**Extion Infotech**

**Project 2**

**Report**

**Investigation to Data Breach**

**Medibank Data Breach Attack**

**Created by: -**

**Sudarshan Sinha**

**Cybersecurity Intern, Extion Infotech**

**About the Company: -**

Here's an edited version with improved clarity and readability:

Medibank Private Limited, commonly known as Medibank, is Australia's largest private health insurance provider, headquartered in Melbourne, Victoria. As of 2024, it provides coverage to approximately 4.2 million customers.

Medibank was originally established in 1976 by the Australian Government as a not-for-profit insurer. In 2009, under the Rudd Government, it transitioned into a for-profit entity, and in 2014, the Abbott Government privatized the company.

Today, Medibank operates as a publicly listed company on the Australian Securities Exchange (ASX).

**Incident Analysis: -**

Incident Title: - Medibank Data Breach Attack

Date of Incident: -October 13, 2022

Location: - headquarters in **Melbourne, Victoria, Australia.**

Incident Type: - Data Breach

**About the Attacker: -**

Here’s an improved version with clearer structure and readability:

**REvil (Ransomware Evil),** also known as **Sodinokibi,** was a Russia-based or Russian-speaking **ransomware-as-a-service (RaaS)** operation. The group specialized in cyber extortion, targeting businesses and organizations worldwide.

After successfully infiltrating a target, REvil would demand a ransom, threatening to publish stolen data on their leak site, known as the **"Happy Blog,"** if the payment was not made.

One of their most high-profile attacks involved breaching a supplier of tech giant **Apple,** where they stole confidential schematics of upcoming products.

In **January 2022,** the **Russian Federal Security Service (FSB)** announced that they had dismantled REvil and arrested several of its members, effectively disrupting the group's operations.

**Key Facts About REvil:**

1. **Origins & Operations:**
   * Believed to have emerged in 2019 from the remnants of another notorious ransomware group called **GandCrab**.
   * Operates primarily from Russia or Russian-speaking regions, often targeting Western countries.
   * Their attacks usually involve double extortion tactics—encrypting data and threatening to leak sensitive information unless a ransom is paid.
2. **Notable Attacks:**
   * **Kaseya (2021):** A large-scale supply chain attack affecting thousands of businesses globally.
   * **JBS Foods (2021):** A major meat supplier paid an $11 million ransom after their systems were compromised.
   * **Acer (2021):** Targeted the tech giant with a demand of $50 million.
   * **Medibank (2022):** Stole personal and medical data from millions of customers.
3. **Tactics Used:**
   * Phishing emails, exploiting software vulnerabilities, and using stolen credentials to gain access.
   * Encrypting critical files and demanding cryptocurrency payments (usually Bitcoin or Monero).
   * Operating through underground forums and the dark web to avoid law enforcement detection.
4. **Current Status:**
   * Despite crackdowns, parts of the group are believed to still be active under different aliases or through other cybercrime networks.

The **Medibank data breach (2022)** was reportedly carried out using a combination of common cyberattack tools and techniques. While exact details have not been fully disclosed, cybersecurity experts and investigations revealed that the attackers likely used the following tools and methods to compromise Medibank’s systems:

**Summary of the Incident: -**

**Date of Incident:**

* The data breach was first detected on **October 13, 2022**, when Medibank identified unusual activity within its systems.

**Nature of the Attack:**

* A cybercriminal group gained unauthorized access to Medibank's internal systems, stealing sensitive customer data.
* The attackers accessed personal information including **names, addresses, dates of birth, Medicare numbers, phone numbers, and health claims data**, covering services such as medical conditions and treatments.
* No financial data or banking details were compromised.

**Number of Affected Individuals:**

* Approximately **9.7 million** current and former customers were affected, including:
  + 3.9 million Medibank customers
  + 1.8 million ahm (a Medibank subsidiary) customers
  + 1.8 million international student customers

**Attacker's Actions:**

* The hackers demanded a ransom, threatening to release the stolen data if the ransom was not paid.
* Medibank refused to pay, citing ethical concerns and advice from cybersecurity experts.
* In response, the attackers published sensitive health records on the dark web, including details of mental health conditions and drug addiction treatments.

