Writing Investigation & Project
Marriott Data Breach

By Evelyn Wolfe

Overview 3

Attack - November 2018 Review 4

Attack - Early 2020 Review 5

Attack - July 2022 Review 6

Citation 7

Overview

The Marriott data breaches of 2018, 2020, and 2022 highlight significant cybersecurity vulnerabilities that led to the exposure of sensitive guest and business information. The 2018 breach was the most extensive, affecting 383 million guests due to a prolonged intrusion in the Starwood network, which Marriott had acquired but failed to properly integrate. It was later discovered that the Starwood network had been compromised as early as 2014, allowing attackers to maintain persistent access to sensitive data for years before the breach was uncovered in 2018. Attackers had access to encrypted passport details, credit card data, and other personal information. The 2020 breach stemmed from compromised employee credentials at a franchised property, leading to unauthorized access to 5.2 million guest records. In 2022, a single Marriott hotel employee was socially engineered into granting access to an internal system, allowing attackers to steal 20GB of business data and attempt extortion, which Marriott refused to pay.

Each attack underscores different cybersecurity risks, from poor network integration and persistent threats in 2018 to credential-based attacks in 2020 and social engineering tactics in 2022. Common themes across these breaches include weak access controls, insufficient security training, and inadequate data protection measures. To mitigate future risks, organizations must implement Zero Trust security models, enhance employee cybersecurity awareness, enforce strict data access controls, and deploy advanced monitoring tools such as User Behavior Analytics (UBA) and Data Loss Prevention (DLP) solutions. Strengthening authentication methods, segmenting networks, and ensuring regular security audits will also be crucial in preventing similar breaches from occurring.

Attack - November 2018 Review

Between 2014 and 2018, a sophisticated cyberattack targeted the Starwood Hotel reservation system, which Marriott later acquired in 2016. The primary victims of this attack were both the Starwood systems that were compromised and the later Marriott guests whose personal data was stolen. A staggering 383 million guest records were affected, including 5.25 million unencrypted passport numbers, 20.3 million encrypted passport numbers, and 8.6 million encrypted credit cards. The attack went undetected for four years, allowing cybercriminals to exfiltrate sensitive data without triggering major alarms. Investigations attributed the breach to a likely nation-state actor, suspected to be China, seeking to collect personal data for espionage purposes, tracking diplomats, business leaders, and foreign travelers. The compromised Starwood systems were not fully integrated or secured following the Marriott acquisition, leaving them vulnerable to continued exploitation.

The attackers leveraged Advanced Persistent Threat (APT) techniques, using stolen credentials, privilege escalation, and remote access tools (RATs) to maintain long-term access. SQL injection and database exfiltration were likely used to extract massive amounts of guest data from Starwood's reservation system. Additionally, poor encryption key management meant that even encrypted data, such as credit card and passport numbers, might have been compromised. Weak security practices within Starwood's IT infrastructure, coupled with Marriott's failure to conduct a thorough security review and integrate the systems post-acquisition, allowed the attackers to operate undetected for an extended period. The breach was eventually discovered in September 2018, leading to significant regulatory scrutiny and legal repercussions, including lawsuits and a £18.4 million fine from the UK's Information Commissioner's Office (ICO).

To prevent similar incidents, recommending companies that are undergoing mergers and acquisitions must conduct extensive cybersecurity audits and ensure proper integration of IT systems before connecting them to corporate networks. Implementing a Zero Trust Architecture (ZTA) with strong network segmentation would limit lateral movement by attackers. Advanced security measures such as Security Information and Event Management (SIEM) solutions and Endpoint Detection and Response (EDR) tools should be deployed to monitor for anomalies and potential threats. Proper encryption and key management practices, including regular key rotation and tokenization of sensitive data, would further enhance data protection. Additionally, regular penetration testing, red teaming exercises, and proactive threat-hunting operations should be conducted to identify vulnerabilities before they can be exploited. Strengthening these security controls would reduce breach dwell time and mitigate risks, ensuring that organizations remain resilient against persistent threats.

