LockBit Got Hacked. Again: Uncovering Insights Into the Leaked Data | Analyst1

By Anastasia Sentsova

Published: 2025-05-15 · Archived: 2026-04-05 16:15:52 UTC

Leaked, Exposed, and Angry: “I’ll Pay for Info on Who Did It”

LockBit ransomware has been having a rough time over the past year. Following the heavy blow dealt by **Operation Cronos**, the group attempted a comeback, aiming to reclaim its previous status as one of the dominant players in the ransomware landscape. As LockBit was trying to recover, it hit another bump in the road. It didn’t take long before yet another breach of its infrastructure occurred.

On **May 7, 2025**, an unknown individual leaked a MySQL database containing multiple tables related to the information from internal servers, exposing details of LockBit’s operations and the actors involved. Within the leak, it was identified: nearly **63,700** addresses (BTC and XMR); affiliates’ requests for or generation of ransomware builds via the affiliate panel, negotiation chats with victims comprising nearly **4,400** messages; **75** usernames; **21** TOX IDs, which might potentially serve a great deal for further research and identifying actors behind LockBit personas and other information.

LockBit’s attitude was to brush it off with a “haters gonna hate,” but we’d say this looks a lot like karma doing its job. As a response to the leak, LockBit posted a message on their data leak site and Telegram with the following: ***“On May 7, the light panel with auto-registration was breached. Not a single decryptor or any stolen company data was affected. I’m figuring out how they got in and rebuilding it. The full panel and blog are up and running. The alleged hacker is someone named Hoho (xoxo) from Prague. I am willing to pay for any info about him, but only if it’s legit.”***

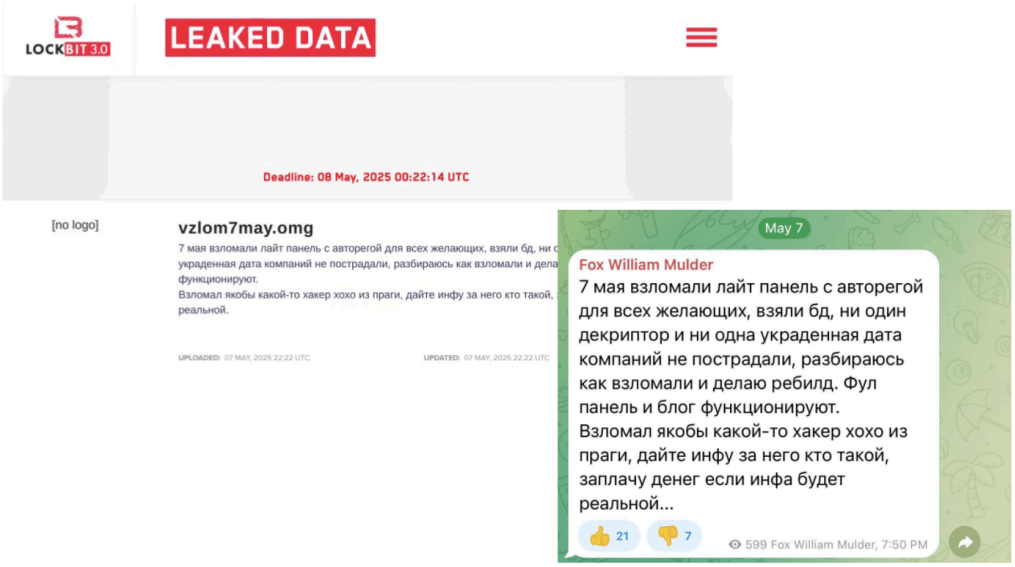

Figure 1: LockBit posted messages on both its Data Leak Site and Telegram, explaining the situation regarding the leak
Source: Analyst1

This leak serves as yet another valuable source of intelligence for researchers and incident responders. In this report, we uncover operational insights and provide detailed blockchain forensic analysis related to LockBit's financial activity. Let's take a closer look at the findings.