**Impact of the Breach:**

* Significant reputational damage to Medibank.
* Customer distress due to exposure of private medical information.
* Increased regulatory scrutiny, with investigations by the Australian government and cybersecurity agencies.
* Potential legal actions and class-action lawsuits from affected customers.

**Response and Mitigation:**

* Medibank implemented enhanced cybersecurity measures and engaged with the Australian Cyber Security Centre (ACSC) to investigate the breach.
* Customers were advised to stay vigilant against phishing attempts and scams.
* Free identity and credit monitoring services were offered to affected individuals.

**Forensic Analysis:**

1. **Attack Method:**
   * The attackers gained access via compromised employee login credentials, likely obtained through phishing or the use of stolen credentials from previous data leaks.
   * Once inside, they escalated their privileges and moved laterally within Medibank’s network.
2. **Data Compromised:**
   * The stolen data included sensitive information such as:
     + Names, addresses, dates of birth.
     + Medicare numbers and phone numbers.
     + Health claims data, including medical procedures and conditions.
   * Approximately 9.7 million current and former customers were affected.
3. **Threat Actor:**
   * The forensic analysis linked the breach to a Russia-based cybercriminal group, believed to be linked to the REvil ransomware gang.
   * The attackers utilized ransomware-as-a-service (RaaS) techniques but did not encrypt Medibank's systems; instead, they focused on data theft and extortion.
4. **Tactics Used by Attackers:**
   * Credential theft: Use of stolen usernames and passwords to gain initial access.
   * Privilege escalation: Gaining higher-level access to sensitive databases.
   * Data exfiltration: Encrypting and stealing sensitive data without deploying traditional ransomware.
   * Extortion attempts: Threatening to release customer data on the dark web if ransom demands were not met.
5. **Medibank’s Response:**
   * Medibank refused to pay the ransom, following advice from cybersecurity experts and law enforcement.
   * The company implemented additional security measures, such as:
     + Enhanced multi-factor authentication (MFA) for all systems.
     + Strengthened network monitoring and segmentation.
     + Employee cybersecurity awareness training.

**Conclusion:**

The forensic investigation into the Medibank data breach revealed it was a highly sophisticated attack, likely orchestrated by professional cybercriminals with ties to **Russian ransomware groups.** The breach underscored the importance of robust cybersecurity measures in protecting sensitive healthcare data and reinforced Medibank's commitment to enhancing its security framework.

The breach emphasized the pressing need for **continuous investment in cybersecurity infrastructure, proactive threat intelligence, and comprehensive employee awareness training** to prevent similar incidents in the future. Medibank’s response, including the decision not to pay the ransom and to work closely with cybersecurity authorities, reinforced the company’s commitment to transparency and ethical handling of cyber threats. Moving forward, the findings from the investigation have driven Medibank to implement **enhanced security measures, such as stronger multi-factor authentication, improved network segmentation, and real-time threat monitoring.** Additionally, the incident highlighted the importance of **collaborative efforts between the private sector, government agencies, and cybersecurity experts** to combat cybercrime and ensure the resilience of critical infrastructure against future attacks.

**Early Measures To Prevent From Data Breach:-**

**1. Cyber Threat Awareness Training**

Cyber threat awareness training teaches employees how to recognize and correctly respond to corporate credential theft attempts from phishing and social engineering attacks.

We don’t yet know how the Medicare credentials that facilitated the breach were stolen, but by teaching your employees how to recognize a phishing attack, you’ll protect your business from the most common method of credential theft.

**2. Implement the Principle of Least Privilege (POLP)**

The principle of least privilege is an account security policy that limits each employee’s account access to the minimum level required to perform daily tasks. This should be a standard security policy for all Australian businesses since excessive privileges present a significant security risk.

