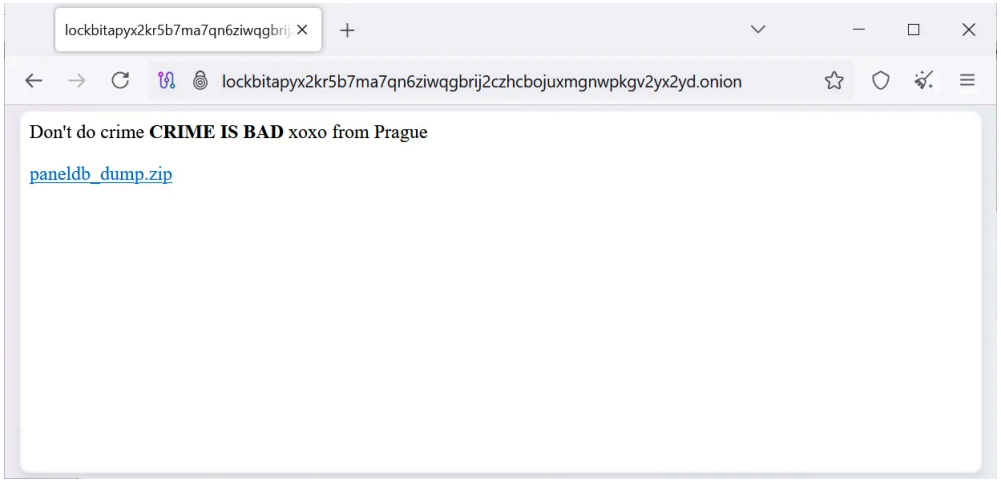
LockBit ransomware gang hacked, victim negotiations exposed

By Lawrence Abrams

Published: 2025-05-08 · Archived: 2026-04-05 15:02:49 UTC

The LockBit ransomware gang has suffered a data breach after its dark web affiliate panels were defaced and replaced with a message linking to a MySQL database dump.

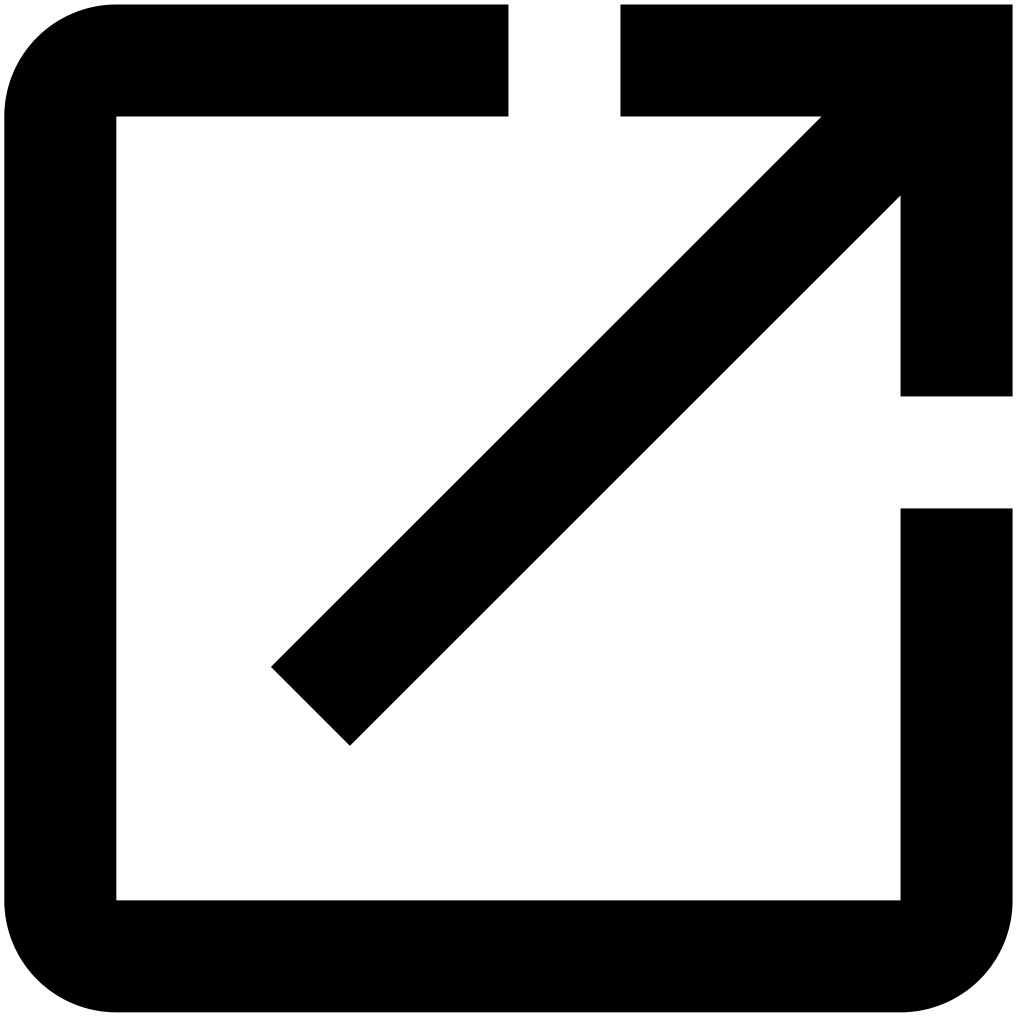
All of the ransomware gang's admin panels now state. "Don't do crime **CRIME IS BAD** xoxo from Prague," with a link to download a "paneldb_dump.zip."



