Metro Vancouver's transit system hit by Egregor ransomware

By Lawrence Abrams

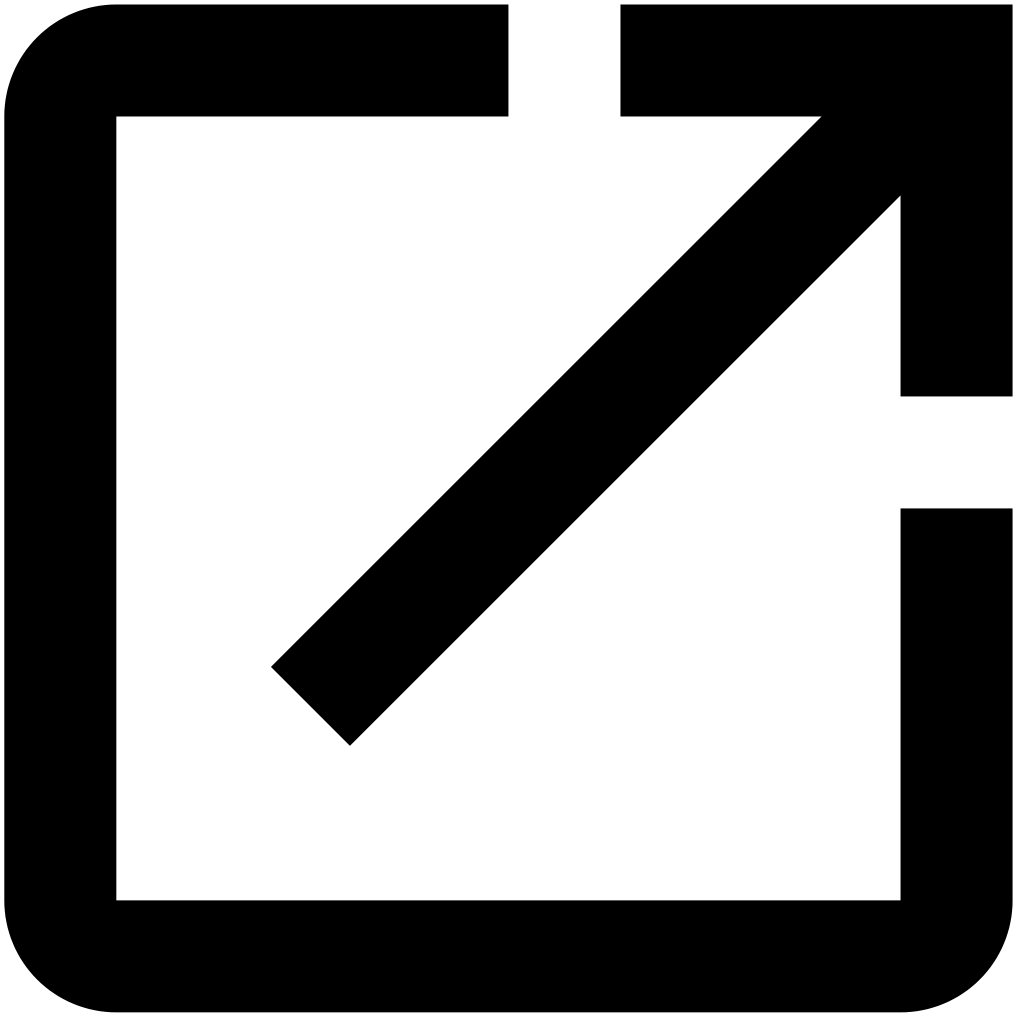
Published: 2020-12-04 · Archived: 2026-04-05 12:57:03 UTC

The Egregor ransomware operation has breached Metro Vancouver’s transportation agency TransLink with the cyberattack causing disruptions in services and payment systems.

On December 1st, TransLink's announced that they were having issues with their information technology systems that affected phones, online services, and the ability to pay for fares using a credit card or debit card. All transit services were unaffected by the IT problems.

After restoring the payment systems, TransLink issued a statement disclosing that a ransomware attack caused the IT problems.