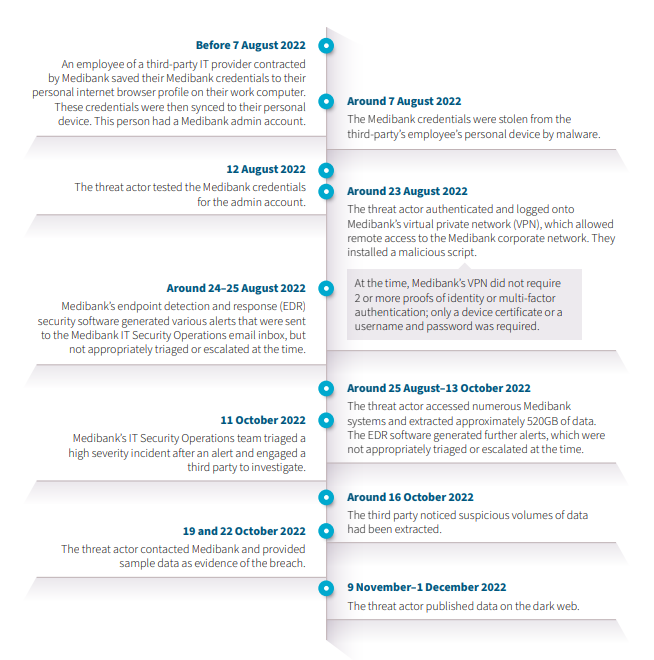
By reducing the chances of hackers bypassing the privilege escalation phase of an attack, a POLP policy forces the entire attack to take longer, which increases the chances of vigilant security teams detecting and intercepting the breach attempt. The Medibank event proved that it’s possible to disrupt a cyberattack while it's still unfolding, reducing its potential damages.

**3. Segment your Network**

A network segmentation strategy separates a network into different segments or “zones” to make sensitive data more difficult to locate and access. In case a sensitive zone is located, connection requests to this region should be passed through a jump server (a hardened system used to manage connection requests to sensitive zones) to further reduce the potential for compromise.

**4. Use Multi-Factor Authentication (MFA)**

It hasn’t yet been confirmed whether multi-factor authentication was bypassed during the Medibank hack. MFA is one of the most effective measures against account compromise attempts.

**Incident Timeline: -**

**Communications And Notification:-**

**October 12 - Suspicious Activity Detected and Reported to Medibank CEO**

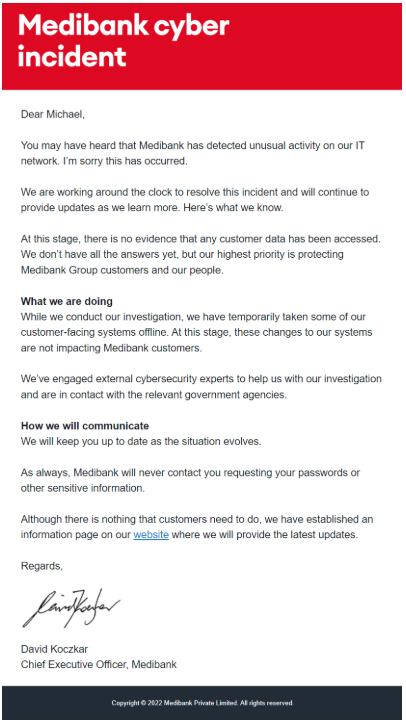
**Medibank Chief Executive, David Koczkar**, receives an internal call notifying him of suspicious activity detected inside the company’s network.

**October 13 - Medibank Announces Suspicious Activity Detection to the Public**

Medibank releases a public statement about a potential cyberattack but says no evidence of customer data compromise has been found.

