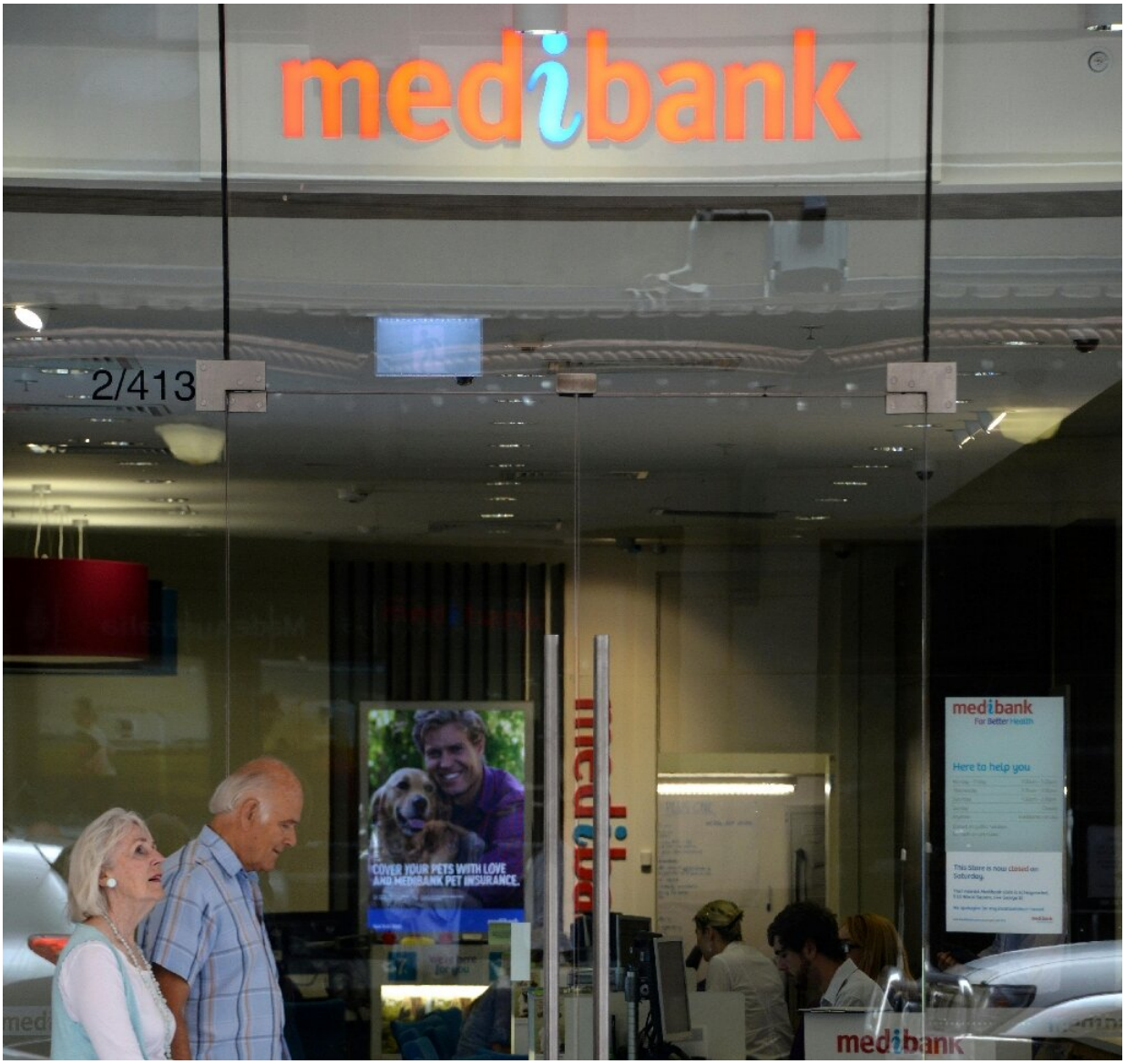
Hackers leak Australian health records on dark web

November 9 2022, by Steven TRASK, Johnny LIEU



Hackers have begun leaking sensitive medical records stolen from Australian

health insurer Medibank, whose customers include the prime minister.

Hackers have followed through on a threat to leak sensitive medical records stolen from a major Australian health company that counts the country's prime minister among nearly 10 million customers.

Medibank told investors that a "sample" selection of customer data was posted on a "dark web forum" on Wednesday after it refused to pay a ransom demand.

The data included names, birth dates, passport numbers and information on medical claims for hundreds of customers who 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.

Medibank is Australia's largest private health insurer and the hack is likely to include some of the country's most influential and wealthy individuals.

Prime Minister Anthony Albanese said he himself was a Medibank customer and that the attack was a "wake-up call" for corporate Australia.

Potential Russian link

The perpetrator of the hack has not yet been publicly identified.

But the Australian Federal Police's Justine Gough said it was the work of a "criminal or criminal groups" that could be operating outside the country.

Sanjay Jha, chief scientist at the University of New South Wales's Institute for Cyber Security, said it was difficult to attribute any attack to a single group.

However, he told AFP it carried some of the hallmarks associated with a Russian hacker group called REvil—which has previously targeted everything from Brazilian meat company JBS to Lady Gaga.

"The pattern matches the behaviour in parts. So that is why there is a serious indication it could be them selling the data," Jha said.

A defunct REvil website has been redirecting traffic to the dark web forum where the Medibank data was leaked.

REvil—an amalgam of ransomware and evil—was the subject of a US$10 million reward from US authorities before being reportedly dismantled by Russia this year.

JBS Foods, one of the largest beef producers in the world, paid REvil a ransom of US$11 million in 2021.

Jha said the hackers could now look to sell the sensitive data to blackmailers and other scammers.

'Scumbags' and 'crooks'

The hackers also uploaded what they said were a series of messages sent to Medibank in the days before the leak.

"We will do everything in our power to inflict as much damage as possible for you, both financial and reputational," one message from the hackers read.

Hundreds of millions of US dollars have been wiped off Medibank's market value, with the company's share price down more than 20 percent since October, when news of the leak first emerged.

Troy Hunt, a cyber security expert working for Microsoft, wrote on Twitter that the breach was "about as bad as we feared it would get".

The Medibank hack followed an attack on telecom company Optus in September that exposed the personal information of some nine million Australians.

Jha said the enormous Medibank and Optus data breaches could make it easier to carry out cyber attacks on different systems in the future.

"A lot of credentials have been stolen in recent months," he said. "That makes the job of attackers easier—they can go and try other systems with millions of credentials."

Australia's assistant treasurer Stephen Jones said the perpetrators were "scumbags" and "crooks".

"We shouldn't be giving in to these fraudsters," he told local media.

As Medibank tried to contain the leak, it was also staring down the barrel of a potentially costly class action lawsuit.