Malaysian Telecom RedOne hit by DESORDEN - DataBreaches.Net

Published: 2022-09-27 · Archived: 2026-04-11 02:09:33 UTC

On September 19, DESORDEN Group claims to have hit redONE Network Sdn Bhd. redONE is a telecom in Malaysia with more than 1.2 million subscribers. redONE also offers financial services via bank partnership (its redCARD program) and insurance services via insurer partnership (its redCARE program).

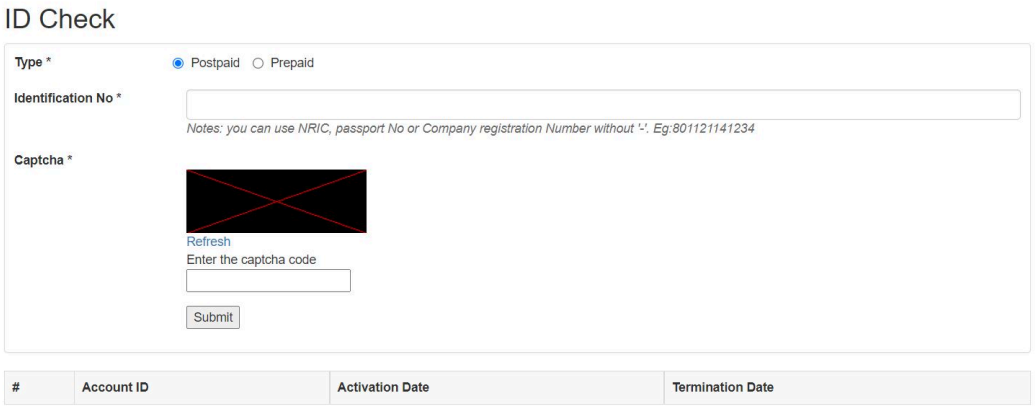
According to statements made to DataBreaches by DESORDEN, when redONE didn't respond to DESORDEN's demands, DESORDEN launched a second attack on or about September 21, hitting their redCARD and redCARE programs.

As DESORDEN wrote on a popular hacking forum:

> This data breach involved both redONE databases and source coding. Personal data include full name, NRIC (national identification number), address, phone, email, etc.

As is their usual pattern, DESORDEN provided samples of data. In this case, there were samples from redONE, redCARD, and redCARE. All three samples included personal information on customers, and all three samples had fields for NRIC.

DataBreaches ran some of the sample data through redONE's site and confirmed that individuals whose NRIC appeared in the sample data from redONE do have or did have accounts with redONE. The ID checker page has since been taken offline by redONE, but an archived copy of the form as it appeared last year appears below. To verify that the data in DESORDEN's sample were real, DataBreaches picked some random entries in the redONE sample, entered the NRIC in the "Identification No" field, and entered the captcha. For each NRIC tested, the redONE checker returned information on the customer's Account ID, when the account was activated and when it terminated.



redONE's ID checker site was taken offline since yesterday. This image is an archived copy from archive.org from 2021..

Although DESORDEN has been just leaking some data recently rather than trying to sell it, they claimed that if they did not hear from redOne within 48 hours of their last email, the data will be posted for sale publicly. It has been about 24 hours or so since their last email.

DataBreaches sent email inquiries to redONE yesterday to ask them if they would confirm or deny DESORDEN'S claims about the breach but has received no reply.
