TransLink confirms ransomware data theft, still restoring systems

bleepingcomputer.com/news/security/translink-confirms-ransomware-data-theft-still-restoring-systems/

Sergiu Gatlan

By
Sergiu Gatlan

- January 4, 2021
- 01:11 PM
- 0

Metro Vancouver's transportation agency TransLink has confirmed that the Egregor ransomware operators who breached its network at the beginning of December 2020 also accessed and potentially stole employees' banking and social security information.

TransLink announced on December 1, 2020, that the transportation network was experiencing issues with their computing systems following a cyberattack.

These information technology issues impacted the company's phones and online services, as well as the customers' ability to pay for fares with a credit card or debit card. TransLink's transit services were not affected by the IT problems caused by the ransomware attack.

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

During the attack, the ransomware operators used the company's printers to print ransom notes which BleepingComputer identified as Egregor ransom notes, a tactic the cybercrime gang also used after infiltrating the network of retail giant Cencosud in November.

Employee banking info stolen

Although immediately after the attack was discovered TransLink representatives said that "there is no cause for concern that personal data has been compromised" when it comes to customers' information, it looks like this is not the case for employees.

TransLink told employees in an internal email seen by Global News that the Egregor operators have "accessed and may have copied files from a restricted network drive" and several other network drives.

According to the email, the accessed drives containing the payroll information of TransLink, Coast Mountain Bus Company (CMBC), and Metro Vancouver Transit Police employees.

"Those restricted network drives include files that contain banking information and some social insurance numbers," TransLink added.

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.

While the company has evidence that the drives were accessed during the attack, it is still working on identifying the impacted employees and the files that were opened or copied by the attackers.

The transportation agency also urges all employees to sign up for two-year credit monitoring — free for all staff— as soon as possible.

"Importantly, as we outlined previously, TransLink does not store or have access to Compass customer fare payment information," Translink spokesperson Ben Murphy told Global News Wednesday.

Most systems still down

At the moment, most of TransLink's systems are still down after the ransomware attack — including real-time GPS data, tracking, and reporting systems — with company technicians working to restore them as soon as possible.

Customers who want to track buses are advised to use Google trip planner "for the time being," until tracking systems are back online.

"We are now in the process of gradually bringing priority systems back online as safely as possible," Murphy added.

> Unfortunately we're not able to confirm this information at this time, as most of our systems remain unavailable after a cyberattack. We're recommending using Google trip planner for the time being, but that also won't be updated for Winter service changes until tomorrow. ^nv
>
> — TransLink BC | Masks Mandatory (@TransLink) January 3, 2021

Egregor is a ransomware operation that partners with affiliates who hack into targets' networks and deploy ransomware payloads, earning 70% of the ransom payments with the Egregor operators getting a 30% revenue share.

The affiliates who infiltrate victims' networks are also known for stealing files before encrypting devices using Egregor ransomware and for using them as leverage under the threat of publicly leaking them unless the ransom is paid.

Egregor started operating in September 2020 after Maze shut down their operation, with many of the Maze affiliates switching to Egregor as threat actors told BleepingComputer.

Since September, Egregor affiliates breached and encrypted the systems of several high-profile targets worldwide, including but not limited to Ubisoft, Kmart, Barnes and Noble, Cencosud, and Crytek.

Related Articles:

Ransomware attack exposes data of 500,000 Chicago students

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- British Columbia
- Canada
- Data Breach
- Egregor
- Ransomware
- TransLink
- Vancouver

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: