Investigation Report on Marriott International Data Breach

November 2023
By: Washif Akhtar

Executive Summary

- Marriott International, a hospitality company that oversees one of the biggest hotel chains in the world, suffered a massive data breach that exposed the personal information of up to 339 million guests who had made bookings with the company's Starwood properties over the past several years[1].
- The breach was discovered in September 2018, but it had been ongoing since 2014, when cybercriminals infiltrated the Starwood guest reservation system via a remote access trojan (RAT)[2].
- The breach was not detected during Marriott's acquisition of Starwood in 2016, due to the lack of a detailed cybersecurity audit and the use of legacy systems and technology[23].
- The breach resulted in significant recovery expenses, legal ramifications, and reputational damages for Marriott. The company faced multiple lawsuits, regulatory investigations, and fines from various countries and jurisdictions[145].
- The breach also posed serious risks for the affected customers, who may have had their sensitive data compromised and used for identity theft, fraud, or espionage[23].
- The breach highlighted the importance of prioritizing cybersecurity during merger and acquisition (M&A) events, as well as the need for implementing robust security measures and best practices to prevent and mitigate such incidents.

Incident Analysis

- The point of entry for the breach was the Starwood guest reservation system, which was compromised by cybercriminals using a RAT in 2014[2].
- The RAT allowed the attackers to gain unauthorized administrative control of the system and access the databases that stored customer data[2].
- The attackers encrypted and exfiltrated the data from the system, which included names, contact information, passport numbers, dates of birth, and credit card details of millions of guests[21].
- The extent of the breach was massive, as it affected up to 339 million guests from various countries who had made bookings with Starwood properties between 2014 and 2018[1].
- The timeframe of the breach was approximately four years, from 2014 to 2018, during which the attackers remained undetected and continued to access and steal customer data[2].

Forensic Analysis

- The breach was discovered in September 2018, when an internal security tool flagged an unusual database query on the Starwood network[2].
- The tool was monitored by Accenture, an IT and security service provider that had been running the Starwood network before and after the acquisition by Marriott[2].
- Marriott initiated an internal investigation and hired external experts to conduct digital forensics on the affected systems[2].
- The investigation revealed that the Starwood network had been compromised by a RAT since 2014, and that the attackers had encrypted and removed data from the system[2].
- The investigation also found evidence and logs of the attackers' activities, such as the use of web shells, credential dumping, and lateral movement[2].
- The investigation also uncovered that Starwood had been targeted by separate attackers in an unrelated incident in 2015, leaving its devices infected with malware[3].

Data Recovery

- Marriott decrypted the data that the attackers had exfiltrated from the system and determined the type and quantity of customer data that was potentially exposed[2].
- Marriott estimated that up to 339 million guest records were affected by the breach, of which 383 million were unique records, 18.5 million were encrypted passport numbers, 9.1 million were encrypted payment card numbers, and 5.25 million were unencrypted passport numbers[1].
- Marriott developed a strategy for data recovery and incident containment, which included the following steps[2]:
  - Isolating and shutting down the compromised systems and devices
  - Migrating the Starwood guest reservation system to Marriott's own reservation system
  - Enhancing the security of the network and the data
  - Implementing additional monitoring and detection tools
  - Offering free identity theft protection and fraud resolution services to the affected customers
  - Establishing a dedicated website and call center to provide information and assistance to the customers

Regulatory Compliance

- Marriott considered the legal and regulatory aspects of the data breach and ensured that the company complied with reporting requirements[2].
- Marriott notified the relevant authorities and regulators of the breach, such as the Information Commissioner's Office (ICO) in the UK, the Federal Trade Commission (FTC) in the US, and the Office of the Privacy Commissioner (OPC) in Canada[145].
- Marriott also complied with the data protection laws and regulations of the countries and jurisdictions where the affected customers resided, such as the General Data Protection Regulation (GDPR) in the European

Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and the California Consumer Privacy Act (CCPA) in California[145].

- Marriott faced several fines and penalties for violating the data protection laws and regulations, such as a £18.4 million fine from the ICO, a $23.8 million fine from the FTC, and a $123 million fine from a group of 30 attorneys general in the US[145].

Communication and Notification

- Marriott developed a communication plan for notifying the affected customers, stakeholders, and regulatory bodies of the breach[2].
- Marriott issued a public statement on November 30, 2018, disclosing the breach and providing the basic details and the steps taken by the company[2].
- Marriott also sent email notifications to the affected customers, informing them of the breach and the actions they should take to protect themselves[2].
- Marriott ensured that the communication was clear and in compliance with the privacy laws, such as the GDPR, PIPEDA, and CCPA[145].
- Marriott also communicated with the media, the investors, the employees, and the partners, addressing their concerns and questions, and providing updates on the situation[2].

Post-Incident Review

- After the breach had been contained and mitigated, Marriott conducted a thorough review to identify the weaknesses in the security posture and provide recommendations for improving security[2].
- The review found that the main causes of the breach were the following[23]:
  - The lack of a detailed cybersecurity audit during the M&A process, which failed to detect the existing compromise and vulnerabilities in the Starwood network
  - The use of legacy systems and technology, which were outdated and insecure, and allowed the attackers to exploit them
  - The insufficient security measures and best practices, such as encryption, segmentation, patching, and monitoring, which could have prevented or minimized the impact of the breach
- The review also suggested the following recommendations for improving security[23]:
  - Conducting regular and comprehensive cybersecurity audits, especially during M&A events, to identify and address any potential risks or issues
  - Adopting uniform and updated systems and technology, and ensuring their integration and compatibility, to reduce the attack surface and complexity
  - Implementing robust security measures and best practices, such as encryption, segmentation, patching, and monitoring, to enhance the protection and resilience of the network and the data
  - Providing security awareness and training to the employees and the partners, and fostering a culture of security within the organization
  - Establishing an incident response plan and team, and testing and refining them regularly, to ensure a swift and effective response to any future incidents

Conclusion

- The Marriott International breach was one of the largest and most serious data breaches in history, affecting millions of customers and exposing their sensitive data to potential misuse and harm[231].
- The breach also caused significant financial, legal, and reputational damages for Marriott, as the company faced multiple lawsuits, regulatory investigations, and fines from various countries and jurisdictions[145].
- The breach highlighted the importance of prioritizing cybersecurity during M&A events, as well as the need for implementing robust security measures and best practices to prevent and mitigate such incidents[23].
- The breach also served as a learning opportunity for Marriott and other organizations, as they can use the lessons learned from this incident to improve their security posture and readiness for the future[23].