Hackers demand $10 mn for stolen Australian health records

November 10 2022, by Steven TRASK

Hackers are demanding US$10 million to stop leaking sensitive records they stole from Medibank, Australia's largest private health insurer.

Hackers on Thursday demanded US$10 million to stop leaking highly sensitive records stolen from a major Australian healthcare company, as they uploaded yet more intimate details about customers.

Medibank, Australia's largest private health insurer, confirmed this week that hackers had accessed the information of 9.7 million current and former clients, including Prime Minister Anthony Albanese.

The hackers on Thursday uploaded a second batch of files to a dark web forum, with more sensitive details about hundreds of Medibank customers.

The first leaks appear to have been selected to cause maximum harm: targeting those who received treatment related to drug abuse, sexually transmitted infections or pregnancy terminations.

"Added one more file abortions.csv," the anonymous hackers wrote on the forum, before detailing their ransom threat.

"Society ask us about ransom, it's 10 million USD. We can make discount... $1 = 1 customer."

Medibank has repeatedly refused to pay the ransom.

'Profit and greed'

The Medibank hack—and an earlier data breach impacting nine million customers at telecom company Optus—has raised questions about Australia's ability to repel cyber criminals.

Dennis Desmond, a former FBI agent and US Defense Intelligence Agency officer, said Australia was no worse "than any other high-value target or Western country".

"It's very unfortunate, but I don't think Australia is any more vulnerable than any other Western developed nation," he told AFP.

Desmond said profit-driven hackers were unlikely to single out a specific country—and were typically more interested in targeting companies holding valuable data.

"It's the data types that are of the most interest to these hackers," he said.

"The healthcare data is a huge target and personally identifiable data is high-value.

"Generally, profit and greed are the number one drivers."

'Scummy criminals'

The Medibank hack is likely to include data on some of the country's most influential and wealthy individuals.

Medibank chief executive David Koczkar condemned the "disgraceful" extortion tactics.

"The weaponisation of people's private information in an effort to extort payment is malicious and it is an attack on the most vulnerable members of our community."

The group behind the attack appears to be pressuring Medibank by hunting for the most potentially damaging personal information within the records.

The first records posted to the dark web forum were separated into "naughty" and "nice" lists.

Some on the "naughty" list had numeric codes that appeared to link them to drug addiction, alcohol abuse and HIV infection.

For example, one record carried an entry that read: "p_diag: F122".

F122 corresponds with "cannabis dependence" under the International Classification of Diseases, published by the World Health Organization.

Names, addresses, passport numbers and birth dates were also included in the data.

Home Affairs Minister Clare O'Neil has described the hackers as "scummy criminals".

© 2022 AFP