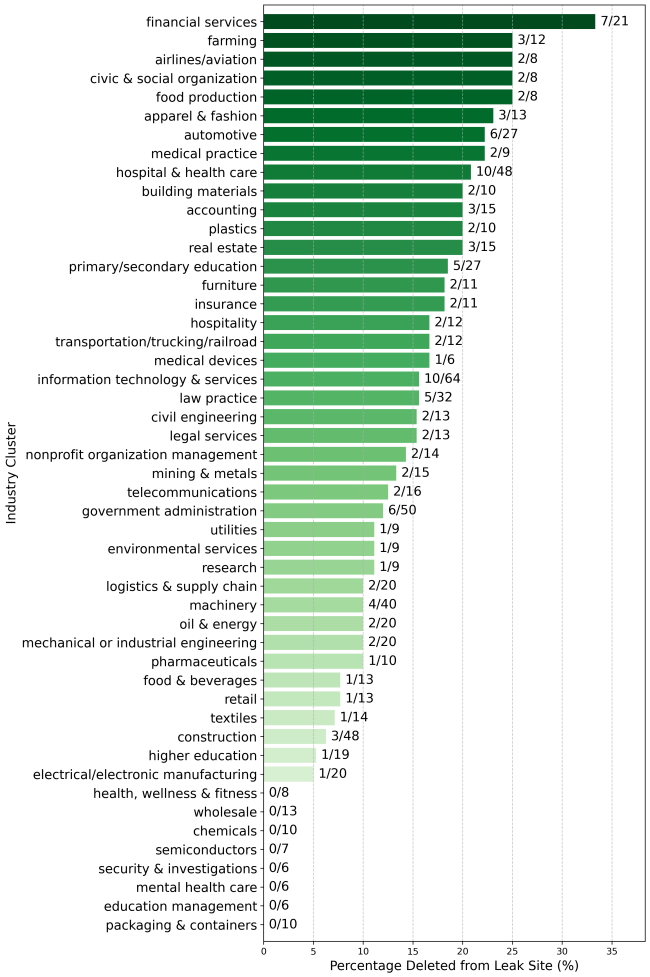

Fig. 12. Percentage of victims deleted during the countdown phase by raw industry label. Only industries with at least five victims are included.

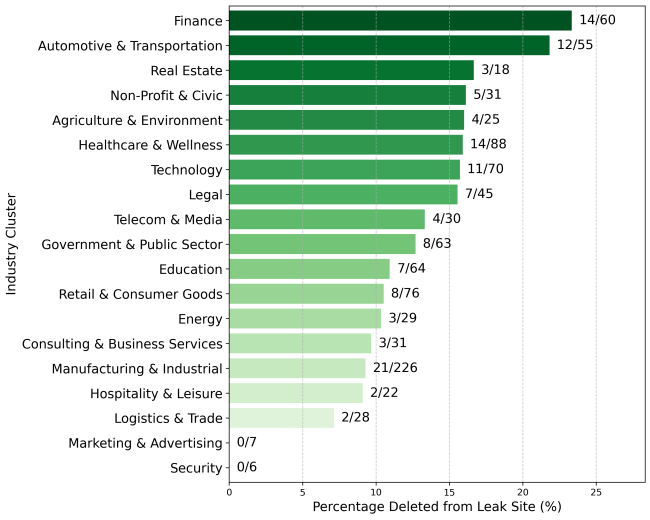

Fig. 13. Percentage of victims deleted during the countdown phase by grouped industry cluster. Only groups with at least five victims are shown.

errors. Caution is warranted, especially for edge cases or ambiguous company names.

- **Unobserved Factors:** We cannot determine the exact reason a victim was removed from the site. Deletion may imply ransom payment, negotiation success, or other factors, but the ground truth is unavailable. Moreover, this analysis only captures victims who entered the second stage of extortion (i.e., public leak site listing). It does not account for pre-listing negotiations or payments, which may vary by country or industry but remain unobservable in our dataset.
- **Categorization Choices:** While we applied consistent industry labels across sources, the grouping into broader sector clusters is interpretive and may obscure relevant nuances present in the raw data.

Despite these constraints, the results provide an empirical foundation for exploring how victim characteristics may correlate with LockBit's operational decisions. Future work with more granular ransom outcome data could deepen these insights.

