A CYBERSECURITY INTELLIGENCE REPORT ON DATA BREACH INCIDENTS.

BY

SOMKENE RICHARD

6TH OCTOBER,2024

EXECUTIVE SUMMARY

An analysis of the cyber incidents at Marriott Hotels in September 2018 and Medibank in October 2022 revealed that these breaches were caused by the continuous use of outdated operating systems and the lack of multi-factor authentication (MFA), respectively. Both incidents resulted in the compromise of billions of customers' personally identifiable information (PII).

These cases highlight the critical importance of regularly patching operating systems and implementing MFA to strengthen security. Proactive security measures are essential to prevent data breaches, minimize financial losses, and protect an organization’s reputation.

INTRODUCTION

In September 2018, after Marriott Hotels acquired Starwood through a merger, it experienced a data breach that impacted approximately 339 million guests. Investigations revealed that the breach had been ongoing since 2014, originating in Starwood’s guest reservation system. Marriott was only alerted to the breach through their incident detection tool after the acquisition.

Between August 25 and October 13, 2022, Medibank, a health insurance company, suffered a data breach and ransomware attack, affecting around 9.7 million customers. The attackers demanded a $10 million ransom and later released some of the stolen data on the dark web. Further investigation revealed that the breach was facilitated by the absence of multi-factor authentication (MFA) in Medibank’s systems.

Details of these attacks are outlined below.

MOTIVATION OF THE THREAT ACTORS AND THEIR GOALS

- Marriott did not disclose the identity of the attacker, but reports from both the New York Times and the Washington Post suggested that the breach was part of a state-sponsored intelligence-gathering operation by the Chinese government.

- The Medibank breach was a ransomware attack, in which the attacker, Aleksandr Ermakov, collaborated with REvil, a Russian ransomware gang, to demand a $10 million ransom. Medibank publicly announced that it would not pay the ransom.

TECHNIQUES/TACTICS AND THE VULNERABILITIES EXPLOITED

- In the case of Marriott Hotels, the attacker exploited several digital vulnerabilities within Starwood's systems. These included the use of outdated versions of Windows Server and the exposure of Remote Desktop Protocol (RDP) ports to the internet, both of which provided entry points for the attackers.

- In Medibank's case, the ransomware attack was made possible due to a vulnerability stemming from the lack of proper multi-factor authentication (MFA) implementation for privileged users.

INDICATORS OF COMPRISE

- In the case of Marriott Hotels, the compromise was discovered when an internal security tool detected a suspicious attempt to access the guest reservation database of Marriott's Starwood brands. Further investigation revealed that the system had been compromised as far back as 2014, well before Marriott's acquisition of Starwood

- The indicator of compromise for Medibank was unauthorized access to their network through stolen credentials belonging to a third-party IT service provider.

IMPACTS OF THE ATTACKS

A. On Marriott Hotel

Human impact:

The personally identifiable information (PII) of approximately 339 million guests was compromised, including names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, etc

Recovery costs:

Marriott incurred nearly $30 million in total recovery expenses as a result of the breach.

Legal impact:

Marriott faced significant legal implications due to the breach. Because the incident affected individuals in the United Kingdom, the Information Commissioner's Office fined Marriott over $120 million for violating British customers' privacy rights under the General Data Protection Regulation (GDPR). In North America, Marriott encountered multiple class-action lawsuits following the breach announcement, one of which requested $12.5 billion in damages.

Stock Impact:

Marriott's stock dropped by 5% following the public announcement of the attack.

Reputational Damages:

In addition to recovery costs, Marriott faced widespread criticism for its cybersecurity shortcomings after the incident.

B. On Medibank

Human Impact:

The compromised data in the Medibank data breach includes the names, dates of birth, addresses, phone numbers, and email addresses of current and former customers. Additionally, it involved some Medicare card numbers, passport numbers, and health claim data—such as service provider names and locations, details of medical services received, and codes associated with diagnoses and procedures. The breach also affected next of kin contact details for My Home Hospital patients, as well as health provider information, including names, provider numbers, and addresses.

Recovery Costs:

Medibank continues to incur ongoing costs related to the breach, with expectations of exceeding $125 million in expenses by the end of the next financial year.

Stock Impact:

Following the public announcement of the attack, Medibank's share price plummeted by 18%.

Legal Impact:

Medibank was faced with Two class action lawsuits on behalf of customers and an additional shareholder lawsuit. Making it a total of three lawsuits.

Medibank is currently under investigation by the Office of the Australian Information Commissioner (OAIC) regarding its information handling practices and could face a $50 million fine if found to have insufficient security measures in place.

RECOMMENDATIONS

Based on the aforementioned incidents, individuals and organizations are encouraged to:

1. Activate two-factor and multi-factor authentication on all their systems.
2. Regularly check for updates and patches on their respective operating systems.
3. Conduct thorough security assessments during the course of mergers and acquisitions.
4. Constantly organize a cybersecurity training and education for their employees

CONCLUSION

Being security-conscious and vigilant should be a top priority for protecting against online threat actors. As the internet and technology advance, these threat actors continually seek new methods to compromise systems.