FBI recovers 7,000 LockBit keys, urges ransomware victims to reach out

By Sergiu Gatlan

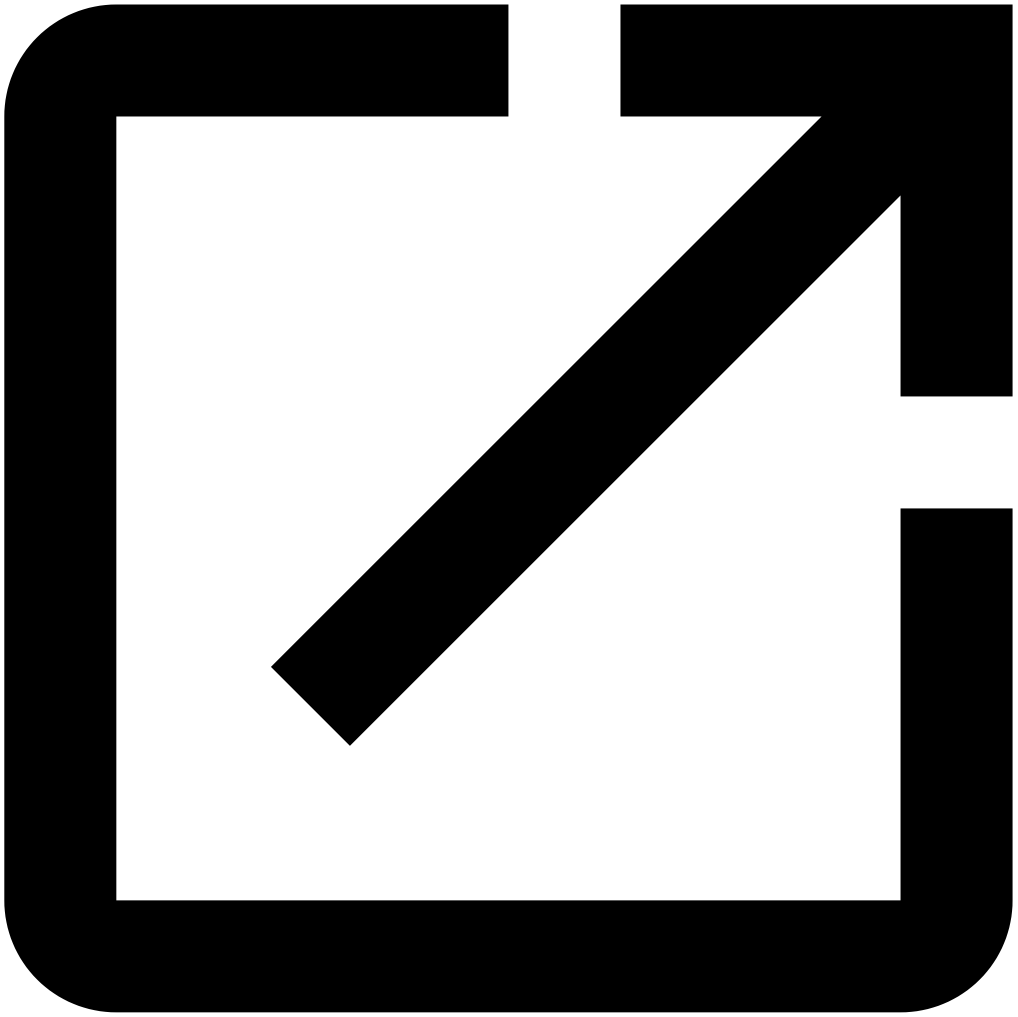
Published: 2024-06-05 · Archived: 2026-04-05 14:17:44 UTC

The FBI urges past victims of LockBit ransomware attacks to come forward after revealing that it has obtained over 7,000 LockBit decryption keys that they can use to recover encrypted data for free.

FBI Cyber Division Assistant Director Bryan Vorndran announced this on Wednesday at the 2024 Boston Conference on Cyber Security.

"From our ongoing disruption of LockBit, we now have over 7,000 decryption keys and can help victims reclaim their data and get back online," the FBI Cyber Lead said in a keynote.


DIE LINKE.
0:00



"We are reaching out to known LockBit victims and encouraging anyone who suspects they were a victim to visit our Internet Crime Complaint Center at ic3.gov."

This call to action comes after law enforcement took down LockBit's infrastructure in February 2024 in an international operation dubbed "Operation Cronos."

At the time, police seized 34 servers containing over 2,500 decryption keys, which helped create a free LockBit 3.0 Black Ransomware decryptor.

After analyzing the seized data, the U.K.'s National Crime Agency and the U.S. Justice Department estimate the gang and its affiliates have raked in up to $1 billion in ransoms following 7,000 attacks targeting organizations worldwide between June 2022 and February 2024.

However, despite law enforcement efforts to shut down its operations, LockBit is still active and has since switched to new servers and dark web domains.

They are still targeting victims around the world and, in retaliation to the recent infrastructure takedown by U.S. and U.K. authorities, they've kept leaking massive amounts of old and new stolen data on the dark web.

Most recently, LockBit claimed the April 2024 cyberattack on Canadian pharmacy chain London Drugs after another law enforcement operation that doxxed the gang's leader, a 31-year-old Russian national named Dmitry Yuryevich Khoroshev who's been using the "LockBitSupp" online alias.

In recent years, other Lockbit ransomware actors have been arrested and charged, including Mikhail Vasiliev(November 2022), Ruslan Magomedovich Astamirov (June 2023), Mikhail Pavlovich Matveev aka Wazawaka (May 2023), Artur Sungatov and Ivan Gennadievich Kondratiev aka Bassterlord (February 2024).

The U.S. State Department now offers $10 million for any information that would lead to LockBit leadership arrest or conviction and an extra $5 million reward for tips leading to the arrest of LockBit ransomware affiliates.
