



| Flash |

Data Breach Exposes Operational LockBit Information

F-2025-05-08a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Dark Web, Data Breach

May 8, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EDT) on May 08, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Data Breach Exposes Operational LockBit Information

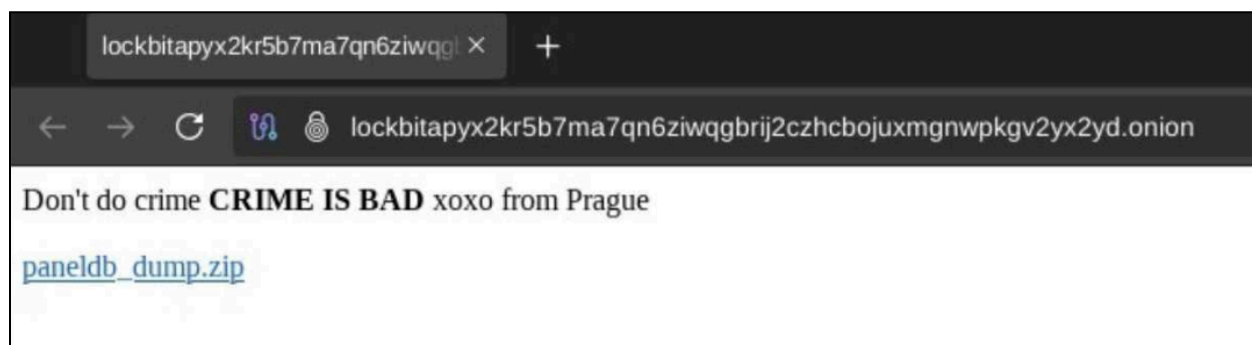
| Key Findings

- On May 7, 2025, actor “Rey” posted on the social media platform X (formerly Twitter) claiming that digital infrastructure associated with the once-prominent ransomware-as-a-service (RaaS) collective LockBit had been breached.
- As of the writing of this report, several of LockBit’s dark web [.]onion blog domains display the message “Don’t do crime **CRIME IS BAD** xoxo from Prague”, accompanied by a download link containing a MySQL data dump.
- Tables available within a MySQL download include information pertaining to ongoing LockBit operations, including victim negotiations, Bitcoin addresses, and malware build configurations.
- At the time of writing, it is unclear who is responsible for the breach, though an almost-identical message was posted on the [.]onion victim leak side of the ransomware collective Everest in April 2025.
- This incident will very likely exacerbate LockBit’s ongoing efforts to re-establish operational continuity, maintain a steady attack tempo, and attract affiliates, following the collective’s February 2024 disruption by law enforcement (LE) entities.

| Details

On May 7, 2025, actor Rey posted on the social media platform X claiming that digital infrastructure associated with the once-prominent Raas collective LockBit had been breached. As of the writing of this report, several of LockBit's dark web [.]onion blog domains display the message "Don't do crime **CRIME IS BAD** xoxo from Prague". The message is accompanied by a download link named "paneldb_dump.zip"—which contains a MySQL data dump.

- Rey is an established actor that carries a well-regarded reputation in numerous deep and dark web (DDW) forums and marketplaces. In April 2025, ZeroFox observed Rey claiming that a recent outage of the popular deep web hacking Forum BreachForums was the result of LE activity.



Message displayed on LockBit [.]onion victim leak domain

Source: ZeroFox Intelligence

The database linked contains multiple SQL tables, including the following:

- A table containing over 4,400 messages sent between LockBit operators and the collective's victim organizations, timestamped and dated between December 19th and April 29th, 2025. ZeroFox observed communications taking place between LockBit and the organization mostly-recently uploaded to their [.]onion victim leak site.
- A table containing varied build configurations, corresponding to different versions of the ransomware executable. These are very likely tailored toward different campaigns or targets, and some of the potential victim organizations are listed.

These rows also contain public keys–used to encrypt victim data. No private keys were observed.