LockBit dark web site defaced with link to database

As first spotted by the threat actor, Rey, this archive contains a SQL file dumped from the site affiliate panel's MySQL database.


DIE LINKE.
0:00



From analysis by BleepingComputer, this database contains twenty tables, with some more interesting than others, including:

- A '**btc_addresses**' table that contains 59,975 unique bitcoin addresses.
- A '**builds**' table contains the individual builds created by affiliates for attacks. Table rows contain the public keys, but no private keys, unfortunately. The targeted companies' names are also listed for some of the builds.
- A '**builds_configurations**' table contains the different configurations used for each build, such as which ESXi servers to skip or files to encrypt.
- A '**chats**' table is very interesting as it contains 4,442 negotiation messages between the ransomware operation and victims from December 19th to April 29th.

```
INSERT INTO `chats` VALUES
(66, 10, 10, 24, 0, 1734583524, 'You can attach a few files for test
decryption by packing them into an archive with zip, rar, tar, 7zip, 7z,
tar.gz extensions of no more than 10 megabytes using the attach button
directly in the chat.\r\n\r\nIf your archive weighs more than 10 megabytes,
please use our file sharing
service.\r\nhttp://lockbitfss2w7co3ij6am6wox4xcurtgwukunx3yubcoe5cbxiqakxqd.oni
on\r\nhttp://lockbitfsvf75glg226he5inkfgtuoakt4vgfhd7nfgghx5kwz5zo3ad.onion\r\n
http://lockbitfskq2fxclyfrop5yizyxpzu65w7pphsgthawcyb4gd27x62id.onion\r\nFor
security reasons we do not click on other links you send in chat.\r\nPlease
wait for a reply, sometimes it takes several hours due to possible time zone
differences.', 0, NULL, NULL, 1, '2024-12-19 04:45:24', NULL, '2024-12-19
05:39:24'),
(67, 10, 10, 24, 0, 1734586509, '', 1, 'realchristmasglobe.zip',
'd43a1040c42f6770eec90c31a3fb88bf6763b08d1b313.zip', 1, '2024-12-19
05:35:09', NULL, '2024-12-19 05:39:24'),
(68, 10, 10, 24, 0, 1734586852, 'how much decrypt file\n', 0, NULL, NULL, 1,
'2024-12-19 05:40:52', NULL, '2024-12-19 05:40:59'),
(69, 10, 10, 24, 1, 1734586873, '4000$\nwe accept bitcoin only', 0, NULL,
NULL, 1, '2024-12-19 05:41:13', NULL, '2024-12-19 05:41:43'),
```

Affiliate panel 'chats' table

- A '**users**' table lists 75 admins and affiliates who had access to the affiliate panel, with Michael Gillespie spotting that passwords were stored in plaintext. Examples of some of the plaintext passwords are 'Weekendlover69, 'MovingBricks69420', and 'Lockbitproud231'.

