Hacker group RansomHouse threatens to sell Shoprite data

Hacker group RansomHouse has been revealed as the culprit behind Shoprite's recent data breach. The hackers are now demanding a ransom from Shoprite and are threatening to sell the compromised data to the public if the company doesn't pay.

Source: Reuters/Siphiwe Sibeko

ITWeb reported that RansomHouse said the following on messaging app Telegram:

“First of all, meet Shoprite! The company that runs your favourite stores if you live in Africa. Truth is, it’s been quite some time since we encountered something THAT outrageous: their staff was keeping enormous amounts of personal data in plain text/raw photos packed in archived files, completely unprotected. Feel free to have a look at the data sample at our website.

“We’ve contacted Shoprite management and invited them to negotiate, but the only thing they did is change their passwords like it solves everything. If their position doesn’t change, most of this data will be sold with something disclosed to the public. Apart from KYC [know your customer] data, we also got lots of other interesting stuff from the company. Yes, they like to keep a lot of things unprotected.”

ITWeb's report defines RansomHouse as a new extortion group that gets into victims’ networks by exploiting vulnerabilities to steal data and coerces victims to pay up, lest their data is sold to the highest bidder.

Potential data breach

Shoprite issued an alert to warn customers of a potential data breach. The group said it became aware of a suspected data compromise, impacting a specific sub-set of data and which may affect some customers who engaged in money transfers to and within Eswatini and within Namibia and Zambia.

The data compromise included names and ID numbers, but no financial information or bank account numbers. Shoprite has notified the Information Regulator.

Shoprite has yet to make a public response to the hackers.