LockBit says they stole data in London Drugs ransomware attack

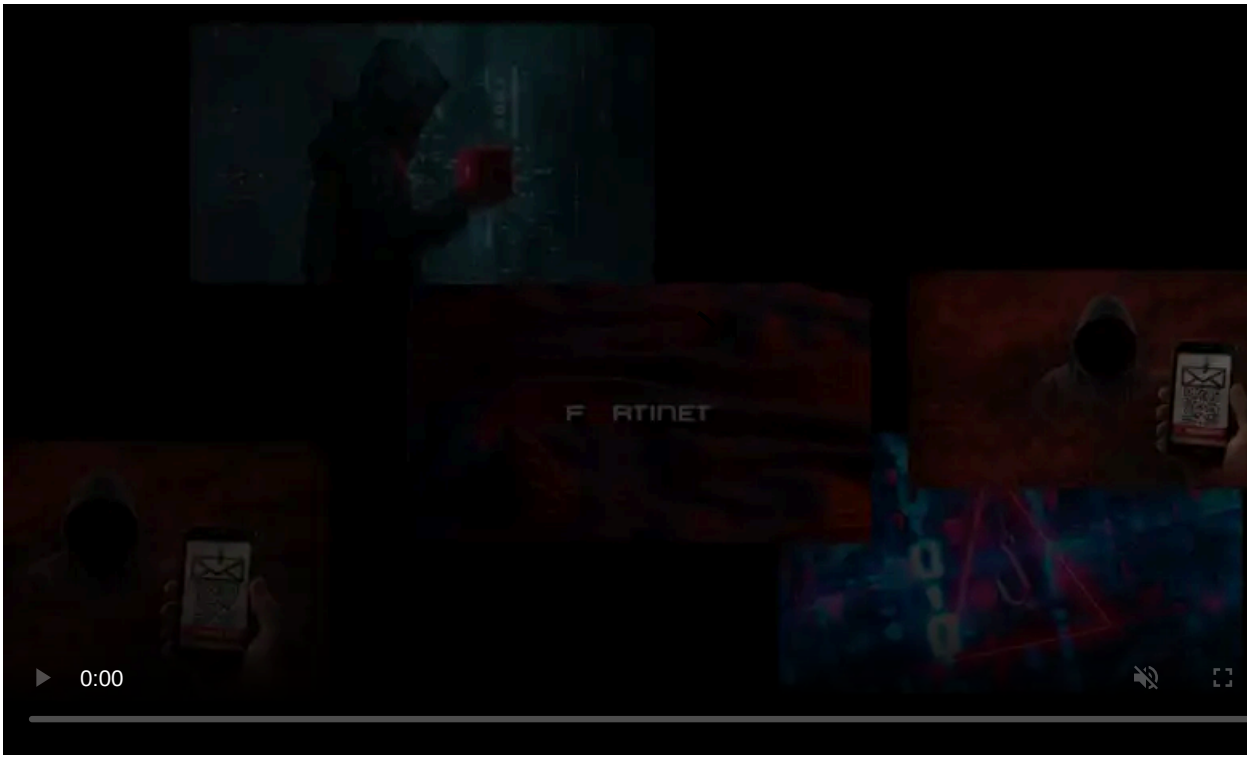
By Sergiu Gatlan

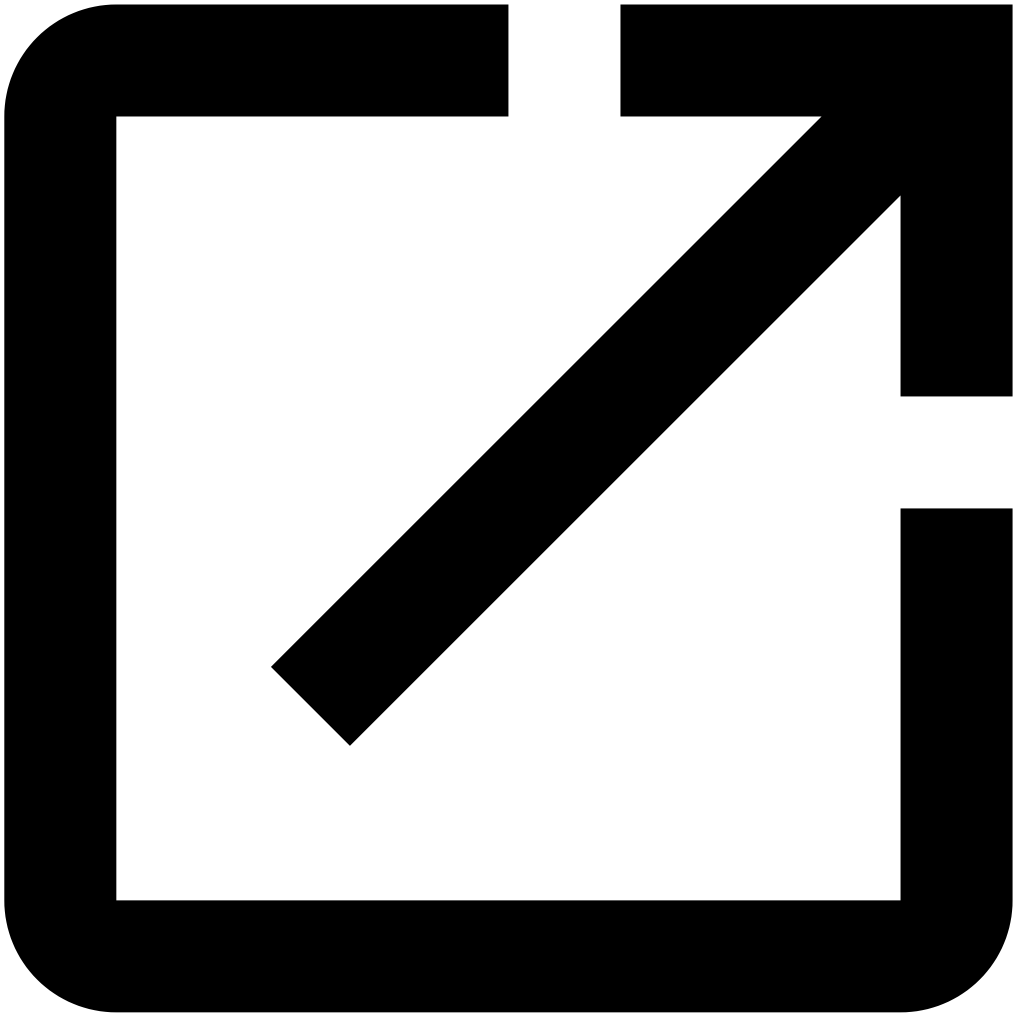
Published: 2024-05-21 · Archived: 2026-04-05 22:20:02 UTC

Today, the LockBit ransomware gang claimed they were behind the April cyberattack on Canadian pharmacy chain London Drugs and is now threatening to publish stolen data online after allegedly failed negotiations.

London Drugs has over 9,000 employees who provide healthcare and pharmacy services in over 80 stores across Alberta, Saskatchewan, Manitoba, and British Columbia.

An April 28 cyberattack forced London Drugs to close all its retail stores across Western Canada. The company said it found no evidence that customer or employee data was impacted.


