Medibank Data Breach 2022

Team

HyunOh Jeon
Jiahe Zhang
Kangning Zhang
John Antony
Michael Matta

Introduction

On October 13th, 2022, one of Australia's largest private health insurers, Medibank, had a security breach. Around 200GB of personal data from about 9.7 million customers, current and former, has been stolen by a group of hackers, who are suspected to be linked with the infamous Russian hacker group REvil. The attacker demanded a $15 million ransom in exchange for stopping the publishing of the stolen data and returning it to Medibank. The ransom was later lowered to its current total, $9.7 million, one dollar per custom. However, Medibank and the Australian government refused to pay the ransom, insisting that paying it would encourage more of these attacks in the future. In this blog post, we will look thoroughly at technical aspects related to the issue, and analyze the possible prevention methods against the attack. Also, we will gain a greater understanding of data privacy breaches by doing an incentive analysis and observing the ethical and legal aspects of the issue.

Technical Details

The attack seems to start with the theft of the internal credentials of an individual with privileged system access. It is most likely that the credentials are stolen via Phishing and social engineering [2], where the attackers build a legit-looking website and send the link to the targets to lure them into entering their credentials on this website. It is also called Spear Phishing, where suspicious links are sent to the target by someone they think they can trust. For example, emails sent from a company email address (suspicous@medibank.com) or messages sent from someone in their social network (a DM on Discord/Twitter). Another theory is that the credentials were stolen via malware. A former Medibank employee claimed that his login credentials were for sale along with URLs that these credentials were valid [21]. Apparently his credentials were stolen by Redline botnet malware, which infected one of his devices at home. One way or the other, even if the attacker only gained access to accounts with limited privileges at first, they can use the lower privilege accounts as their ladder to find more information about accounts that might have higher privileges [2]. For example, once they log in to an employee account, they should be able to figure out the supervisor of this employee and the company's social network, as well as everyone's contact information, which enables further phishing attacks. Based on AFP Commissioner Reece Kershaw's statement: "Our intelligence points to a group of loosely affiliated cyber criminals, who are likely responsible for past significant breaches in countries across the world" [16], the attackers are "experienced" hackers and should have the ability to social engineering and use sophisticated phishing skills due to their known hacking ability.

After the attackers gained access to the internal system, it is believed that they “set up two backdoors into the Medibank network” [7] and “access to the system via a virtual private network connection [17].” The attackers must have used proxy servers or Tor, where the IP address of the source is very different to identify. Before building the backdoor and starting to steal data, the attacker claimed they spent a month of time learning the structure of Medibank’s internal system, “guided by source code and documentation” [21]. The attackers claimed “access to Medibank’s Confluence server and grabbed source code from Stash“ and also accessed Redshift via jump servers [6][21]. Redshift is the data warehouse product by Amazon and it should be where Medibank stores and manages their database. Jump server is usually used to access and manage devices in different security zones, similar to remote control of devices. At least one firewall is present between the two security zones and the jump server is in between to control what traffic goes in and out [22]. I think the attackers got access to the jump server that’s in charge of Redshift using the credentials they stole, which grants them access to the data stored in Redshift passing the firewall. Ironically, jump servers are usually used to protect the internal network from outside access. But in this case, it was exploited by the attackers to gain access.

It must have been during that month that the attackers learned the vulnerable points of the internal network. First of all, figuring out the MAC address and IP address of all the routers and devices would be helpful when redirecting traffic inside the network. There might be devices that are less occupied and thus less noticeable if it is used to store the stolen data until they are transferred out of the network. The location of an escape router is also necessary to transfer the data to the outside. I believe that they found more than one router as their “backdoors”. The attackers might have been connected to an escape router via a proxy server or Tor for the final data transfer. They could have also used ARP spoofing or DNS spoofing to trick the routers and devices inside the internal system to send data to places they are not supposed to send or even to trick the firewall (if there is any).

