TechXplore

Medibank won't pay hackers ransom. Is it the right choice?

November 8 2022, by Mohiuddin Ahmed and Paul Haskell-Dowland

Credit: AI-generated image (disclaimer)

Medibank is still refusing to pay a ransom of an undisclosed amount to cybercriminals, despite the hackers now allegedly threatening to release the stolen data on the dark web.

It's reported the data of about 9.7 million current and former Medibank customers were compromised in a breach first confirmed by Medibank on October 13.

The data are said to include customers' names, dates of birth, addresses, phone numbers and email addresses—as well as some 500,000 health claims with information such as patients' service provider details, where they received medical services and the types of treatments they claimed.

Medibank's chief executive has said the company won't be paying up—a decision endorsed by Home Affairs Minister Clare O'Neil. But what does the evidence say?

How were the data stolen?

According to various reports, it all started when a hacker compromised the credentials of a Medibank employee who had access to a number of the company's data repositories. It's unclear whether the employee would have needed multifactor authentication to access these data—and, if so, whether this was also compromised.

It's believed this hacker then sold the employee's credentials to notorious cybercriminal group REvil via an online Russian language forum. Around midnight, REvil posted on the dark web threatening it would release the data in the next 24 hours should the ransom not be paid.

While there's no evidence REvil does indeed have access to the stolen data, historically the REvil group has not been found to bluff. There's no reason to believe this time is different.

Medibank first identified unusual activity on its network on October 12. It then launched a follow-up investigation that confirmed the breach. We don't know how long the cybercriminals may have had access to its systems before then.

It's reported they stole some 200GB of data in total. This is quite a large amount, and it would be unusual not to notice the exportation of this much sensitive data.

In this case, however, it seems the criminals used some sort of compression algorithm to minimize the data file size. This may have allowed the data extraction to be less obvious, perhaps also through splitting the data into smaller data packages.

To pay or not to pay?

Medibank chief executive David Koczkar has said the ransom request would not be paid, and "making any payment would increase the risk of extortion for our customers, and put more Australians at risk". He said the decision is consistent with advice from cybersecurity experts and the Australian government.

This is, in fact, a smart decision. Even if the ransom is paid, it does not guarantee the cybercriminals will not use the stolen data for other malicious purposes, or won't undertake further attacks against Medibank.

Law enforcement agencies across the world are against paying ransoms. However, there are life-threatening situations in a healthcare context, such as during remote surgery, when there may be no choice.

Cybercriminals take advantage of vulnerabilities in healthcare IT infrastructure—largely because there's a higher chance of getting a ransom paid in healthcare than in any other sector.

Often, organizations targeted will have to pay a ransom to get back access to data and continue providing healthcare services. According to one recent report the majority of ransomware attack victims in healthcare end up paying the ransom.

As to why Medibank hasn't disclosed the specific ransom amount, this is because this information could encourage other cybercriminals to aim for similar targets in future ransom events.

If the ransom were disclosed, and later had to be paid, Medibank's reputation as an insurance provider would hit rock bottom. When Colonial Pipeline's fuel pipeline infrastructure in the US was hit by a ransomware attack, the hefty ransom payment of US$4.4 million left a permanent scar on the operator's reputation.

The risks as the situation unfolds

The risks for victims of the Medicare data breach must not be underestimated. This sensitive information could be used in various types of fraud. For example, hackers may call victims of the data breach pretending to be Medibank, and ask for a service charge to have their data safeguarded. Healthcare data can also be used for blackmail and fraudulent billing.

What's more, hackers can identify the most vulnerable individuals among the list of victims and create customized attack vectors. For example, individuals with implanted devices (such as pacemakers) can be targeted with blackmail and threats to their life.

Beyond this, cybercriminals could also use victims' personal information to conduct a number of other scams unrelated to Medibank or healthcare. After all, if you have someone's details it's much easier to pretend to be any organization or company with authority.

For those potentially affected by the Medicare data breach, the most important thing now is to remain vigilant about all types of online activity. You can start by replacing your passwords with more secure passphrases. You should also consider running a credit check to see if any suspicious activity has been conducted in your name.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Medibank won't pay hackers ransom. Is it the right choice? (2022, November 8) retrieved 10 May 2024 from https://techxplore.com/news/2022-11-medibank-wont-hackers-ransom-choice.html