# **LockBit Ransomware Gang Hacked, Operations Data Leaked**

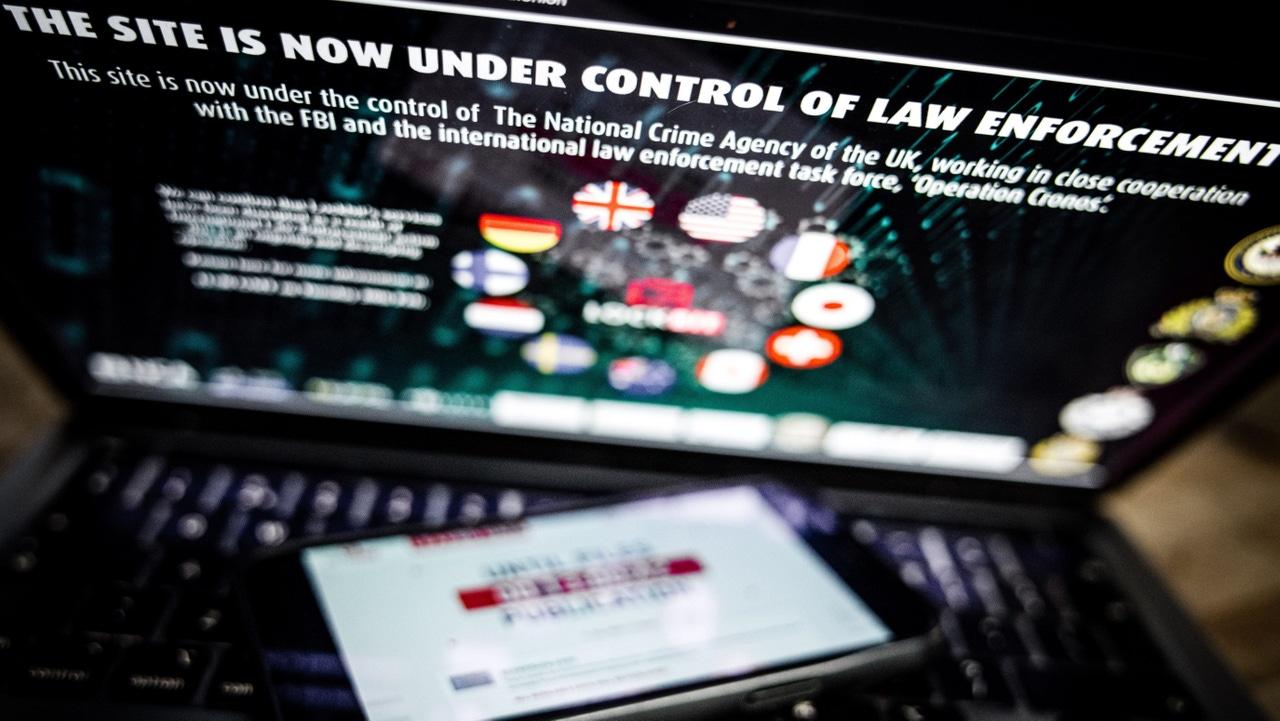
Exposed data from LockBit's affiliate panel includes Bitcoin addresses, private chats with victim organizations, and user information such as credentials.



[Rob Wright](https://www.darkreading.com/author/robert-wright), Senior News Director

May 9, 2025

4 Min Read



Source: ANP via Alamy Stock Photo

The notorious ransomware gang LockBit appeared to suffer another setback this week after its network was compromised by an unknown adversary.

On May 7, a range of security researchers observed that LockBit's Dark Web leak site had been altered. Instead of listing victim organizations, the site now features a simple message: "Don't do crime CRIME IS BAD xoxo from Prague," along with a link to a zip archive.

The archive, [according to analysis](https://blog.qualys.com/vulnerabilities-threat-research/2025/05/08/inside-lockbit-defense-lessons-from-the-leaked-lockbit-negotiations) from Qualys yesterday, among others, includes a SQL database file from LockBit's affiliate panel. Coalition researchers, meanwhile, noted the file includes [extensive internal data](https://www.linkedin.com/feed/update/urn:li:activity:7326004945583792128/) from the ransomware-as-a-service operation, including nearly 60,000 Bitcoin addresses and more than 4,000 chats with victim organizations from between Dec. 19, 2024, and April 29, 2025.

The file also contains information on more than 70 LockBit administrators and affiliates, researchers noted, including plaintext passwords, as well individual builds and configurations of the LockBit ransomware code. However, the leaked data did not include decryptors or private keys.