It seems that the attackers wrote scripts that would automatically query data from Medibank’s internal database server [7]. Redshift uses SQL to manage and analyze data, and thus is vulnerable to SQL injection. SQL injection can be used to learn the data structure inside the database. Once they’ve learnt the table names and attribute names, they can start query data from the database. Eventually, the data was pulled together into one single ZIP file and was eventually noticed by Medibank.

Once the data was obtained, the attackers claimed that they “will take some time to sort it out”, and started to release part of the data to the dark web. Based on the JSON file they have released so far, it seems that not all data obtained are well-structured. Some of the files contain column names. And other files don't have headers and contain data that looks like junk [18]. These details might mean that the attackers didn’t have enough time to learn the data structure before they started to pull data out of the database. They aren't entirely sure what they have and they are also trying to figure it out themselves.

The details of the attack are still under investigation, and the attackers could have used completely different approaches than the ones I pointed out. However, it is not hard to imagine that the attackers must have found some protocols or mechanisms that can be manipulated for their use.

Mitigation and prevention

Due to the limited resources for technical details of this data breach attack, it is hard to give specific advice on how the attack could have been prevented. However, based on our theory of what happened, some general protection against such attacks should be properly deployed by Medibank to prevent the data breach.

First of all, education on phishing and how to prevent phishing is necessary for all employees. Second, Medibank should implement the Principle of Least Privilege (POLP). POLP is a policy that limits the employees to the minimal privilege that they need to perform their daily tasks. As excessive privileges present a significant security risk, removing the excessive administrative power from developers would reduce the possibility of bypassing the privilege escalation phase of the attack. This means that the hackers will have to dedicate more time to the attack, and engineers at Medibank would have more time to discover and fix the security flaw. Third, Medibank could segment its network into fragments. By segmenting the network, Medibank makes it more difficult for external attackers to locate or access sensitive data. [2] Fourth, using multi-factor authentication (MFA) for logging in. MFA is one of the most effective measures against account compromise attempts. Yet, the attack was still successful despite the evidence from Medibank chief executive David Koczkar that suggests that multifactor authentication has been deployed in Medibank's environment and they have already taken steps to further strengthen it. [5] Lastly, based on a former employee, his credentials were still valid after he left the job [21]. Medibank should follow good IT security practices to revoke former employees' accounts right away.

On the other hand, hackers were able to compromise 200 GB of secret information and post the results directly. It means that the data is more likely to be stored in a single database without any form of encryption. What Medibank could do is to separate user data into different repositories/databases and then encrypt them using different keys to minimize the consequences of single attacks. In general, Medibank should keep educating its employees to be aware of Spear Phishing attacks and ask them to keep their working platform/software up to date to eliminate any potential personal mistakes and technical flaws.

Incentive Analysis

Motivation

The attackers are motivated by money and notoriety. The attackers appear to be "linked to REvil, a Russian ransomware gang notorious for large attacks on targets in the United States and elsewhere" [1]. Their strategy revolves around slowly leaking sensitive customer data, while maintaining a $9.7 million bounty to stop publishing the data and return it to Medibank [1]. The 9.7 million is meant to represent $1 for each customer affected by the breach. Although they are unfairly targeting customers with records of "HIV, drug addiction or alcohol abuse or for mental health issues," this seems to be a ploy to force Medibank to pay the ransom, rather than an intentional attack on the customers themselves [5].

Harm Caused

This attack is a complete disaster for a company like Medibank that handles massive amounts of extremely private customer data. Medibank stated "the stolen data belongs to 9.7 million past and present customers, including 1.8 million international customers" and "the files include health claims data for almost half a million people." [1]. Medibank even accounts the country's prime minister as their customers [21]. The information allegedly contains “email addresses, phone numbers, addresses, Medicare numbers, names, dates of birth, passport numbers and visa details” [8]. It also contains highly sensitive health claims data for 192,000 customers. This includes patient service providers, diagnoses and procedures [8].