Actors' Target Preferences & Other Operational Insights

As we examined the leak, one thing quickly became clear: the actors observed do not demonstrate a high level of experience. Several indicators support this conclusion, most notably, the questionable conduct of affiliates during negotiations, ransom demands appear significantly lower than those typically associated with historical LockBit attacks, and a consistent pattern of careless on-chain behavior.

Based on LockBit's statement and leaked information, the **"Lite panel"** is designed specifically for low-tier affiliates who can purchase access for a **$777 USD** fee. This lower-level access tier allows criminals to participate in ransomware operations with minimal entry barriers. The first mention of this panel appeared in an interview that LockBit gave to **DeepDarkCTI** in **December 2024**. When discussing its current position in the ransomware market following Operation Cronos, LockBit stated: ***Now, anyone can access a Ransomware panel and start working within five minutes after paying a symbolic fee of $777. Those who prove themselves as experienced pentesters will gain access to a more advanced and functional Ransomware panel.***

While the existence of multiple panels cannot be confirmed at the moment, the **Lite panel** may represent a new model, suggesting that the rules have changed. Previously, affiliates were required to deposit **1 Bitcoin** to a LockBit wallet as an upfront joining fee, which was later used as credit to cover the operator's 20% share of ransom payments. This approach served to establish trust between the affiliate and the operator while also raising the barrier to entry, to deter potential law enforcement agents and researchers from infiltrating the program, as stated by LockBit under their affiliate rules.

Among the users registered on the panel, **75** usernames were identified. Two of them, **admin** and **matrix777,** are likely associated with the LockBit operator. This conclusion is based on the presence of the same TOX ID (A1A6D2ECC8DB18DA0D5F04C5ED01A565B5A46E4012FAE627ACCB5D709BB89477D26BE7EF852C) linked to both accounts. The remaining usernames are likely affiliates, including one notable actor operating under the alias **"Christopher."** After registering on the panel on **December 20, 2024**, Christopher quickly became one of the most active participants in LockBit's affiliate program. The chart below illustrates the distribution of total messages exchanged between victims and affiliates, with Christopher responsible for nearly 47% of all activity.