## **More Trouble For LockBit**

It's unclear who is behind the breach of LockBit's network. A [Bleeping Computer report](https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/) noted the same "Don't do crime" message was left on the leak site of the Everest ransomware gang when it was compromised last month.

**Related:**[Insight Partners Data Breach: Bigger Impact Than Anticipated](https://www.darkreading.com/threat-intelligence/insight-partners-data-breach-bigger-impact)

The breach marks the latest setback for LockBit, which was once the most prolific and well-known RaaS operation on the threat landscape. The gang [suffered a massive disruption](https://www.darkreading.com/threat-intelligence/lockbit-ransomware-takedown-strikes-brand-viability) in early 2024 when an international law enforcement effort, dubbed "Operation Cronos," infiltrated LockBit's network and seized domains, infrastructure, decryptors, source code and other crucial data.

LockBit attempted a comeback in the months following the takedown, claiming to have breached several high-profile organizations. However, cybersecurity vendors such as Trend Micro said [the effort failed](https://www.techtarget.com/searchsecurity/news/366577762/Trend-Micro-LockBit-ransomware-gangs-comeback-is-failing). Moreover, later phases of Operation Cronos in 2024 led to the arrests of several LockBit members as well as [charges and sanctions against Dmitry Yuryevich Khoroshev](https://www.techtarget.com/searchsecurity/news/366583734/Authorities-identify-sanction-LockBit-ransomware-ringleader), a Russian national and the alleged ringleader of the RaaS operation known as "LockBitSupp."

## **LockBit Data Offers Insights**

The exposed SQL database file offers insights into LockBit's operations and activity. For example, according to an analysis by Informa TechTarget publication [LeMagIT](https://www.lemagit.fr/actualites/366623587/Ransomware-ce-que-revele-la-fuite-de-donnees-de-LockBit-30), the majority of LockBit victims during the five-month stretch were in the Asia Pacific region (35.5%), while just 10.8% of victim organizations were based in North America.

**Related:**[Operation PowerOFF Takes Down 9 DDoS-for-Hire Domains](https://www.darkreading.com/threat-intelligence/operation-poweroff-takes-down-nine-ddos-domains)

LeMagIT's analysis also revealed that only a handful of affiliates were highly active during this time period, which suggests the gang's reputation was diminished following Operation Cronos. As for ransom demands, the typical amount was less than $20,000 — a far cry from the massive, eight-figure demands LockBit had made in reported attacks against major enterprises like Royal Mail and [TSMC](https://www.informationweek.com/cyber-resilience/lockbit-hits-tsmc-for-70-million-ransom-what-cios-can-learn).

In its blog post Thursday, Qualys offered more insights from the leaked LockBit data. Ransom demands ranged between $4,000 for "smaller incidents" to $150,000 for larger attacks that included encryption and data exfiltration. Additionally, Qualys noted that LockBit actors sometimes offered discounts on ransom demands of up to 20% if the payment was made in Monero instead of Bitcoin.

"This isn’t just a random perk; it signals a deliberate preference for Monero, likely due to its privacy-centric design," wrote Saeed Abbasi, vulnerability research manager at Qualys' Threat Research Unit.

Qualys also highlighted how the leak revealed some of the gang's tactics and strategies. For example, LockBit actors referenced removing administrators from victims' domain controller infrastructure, which Abbasi said suggests they exploited misconfigured or overly privileged domain controllers.

**Related:**['CoGUI' Phishing Kit Helps Chinese Hackers Target Japan](https://www.darkreading.com/threat-intelligence/cogui-phishing-kit-chinese-hackers-japan)

The affiliates also frequently discussed targeting organizations' backups and NAS devices. Abbasi noted that several known vulnerabilities in Veeam backup software have been [exploited by ransomware actors](https://www.cybersecuritydive.com/news/veeam-cve-exploit-frag-ransomware/732670/) over the past several years. While the leaked data doesn't include direct technical analysis of backup or NAS environments, the files on LockBit builds and configurations contain valuable information on "process/service kill lists" that the ransomware targets.

"These lists target backup-and-recovery agents, disk-encryption utilities, and enterprise backup solutions (for example, Citrix Encryption Service Utility and Storage Sync Agent) to ensure maximum file encryption and minimize any chance of recovery," Abbasi tells Dark Reading. "By disabling or terminating these services, the ransomware prevents backups from running or restoring data, thereby increasing the overall impact of the attack, the lists of items in configs are known to be associated with LockBit in the past as well."

Qualys urged organizations to prioritize the mitigation of known exploited vulnerabilities and securing backup and NAS infrastructure and isolating them from the rest of the network. The vendor also recommended implementing stronger access controls and credentials.