F RTINET
0:00

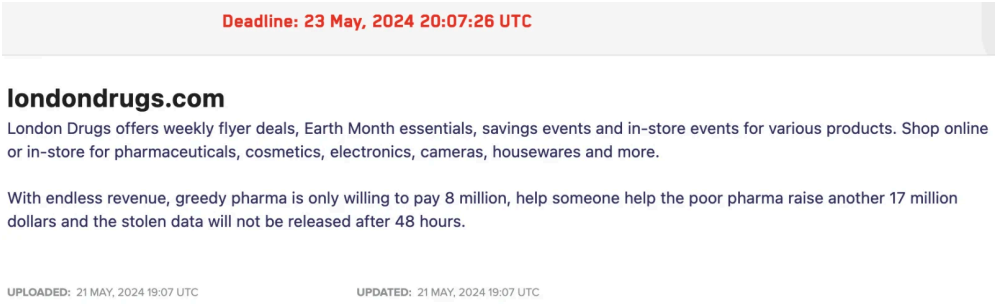


"Should our investigation indicate any personal information has been compromised, we would notify those impacted and applicable privacy commissioners in accordance with applicable privacy laws," the pharmacy chain said at the time.

On May 9, London Drugs' President and Chief Operating Officer (COO) Clint Mahlman confirmed again that third-party cybersecurity experts hired to conduct a forensic investigation found no evidence that "customer databases, including our health data and LDExtras data," were compromised.

While London Drugs has since re-opened all shutdown stores, the company's website is still down and displaying an error stating, "The server encountered an internal error that prevented it from fulfilling this request."

Earlier today, the LockBit ransomware operation added London Drugs to its extortion portal, claiming the April cyberattack and threatening to publish data allegedly stolen from the company's systems.



London Drugs listed on LockBit's extortion website (BleepingComputer)

The ransomware gang has yet to provide proof that they stole any files from London Drugs servers, claiming only that negotiations with London Drugs to pay a $25 million ransom have failed.

While it didn't confirm LockBit's claims, a London Drugs statement shared with BleepingComputer says the company is aware the ransomware gang said they stole "files from its corporate head office, some of which may contain employee information"—as seen in the screenshot above LockBit only mentioned "stolen data."

London Drugs added that they will not and cannot pay the ransom requested by LockBit, but acknowledged that the gang "may leak stolen London Drugs corporate files, some of which may contain employee information on the Dark Web."

"At this stage in our investigation, we are not able to provide specifics on the nature or extent of employee personal information potentially impacted. Our review is underway, but due to and the extent of system damage caused by this cyber incident, we expect this review will take some time to perform," London Drugs said.

"Out of an abundance of caution, we have proactively notified all current employees and provided 24 months of complimentary credit monitoring and identity theft protection services, regardless of whether any of their data is ultimately found to be compromised or not."

LockBit ransomware's rise and fall

This ransomware-as-a-service (RaaS) operation surfaced in September 2019 as ABCD and then rebranded as LockBit.

Since its emergence, LockBit has claimed attacks against many government and high-profile organizations worldwide, including Boeing, the Continental automotive giant, the Italian Internal Revenue Service, Bank of America, and the UK Royal Mail.

Law enforcement took down LockBit's infrastructure in February 2024 in an action known as Operation Cronos, seizing 34 servers containing over 2,500 decryption keys that helped create a free LockBit 3.0 Black Ransomware decryptor.

Based on the seized data, the U.S. DOJ and the U.K.'s National Crime Agency estimate that LockBit has extorted between $500 million and $1 billion after 7,000 attacks targeting organizations worldwide between June 2022 and February 2024.

LockBit domain seizure (BleepingComputer)

However, LockBit is still active and has moved to new servers and dark web domains. It keeps targeting victims around the world and releasing massive amounts of old and new data in retaliation to the recent infrastructure takedown by U.S. and U.K. authorities.

LockBit's claims that it was behind the London Drugs cyberattacks come after another international law enforcement operation doxxed and sanctioned the ransomware gang's leader as a 31-year-old Russian national named Dmitry Yuryevich Khoroshev, using the "LockBitSupp" online alias.

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

Previous charges and arrests of Lockbit ransomware actors include 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).

Source: https://www.bleepingcomputer.com/news/security/lockbit-says-they-stole-data-in-london-drugs-ransomware-attack/