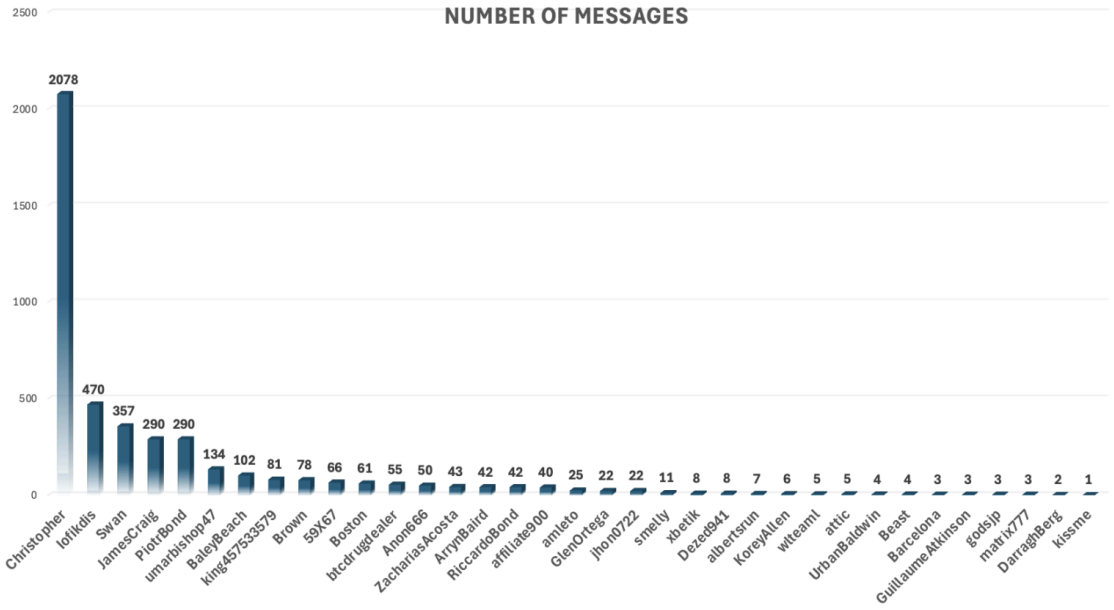

Figure 2: Distribution of messages across usernames. The total count reflects both actor messages and victims' replies

Source: Analyst1

Another revelation comes from analyzing affiliate targeting preferences. Perhaps the most striking finding is the active targeting of APAC countries by affiliates, something not commonly observed in previous LockBit campaigns. China, in particular, stands out. Traditionally, it is avoided by most Russian ransomware groups and considered a "friendly" nation within that ecosystem. While China has occasionally appeared on LockBit's data leak site, it has typically represented only a tiny fraction of total victims compared to other countries. During the operational span of **LockBit 2.0** and its rebrand as **LockBit 3.0**, from **July 18, 2021,** to **May 9, 2025**, China was listed **28** times out of a total of **2,879** public claims, accounting for approximately **1%** of all entries on LockBit's leak site. (data source: eCrime.ch)

Christopher, the central figure in our investigation, also appears to have a clear preference for targeting Asia–Pacific (APAC) countries. The graph below, along with the earlier published report by Valéry Rieß-Marchive, illustrates the regional distribution of targets identified in the leak. This data is sourced from the **builds** table, which documents affiliate requests for the generation of ransomware builds through the affiliate panel. Notably, APAC countries appear in the targeting preferences of nearly every affiliate, highlighting a significant shift in operational focus that deviates from traditional LockBit practices, a trend that was not as apparent when analyzing activity on their public data leak site.

