Montreal electricity organization latest victim in LockBit ransomware spree

By Jonathan Greig

Published: 2023-08-30 · Archived: 2026-04-05 23:50:56 UTC

The LockBit ransomware gang continues to dominate headlines and cause concern among cybersecurity experts with a spate of attacks on critical organizations, governments and businesses.

On Wednesday, the gang took credit for an attack on the Commission des services electriques de Montréal (CSEM) — a 100-year-old municipal organization that manages electrical infrastructure in the city of Montreal.

The organization confirmed the incident on Tuesday, writing in a statement that it was hit with ransomware on August 3 but refused to pay the ransom. It contacted national authorities and law enforcement in Quebec while making every effort to restore its systems. Its IT infrastructure has already been rebuilt, the company said.

“The criminal group at work in this case has made public today some of the stolen data. The CSEM denounces this illegal gesture, while specifying that the data disclosed represents a low risk for both the security of the public and for the operations carried out by the CSEM,” they said.

“It should be noted that all CSEM projects are the subject of public documents. Therefore, all these plans – engineering, construction and management – are already publicly available through the official process offices in Quebec.”

LockBit threatened to leak the data Wednesday, the same day it claimed the attack.

The incident caps a week of high-profile incidents and news surrounding the gang, which far outpaces all other ransomware groups in terms of the number of attacks launched.

Last Friday, the Spanish National Police warned that it was seeing a wave of highly-sophisticated phishing emails sent by LockBit actors targeting architecture firms.

The emails purport to be from a photography company asking for a budget to take pictures of buildings. After exchanging emails, the fake company sends along a planning document for the photo session that encrypts victim devices when downloaded.

That campaign is part of a wide variety of LockBit attacks on European targets, including a French regional agency in charge of natural areas in Île-de-France and Capodimonte Museum in Italy.

Despite the gang’s torrid pace, cybersecurity experts are questioning the cybercrime group’s operational strength after the release of a bombshell report from Jon DiMaggio, chief security strategist at Analyst1.

In a followup to his previous report on the gang, DiMaggio said LockBit’s leadership vanished and was unreachable over the first two weeks of August before resurfacing on August 13.

Due to issues with its backend infrastructure and available bandwidth, the group is struggling to publish the data it steals during attacks, DiMaggio said. LockBit is essentially pressuring victims to pay ransoms purely off of its reputation as the most prolific ransomware group currently operating, he said.

That report was followed by another this week from Kaspersky showing that the reported leak of the LockBit 3.0 ransomware builder has led to threat actors abusing the tool to spawn new variants. They found 396 different samples based on the LockBit code.

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.
