The Medibank hack began with the theft of credentials belonging to a[n individual with privileged access](https://www.theguardian.com/technology/2022/oct/24/medibank-hack-started-with-theft-of-staff-members-credentials-investigation-suggests#:~:text=The%20attack%20is%20believed%20to,not%20authorised%20to%20speak%20publicly.) to Medibank’s internal systems.[These credentials were sold](https://www.theguardian.com/technology/2022/oct/24/medibank-hack-started-with-theft-of-staff-members-credentials-investigation-suggests#:~:text=The%20attack%20is%20believed%20to,not%20authorised%20to%20speak%20publicly.) and purchased on the dark web by an unconfirmed buyer who used them to gain access to Medibank’s internal system.

Once inside, the threat actor identified the location of a customer database and then used the stolen privileged credentials to write a script to automate the customer data exfiltration process - a similar data theft mechanism was used in[the Optus data breach](https://www.upguard.com/blog/how-did-the-optus-data-breach-happen).

This stolen data was placed into a zip file and extracted through two established backdoors. Medibank’s security team allegedly detected suspicious activity at this point and shut down both back doors, but not before 200GB worth of customer data was stolen,

9.7 million Medibank customers were impacted by the breach. Compromised records include:

* Names
* Birth dates
* Passport numbers
* Information on medicare claims

News of the successful attack was published on the dark web blog associated with a ransomware gang tracked as BlogXX (a cybercriminal group believed to be a reformation of the notorious ransomware gange REVil). The hackers posted a sample of the stolen data to prove the legitimacy of their claims and demanded Medibank pay a US$10m ransom to prevent the entire database from being freely published on the dark web.

To force Medibank to pay the ransom, the cybercriminal group will continue posting segments of the stolen database until the ransom is paid completely.

Corporate Credential Theft: The Reason the Medibank Breach was Possible

The Medibank data breach was made possible by the theft of internal credentials believed to belong to an individual with privileged system access. Internal credential theft is one of the first objectives of almost every cyberattack. It hasn’t yet been confirmed how the Medibank credentials were stolen, but the most common method of stealing account information is through a tactic known as Phishing - a style of cyberattack where hackers send fraudulent emails with malicious links leading to credential-stealing websites.

When hackers steal “disappointing” account credentials with limited user permissions, they use them to get inside a network and then clandestinely examine every region of it, searching for higher privilege credentials to steal - a process known as ‘lateral movement.’

By instantly getting their hands on privileged account details, the Medibank hackers bypassed the arduous lateral movement stage of the attack and skipped straight to the final data breach stage. This compressed the cyberattack pathway, allowing the breach to be completed much faster.