VIII. Discussion

A. *LockBit 3.0 as a Structured Extortion Business*

Our findings reveal that LockBit 3.0 does not operate opportunistically, but rather runs a highly structured extortion business that strategically manages victims across multiple stages of pressure and monetization. The three-stage lifecycle—comprising pre-listing negotiation, countdown negotiation, and post-leak monetization—demonstrates an intentional design to extract value at distinct points in time. Each stage provides a different form of leverage, from private threats to public shaming and post-leak revenue generation.

In particular, our analysis of post-leak monetization reveals that price-tags are not merely symbolic. Victims with price tags exhibited significantly more variable deletion timing than those without, despite sharing the same median exposure time of 7 days. Specifically, the interquartile range (IQR) for price-tagged victims was 6.25 days and the standard deviation was 22.58 days, with some listings remaining online for up to 69 days. In contrast, victims without price tags had an IQR of 8.00 days and a standard deviation of 14.19 days, with the vast majority removed within the first three weeks. This disparity, confirmed by a Mann–Whitney U test ($p = 0.0019$), suggests that LockBit does not treat published victims uniformly. Instead, listings with monetization interfaces may be selectively retained and managed based on ongoing negotiation potential or perceived payment likelihood.

These results challenge the common assumption that public data leaks mark the end of ransomware extortion. Instead, LockBit's infrastructure supports continued monetization well into the post-leak phase, leveraging price-tags as dynamic tools to prolong pressure and recover late-stage revenue. This operational behavior underscores the importance of tracking extortion beyond initial exposure and reinforces the value of long-term leak site monitoring as a window into attacker strategy.

B. *Impacts of Law Enforcement: Recovery is Swift, But Not Infinite*

Operation Cronos and the October arrests show that law enforcement actions can meaningfully disrupt ransomware groups—but with important caveats. LockBit 3.0 demonstrated impressive short-term resilience by rebuilding its infrastructure, shifting domains, and relisting victims. However, our longitudinal analysis suggests that its momentum was not fully restored.

We observed a sustained decline in new victim onboarding and countdown-stage listings after October 2024. The group also reduced its number of mirror sites and introduced (then removed) access restrictions such as CAPTCHA and passwords—possibly to defend against scraping and surveillance. These shifts suggest LockBit 3.0 entered a more defensive and cautious operational mode, trading reach for survivability.

C. *Changes in Victim Behavior*

Victim responses to LockBit 3.0's tactics also evolved after the takedown. Before Operation Cronos, victims made payments across a wide range of countdown durations—including early-stage payments. After the takedown, payments became concentrated in the final few days before deadlines.

This behavioral shift indicates a change in perceived threat credibility. Victims appear to have grown less confident in LockBit's ability to carry out threats quickly, opting to delay decisions and potentially wait out the pressure. This aligns with law enforcement goals: even temporary disruptions may shake the trust-based mechanisms ransomware groups rely on.

D. *Implications for Counter-Ransomware Strategies*

Our results provide several insights for practitioners and policy-makers:

- **Takedowns matter—but sustained pressure is key.** Single events like Operation Cronos can cause temporary disruption, but lasting impact may require follow-up actions such as arrests and public attribution.
- **Post-leak monetization should be monitored.** In the post-leak phase, victims with price tags were not necessarily deleted faster in absolute terms, but exhibited significantly more variable deletion timing. This suggests LockBit selectively manages these listings, possibly based on ongoing negotiations or the perceived value of each case.
- **Victim behavior is adaptive.** Ransomware mitigation efforts should recognize that victims respond not just to attackers, but also to the broader environment—including media coverage, law enforcement signals, and public messaging.

E. *Limitations and Future Work*

Our analysis relies entirely on publicly accessible data from LockBit 3.0's leak site infrastructure. While we are able to observe victim status transitions, price-tag displays, and published negotiation chat logs, we cannot directly verify ransom payments, affiliate identities, or the intent behind deletions and relistings. Some removals may reflect successful negotiation, while others may result from operational cleanup, infrastructure instability, or external intervention—distinctions that remain opaque in the absence of insider visibility.

Several methodological limitations should be acknowledged. First, our pre-listing negotiation analysis is based on only three chat logs, which limits the generalizability of insights into early-stage extortion behavior. Second, we infer payment events from victim deletion timing, which introduces uncertainty and may conflate negotiation outcomes with other backend activities. Third, our analysis does not distinguish between LockBit affiliates, despite the possibility of behavioral variation across actors.

Despite being centered on a single group, our findings provide broader implications for understanding ransomware ecosystems. To our knowledge, this is the first longitudinal study to use public leak site data to model extortion stages and quantify post-leak monetization strategies. This approach reveals negotiation signals and adaptation patterns as emergent side effects of double extortion operations, and uniquely captures attacker behavior before and after law enforcement takedowns.