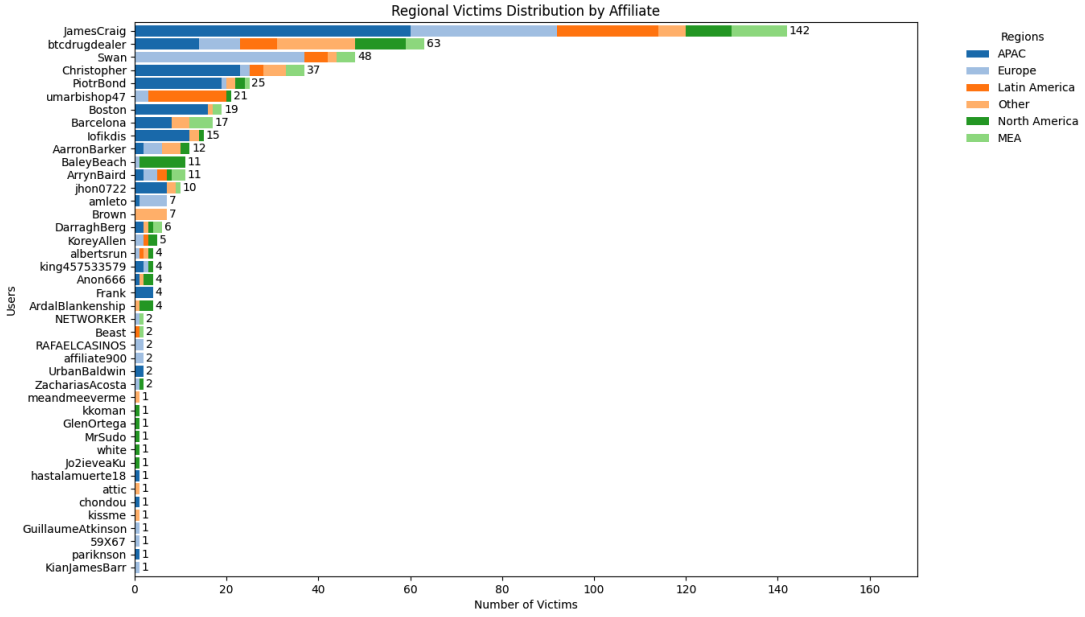

Figure 3: Distribution of targeted regions by usernames

Source: Courtesy of Valéry Rieß-Marchive

In some cases, however, affiliates themselves appear confused about the countries they are targeting. In one such instance, Christopher references a private cryptocurrency exchange in China, providing a link as part of the negotiation. The victim responds: ***"Bro, we are in Taiwan, not China. We hate China."*** The conversation takes an unexpected and somewhat humorous turn when the victim asks the affiliate to consider attacking a Chinese company, to which Christopher replies that ***"they will check it out."*** The victim clearly exhibiting a sense of humor and perhaps lacking negotiation experience continues: ***"We will pay, but you need to give me some time to convince my boss. But you must say China is shit!!!!!!".***

In yet another **unexpected and revealing exchange**, a victim appears to flirt with the idea of joining the ransomware ecosystem:

Victim: "Bro, I want to ask for your advice. If I want to make some extra money on the side but do it safely like you guys, do you have any recommended directions?"

Christopher: "We now have open registration in the LockBit panel, but it costs $777."

Victim: "After joining, what can I help with? I don't have any particular skills. If possible, can I join?"

Christopher: "You don't need it."

While this exchange might seem humorous or perhaps someone trying to infiltrate the group, the key takeaway is clear: victims should seriously consider assigning or hiring a qualified professional to handle ransomware negotiations. And no, your chats are not being deleted, even if the actor promises to do so. In fact, they can become very public, as seen in cases like this.

And ladies and gentlemen, if you ever consider joining the dark side, don't take advice from actors like Christopher. Their *"you don't need any skills"* attitude perfectly reflects today's reality, where ransomware has become a commodity, not an elite cyber weapon, and comes with a very low barrier to entry. The good news? That

same *"no skills needed"* mindset doesn't serve them well. In fact, it's exactly what leads affiliates like Christopher to eventually get caught, from their primitive technical abilities to their sloppy money laundering practices. And as for Christopher's on-chain behavior — how to put it? Well… it's extremely careless. Let's take a look at some of Christopher's profits and laundering efforts, which, surprise… there are basically none.

Uncovering LockBit On-chain Behavior

This leak has provided an incredible volume of cryptocurrency addresses. Specifically, three tables within the leak contain cryptocurrency addresses: **btc_addresses**, **chats**, and **invites,** with nearly **63,700** addresses in total. So, how do we interpret them? Based on our analysis, all of these addresses can be attributed to LockBit as an entity. However, we went a step further and performed actor-level attribution for a portion of them.

When it comes to the addresses from the **chats** table, attribution is relatively straightforward. By analyzing the context surrounding each address and the specified actor ID, we can map addresses to individual affiliates with a high level of confidence.

Meanwhile, addresses in the **btc_addresses** table appear to be operator-controlled. This conclusion is based on a blockchain investigation, where we traced affiliate transactions and identified a consistent **80/20** profit-sharing pattern, known to be LockBit's revenue model. In multiple cases, 20% of the ransom proceeds were sent to addresses listed in the **btc_addresses** table. Based on this consistent pattern, we conclude that all addresses in the **btc_addresses** table are likely under operator ownership.

In addition, the **invites** table likely contains addresses provided to actors who are just joining the LockBit affiliate program. As mentioned earlier, LockBit sometimes requires an entry fee to participate, and these addresses may have been used to collect those initial payments.

Overall, distinguishing between operator- and affiliate-controlled addresses is essential for accurate blockchain tracing. From a research perspective, this distinction, when combined with a broader dataset of cryptocurrency addresses, provides valuable insights into potential cross-group collaboration, especially among affiliates who may be working with multiple ransomware groups. For example, if an actor provides a ransom address during negotiations, often accompanied by self-attribution or branding, and a portion of the ransom is later transferred to an address known to be controlled by the **LockBit** operator, this indicates collaboration between groups.

