

Customer data from hundreds of Indonesian and Malaysian restaurants hacked by DESORDEN

databreaches.net/customer-data-from-hundreds-of-indonesian-and-malaysian-restaurants-hacked-by-desorden/

Dissent

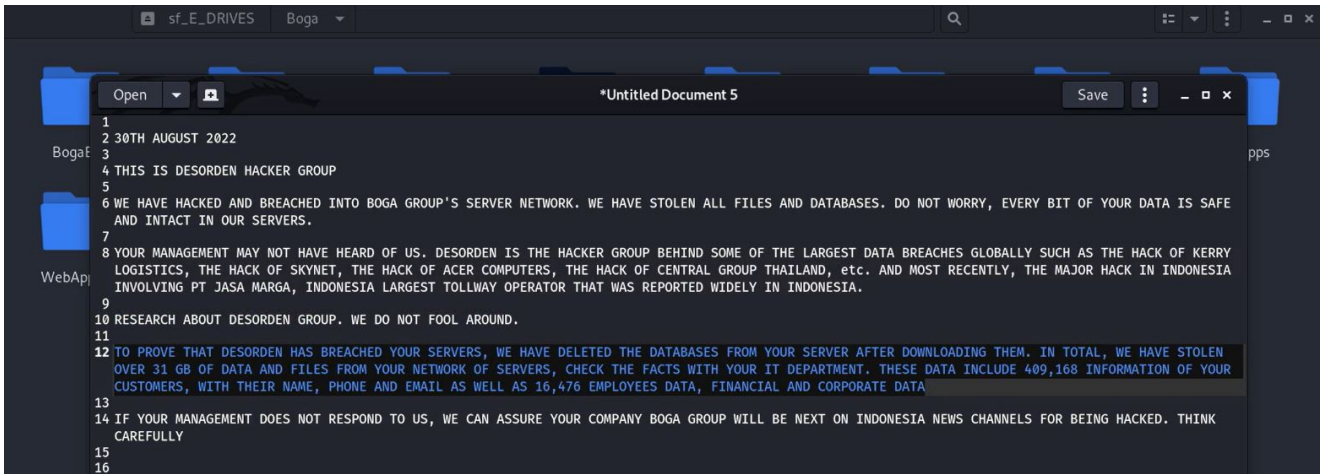
September 2, 2022

Hackers known as DESORDEN have hit another big Indonesian business. This time, their victim was BOGA Group, which operates more than 200 restaurants and outlets across Indonesia and Malaysia under brand names including Bakerzin, Pepper Lunch, Paradise Dynasty, Paradise Inn, Shaburi, Kintan Buffet, Onokabe, Putu Made, Kimukatsu, Yakiniku Like, Ocean 8, Sushi Kaiyo, and Boga Kitchen. Boga Group also operates Boga Catering, a premium catering service.

More than 400,000 customer records and 16,000 employee records were acquired by the hackers.



As is their usual style, DESORDEN provided proof in the form of samples drawn from the corporation's .csv files. They also created a recording showing directories, opened files, documents and spreadsheets. The recording includes a message to their target:



A message to BOGA from DESORDEN was part of a recording showing access to their files. Image: DataBreaches.net

The highlighted portion of the recording reads:

“To prove that DESORDEN has breached your servers, we have deleted the databases from your server after downloading them. In total, we have stolen over 31 GB of data and files from your network of servers. Check the facts with your IT department. These data include 409,168 information of your customers, with their name, phone, and email as well as 16,476 employees data, financial, and corporate data.”

The numbers correspond to the rows displayed in the .csv files shown in the recording.

	A	B	C	D	E	F	G	H	I	J	K
1	Transactio	TransactionDate	OutletID	Email	Name	Phone	IDNumber	BodyTemp	PersonQty	CheckIn	CheckOut
2	BICP/2020	6/25/2020 11:58	BICP	[REDACTED]	[REDACTED]	[REDACTED]		-1	1	58:33.3	13:33.3
3	BICP/2020	59:08.7	BICP	[REDACTED]	[REDACTED]	[REDACTED]		-1	1	59:08.7	14:08.7
4	BICP/2020	28:00.3	BICP	[REDACTED]	[REDACTED]	[REDACTED]		-1	1	28:00.3	43:00.3
5	BICP/2020	58:52.5	BICP	[REDACTED]	[REDACTED]	[REDACTED]		-1	1	58:52.5	13:52.5

A few records from a customer database. DataBreaches.net redacted customers' names, email addresses, and phone numbers.

When asked about the deletion of databases mentioned in their recording, DESORDEN replied, “They have backups. Delete is only for them to know we breached.”

DataBreaches sent an email inquiry to BOGA Group about the attack. No reply has been received.

In discussing this attack with DESORDEN in an online chat, DataBreaches pointed them to [an article](#) from The Jakarta Post about all the leaks and breaches appearing online. DESORDEN commented that the report did make a point. They say it is easy to go after smaller companies in Indonesia because most small companies have little or no security (an observation that applies to small companies worldwide). But DESORDEN also notes that these countries often have weak or no regulations imposing security standards or requiring notification in the event of breaches.

“Countries like India, Malaysia, Indonesia, Thailand. We do not really expect responses from them. Informing them is only for courtesy,” DESORDEN told DataBreaches.

“Selling their data is also as profitable. While it doesn’t fetch as much as victim paying, but a single job data can profit as much as \$20,000 USD in sales of data easily.”

DESORDEN has also recently been telling DataBreaches to expect more breaches in South Korea, Taiwan, Vietnam, and Japan and continuing interest in data from Thailand. The current market is looking for personal information from these countries, DESORDEN states, from “mostly Chinese buyers.”