Future work should expand the scope of analysis to include other RaaS groups such as RansomHub [15], Medusa [32] to assess whether similar lifecycle patterns emerge. Comparing group-level responses to takedowns, and analyzing how victim information is transferred or cross-posted—via affiliate overlap or migration—may help expose interdependencies across ransomware ecosystems. Additionally, integrating leak site monitoring with cryptocurrency tracing and affiliate network inference could support attribution, reveal monetization pathways, and further distinguish affiliate-specific negotiation styles, payment behaviors, and post-leak strategies.

F. *Dataset Limitations and Confounding Variables*

While our dataset provides visibility into LockBit 3.0's public extortion infrastructure, it lacks verified payment records and complete chat transcripts. As a result, key outcomes—such as whether a victim paid, re-engaged, or was abandoned—must be inferred from leak site behavior, including entry removals and price-tag displays. We interpret these signals cautiously, and we acknowledge that deletions may also reflect operational errors, attacker discretion, or other unobservable factors. Similarly, while chat transcripts offer valuable glimpses into negotiation dynamics, they represent only a small, curated subset of communications.

To address potential confounding factors, we conducted targeted case studies examining geography and industry sector. These examples suggest possible correlations between victim attributes and extortion outcomes, but the limited scope and absence of payment ground truth preclude broader generalization. These limitations constrain the causal claims we can make and underscore the need for future work with more comprehensive or corroborated data sources.

IX. Conclusion

This paper presents a 532-day longitudinal study of LockBit 3.0, one of the most prolific ransomware groups in recent years. By systematically monitoring its leak site infrastructure, we reconstructed a structured, three-stage extortion lifecycle that captures how victims progress from private negotiation, to public pressure through countdowns, and finally to post-leak monetization via price-tags.

To answer **RQ1**, we analyzed over 1,800 victim listings and chat logs, identifying patterns in victim transitions and monetization tactics. Our findings highlight that LockBit 3.0 strategically manages victim states to maximize revenue at multiple stages, including after public disclosure.

To address **RQ2**, we evaluated the impact of Operation Cronos and subsequent law enforcement actions. Although LockBit demonstrated short-term resilience through rapid infrastructure recovery and victim relisting, our longitudinal analysis reveals a sustained decline in victim onboarding and payment urgency—suggesting long-term weakening of its operational capacity.

Overall, this work sheds light on the economic and operational mechanisms behind ransomware extortion, emphasizing the value of longitudinal monitoring. Our findings can inform more effective countermeasures that disrupt not just infrastructure, but the business logic that underpins modern ransomware ecosystems.

X. Ethical Considerations

This study exclusively analyzes publicly accessible information from LockBit 3.0's leak site infrastructure on the Tor network. We did not access private services, interact with ransomware actors, or engage in any intrusive activities. No leaked files were downloaded, browsed, or inspected. Our dataset consists solely of metadata intentionally made public by LockBit—such as victim listing timestamps, countdown deadlines, and published negotiation chat logs.

To minimize potential harm, we omitted victim organization names in all results and visualizations, and we report findings only in aggregate when possible. We made no attempt to influence active extortion cases, interfere with attacker infrastructure, or affect ongoing negotiations.

Continuous monitoring of leak sites offers a unique, non-intrusive lens into attacker behavior and strategy. Our passive measurement approach avoids direct engagement with human subjects and aligns with emerging norms in cybersecurity research that prioritize non-interference, reproducibility, and harm reduction.

This work adheres to established ethical standards in the security research community and is intended to inform defensive strategies for policy-makers, incident responders, and the broader cybersecurity ecosystem.

Acknowledgement

This paper is based on results obtained from project JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO). This work was supported by JSPS KAKENHI Grant Number 21KK0178.

References

[1] "2023-03: Asd's acsc ransomware profile – lockbit 3.0," https://www.cyber.gov.au/about-us/advisories/2023-03-asdacsc-ransomware-profile-lockbit-3.0.

[2] "Most detected ransomware attacks worldwide in 2023, by type," https://www.statista.com/statistics/1475291/most-detected-ransomware-types-worldwide/.

[3] "Uncover the hidden story of ransomware victims - they're not who you think," https://www.trellix.com/blogs/research/uncover-the-hidden-story-of-ransomware-victims/.

[4] Eliando and Y. Purnomo, "Lockbit 2.0 ransomware: Analysis of infection, persistence, prevention mechanism," *CogITo Smart Journal*, vol. 8, no. 1, pp. 232–243, 2022.