Yesterday the Medibank Group detected unusual activity on its network.In response to this event, Medibank took immediate steps to contain the incident and engaged specialised cyber security firms.At this stage, there is no evidence that any sensitive data, including customer data, has been accessed.As part of our response to this incident, Medibank will be isolating and removing access to some customer-facing systems to reduce the likelihood of damage to systems or data loss.As a result, our ahm and international student policy management systems have been taken offline. We expect these systems to be offline for most of the day.This will cause regrettable disruptions for some of our customers. ahm and international student customers will still be able to contact our customer teams via phone but at this stage our people won’t be able to access policy information.- Medibank statement published at 11 am, Thursday, 13 October 2022

**October 14 - Medibank Contact’s Impacted Customers**

Medibank send an email to its customer base announcing the incident. Around 2.8 million emails are sent with text messages sent to customers preferring this communication method. The email echoes Medibank’s initial statement that no evidence of customer data compromise has been detected.

**October 17 - Medibank Says Still no Evidence of Customer Data Compromise Found**

Medibank releases an update saying that their investigation efforts still haven’t found evidence that customer data was compromised.

"Our ongoing investigation continues to show no evidence that any customer data has been removed from our IT environment."We have resumed normal activity for our customers, after temporarily removing access to some of our customer systems as a precautionary measure last week."We’re sorry for the inconvenience and concern this may have caused."Our ongoing investigation has found the unusual activity we detected in part of our IT network was consistent with a possible ransomware threat. Ransomware is a common and dangerous type of malicious software that works by locking up or encrypting files, so they are no longer accessible. Our systems were not encrypted by ransomware during this incident."As a further precaution, we’ve put in place additional security measures across our network and we continue to work with external cybersecurity experts and the Australian Government’s lead cyber agency, with our forensic investigation continuing."We remain vigilant and will take necessary steps in the future to protect your data. Although there is nothing that customers need to do, you can contact us by phone."- Medibank update published at 11 am, Thursday, 13 October 2022

**October 19 - Hackers contact Medibank**

The hackers contact Medibank and provide a sample of 100 stolen customer records to prove that customer data was indeed compromised.

**October 20 - Medibank Confirms that AHM Customer Data was Compromised**

Medibank announces that AHM (an insurance brand backed by Medibank) customer data was compromised in the attack.

We wanted to update you on the latest development, which the Australian Federal Police is investigating as a crime.Medibank has been contacted by a criminal claiming to have stolen data and who has provided a sample of records for 100 policies which we believe has come from our ahm and international student systems. This information includes:- First names and surnames- Addresses - Dates of birth- Medicare numbers- Policy numbers- Phone numbers - Some claims data, including the location of where a customer received medical services and codes relating to their diagnoses and procedures.The criminal also claims to have stolen other information, including data related to credit card security. This has not yet been verified by our investigations. We’re working around the clock to understand what additional customer data has been affected and how this will impact them.We are making direct contact with the affected customers to inform them of this latest development, and to provide support and guidance on what to do next. We expect the number of affected customers to grow as the incident continues.Medibank urges customers to remain vigilant, and encourages them to seek independent advice from trusted sources, including the Australian Cyber Security Centre at [cyber.gov.au](https://web.archive.org/web/20221020150516/https:/www.cyber.gov.au/)As always, Medibank will never contact customers requesting passwords or other sensitive information.- Medibank cyber attack update published at 1:25pm, Thursday 20 October

**October 25 - Medibank Announces their customers were also Impacted**

After reviewing an addition series of files provided by the attackers, Medibank discovers that its direct customers were also compromised in the data breach.

There has been a further development in Medibank’s cybercrime event.It has become clear that the criminal has taken data that now includes Medibank customer data, in addition to that of ahm and international student customers.We have received a series of additional files from the criminal. We have been able to determine that this includes:- A copy of the file received last week containing 100 ahm policy records – including personal and health claims data- A file of a further 1,000 ahm policy records – including personal and health claims data- Files which contain some Medibank and additional ahm and international student customer dataGiven the complexity of what we have received, it is too soon to determine the full extent of the customer data that has been stolen. We will continue to analyse what we have received to understand the total number of customers impacted, and specifically which information has been stolen.We will also continue to contact our customers as we are able to confirm whether their data has been compromised.-  Medibank cyber attack update published at 8:30am, Thursday 25 October

