One month later, Ranhill still hasn’t fully recovered from cyberattack

databreaches.net/one-month-later-ranhill-still-hasnt-fully-recovered-from-cyberattack/

Dissent August 31, 2023

On July 26, DataBreaches reported that DESORDEN had attacked **Ranhill Utilities Berhad,** a provider of water and power supply in Malaysia.

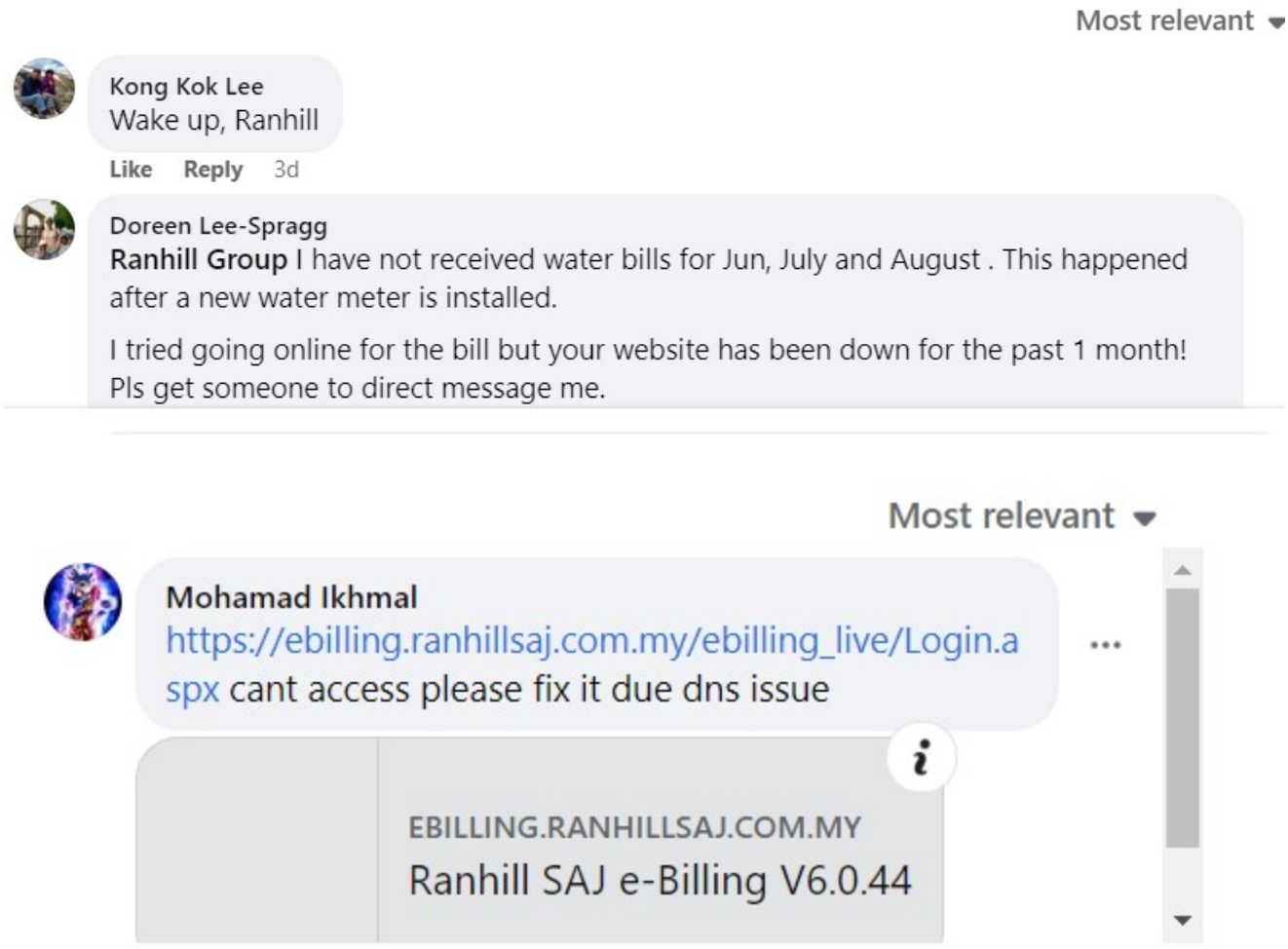
At the time, DESORDEN claimed, in part:

> The initial data breach was initiated on Nov 2021. For over 18 months, DESORDEN has been in their systems. On 17th July 2023, our group infiltrated their LIVE Billing System which handles online payment for more than a million of their customers. Between 18th July to 19th July, DESORDEN stole all of the databases in their billing system, deleted their backups and removed the databases entirely. On 19th July 2023, DESORDEN informed Ranhill management about the data breach and provided a deadline to respond by 21st July 2023. On 20th July, Ranhill company took all of their systems offline and brought the systems back online on 21st July 2023, without responding to DESORDEN (Live Billing System was still unrecoverable). On 23rd July 2023, DESORDEN launched a 2nd attack on their critical online system, AquaSmart which is Ranhill operational tool for managing water-related activities, repair scheduling and reservoir monitoring. Since 23rd July 2023, Ranhill systems are mostly taken offline without notifying the public.

Ranhill did not respond to this site’s inquiries at the time.

More than one month later, it appears that Ranhill has still been unable to fully recover. DataBreaches previously reported complaints on Facebook about the payment app not working. It still isn’t working, and Ranhill does not even reply Facebook to customers who are frustrated and complaining about the inability to pay, as a “Wake up, Ranhill” message posted a few days ago suggests. Another customer complains because they have not received their bills for the past three months and can’t get them because the website is (still) down.

Ranhill has not responded to them.



So What Has Ranhill Done In Response to the Attack?

It's hard to tell. Ranhill never replied to DataBreaches' inquiries in July, and DataBreaches emailed them again on August 27 with a cc: to their investors relations email address. A copy was also sent to the country's data protection regulator. In that email to the firm, DataBreaches posed a number of questions:

1. Did the attack impact the production or delivery of clean water at all?

2. Has Ranhill been unable to restore the payment system? People complain about months of impairment. Why hasn't Ranhill even answered these customers on Facebook?

3. Has Ranhill notified law enforcement about the attack? If so, when did it notify them?

4. Has Ranhill notified any regulators about the attack? If so, which regulators and when did it notify them?

5. Has Ranhill notified employees that their information has been stolen? If so, when did it notify them and what is the company doing to help them protect themselves from fraud?

6. Has Ranhill notified all of its investors about the massive data theft and theft of backups? If so, when and how did it notify them?

No response has been received from Ranhill or the data protection regulator.

At one point, DESORDEN had indicated that the data would be put up for sale, but DataBreaches has not seen any sign of that yet.