Another Malaysia carrier allegedly hacked and data exfiltrated -- Skynet - DataBreaches.Net

Published: 2021-10-01 · Archived: 2026-04-09 02:04:37 UTC

Desorden Group, who recently claimed to have successfully breached ABX Express, has contacted DataBreaches.net to report yet another logistics firm breach. This time, the claimed victim is Skynet.com.my. Skynet is a carrier company in Malaysia that provides domestic and international carrier services.

Desorden Group provided DataBreaches.net with proof of claim — a video taken showing Skynet's folders, and some of the files within the folders. One file included 10,000 airwaybill records, while another .csv file contained information on 3,600 employees. Personal information in the files included names, date of birth, account numbers, phone numbers, address, email addresses, encrypted passwords but also passwords in plaintext, and more.

A message included with the video to Skynet reads:

> THIS IS DESORDEN GROUP. WE HAVE HACKED AND BREACHED SKYNET.COM.MY SERVERS FOR 3 WEEKS AND STOLEN MAJORITY OF THE DATABASES, RANGING FROM CORPORATE, FINANCIAL TO CUSTOMER PERSONAL DATA.
>
> WE KNOW YOUR IT DEPARTMENT HAS DISCOVERED THE DATA BREACH ON 27TH SEPTEMBER 2021 AND CLOSED ONE OF THE MANY VULNERABILITIES WHICH WERE USED TO BREACH YOUR SERVERS.
>
> HERE IS A VIDEO RECORDING OF YOUR FILES AND DATABASES FOR VERIFICATION.

According to Desorden Group, the breach involves millions of Malaysian customers' data. And as with the ABX Express breach, Desorder claims that Shopee and Lazada customer data is caught up in the breach. Lazada had never responded to DataBreaches.net's inquiries about the ABX Express, and DataBreaches.net has now reached out to them again to ask what they are doing in response to these claims.

Kerry Logistics never responded to the ABX Express breach, and this site has reached out to them again, too.

DataBreaches.net has also reached out to Cybersecurity Malaysia to see what they can tell us about their efforts to deal with the rising cybercrime in the business sector.

A popular forum where Desorden Group had posted notices about their databases, is not reachable this morning on clearnet, but is reachable on Tor. Whether there is any connection between specific posts on that forum and what is going on is unknown. In recent months, the forum has listed a number of hacks or leaks from ASEAN countries, including some very large firms. Last month, threat actors known as ALTDOS reported that some of their servers had been taken down by their host, but they did not know at whose request or under what legal process. Desorden posted the Skynet incident within the last 12 hours to the same forum ALTDOS has used to list its hacks and leaks. And then the forum was no longer reachable…?

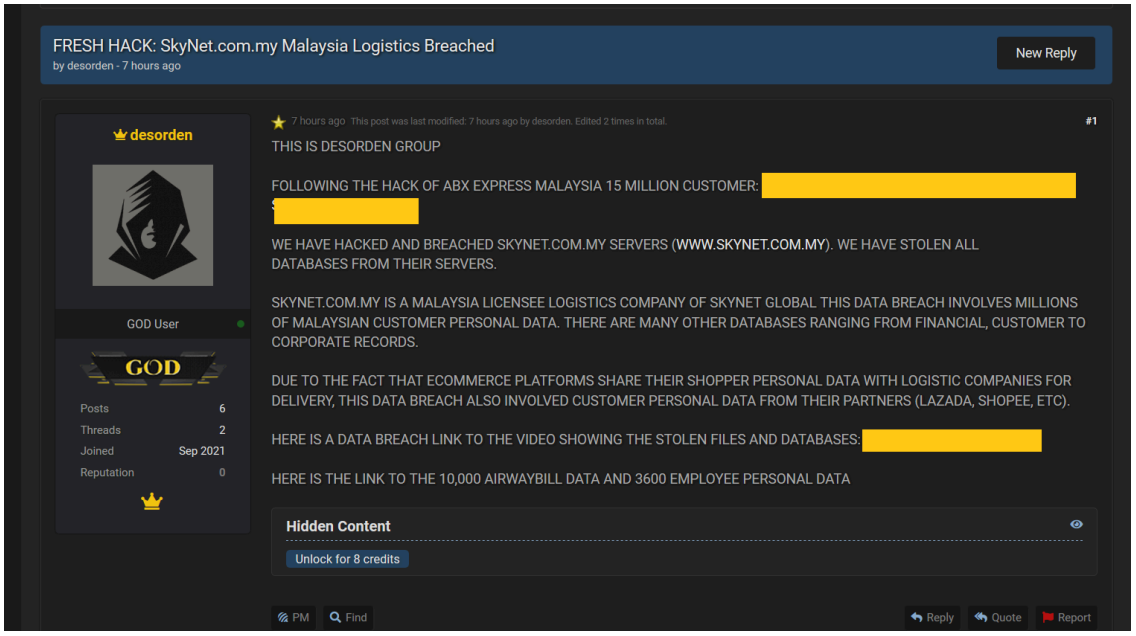

Image: Redacted by DataBreaches.net

Is the forum being down on clearnet related to all the recent uptick in posts from Malaysia and other ASEAN countries or is this a coincidence? DataBreaches.net will be watching the situation.

Updated 11:55 am: *RaidForums is back online on clearnet.*

Source: https://www.databreaches.net/another-malaysia-carrier-allegedly-hacked-and-data-exfiltrated-skynet/