Attack - Early 2020 Review

In early 2020, Marriott suffered a data breach after attackers gained access to the login credentials of two employees at a franchised property. This compromise, likely achieved through credential stuffing or phishing attacks, allowed unauthorized access to Marriott's cloud-based guest management and loyalty program system. As a result, 5.2 million guests had their personal information exposed, including contact details, loyalty account numbers, birth dates, and stay preferences. While no payment information or passwords were stolen, the breach highlighted weak authentication controls, particularly the lack of Multi-Factor Authentication (MFA), which would have mitigated the attack. Additionally, the attackers were able to access and extract large amounts of data without triggering security alarms, suggesting Marriott lacked effective anomaly detection mechanisms.

The motivation behind this breach remains unclear, but it is suspected that the attackers sought financial gain by selling personal data on the dark web or leveraging the information for fraudulent activities. Unlike the 2018 breach, no strong evidence links this attack to nation-state actors. The incident resulted in reputational damage for Marriott and legal consequences, including fines imposed by the UK's Information Commissioner's Office (ICO) and a broader $52 million USD settlement in 2024 with the U.S. Federal Trade Commission (FTC) and 49 states. To prevent similar attacks in the future, Marriott and other organizations should enforce phishing-resistant MFA (such as FIDO2 tokens), adopt least privilege access controls to limit user permissions, and implement Privileged Access Management (PAM) to secure and monitor high-risk accounts. Additionally, behavioral analytics and real-time identity threat detection should be deployed to identify unusual login activities, such as access from foreign locations or unrecognized devices. By strengthening authentication and access controls, organizations can significantly reduce the risk of credential-based attacks.

Attack - July 2022 Review

The 2022 Marriott attack involved a social engineering scheme in which a single hotel employee was tricked into granting system access. The attacker, likely using phishing or pretexting tactics, gained entry into an internal system of a specific Marriott property. While the breach did not extend to Marriott's corporate network, it still resulted in the exposure of internal business-related data affecting around 400 individuals. The hackers stole approximately 20GB of data, including guest reservation details, business operations files, and some payment information. Following the breach, the attackers attempted to extort Marriott by demanding payment in exchange for not leaking the stolen data, but Marriott refused to comply.

This breach highlights the dangers of social engineering and inadequate access controls at localized levels. The attack could have been mitigated with stronger employee security training, enforcing strict identity verification policies, and implementing endpoint security solutions. By training employees to recognize phishing, vishing, and other deceptive tactics, Marriott could reduce the likelihood of successful social engineering attempts. Additionally, using Data Loss Prevention (DLP) tools to monitor and block unauthorized data transfers, enforcing restricted USB access, and applying encryption to sensitive files would help prevent data exposure.

To further strengthen security, Marriott should implement Insider Threat Detection and User Behavior Analytics (UBA) to identify anomalies, such as unusual data access patterns. Employing immutable backups and deploying Endpoint Protection Platforms (EPP) would also protect against potential ransomware threats. Finally, enforcing a Zero Trust security model with strict access controls and network segmentation would limit the impact of compromised credentials, ensuring that breaches remain contained and do not escalate into widespread incidents.

Citation

Office of the Privacy Commissioner of Canada. (2022, September 29). *PIPEDA Findings #2022-005: Hotel chain discovers breach of customer database following acquisition of a competitor.* https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-005

Veiga, A. (2024, October 9). *Marriott to pay $52 million, beef up security after data breaches | AP News.* AP News. https://apnews.com/article/marriott-data-breach-settlement-97534838b650bfc7a9e73a5336b2988e

Del Valle, G. (2024, October 10). *Marriott agrees to pay $52 million settlement after multiple data breaches.* The Verge. https://www.theverge.com/2024/10/10/24267048/marriott-ftc-settlement-agreement-52-million-fine

Page, C. (2022, July 6). *Hotel giant Marriott confirms yet another data breach.* TechCrunch. https://techcrunch.com/2022/07/06/marriott-breach-again