


Major Malaysian water utilities company hit by hackers; Ranhill offline; hackers claim databases and backups deleted

 databreaches.net/major-malaysian-water-utilities-company-hit-by-hackers-ranhill-offline-hackers-claim-databases-and-backups-deleted/

Dissent

July 26, 2023

After a period of quiet, DESORDEN Group has re-emerged as a threat to Malaysian entities, and now, it seems, to providing drinkable water to Johor (see [this post from 2021 for an overview of Ranhill Utilities Berhad in the environment sector and the role of AquaSmart](#)). In a statement sent to DataBreaches this morning, DESORDEN writes:

This is DESORDEN Group.

We take responsibilities for the recent data breach of a Malaysian conglomerate, **Ranhill Utilities Berhad**, providing water and power supply in Malaysia. Our attack has disrupted Ranhill operations in billing operations and water disruptions, affecting over 1 million customers. Affected systems include Ranhill's **Live Billing System**, **Mobile Application**, and importantly their **AquaSmart** water management system.

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.

On our end, DESORDEN has already stolen hundreds of gigabytes of files and databases, including sensitive personal information of their customers such as name, address, id card number, phone, email, payment information, etc. As well as their sensitive corporate information including both files, coding and data. We have included the evidences here: [redacted by DataBreaches]

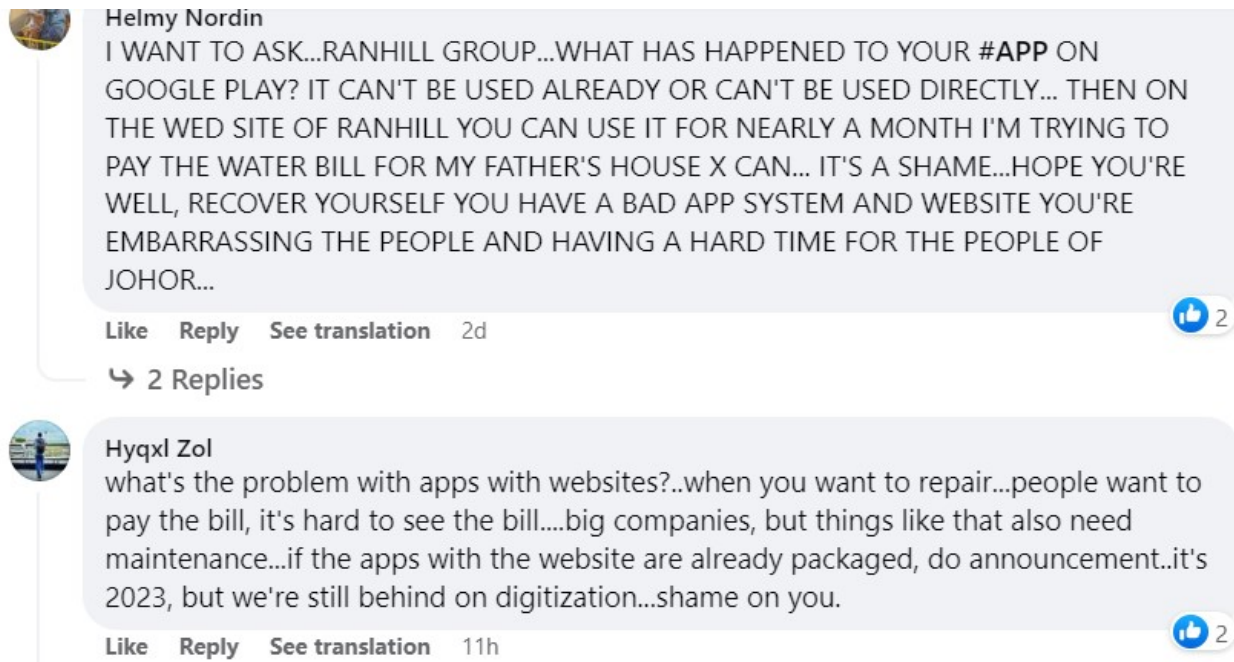
As of today, DESORDEN has not received any responses from Ranhill management. Our group will begin releasing personal details of their customers every week on hacker forums until we receive a response from Ranhill.

As they have always done in the past, DESORDEN does provide proof of claims. In this case, there are seven files or archives with some screenshots, .csv files, and .mkv files that they created. The files include notes left to Ranhill on their server telling them what DESORDEN acquired and how to contact them to prevent further leaks or attacks.

aquasmart.mkv	1 downloads 591.1 KB	2023-07-26 08:35:24	Download Play ...
BSCUSTOMER-Sample.csv	1 downloads 1.5 MB	2023-07-26 08:35:26	Download ...
email-server.png	1 downloads 51.9 KB	2023-07-26 08:35:26	Download Play ...
IBSPASSWORD.csv	1 downloads 2.9 MB	2023-07-26 08:35:29	Download ...
IBSPASSWORD_STAFF.csv	1 downloads 18.1 KB	2023-07-26 08:35:29	Download ...
PAYMENT.csv	1 downloads 24.1 MB	2023-07-26 08:35:38	Download ...
RANHILL-DATA.mkv	1 downloads 2.0 MB	2023-07-26 08:35:40	Download Play ...

Proof of claim files offered to DataBreaches by DESORDEN Group. Image: DataBreaches.net

Ranhill does not appear to have issued any statement about the breach and has not responded to its customers who have been leaving comments and complaints on the firm's Facebook page. The firm stopped updating its posts on July 13, prior to being notified by DESORDEN of the attack and financial demands, but the customers are using previous posts to make comments and ask questions.



Machine translated version of some comments on Ranhill's Facebook page. Image: DataBreaches.net .

As one example, one customer wrote (machine translation):

I WANT TO ASK... RANHILL GROUP... WHAT HAS HAPPENED TO YOUR #APP AT GOOGLE PLAY CAN'T YOU REALLY USE IT OR CAN'T YOU USE IT IMMEDIATELY... AFTER THAT AT WED SITE RANHILL SAJ YOU COULDN'T USE IT FOR NEARLY A MONTH I TRIED TO PAY THE WATER BILL AT MY FATHER'S HOUSE I COULDN'T... IT'S A SHAME... HOPE YOU ALL RECOVER YOUR APP SYSTEM AND WEB SITES THAT ARE BAD EMBARRASSING THE PEOPLE AND HURTING THE PEOPLE OF JOHOR.

Others complain about having no water or too little water, but it is not clear whether that may be due to issues other than the attack.

As of publication time, Ranhill's website remains down. DataBreaches sent an email inquiry to them using their customer support email address and info@ address, but no replies were immediately received. Also as of publication, DESORDEN has listed this incident on a popular hacking forum.