LockBit 3.0 Says It's Holding a Canadian City for Ransom

By Mihir Bagwe

Archived: 2026-04-05 16:07:10 UTC

Cybercrime , Cybercrime as-a-service , Fraud Management & Cybercrime

Ransomware Attack Locks Up Westmount Services and Takes Down Email System (MihirBagwe) • November 22, 2022

Westmount City Hall (Source: City of Westmount)

The nefarious LockBit 3.0 cybercriminal group is claiming responsibility for the ransomware attack that halted municipal services and shut down employee email accounts in Westmount, Quebec, giving the city a deadline of Dec. 4 to make an undisclosed ransom payment.

See Also: Experts Offer Insights from Theoretical to the Realities of AI-enabled Cybercrime

Westmount, a city with nearly 21,000 residents in southwestern Quebec, on Monday initially reported that the city's email services were unavailable because of an unidentified computer outage. Later, the city confirmed the outage also affected other municipal services and stemmed from a targeted cyberattack.

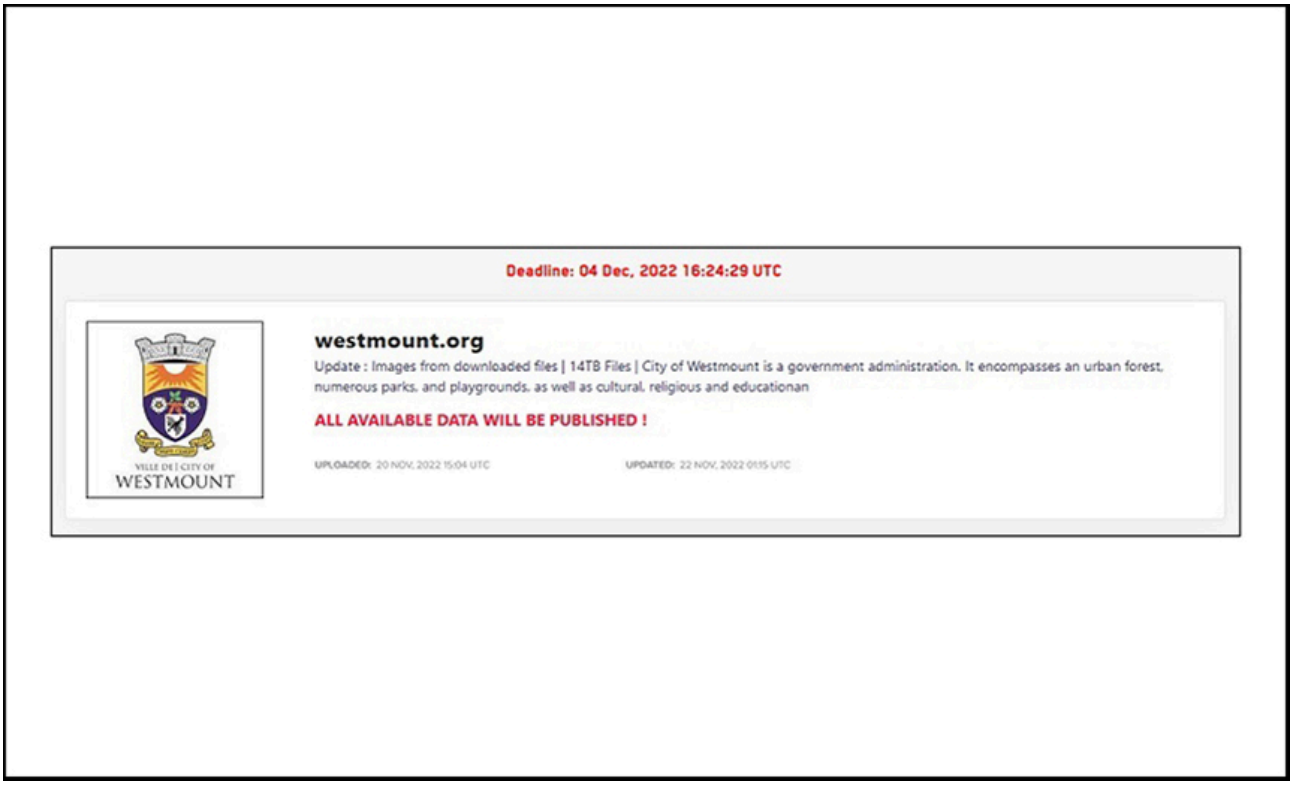
"Cyberattacks are unfortunately becoming more and more prevalent and sophisticated in our society, and despite all the measures we put in place, public administrations are not completely immune to this sad reality," Westmount Mayor Christina Smith says in a statement. "I want to reassure all Westmounters that our teams are working seriously and diligently to remedy this situation, and we will keep residents informed."

The city did not comment on the extent of the attack but says it hired a cybersecurity firm to investigate and to restore its systems as soon as possible.

La Presse, a local digital news agency in Quebec, quoted Claude Vallières, the city's head of IT, who said, "We know we have encrypted servers, but we don't know who attacked us. We are still investigating the infected servers, but we have not had any communication with anyone."

LockBit Claims Responsibility

The LockBit 3.0 ransomware group claimed responsibility for the attack and says it has successfully downloaded 14 terabytes of sensitive data. LockBit, which operates as a ransomware-as-a-service group, says it will release the stolen data if a ransom payment is not made in the next two weeks.



This message to Westmount is posted on the LockBit dark web blogging site. (Source: ISMG)

Best known for its 2021 ransomware attack against Accenture, the LockBit ransomware gang launched its LockBit 3.0 malware in June 2022, after conducting two months of beta testing and offering a bug bounty for ethical hackers to inspect the decryption code.

LockBit operators posted screenshots showing files of different departments and other data as a proof for their claim, but Information Security Media Group was unable to immediately contact the municipality and confirm the authenticity of the documents.

The attack comes on the heels of a new National Cyber Threat Assessment 2023-2024 by the Canadian Center for Cyber Security. The report, which says ransomware is "the most disruptive form of cybercrime facing Canadians," adds that ransomware benefits significantly from the specialized cybercrime economy and the growing availability of stolen information.

"So long as ransomware remains profitable, we will almost certainly continue to see cybercriminals deploying it," the report says.

The city of Westmount's official website was not affected by the attack, and the municipality says any updates on the recovery will be communicated on the site. The mayor assured residents that data security is its "top priority" and so "is the protection of our residents' and employees' information."
