

Major Indonesia tollroad operator hacked by DESORDEN (Updated)

 databreaches.net/major-indonesia-tollroad-operator-hacked-by-desorden/

Dissent

August 25, 2022

On August 23, DESORDEN alerted DataBreaches to another one of their attacks. This one involved the PT JASAMARGA TOLLROAD OPERATOR, Indonesia's largest major tollway and highway operator. According to DESORDEN's statement:

This data breach involved 252 GB of data, coding and documents, across 5 of their servers. The data breach involves their users, customers, employees, corporate and financial data.




As they always do, they provided proof of claims. In this case, the proof pack consisted of some individual files and a screencap showing properties of a drive they accessed. The claims and links to proof were also posted on a popular hacking forum.

Indonesia's Largest Tollway Operator PT JASAMARGA Hacked by DESORDEN
by desorden - Tuesday August 23, 2022 at 12:43 PM

August 23, 2022, 12:43 PM (This post was last modified: Yesterday, 04:03 PM by desorden.)


THIS IS DESORDEN GROUP

We take responsibilities for the hack and data breach of **PT JASAMARGA TOLLROAD OPERATOR** (<https://www.jmto.co.id>), Indonesia's largest major tollway and highway operator, with a net profit of Rp1.62 trillion in 2021. This data breach involved 252 GB of data, coding and documents, across 5 of their servers. The data breach involves their users, customers, employees, corporate and financial data.

Here are samples of their users' national ID cards and company internal docs: 

News Report of Data Breach:
<https://www.cnnindonesia.com/teknologi/2...duga-bocor>
<https://www.suara.com/teknologi/2022/08/24/1...rum-hacker>
<https://teknologi.bisnis.com/read/202208...duga-bocor>

Attached below is the proof of the total size of data stolen

Attached Files
Thumbnail(s)


Profile: **desorden**
Premium Data Hacker
GOD
Posts: 116
Threads: 16
Joined: Jun 2022
Reputation: 363

DESORDEN listing provided some small proof of claims and filesize of data accessed. Redacted by DataBreaches.net.

Since then, the Jasamarga Tollroad Operator (JMTO) has responded to the claims. Tempo.co [reports](#) their statement that the data acquired is only internal data and company-related information — but not customer data in the JMTO app [SEE UPDATE AT BOTTOM OF THIS STORY]:

“It has been confirmed that it is not related to customer data in the JMTO app,” said JMTO corporate communication community Lisye Octaviana in a statement on Thursday, August 25, 2022.

Lisye said that PT JMTO has now disabled the servers affected by the attack. Lisye added that the company is in the process of recovering the data and moving the system to a more secure server, and closing the security vulnerabilities.

“We are cooperating with competent people in conducting cyber security assessments in the system at PT JMTO,” Lisye said.

DataBreaches was unable to connect to JMTO’s website today. After earlier attempts timed out, later attempts returned an error message that the name had not resolved. As one result, DataBreaches was unable to try to send them any updated inquiries. This site was able to reach DESORDEN, however, to ask them to respond to JMTO’s claims that no customer data from the JMTO app had been compromised.

DESORDEN informs DataBreaches that they are aware of JMTO’s statement and are checking all the 200+ GB of data to determine if JMTO is correct or not about customer data in the app. They anticipate it will take a few days to check through all the data.

In response to other questions from this site, DESORDEN confirmed that no ransomware had been involved in the incident. Of special note, they wanted JMTO to know that there were still open vulnerabilities for JMTO to be aware of, even though they say that JMTO has already addressed two vulnerabilities.

DESORDEN seemed well aware of what steps JMTO has taken and is taking.

Last check, they shut down public access to most servers in JMTO network, but there are other networks like jasamarga.com

There are still open vulnerabilities and if wanted, we can still access other parts of their network,” DESORDEN told DataBreaches. “We have been inside their network since early August. They have a huge network of servers. Vulns are something they really need to look at,” they added.

For now, then, it’s unclear whether customer data from the JMTO app was involved — JMTO says it wasn’t, and DESORDEN is attempting to confirm or refute that but it will take some time.

Eventually, though, after they sort through and organize all the data, DESORDEN will be putting it up for sale.

Update and Correction of September 13: In light of Jasamarga's claims that no customer data was involved, DESORDEN did review the data they had acquired. They inform DataBreaches that there was no customer data — only corporate information and employee information.