**October 26 - Medibank Announces the Scope of Customer Data the Hackers Accessed**

Medibank releases an announcement revealing that the hackers had full access to three primary customer data categories - AHM customer data, International customer data, and Medibank customer data.*‍*

Since yesterday’s announcement, our cybercrime investigation has now established that the criminal had access to:- All ahm customers’ personal data and significant amounts of health claims data - All international student customers’ personal data and significant amounts of health claims data - All Medibank customers’ personal data and significant amounts of health claims dataAs previously advised, we have evidence that the criminal has removed some of this data and it is now likely that the criminal has stolen further personal and health claims data. As a result, we expect that the number of affected customers could grow substantially.-  Medibank cyber attack update published at 9:30am, Wednesday 26 October

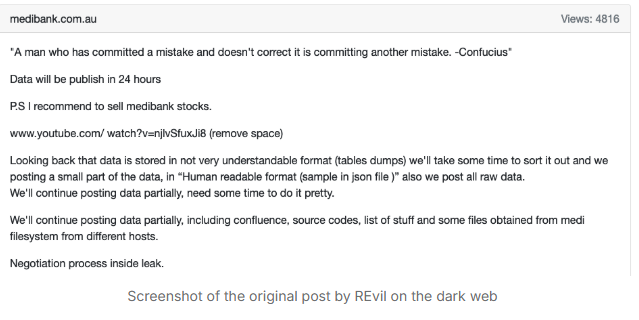
**November 7 - Medibank Announces that 9.7 Million Customers were Impacted in the Data Breach**

Medibank announces that 9.7 million customers were likely impacted in the data breaches. The hackers contact Medibank and threaten to publish the stolen data on the dark web unless a ransom of US$10 million is paid. Medibank refuses to pay the ransom.

Today, we’ve announced that no ransom payment will be made to the criminal responsible for this data theft. Based on the extensive advice we have received from cybercrime experts we believe there is only a limited chance paying a ransom would ensure the return of our customers’ data and prevent it from being published.  In fact, paying could have the opposite effect and encourage the criminal to directly extort our customers, and there is a strong chance that paying puts more people in harm’s way by making Australia a bigger target.This decision is consistent with the position of the Australian Government. Based on our investigation to date into this cybercrime we currently believe the criminal has accessed:- Name, date of birth, address, phone number and email address for around 9.7 million current and former customers and some of their authorised representatives.  This figure represents around 5.1 million Medibank customers, around 2.8 million ahm customers and around 1.8 million international customers- Medicare numbers (but not expiry dates) for ahm customers- Passport numbers (but not expiry dates) and visa details for international student customers -Health claims data for around 160,000 Medibank customers, around 300,000 ahm customers and around 20,000 international customers.  This includes service provider name and location, where customers received certain medical services, and codes associated with diagnosis and procedures administered.  Additionally, around 5,200 My Home Hospital (MHH) patients have had some personal and health claims data accessed and around 2,900 next of kin of these patients have had some contact details accessed-Health provider details, including names, provider numbers and addressesWe believe the criminal has not accessed:- Credit card and banking details- Primary identity documents, such as drivers’ licences, for Medibank and ahm resident customers.  Medibank does not collect primary identity documents for resident customers except in exceptional circumstances  -Health claims data for extras services (such as dental, physio, optical and psychology)Given the nature of this crime, unfortunately we now believe that all of the customer data accessed could have been taken by the criminal.-  Medibank cyber attack update published on 7 November, 2022

**November 8 - Hackers Threaten to Publish Stolen Data in 24 Hours**

Up until this point, the hackers had only shared fragments of stolen data with Medibank. In an effort to force Medibank’s hand into paying the ransom, the hackers announce that they will commence publishing increasing segments of the stolen data on a cybercriminal forum in 24 hours.

