Montreal's STM public transport system hit by ransomware attack

By Lawrence Abrams

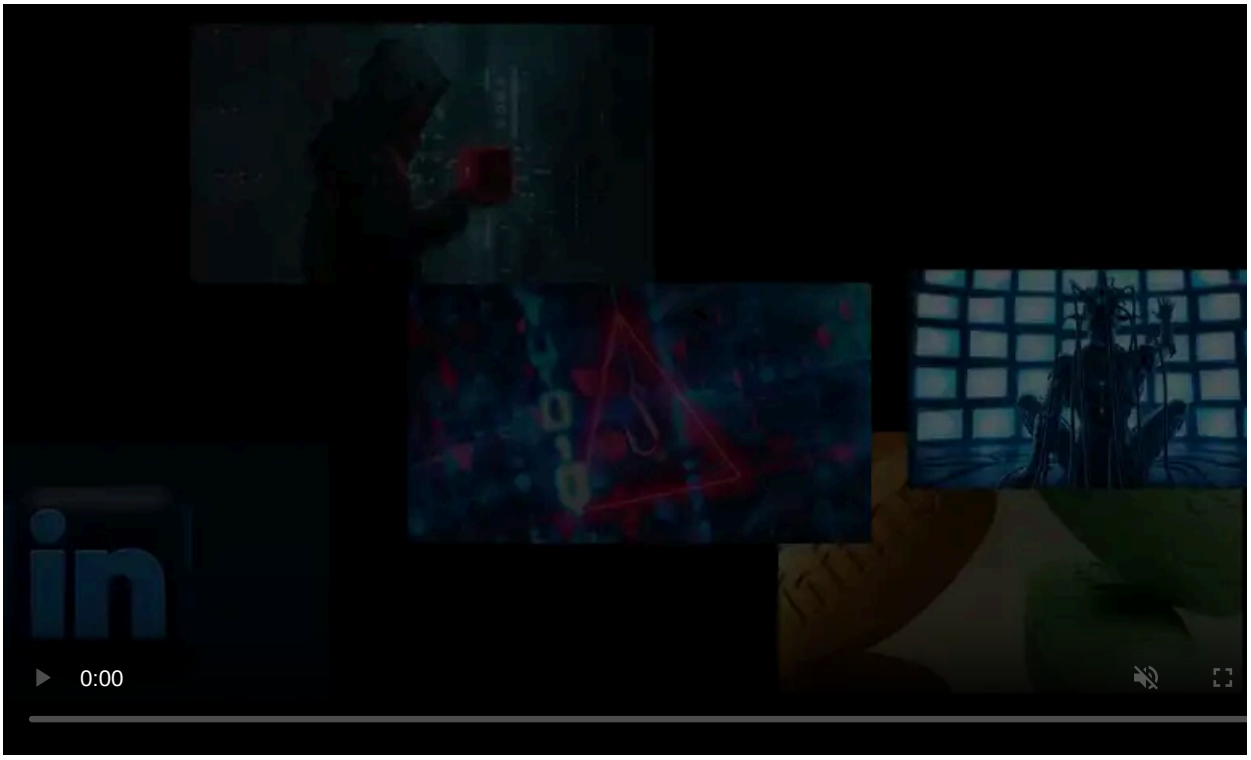
Published: 2020-10-21 · Archived: 2026-04-05 18:38:55 UTC

Montreal's Société de transport de Montréal (STM) public transport system was hit with a RansomExx ransomware attack that has impacted services and online systems.

On October 19th, STM suffered an outage that affected its IT systems, website, and customer support.

While these outages did not affect the operation of buses or metro systems, people with disabilities who rely on STM's door-to-door paratransit service are affected as it uses an online registration system.

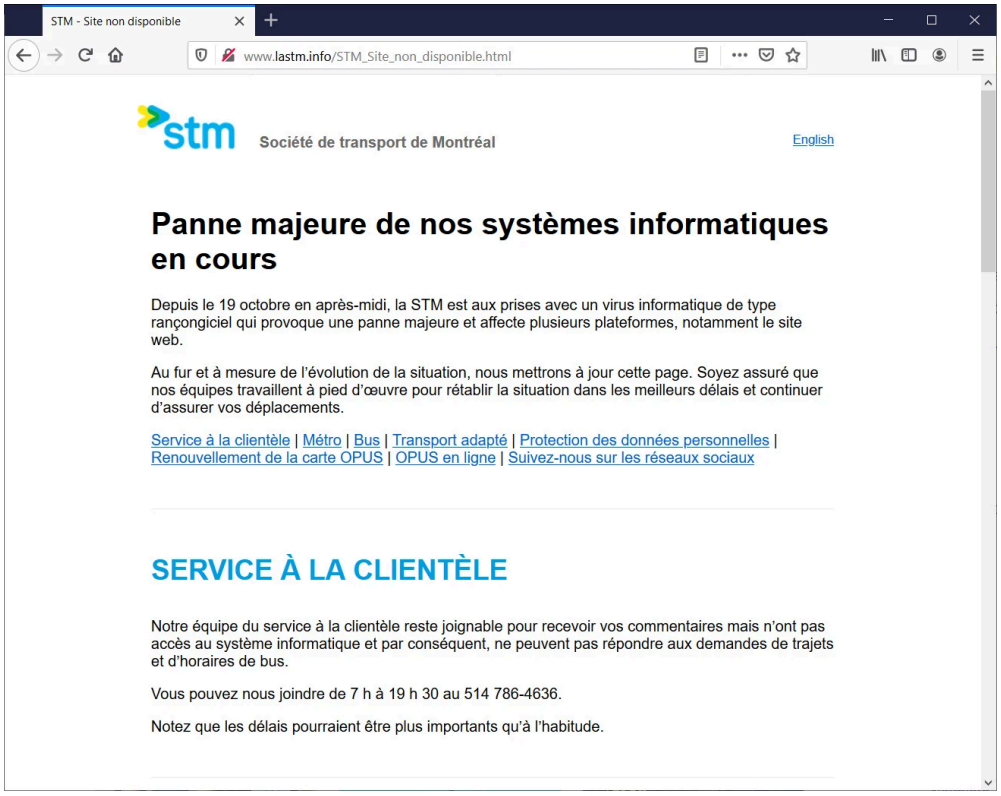
On Tuesday morning, STM announced that the outages were caused by a 'computer virus that caused a major failure on various platforms."


0:00

Later that evening, STM confirmed that they had suffered a ransomware attack and are working with law enforcement and external experts to restore their systems and investigate the attack.

"The Société de transport de Montréal (STM) wishes to inform its customers that the major computer failure it has suffered since October 19 in the afternoon is the consequence of a ransomware type, targeting all applications, despite the various defenses that are in place to deal with this type of eventuality,"

The STM website is still down, but visitors are now redirected to www.lastm.info, where information about public transport services and the attack is posted.



STM website outage information

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

RansomExx gang behind attack

According to a source familiar with the situation, STM suffered an attack by the RansomExx ransomware operation.

RansomExx is a rebranded version of the Defray777 ransomware that become more active in June, with attacks against organizations such as the Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and more recently, Tyler Technologies.

When conducting attacks, RansomExx operators will compromise a network and steal unencrypted files as they spread laterally through the system. Once they gain access to the Windows domain controller, they deploy the ransomware on all available devices.

It is not known if STM has been in contact with the ransomware operators or the ransom amount.

This is a developing story.

Source: https://www.bleepingcomputer.com/news/security/montreals-stm-public-transport-system-hit-by-ransomware-attack/