“Multifactor or two-factor authentication has been in our environment and we’ve taken steps to further strengthen that,” Medibank chief executive David Koczkar told the Financial Review.

“The full investigation of what happened, how the credentials were compromised, and how they got in will be the focus of the forensic investigation to ensure that that was actually working properly.

“But we did have those controls, but this is an evolving space, we really continue to look at the latest solutions that are available to protect customer data.”

The stolen Medibank login credentials were put up for sale on a number of Russian language forums, on both the regular internet and dark web, where they were acquired by the criminal group, which has since been in touch with Medibank to prove it had genuine data.

Once it got the credentials the criminal group is believed to have set up two backdoors into the Medibank network, before lurking on the Medibank networks for an unknown period of time performing reconnaissance. This would have involved accessing internal documentation to understand how the different systems and internal applications work, and how they are structured to share information.

Investigators believe the crooks were then able to build a bespoke tool that was uniquely configured to work within Medibank’s network, with the specific purpose of large-scale data theft.

It worked by building automated queries that interrogated Medibank’s internal databases and prepared huge volumes of data to be taken out of the system undetected.

Since the hack became public knowledge [experts have questioned how up to 200 gigabytes of ultra-sensitive customer data could be removed](https://www.afr.com/technology/medibank-mystery-was-a-user-credential-all-that-was-needed-for-hack-20221021-p5brqv) from Medibank’s systems without anyone noticing. Investigators believe the data was probably compressed in a way familiar to anyone who has ever had to send multiple large files from a regular email system.

All the reports run by the crooks’ algorithms were thought to have been pulled together into a single ZIP file. It was around this time that Medibank noticed suspicious activity on the network, but it was too late to stop the theft.

Investigators, including Australian cyber security consultancy CyberCX, are still in the process of understanding exactly how and when the data left Medibank’s networks.

According to the investigators’ timelines Medibank was able to close the two backdoors created by the thieves, but the company was then contacted by the Australian Signals Directorate to say it had noticed some online chatter, suggesting a ransomware attack was on the way.