- A table detailing at least 75 users that had previously accessed LockBit’s affiliate panel.
- A table containing almost 60,000 unique Bitcoin (BTC) addresses–used to receive cryptocurrency payments. Despite operating on a public blockchain, Bitcoin remains the vast majority of ransomware collectives’ favoured cryptocurrency, due in part to its widespread use and familiarity–leading to higher chances of extortion demands being satisfied.

Rey	LockBit pwned? Anything on that?	22:16:37
LockBitSupp	only the light panel with autoregistration was hacked, not a single decryptor and stolen company data were damaged	22:17:45
Rey	Yes, but that just means bitcoin addresses, conversations, keys.. It also affects your reputation Locker Builder or source code was not stolen?	22:18:57
	Will you return to work? How long will it take, if so?	22:20:18
		22:22:56
LockBitSupp	bitcoin addresses and conversations, that's all that was stolen, not a single decryptor was stolen, yes it affects reputation, but recovery from hacking also affects reputation the source code is not stolen I'm already working on getting back to work	22:26:37
Rey	Okay, good luck with that. Thanks for the answers.	22:27:18

TOX conversation between Rey and LockBitSupp

Source: ZeroFox Intelligence

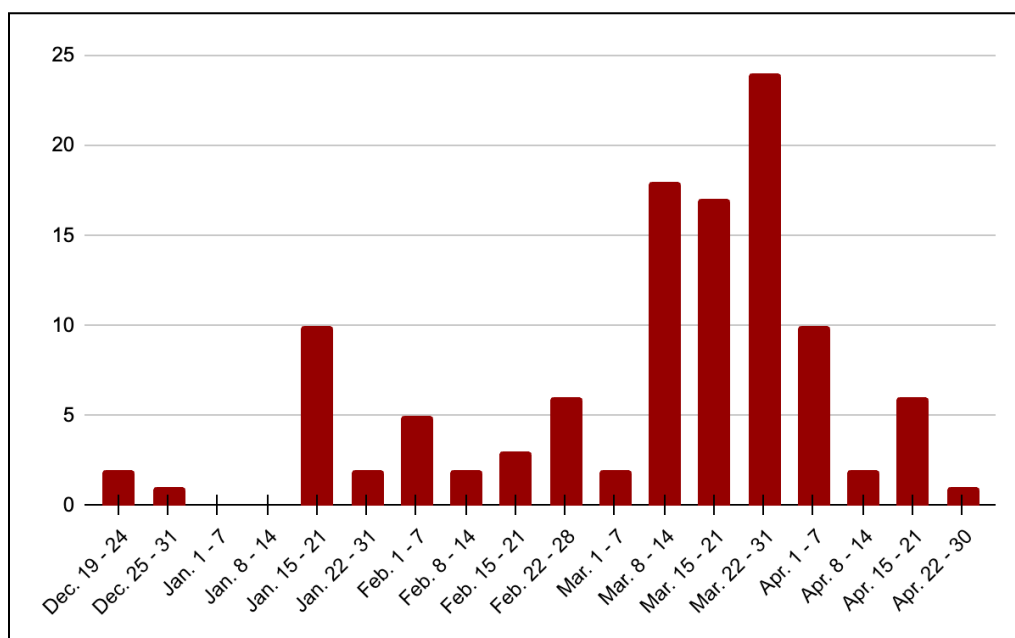
Rey also posted a TOX chat log on X, which allegedly took place between them and the actor “LockBitSupp” (referred to as “Dimon” in some communities)–an alleged leadership figure associated with the LockBit Collective, who was charged as a developer, creator, and administrator by the U.S. Department of Justice in May 2025.¹ In the conversation, LockBitSupp appears to confirm that the breach took place, while caveating with a claim that no decrypting keys–used to decrypt compromised data–, or source code–likely relating to malware–were stolen. LockBitSupp also notes that this breach is expected to damage the collective’s reputation.

