DC city agency says LockBit claims tied to third-party attack

By Jonathan Greig

Published: 2024-04-19 · Archived: 2026-04-05 15:29:00 UTC

A Washington, D.C., government agency confirmed that data stolen and leaked by the LockBit ransomware gang was taken from a third-party technology provider.

On April 13, the LockBit ransomware gang claimed it attacked the D.C. Department of Insurance, Securities and Banking (DISB) and stole 800GB of data. DISB is a regulatory agency designed to protect consumers from abuses by financial institutions like insurance companies, investment firms, banks and mortgage lenders.

LockBit said on Thursday evening that negotiations had broken down and it planned to leak 1GB of data in order to further push the organization into paying a ransom.

After repeated requests for comment throughout the week, DISB responded to an inquiry on Friday morning, directing Recorded Future News to a statement and declining to comment further on the incident.

The statement says DISB was notified by third-party software provider Tyler Technologies that it "has experienced a data breach related to securities data."

"Tyler Technologies discovered unauthorized access to their cloud that stores DISB's STAR system client data," DISB said, directing people to an alert from Tyler Technologies.

Tyler Technologies is a public company that serves government agencies and schools around the world, reporting a revenue of $1.95 billion in 2023.

Company officials explained that late last month its IT team discovered "unauthorized activity in an isolated segment of a private cloud hosting environment that stored limited STAR system client data."

"We immediately took the system offline and have been in close contact with affected clients. In coordination with third-party experts, we launched an incident response investigation," they said.

"In parallel, our security and technical support teams began working to restore system access in a safe and secure manner. Known, good (immutable) backups were available, and recovery of the application environment and associated data have been a focus for Tyler since we discovered this situation. Our investigation found that a threat actor encrypted the system and acquired data."

In an update published on Friday, Tyler Technologies confirmed that LockBit released some of the information taken from the STAR system.

The company said it has been in contact with law enforcement about the issue and has hired a cybersecurity firm to investigate.

The company did not respond to requests for comment about whether it had been negotiating with LockBit or if a ransom would be paid. It is unclear whether other clients of the company were affected by the attack.

In an FAQ alongside the statement, Tyler Technologies confirmed that it is likely the ransomware gang stole personal information and it is currently "working to identify which individuals' personally identifiable information (PII) may have been acquired by the threat actor."

The company said this incident is not tied to a September 2020 data breach where hackers accessed internal phone and information technology systems.

DISB is the latest Washington, D.C., government organization to face a data theft incident following an attack on the city's healthcare exchange platform last year that saw sensitive information of thousands — including Congress members and staff — leaked.

Thousands of people who signed up for DC Health Link — a health insurance marketplace for city residents —- had their names, ID numbers, policy IDs, Social Security numbers and more accessed by hackers and eventually leaked.

Officials at Washington, D.C.'s Board of Elections (DCBOE) also confirmed in October that hackers accessed the city's voter rolls, which includes personal information such as partial Social Security numbers and driver's license numbers.

Despite a widely publicized international law enforcement takedown in February, LockBit has continued to launch successful ransomware attacks. A Nasdaq-listed pharmaceutical development company and a prominent South African company were LockBit victims last month.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