****

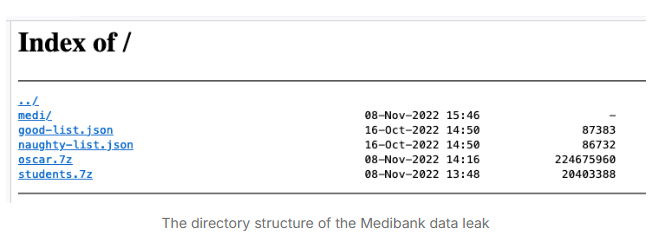
**November 9 - Hackers Publish a Segment of Customer Data on the Dark Web**

The hackers follow through with their threats and published a segment of the stolen database. The data is published across two categories, a “good list” and a “naughty list,” with the naughty list identifying customers that have undergone treatment for drugs, alcohol, and those with mental disorders.

The data is published on a ransomware leak website with ties to Blog XX - a cybergang believed to be a re-grouping of the defunct Russian ransomware gang REvil.

With the likely link to a ransomware gang and the use of extortion tactics, the incident bears all the hallmarks of a ransomware attack with the exception encryption.- possibly because [the attack was intercepted](https://www.upguard.com/blog/what-caused-the-medibank-data-breach) before the hackers had time to encrypt Medicare’s systems.

The customer data dump included two small files of sample data, screenshots of the group's negotiations with Medibank, and two large compressed files each containing approximately 800k rows of personally identifiable information.



****Two JSON files each contained personal information for one hundred people each. The data points included Medicare number, name, home address, date of birth, phone number, name of their medical provider, and diagnosis codes. Natural persons were easily corroborated based on the given names and addresses in the data

**November 10 - Hackers Publish Customer Abortion Information**

The hackers publish more customer details on the dark web. This time, its a database revealing customer information pertaining to abortions, non-viable pregnancies, ectopic pregnancies, molar pregnancies, and miscarriages.

**Post-Incident Review : -**

1. **Root Cause Analysis (RCA):**
   * **Primary Cause:** Attackers gained access through compromised employee credentials, possibly acquired via phishing or credential leaks.
   * **Security Weaknesses Identified:**
     + Lack of stringent multi-factor authentication (MFA) across all access points.
     + Insufficient real-time monitoring to detect and contain the attack earlier.
     + Poor network segmentation, allowing lateral movement once attackers gained access.
2. **Effectiveness of the Incident Response:**
   * **Strengths:**
     + Quick public disclosure of the breach, demonstrating transparency.
     + Engagement with law enforcement and cybersecurity agencies for support.
   * **Weaknesses:**
     + Delayed detection of the breach allowed attackers to exfiltrate large amounts of sensitive data.
     + Communication gaps internally, leading to slower response coordination.
3. **Impact Assessment:**
   * **Financial Impact:** Significant costs associated with response efforts, legal fees, and potential class-action lawsuits.
   * **Reputational Damage:** Loss of customer trust and increased regulatory scrutiny.
   * **Operational Disruptions:** Increased customer inquiries and support requirements.

**Lessons Learned:**

1. **Stronger Identity and Access Management (IAM):**
   * Implementation of company-wide **multi-factor authentication (MFA)** for all systems and users.
   * Regular credential audits and stricter password policies.
2. **Enhanced Security Monitoring and Detection:**
   * Deployment of advanced threat detection tools with real-time alerting.
   * Increased investment in **Security Operations Center (SOC)** capabilities.
3. **Improved Employee Awareness:**
   * Regular cybersecurity training to help employees recognize phishing attempts and social engineering tactics.
   * Simulated phishing exercises to assess and improve employee readiness.
4. **Data Protection Enhancements:**
   * Stronger encryption measures for sensitive data at rest and in transit.
   * Stricter access controls limiting employee permissions based on job roles (least privilege principle).
5. **Incident Response Plan Updates:**
   * Refinement of response procedures for faster containment and escalation.
   * Regular tabletop exercises to test response readiness under simulated attack scenarios.