In a Tox conversation with Rey, the LockBit operator known as 'LockBitSupp' confirmed the breach, stating that no private keys were leaked or data lost.

Based on the MySQL dump generation time and the last date record in the negotiation chats table , the database appears to have been dumped at some point on April 29th, 2025.

It's unclear who carried out the breach and how it was done, but the defacement message matches the one used in a recent breach of Everest ransomware's dark web site, suggesting a possible link.

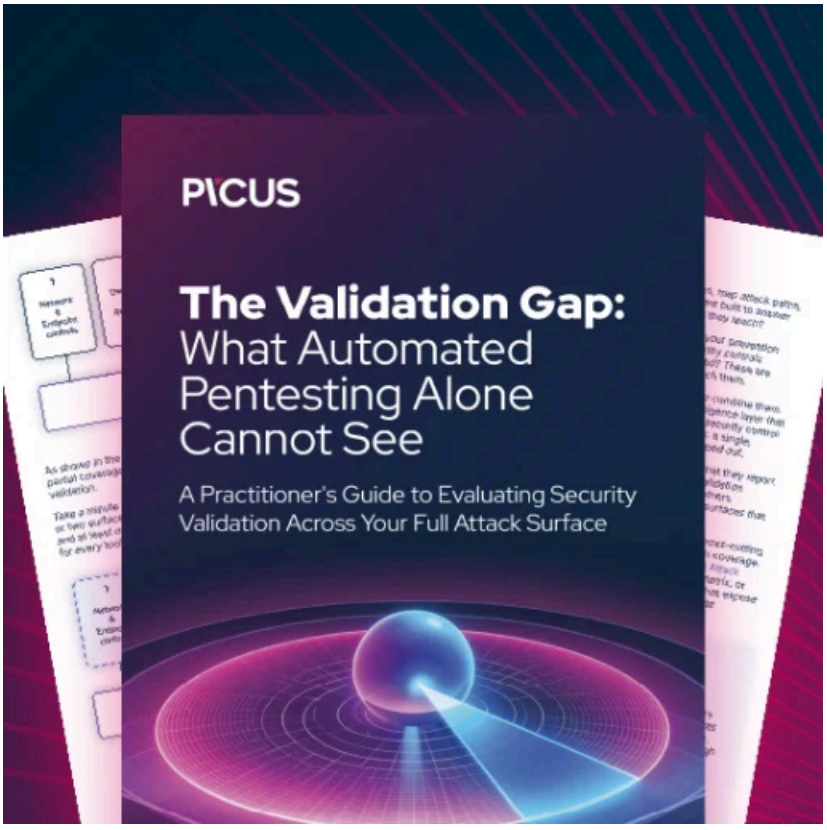
In 2024, a law enforcement operation called Operation Cronos took down LockBit's infrastructure, including 34 servers hosting the data leak website and its mirrors, data stolen from the victims, cryptocurrency addresses, 1,000 decryption keys, and the affiliate panel.

Although LockBit managed to rebuild and resume operations after the takedown, this latest breach strikes a further blow to its already damaged reputation.

It's too early to tell if this additional reputation hit will be the final nail in the coffin for the ransomware gang.

Other ransomware groups who have experienced similar leaks include Conti, Black Basta, and Everest.

Update 5/8/25: Updated article to remove potential PHP CVE the server was vulnerable to as that CVE only impacted Windows. Thanks Christopher.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/