Thai loyalty membership card data of 5 million customers put up for sale on hacking forum - DataBreaches.Net

Published: 2024-11-20 · Archived: 2026-04-11 02:14:19 UTC

Central Group is a multinational conglomerate in Thailand that describes itself as one of the largest private commercial conglomerates in Thailand with more than 50 subsidiaries and six key business lines. In October 2021, DataBreaches reported an attack on the Central Restaurant Group by threat actors called DESORDEN. When negotiations failed, DESORDEN revealed details about the scope of the attack. Now, it seems another threat actor has obtained data from another Central Group subsidiary.

On November 19, DataBreaches received an email from someone identifying themself as "0mid16B, the same hacker who breached BlackCanyonThai and AIS Serenade on Nov 2024, and shocked the Thai society by bulk notifying over 700,000 of their members at 4am in the morning, resulting in massive news coverage the next following day." The remainder of the email described an incident involving the **Central Retail Corporation**, a publicly owned subsidiary of Central Group.

0mid16B, who tells DataBreaches that they* have never worked with DESORDEN or ALTDOS, wrote:

> Between August to November 2024, i have accessed and stolen 5,108,826 records of Central Group's The1 Card member personal information via an exposed compromised API endpoint of Central Retail network.

Central Group uses The1 Card membership system across every retail and consumer brand under the Central Group. **The1 Card** describes itself as Thailand's largest loyalty platform, with over 17 million members, or about 25% of Thailand's population.

"Due to failed negotiation with Central Group," 0mid16B reportedly decided to sell the data of 5,108,826 records of The1 member personal information. "The stolen information includes First Name, Last Name, Membership Number, National Card ID Number, Country, Mobile Phone and Email. Total size is 582MB," 0mid16B wrote.

0mid16B provided a sample of the data with a way to verify its authenticity. Hours later, the listing appeared on the hacking forum. In the listing, 0mid16B offered to use a middleman escrow service. That is usually (but not always) an indicator of a legitimate seller. The ability to test the sample of data to confirm its validity and the video will also likely persuade potential buyers.

Image: DataBreaches.net

0mid16B also posted the listing on X.com, commenting, "Thai companies do not care about protecting data. Because nothing will happen to them – no PDPA fines, no compensation for customers and no liability #lmao Thai people does not demand for their rights."

DataBreaches asked 0mid16B what happened with the negotiations, curious as to whether Central Group had made a deal with them and then broken it as they had allegedly done to DESORDEN. 0mid16B informed DataBreaches that they had been exfiltrating data until they were detected. Then:

> I contacted the management, and an unidentified person contacted me with a request to hold off any intention to publish. No monetary value was discussed, however a ton of questions on how i stole the data. The contact went uncontactable, and i decide it is time to publish it.

DataBreaches emailed Central Group's contact email and data protection office last night but has received no reply by publication. DataBreaches also sent email inquiries to Central Group's email contacts for investor relations and public relations. Both of those bounced back with "Recipient address rejected: undeliverable" failure messages. This post may be updated if a reply is received.

** 0mid16B informed DataBreaches that they are one individual and not a group. DataBreaches is using "they/them" because they did not indicate their gender pronoun preference.*