DIE LINKE.
0:00



"We are now in a position to confirm that TransLink was the target of a ransomware attack on some of our IT infrastructure. This attack includes communications to TransLink through a printed message," TransLink disclosed in a statement.

Egregor ransomware was behind TransLink's attack

Global BC reporter Jordan Armstrong tweeted a picture of the ransom note and stated that TransLink printers were repeatedly printing ransom notes.

From the picture of the ransom note, BleepingComputer can confirm that it was the Egregor ransomware operation behind the attack.

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.

Egregor is also the only ransomware known to run scripts that print bomb ransom notes to available printers, as described by Armstrong in his tweet. The Egregor gang performed this same tactic during a recent Cencosud cyberattack, where receipt printers began repeatedly printing ransom notes to draw public attention to the attack.

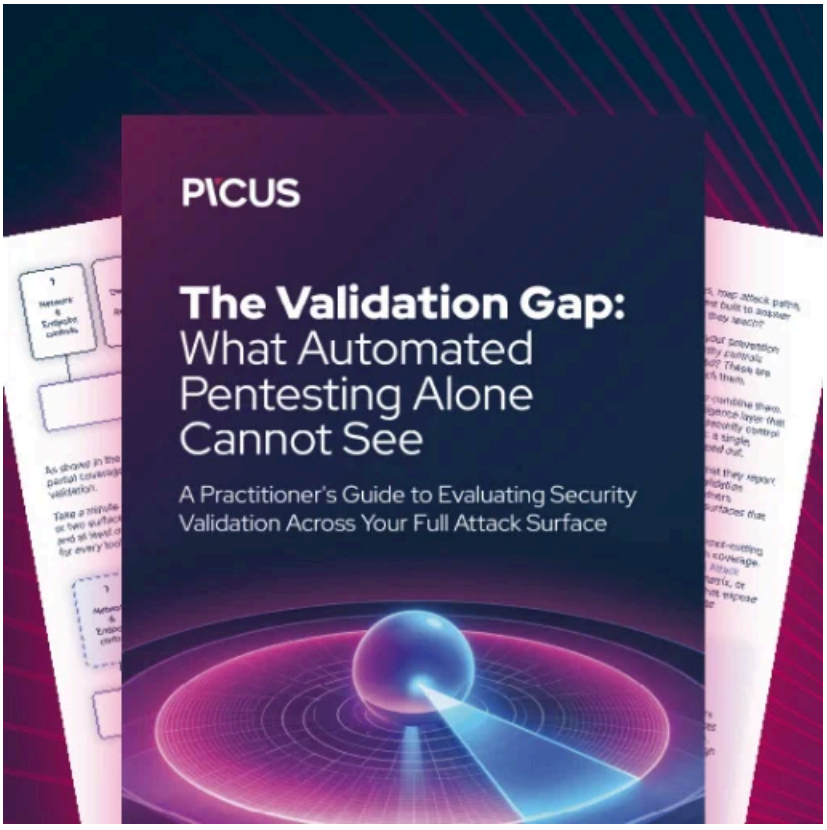
Egregor is a new organized cybercrime operation that partners with affiliates to hack into networks and deploy their ransomware. As part of this arrangement, affiliates earn 70% of ransom payments they generate, and the Egregor operators make a 30% revenue share.

The affiliates who compromise a network are known to steal unencrypted files before encrypting devices with the Egregor ransomware. The hackers then use these stolen files as further leverage by telling victims they will be publicly released if a ransom is not paid.

This ransomware gang began operating in September 2020 after another ransomware group known as Maze shut down their operation. Threat actors told BleepingComputer that many of the affiliates that worked with Maze moved over to Egregor, which allowed the new operation to amass many victims quickly.

These attacks include numerous high-profile companies worldwide, including Kmart, Cencosud, Crytek, Ubisoft, and Barnes and Noble.

Thx to Jack Zhang for the tip!



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/metro-vancouvers-transit-system-hit-by-egregor-ransomware/