¹

[hXXps://www\[.\]justice\[.\]gov/archives/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware](https://www.justice.gov/archives/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware)

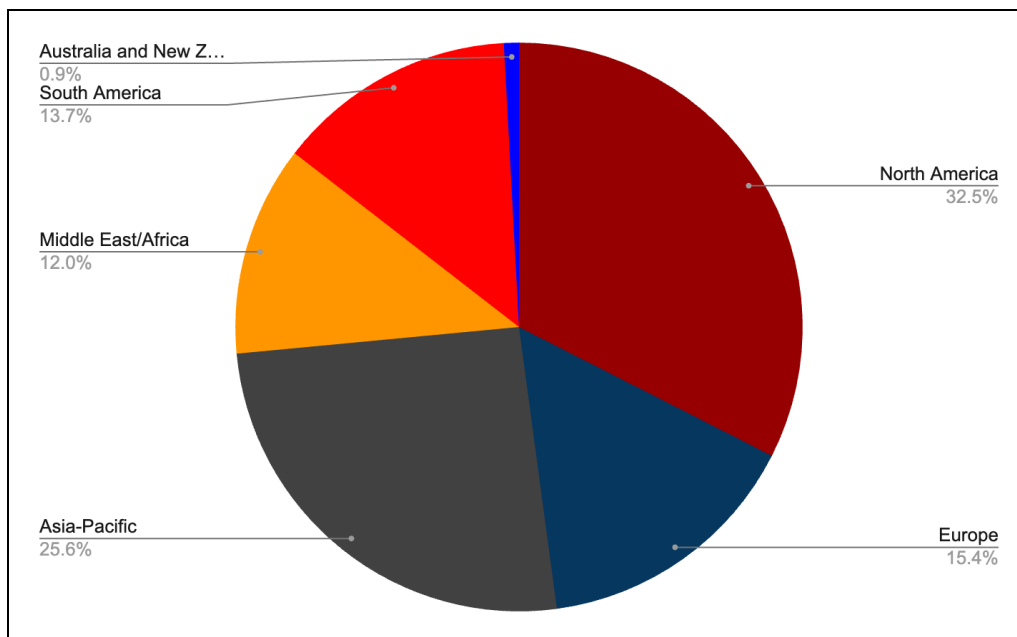
LockBit has almost certainly struggled to garner the reputation necessary to attract and retain affiliates since the collective's February 2024 disruption by LE entities. Prior to this, LockBit was amongst the most prominent of ransomware collectives, conducting more attacks during 2022 and 2023 than any other outfit. LockBit has continued to conduct attacks throughout 2024 and 2025, though at a much lower tempo. So far in 2025, the collective has accounted for approximately 1.5 percent of global ransomware attacks—equating to roughly 40 separate incidents.

- During the timeframe corresponding to the data breach, LockBit has disproportionately targeted organizations located in the Asia-Pacific and Middle East/North Africa regions. This is a notable diversion from the collective's targeting patterns pre-LE disruption, when the vast majority of victims were located in the North America and Europe regions.



LockBit attacks by week, December 19 2024–April 30 2025

Source: ZeroFox Intelligence



LockBit attacks by region, December 19 2024–April 30 2025

Source: ZeroFox Intelligence

At the time of writing, it is unclear who is responsible for the breach, though an almost-identical message was posted on the [.]onion victim leak side of the ransomware collective Everest in April 2025. Unlike the LockBit site, however, no data breach was associated. Separately, in February 2025, Matrix chat logs related to the long-standing RaaS outfit Black Basta were leaked via a Telegram Channel.

Since LockBits 2024 disruption, the collective has made continued attempts to re-establish continuity and maintain a steady attack cadence. In May 2024 a large backlog of alleged victims was uploaded to their victim leak page, in a likely attempt to inflate their perceived operational tempo. In February 2025, the collective launched a new version of their malware–LockBit 4.0, likely intended to attract affiliates. There is a very likely chance that this incident will exacerbate this continued pursuit of brand re-establishment, resulting in a continually reduced threat.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%