This is not totally surprising, as such collaboration may occur when smaller ransomware groups with their own established identities partner with larger operations like LockBit. In these cases, although the attack may appear to be carried out under one brand, the encryption tools, infrastructure, or negotiation support may actually originate from a different group. Within the leak, for example, we observed two affiliates introducing themselves as RansomHub and Hellcat.

On **April 4, 2025**, an affiliate operating under the alias **BaleyBeach** stated: ***"We were affiliates of RansomHub. Now RansomHub is closed, so we moved here. Existing companies (including yours) that we were dealing with still have a chance to prevent their data leak."*** Another reference to a different group occurred on **March 20, 2025**, when an actor using the alias **KoreyAllen** made the following claim: ***"LockBit & HellCat encrypted your network. You have 39 days to negotiate."***

Identifying potential affiliate-operator relationships on the blockchain is possible by analyzing transaction patterns, particularly profit-sharing splits, such as LockBit's well-documented 80/20 model. When investigating addresses attributed to Christopher, we observe a consistent pattern in line with this model: 80% of the ransom proceeds go to the affiliate, while 20% is allocated to the operator. Below are several examples that illustrate this behavior, starting from receiving ransom payment and tracing the subsequent distribution of funds.

To make our findings easier to follow, in the examples provided below, we will specify each address with its corresponding source table (btc_addresses OR chats). As established earlier, the **btc_addresses** table relates to addresses attributed to the operator, while the **chats** table relates to addresses attributed to affiliates.

Example 1

The actor initially demanded $80,000 and offered a 20% discount after the victim requested a reduction in the ransom amount. The victim agreed to pay $50,000, after which the actor provided the Bitcoin address **1PKzZhK35fvszaHBdyAwHTRtEoJwjR1ocD** (**chats** table). The victim first conducted a test transaction of **0.00010389 BTC** (equivalent to **$9.94 USD** at the time of the transaction), transaction hash: ***afa41038f76e6616814e5c4d4bc7a4907d15d41dac5bf782af42dc2fbbc5c11f***
Subsequently, the victim proceeded with the full payment of **0.51889581 BTC** (equivalent to **$49,073.92 USD** at the time of the transaction), sent to the same address **1PKzZhK35fvszaHBdyAwHTRtEoJwjR1ocD** on **December 27, 2024**. The transaction hash for this payment is: ***c3137291d4c673e21f282e346338568f26f7b7c3558c82392bca6d31c66166b2***

Figure 4: The image shows victims making a ransom payment in two transfers: a test transaction followed by the main payment
Source: blockchair.com

Further investigation revealed that approximately **0.104 BTC** (equivalent to **$9,954 USD** at the time of the transaction), or roughly **20%** of the total payment, was transferred to the Bitcoin address **bc1qmydvt6xz9rkw36yvw2qztgxexz8dp40pxgklhq** listed in the **btc_addresses** table, where the funds remain as of **May 9, 2025**. Given the 20% share, this payment is likely a profit distribution to the LockBit operator. Another portion of the ransomware proceeds in the amount of **0.41485 BTC** (equivalent to **38,767 USD** at the time of transaction) was transferred to **3Ctfikx36y52Kvg8f8WSsFGu2gzax9ZXDu**, and subsequently sent to the **WhiteBIT** exchange at **bc1qng0keqn7cq6p8qdt4rjnzdxrygnzq7nd0pju8q**