They have been releasing this data on the dark web in files such as “psycho.csv, hiv.csv, viral_hepatitis.csv, std.csv.” Although Medibank appears to deny the leak of sexually transmitted diseases, they did confirm the leaked files could have info on people with “chronic conditions such as heart disease, diabetes and asthma, people with cancer,” mental health issues, and more [9]. As these hackers continue to leak patient data or sell it to third parties, an increasing number of customers will be affected and outrage will grow. There is a huge amount of trust given to private health insurance companies, and as this situation continues to transpire, it is hard to imagine that Medibank will ever recover.

Other Parties Affected

Patients and shareholders were strongly negatively affected. Medibank is a publicly traded company and its stock dropped 20% after news of the breach. Potentially millions of patients had their names, birthdates, passport numbers, and medicare claims leaked. Not only is this information highly sensitive, but it is also directly tied to the corresponding customer. As this staredown between Medibank and the hackers continues, only more and more customers will be negatively affected.

Misalignment of Incentives

There was no misalignment of incentives between the company and those harmed (the customers); this is essentially the worst-case scenario in terms of a cyberattack for the company. Between having the employee’s credentials compromised, having the compromised account not being protected by multi-factor authentication, and having wide-scale availability of personally identifiable private health information, it is safe to say this was a devastating lapse in security by Medibank. Medibank let its clients down massively and it will be difficult to build back trust with its clients.

Ethical Issues Raised by the Incident

The field of cybersecurity faces ethical issues more so than people may think. From security to confidentiality and functionality, cyber security experts must exercise ethical practices. The Medibank breach cyber attack affects many different groups such as the users who directly got information leaked, the company integrity, the integrity of the cyber security experts as well as the image of the country attacked [12].

About 9.7 million people had confidential information leaked from this cyber attack. Sensitive information such as names, medical history, appointment information, and addresses was leaked in this Medibank breach. The individuals who launched the cyber attack wagered a ransom of $10 million dollars for the removal of leaked user information onto the dark web [1]. Furthermore, the idea of a ransom is an ethical dilemma in itself because the company cannot afford to have such sensitive information to be leaked, but Medibank cannot trust the legitimacy of the attacker’s claims. The CEO of Medibank states that agreeing to pay the ransom would only “fuel cybercriminal business models” [1]. In addition to supporting the cybercriminal business, agreeing to pay the ransom may in fact increase the potential risk for users and various other users across the world. The attackers will now know that these companies can be easily exploited for a large sum of money, and still choose to sell sensitive information elsewhere. Arguably even more important, the company's integrity plummets, potentially causing various investors, clients, and users to lose trust in the company [12]. Medibank would not be able to completely confirm that the attackers will fully remove stolen sensitive information from the dark web. Alternatively, if Medibank chooses to not pay the ransom, then the risk of cyber criminals furthering the attack is present. The adversaries may attempt to leak even more information or directly affect users whose information has been leaked in order to fetch a larger price from the company.

Moreover, cyber security specialists face an ethical crisis. To combat these issues, specialists may need to increase security at the expense of functionality and user experience. This can be crucial, especially for medical institutions that may need to access login quickly for an emergency. Resource allocation plays a role in the implementation of cybersecurity for a company. If not enough resources are available for a cybersecurity specialist, then the security procedure may not be at its fullest potential. The cybersecurity specialist may decide to prioritize their own time and money rather than the security of the clients [11]. Additionally, hiring managers must be able to place a high degree of trust in their security specialists because they are handling extremely sensitive information and cannot afford a mishap [13]. There are regulations placed by the government to ensure companies will be motivated to not be vulnerable to such attacks due to these ethical issues present.

Legal Issues Raised by the Incident

Cybercriminal activity is a serious issue that can lead to millions of people being affected and involve millions of dollars. The Medibank situation is an imperative event that will be costly for parties involved. Australia, the country that was directly affected by the Medibank breach follows protocol from parts 10.7 and 10.8 of the Criminal Code Act 1995. These sections state that a sentence for a cyber-criminal offense can range from 2-10 years for an offense. Serious offenses are considered offenses that will result in at least 10 years of imprisonment [14]. The Medibank breach would most likely be classified as a serious offense because of the severity of the damage dealt from the breach. Due to the severity of this breach, the federal government states that fines to up $50 million dollars or 3 times the value of any benefit from data misuse, or 30% of the company's adjusted turnover, whichever is greater could be issued to the company that was on the receiving end of a cyber-attack [4]. This legal incentive can be placed for companies to prioritize cybersecurity for their company in order to help defend against malicious attacks and to avoid large fines from the government. With a regulation like this in place, companies will be more inclined to invest more in cybersecurity to prevent disastrous cyber attacks.