[5] A. Tyagi, "Analysis of LockBit black ransomware to identify its static, dynamic and network footprints for generating its detection signatures," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 11, no. 9, pp. c703–c717, September 2023. [Online]. Available: http://www.ijcrt.org/papers/IJCRT2309316.pdf

[6] "LockBit 3.0 technical analysis report," https://brandefense.io/blog/ransomware/lockbit-technical-analysis-report.

[7] "Assemble LockBit 3.0," https://www.cybereason.com/hubfs/dam/collateral/reports/Threat-Analysis-Assemble-LockBit-3.pdf.

[8] K. O'Flaherty, "The lowdown on the takedown: LockBit ransomware group," https://assured.co.uk/2024/the-lowdown-on-the-takedown-lockbit-ransomware-group/.

[9] Cybereason Nocturnus Team, "Assemble lockbit 3.0," Cybereason, Tech. Rep., 2022, accessed April 2025. [Online]. Available: https://www.cybereason.com/blog/threat-analysis-assemble-lockbit-3

[10] CISA, FBI, N. S. Agency, and I. Partners, "stopransomware: Lockbit 3.0," Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep., 2023, accessed April 2025. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

[11] I. W. Gray, J. Cable, B. Brown, V. Cuiujuclu, and D. McCoy, "Money over morals: A business analysis of conti ransomware," *arXiv preprint arXiv:2304.11681*, 2023.

[12] T. Meurs, E. Cartwright, A. Cartwright, and M. van Eeten, "Deception in double extortion ransomware attacks: An analysis of profitability and credibility," *Computers & Security*, vol. 138, p. 103670, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823005801

[13] Ankura and N. Schubert, "LockBit implements new technique by leaking victim negotiations," https://www.jdsupra.com/legalnews/lockbit-implements-new-technique-by-2887557.

[14] "Ransomware live," https://www.ransomware.live/.

[15] Cybersecurity, I. S. A. (CISA), F. B. of Investigation (FBI), U. D. of Health, and H. S. (HHS), "New ransomware actor ransomhub," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a, 2024, accessed: 2025-04-25.

[16] Cybersecurity and Infrastructure Security Agency (CISA), "StopRansomware: Play Ransomware," https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a, December 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a.

[17] ——, "StopRansomware: Black Basta," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a, May 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

[18] ——, "StopRansomware: MedusaLocker Ransomware," https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a, March 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a.

[19] D. Croft, "4 LockBit members arrested, major affiliates ousted in latest operation cronos activity," https://www.cyberdaily.au/security/11181-four-lockbit-members-arrested-major-affiliated-ousted-in-latest-operation-cronos-activity.

[20] Selenium Project, "Selenium WebDriver Documentation," https://www.selenium.dev/documentation/webdriver/, 2024, accessed: 2025-07-13.

[21] D. Person, "dperson/torproxy," https://github.com/dperson/torproxy, 2024, accessed: 2025-07-13.

[22] "Beautiful soup," https://www.crummy.com/software/BeautifulSoup/.

[23] A. Sweigart, "PyAutoGUI Documentation," https://pyautogui.readthedocs.io/en/latest/, 2023, accessed: 2025-07-13.

[24] OpenAI, "GPT-4o," https://platform.openai.com/docs/models/gpt-4o, 2024, accessed: 2025-07-13.
[25] Plotly Technologies Inc., "Plotly: Collaborative data science," https://plotly.com, 2015, accessed: 2025-07-19.
[26] Streamlit Inc., "Streamlit: The fastest way to build data apps," https://streamlit.io, 2019, accessed: 2025-07-19.
[27] J. T. McClave and T. Sincich, *Statistics*, 13th ed. Pearson Education, 2017.
[28] Reuters, "Us charges russian-israeli dual national tied to lockbit ransomware group," https://www.reuters.com/technology/cybersecurity/us-charges-russian-israeli-dual-national-tied-lockbit-ransomware-group-2024-12-20/.
[29] T. E. Team, "LockBit: Europol coordinates four new arrests," https://incyber.org/en/article/lockbit-europol-coordinates-four-new-arrests/.
[30] vx-underground, "[post]," https://x.com/vxunderground/status/1807075741630071083, June 2024.
[31] Apollo.io, "Apollo api: Company and contact data enrichment," https://apollo.io, 2025, accessed via API for company industry and location information.
[32] Cybersecurity, I. S. A. (CISA), F. B. of Investigation (FBI), and U. D. of the Treasury, "Medusalocker ransomware," 2025, available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a.