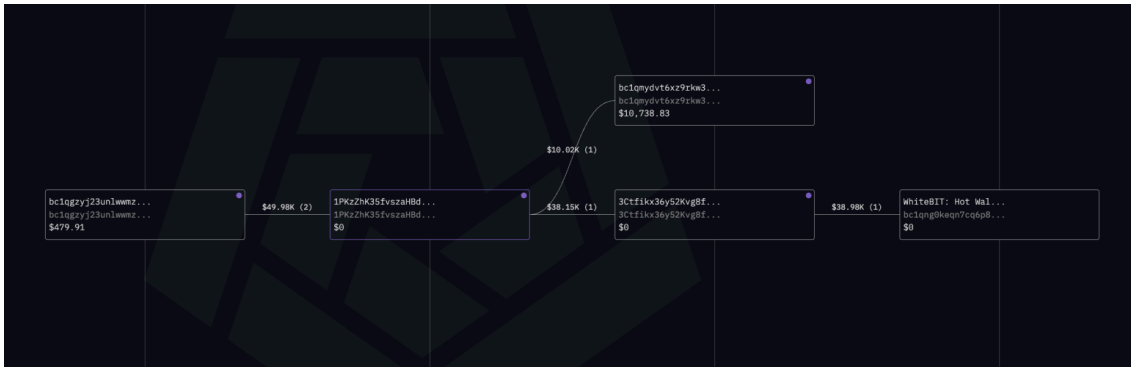

Figure 5: The image shows the flow of ransom proceeds, distributed between the affiliate and the operator, with the affiliate's portion eventually transferred to the WhiteBit exchange
Source: Graph made through arkhm.com

Example 2

The victim agreed to pay a ransom of **$15,000 USD** and initiated the process with a test transaction of **0.005214 BTC** (equivalent to **$497.20 USD** at the time of the transaction) on February 13, 2025. This amount was sent to the Bitcoin address **1LZCdUhTZexZoRdS55wTcK1tAZrs8p7384** (**chats** table)**,** which the actor had provided. The transaction hash for this test payment is: ***64249c14cb6d2b78916f285259359a16c13cfd08635b1da53d5d7e715ae7487f***. Following the test, the victim proceeded with the full ransom payment of **0.1512 BTC** (equivalent to **$14,514.89 USD** at the time of the transaction), sent to the same address **1LZCdUhTZexZoRdS55wTcK1tAZrs8p7384**. The transaction hash for the final payment is: ***6558bf1c88795c00fad711453402e0df4fd3a33e72085e4c1e83f4a8c694bd3c***.

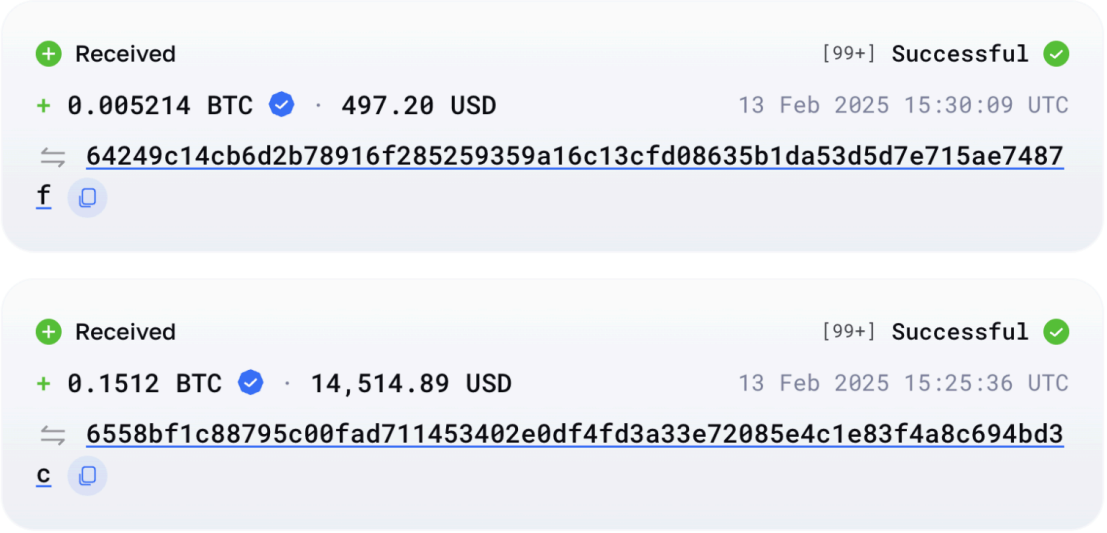

Figure 6: The image shows victims making a ransom payment in two transfers: a test transaction followed by the main payment
Source: blockchair.com

