Desorden Group claims to have stolen 200 GB of data from ABX Express

databreaches.net/desorden-group-claims-to-have-stolen-200-gb-of-data-from-abx-express/

DataBreaches.net has been contacted by a threat actor or group calling themselves "Desorden Group" ("Desorden"). The group claims to have hacked ABX Express Enterprise servers in Malaysia on September 23.

> We have stolen more than 200 gigabytes of files and databases, tens of millions of customers personal data from their servers, wiped their drives and left a note about the data breach on their servers.
>
> [ABX] took down their services entirely, informing their customers that they were performing system maintenance, instead of announcing the data breach.

By the time DataBreaches.net checked ABX's web site today, there was no evidence of any maintenance notice.

As proof of their claims, Desorden uploaded two files to a file-sharing service for journalists to download. One showed directories of folders and files on drives C, D, and E. There was also a file with a report that dealt with shipping orders.

ABX Express is a subsidiary of Kerry Logistics. Desorden claims the breach involves millions of Malaysian customers' personal data, with the airway bill database containing more than 15 million records that each contain information on both sender and receiver. Other databases reportedly include financial information, customer, and corporate records.

> Due to the fact that ecommerce platforms share their shopper personal data with logistic companies for delivery, this data breach also involved customer personal data from their partners (Lazada, Shopee, etc.). Their source code files of apps and individual web services have also been stolen by us.

When DataBreaches.net's email to ABX bounced back as rejected due to possible spam, and their web site contact form did not work, DataBreaches.net sent a contact form inquiry to Kerry Logistics to ask them about the claimed breach. An acknowledgement was received but no response has been received as of the time of this publication.

In addition to contacting journalists, Desorden Group also created a listing on a popular forum for buying, trading, or selling data. In that listing, they also offered 100,000 airway bills, and said they would be uploading more data.

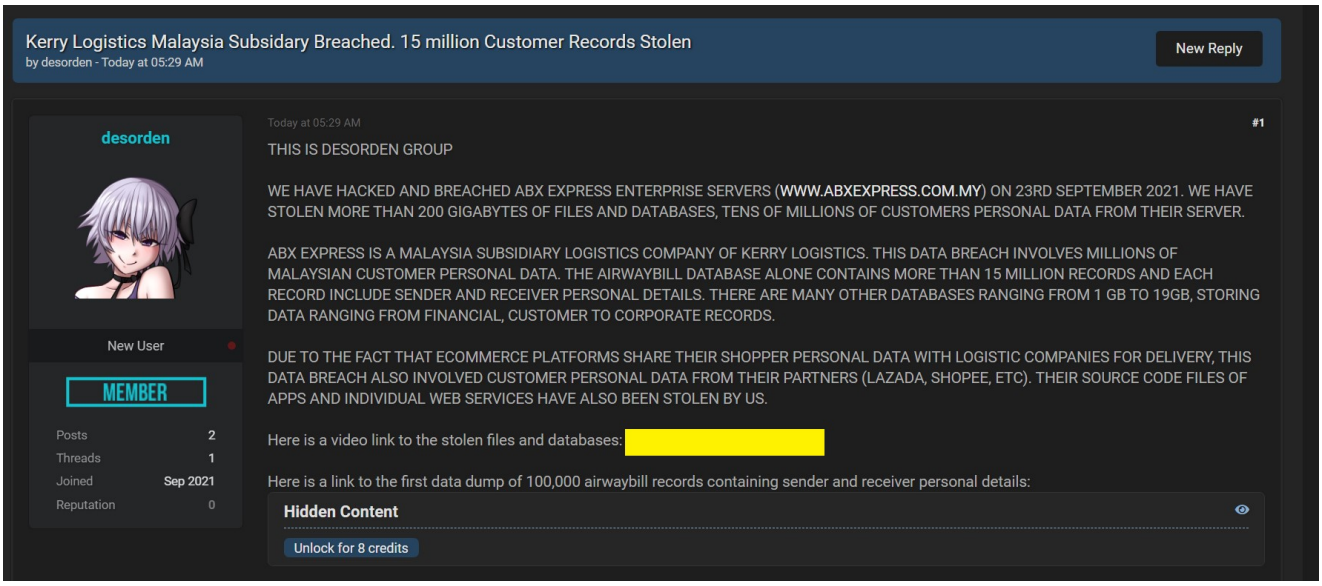

Image: Forum listing. Redacted by DataBreaches.net

When asked how they were able to gain access to ABX, Desorden answered:

> We breached their intranet servers through their front-facing server and maintained APT on servers. They recovered most of their source codes with backups, and are still recovering databases.

The threat actors also told DataBreaches.net that their victim did not respond at all to their notes.

Who is Desorden Group?

In follow-up communications with DataBreaches.net, Desorden described themselves as former associates of Chaos. They:

> Reformed ourselves as Desorden Group which stands for Chaos & Disorder. You might previously know us as ChaosCC but today we no longer have associations with ChaosCC.

As they describe themselves, their targets are supply chain networks and public services, “the name chaos & disorder.”

> Desorden attacks on supply chains create higher level of disorder & chaos affecting many parties rather than the victim itself. If victim fails to pay, Desorden sells the data on black market in a few days. We have another automotive supply chain victim in Italy under negotiation. We will update if it fails.

This post will be updated if a reply is received from Kerry Logistics or more information becomes available.

Related Posts:

- Another Malaysia carrier allegedly hacked and data…
- Desorden Group expands attack on Central Group after deal to…
- Acer under fire: Now hackers claim to have hit Acer Taiwan,…
- Acer India hacked -- again?
- Central Restaurants Group in Thailand hit by Desorden