Because of the weakness of Medibank’s cybersecurity, a class action lawsuit could potentially reach the High Court. Already at least 15,000 former Medibank customers are ready to file a lawsuit with Medibank over the exposure of highly sensitive information. The group of people can sue for a “breach of privacy” which if exists, must be settled in the High Court [15]. Moving forward, such a right would be beneficial allowing individuals to sue over any form of privacy breach. This will create a precedent to show the importance of the protection of privacy. Prior to this incident, individuals affected could seek compensation for privacy data breaches under the Privacy Act 1988 [19]. In regards to privacy, Australia follows the Privacy Act 1988 which does not state that an individual can sue for a breach of privacy [20].

Unlike the UK, the right to sue for a breach of privacy would be considered novel in Australia. Additionally, it was revealed by a Medibank staff member that the company did not utilize multi-factor authentication in its system. Such a late implementation of authentication clearly is costly and could have potentially avoided or at least lowered the severity of the breach. A company that fails to implement MFA, is setting itself for legal action to take place [15].

References

[1]https://www.cnn.com/2022/11/11/tech/medibank-australia-ransomware-attack-intl-hnk
[2]https://www.upguard.com/blog/what-caused-the-medibank-data-breach
[3]https://www.reuters.com/business/healthcare-pharmaceuticals/australias-no-1-health-insurer-says-more-patient-data-stolen-hack-2022-10-24/
[4]https://www.zdnet.com/article/australia-beefs-up-scrutiny-of-medibank-following-data-breach/
[5]https://www.cshub.com/attacks/news/iotw-everything-we-know-about-the-medibank-data-leak
[6]https://twitter.com/Jeremy_Kirk/status/1590517192080388096
[7]https://www.afr.com/technology/revealed-how-crooks-got-inside-medibank-20221024-p5bsg4
[8]https://www.cshub.com/attacks/news/we-know-who-are-says-afp-to-medibank-hackers
[9]https://7news.com.au/news/cyber-security/fresh-blow-for-medibank-customers-after-hackers-release-more-data-c-8911576
[10]https://www.thesaturdaypaper.com.au/news/politics/2022/11/19/how-it-happened-medibank-hack-came-via-single-login#hrd
[11]https://swisscyberinstitute.com/blog/a-holistic-approach-to-ethical-issues-in-cyber-security/
[12]https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/
[13]https://online.maryville.edu/blog/cyber-security-ethics/
[14]https://www.imolin.org/doc/amlid/Australia/Australia_Criminal_Code_1995_No.12-1995.pdf
[15]https://www.afr.com/technology/medibank-class-action-could-go-all-the-way-to-the-high-court-20221111-p5bxm6
[16]https://www.afp.gov.au/news-media/media-releases/statement-afp-commissioner-reece-kershaw-medibank-private-data-breach
[17]https://www.theguardian.com/australia-news/2022/nov/12/medibank-v-the-hackers-how-the-health-insurer-fell-to-a-mass-data-theft
[18]https://www.upguard.com/breaches/medibank-data-leak#toc-original-post
[19]https://stephens.com.au/compensation-privacy-breaches-privacy-act-1988-cth/
[20]https://www.theguardian.com/commentisfree/2022/nov/17/australian-companies-dont-value-keeping-our-data-safe-because-they-have-little-to-lose-our-laws-need-to-change-that
[21]https://www.bankinfosecurity.com/blogs/australia-faces-consequences-standing-up-to-ransomware-p-3312
[22]https://www.ssh.com/academy/iam/jump-server