Further investigation revealed that the actor transferred **0.03113 BTC** (equivalent to **$3,047 USD** at the time of the transaction), or approximately **20%** of the total ransom payment, to the Bitcoin address **bc1qv4j45knlkeazg0n0ymv3e3rpcv4gc8qqmrhp20** listed in the **btc_addresses** table. The transaction hash associated with this transfer is: ***9c5f019dfa5c474dfa265f62f1a9aa1aabb40e9c1a62c1b608d718619c233a35***. This

transaction is likely a profit share with the LockBit operator, consistent with the **20%** cut typically attributed to the ransomware group's revenue-sharing model. Another portion of the proceeds, totaling **0.1247 BTC** (equivalent to **$11,972 USD** at the time of the transaction), was sent to **3Hmc4YJZbhJtjos9cMch6iNAMZQ63J2CY5**, an address identified as belonging to the **KuCoin** exchange.

Figure 7: The image shows the flow of ransom proceeds, distributed between the affiliate and the operator, with the affiliate's portion eventually transferred to the KuCoin exchange
Source: Graph made through arkhm.com

Example 3

Upon agreeing to a **$24,000 USD** ransom payment, on **February 16, 2025**, the victim made two separate payments to the address **1BWbqn6xdFat3zLiaHPuFLqnZL7Q4obSKC** (**chats** table), which was provided by the actor.

The first payment was for **0.07 BTC** (equivalent to **$6,802.66 USD** at the time of the transaction).

Transaction hash: ***2a02036ccd63dfa54ddd209b4e2839257d6b682489bda54f3cb9bcd70ebd6904***

The second payment was for **0.175 BTC** (equivalent to **$17,006.67 USD** at the time of the transaction).

Transaction hash: ***1bc3f4b04a1ad974eee10d711e71d526e835e0e14beedc50a889d35c30dfac2f***

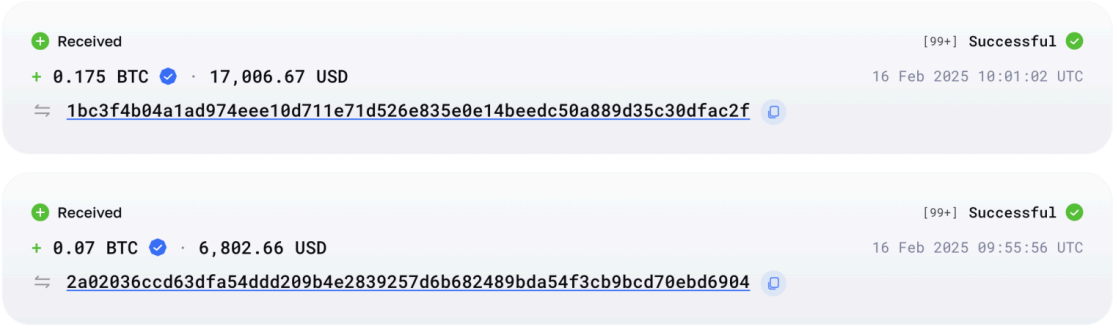

Figure 8: The image shows a ransom payment made by the victim in two parts
Source: blockchair.com

Further investigation revealed that **0.04621 BTC** (equivalent to **$4,510 USD** at the time of the transaction), or approximately **20%** of the total ransom payment, was sent to the Bitcoin address **bc1q5xpf5anwuz75vhlc00g2ec6teu3zvud3axeqcw**, which was also identified to be listed in the **btc_addresses** table. This transaction is likely a profit share with the LockBit operator, consistent with the **20%** correlating with

the group's revenue-sharing model. Another portion of the ransom proceeds **0.198745 BTC** (equivalent to **$19,081 USD** at the time of the transaction) was sent to **39NvyhFJwXUXwjjVTUXtXYVbWE1E7572DC**, an address identified as belonging to the **KuCoin** exchange.

