In ransomware attacks, the [**initial access**](https://socradar.io/top-5-tactics-threat-actors-use-for-initial-access/) point is generally gathered using **phishing attacks**. We do not know how threat actors stole the initial credentials in this attack. What we know is that the credential used for the attack was bought and sold in a [**Telegram channel**](https://socradar.io/the-top-10-dark-web-telegram-chat-groups-and-channels/). An unidentified bidder bought and sold these credentials on the dark web, then used them to access Medibank’s internal network.

Once inside, the threat actor located a customer database and then utilized the privileged credentials that were taken to develop a script to **automate the exfiltration** of customer data. After compressing **200 GB** worth of data from Medibank’s systems to **5GB**, they used two established backdoors to extract this stolen data from a zip file after compressing it. At this time, the security team at Medibank allegedly noticed unusual behavior and sealed both backdoors—but not before the data had been stolen.