TransUnion South Africa in $15m ransom battle with hacker group

On 17 March, *ITWeb* reported that credit bureau, TransUnion South Africa, is currently in an ongoing battle with a hacker group that is demanding a $15m (R223m) ransom over four terabytes of compromised data.

Source: Pixabay

The hacker group, going by the name N4aughtysecTU, which claims to hail from Brazil, is alleging it breached TransUnion South Africa and accessed 54 million personal records of South Africans.

Speaking to ITWeb via Telegam, the hacker group claims the information it is in possession of credit scores, banking details and ID numbers.

TransUnion South Africa has issued a statement confirming that a criminal third-party obtained access to an isolated South African server, through misuse of an authorised client's credentials.

"This alarming news is further indication that every company that holds personal information is a potential target. The consumer desperately needs an extra layer of protection on their identity against criminals who will turn their lives upside down without a second thought," reports Manie van Schalkwyk, CEO of the Southern African Fraud Prevention Service (SAFPS), who estimated that there are 17 billion cyberattacks that take place around the world every day, not all being successful.

A history of breaches

Over the past two years, South African companies have been reporting that they have been victims of cyberattacks and data breaches. Some of these breaches include the compromise of personal information of consumers.

No organisation is immune against cyber attacks and the Department of Justice recently announced that it was a victim of a cybercrime. In a separate incident, Debt-IN Consultants, a professional debt-recovery solutions partner to many South African financial services institutions, announced on 22 September that a ransomware attack by cyber criminals resulted in a significant data breach of consumer and employee personal information.

It is suspected that consumer and personal information of more than 1.4 million South Africans was compromised through the Debt-IN attack in April last year. The breach only came to light last week.

Common practice

“Data breaches have been on the rise globally and South Africa has seen unprecedented increases in the number of cyber victims,” says Dalene Deale, executive head of Secure Citizen.

Secure Citizen was created through a collaboration with SAFPS and OneVault in response to a rapid growth in identity theft following online fraud. “Fraudsters do not discriminate. As we continuously move towards the adoption of a digital and more importantly ‘touchless’ era, the platform for fraud increases.

"Fraud is a fraudster’s business and they often use the same business tactics we use in legitimate business, the difference being that they don’t have customers, they have victims. Thanks to an increase in data breaches, fraudsters are motivated and armed with the correct information, meaning that they are capable of impersonating an individual. The impacts of this are catastrophic,” says Deale.

Van Schalkwyk points out that the TransUnion breach is concerning as the records of 54 million South Africans may have been compromised. “In a country where identity fraud is common practice, this is extremely concerning. It is critical that consumers act now before significant fraud is unknowingly committed on their behalf. In the last significant data compromise in 2020 - where more than 20 million records were compromised with another credit bureau - the SAFPS saw a rise of impersonation of more than 300%,” says Van Schalkwyk.

Digital Protective Registration (powered by Secure Citizen)

One of the most important services, and the core of SAFPS’ service offering, is Protective Registration. Protective Registration is a free service protecting individuals against identity theft. Consumers apply for this service and the SAFPS alerts its members to take additional care when dealing with that individual’s details.

Protective Registration provides an added layer of protection and peace of mind regardless of whether the identity of the applicant has been compromised.

“As a society, it is important that we move towards creating a world where the fight against fraud becomes protective and proactive,” says Van Schalkwyk.