Figure 9: The image shows the flow of ransom proceeds, distributed between the affiliate and the operator, with the affiliate's portion eventually transferred to the KuCoin exchange

As demonstrated in all three examples, Christopher consistently transfers ransom proceeds directly to cryptocurrency exchanges such as KuCoin and WhiteBIT, almost immediately after receiving the funds. This behavior suggests a very low level of operational security and minimal effort to obfuscate the transaction trail, compared with sophisticated money-laundering tactics used by more experienced threat actors.

Another important observation emerges when analyzing the **20%** operator share: surprisingly, none of these funds have been moved. As of **May 15, 2025**, all three addresses attributed to the **LockBit** operator still hold their full balances. At this time, we cannot provide a definitive explanation for this inactivity. The initial assumption was that the relatively small ransom amounts were simply left for later withdrawal. However, we've observed similar behavior even with significantly larger ransoms, which challenges that assumption.

For example, the address **bc1q5tanumnzxuhk0vxkmaqvhqgnq6sf0855trrmjw**, listed in the **btc_addresses** table, was used to receive a ransom payment based on typical on-chain behavior. It is unclear whether the n operator collaborated with any outside affiliates or engaged in an attack, solely assuming that it might have been a purchased access. However, we are clearly seeing that the received funds are most likely a ransom payment. In such behavior of identifying a ransom payment, it is typical to observe the test transaction first, followed by the remaining payment. On **April 30, 2025**, the victim first made a test transaction of **0.0011 BTC** (equivalent to **$102.33 USD** at the time), followed by a main payment of **4.22 BTC** (equivalent to **$396,699.53 USD** at the time of the transaction). Yet, as of **May 15, 2025**, the balance of **bc1q5tanumnzxuhk0vxkmaqvhqgnq6sf0855trrmjw** remains untouched. This shows anomalous behavior, given that ransom payments are typically moved the same day or the following day in most ransomware operations.

Conclusion

The democratization of ransomware, its increasingly low barrier to entry, and collaboration between actors have created a far more complex landscape for investigation and attribution. While prevention remains the most critical line of defense, the unfortunate reality is that determined threat actors continue to find ways into victims' networks. Identifying evidence across multiple layers of criminal operations, from infrastructure to negotiation behavior to on-chain activity, is essential for effectively combating ransomware.

That’s why tracking, tracing, and attributing individuals behind ransomware operations is equally vital. These actors often operate with a false sense of invincibility, but that illusion shatters the moment they are exposed. Attribution efforts must happen at both the entity level, such as identifying ransomware groups, and the individual level, targeting individuals within those groups. This leak of LockBit’s internal database provides valuable intelligence for ransomware investigations and significantly advances our efforts to map their illicit infrastructure, adding numerous new data points to the broader collection of intelligence.

Analyst1 is continuing to investigate LockBit and report on our findings.

About Analyst1

Threat intelligence teams often struggle to bridge the gap from insight to action. Analyst1 is the Orchestrated Threat Intelligence Platform designed to resolve this issue. It automatically organizes threat data, links it to your assets and vulnerabilities, and customizes views for different roles. Analyst1’s orchestration layer streamlines workflows and automates reliable actions by integrating with SIEM, ticketing, and vulnerability management systems. From Fortune 500 financial institutions to national security agencies, enterprises trust Analyst1 to unify their defenses, significantly reducing their response time from days to minutes.
