Marriott Data Breach 2018

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document aims to provide a detailed overview of the 2018 Marriott data breach. The Marriottt 2018 data breach, affected the personal information of approximately 383 million global customers. The breach involved unauthorized access to the Starwood Hotels reservation system, which Marriottt had acquired in 2016. The attackers gained access to the system in 2014, and had been operating undetected for several years, stealing sensitive data such as names, phone numbers, email addresses, passport numbers, and payment card details. Marriottt's investigation revealed that the attackers used sophisticated tactics, including malware and remote access tools, to maintain persistence in the system. Given the extended time period that the attackers remained undetected in Marriott's systems, the effects of the breach were expensive and costly in more than monetary terms as it made public the obsolete encryption methods used and lax security of Marriott's data systems. This resulted in a loss of consumer trust, legal compliance issues as well as substantial penalty fines.

Following the summary of the Marriott case, relevant MITRE ATT&CK mitigation techniques as well as NIST security controls will be provided as recommendations for this particular case. The MITRE ATT&CK mitigation techniques will address the specific vulnerabilities that the attackers in the data breach. The NIST security controls have been chosen with the additional intention of cementing a more robust security posture by covering more of the basics of securing data systems in a company environment. Generally, it be in good practice to exercise preventative measures such as continuous monitoring, incident response planning, regular auditing, prompt incident reporting, and the utilization of modern encryption methods.

VICTIMS AND SCOPE

The Marriott data breach affected guests who had stayed at Starwood hotels (which was acquired by Marriott in 2016) between 2014 and September 2018 (Security Team, 2024). Starwood's portfolio includes brands like Sheraton, Westin, Le Meridien, W Hotels, St. Regis, and several others that fall within its 895 properties in 100 countries (Starwood Captial Group, 2022). Victims were **primarily hotel guests** whose personal details, including **names, addresses, phone numbers, email addresses, passport numbers, dates of birth, and payment card details**, were exposed (Security Team, 2024). **The scale of the data breach has been determined to be have affected approximately 383 million guests globally**, roughly 5.25 million unencrypted passports were accessed by an unauthorized party as well as 20.3 million encrypted passport numbers (Marriot International, 2024).

The scale of the breach made it a global event, with victims across multiple countries. The breach involved sensitive data like passport numbers and payment card details—information that could be exploited for identity theft, fraud, and other malicious purposes.

METHODS AND TECHNOLOGIES

EXPLOITED VULNERABILITY AND OUTDATED ENCRYPTION

Marriottt's recent statement clarified: "Following an investigation with several leading data security experts, Marriottt initially determined that the payment card numbers and certain passport numbers in the database tables involved in the Starwood database security incident that Marriottt **reported on November 30, 2018, were protected using Advanced Encryption Standard 128 encryption (AES-128).** Marriottt has now determined that the payment card numbers and some of the passport numbers in those tables were **instead protected with a**

different cryptographic method known as Secure Hash Algorithm 1 (SHA-1)" (Marriot International, 2024). Their original statement incorrectly stated that their data was protected with the standardized AES-128 encryption algorithms, however, it was in fact found that **they had been using the outdated SHA-1 which is not considered encryption by contemporary standards**.

KEY TECHNOLOGIES INVOLVED

The malicious actors used a **Remote Access Trojan (RAT) which is a malware that allows a malicious actor to gain remote access to a target's computer** (NewsomeTiffany, 2019). The attackers also used an open-source tool called Mimikatz which searches a device or system's memory for user credentials (NewsomeTiffany, 2019). Both tools were leveraged to maintain access to the breached systems, move laterally within the network, and to escalate privileges on compromised systems for further access to sensitive information.

TIMEFRAME

The breach originated from a vulnerability in Starwood's guest reservation system (NewsomeTiffany, 2019). **Attackers gained access in 2014**, two years before Marriottt acquired Starwood in 2016. Despite the acquisition, **Marriottt did not discover the breach until September 2018** – but it was revealed to the public on November 30, 2018 – allowing the attackers uninterrupted access to sensitive information for several years (VeigaAlex, 2024). The breach affected data stored in the Starwood network long before Marriottt had taken full control over Starwood's IT systems after acquiring the company in 2016, though, the acquisition of the outdated security of Starwood's reservation system platform exacerbated the scope of the initial breach (Rowan KelleherSuzanne, 2024).

TARGETED SYSTEMS

The systems affected by the breach were primarily related to Starwood's compromised reservation system platform, which housed guest information. The included systems were the **reservation systems** used to track guest bookings, **payment processing systems** that handled billing and payment card information and **customer loyalty program databases** that stored sensitive personal details of frequent guests (Marriot International, 2024).

MOTIVATIONS AND OBJECTIVES

Though the perpetrators have not been identified, the motivation behind the Marriottt breach was likely financial gain, as the stolen data could be used for various malicious activities. **Possible motives include identity theft** as the personal details breached (passport numbers and dates of birth) could be used to commit fraud, **fraudulent financial activitiess** as the stolen payment card information could be sold on the dark web or used for unauthorized transactions and **espionage** as it has been suggested that the attack has been linked to a Chinese hacker group, making espionage a potential factor, particularly if sensitive travel or political information about high-profile guests were exposed (SangerDavid, PerlrothNicole, ThrushGlenn, RappeportAlan, 2018).

OUTCOME

The Marriottt data breach had significant repercussions in regards to the brand's reputation, legal and financial consequences. In regards to Marriott's reputational consequences, though Marriott's delay in making the data breach public played a significant role as well, **Marriottt faced widespread public backlash due to the breach and the fact that it had**

occurred over a long period without detection (Security Team, 2024). It damaged their reputation and consumer trust. Legally, **Marriottt faced investigations by regulatory bodies**, including the UK Information Commissioner's Office (ICO) and EU regulators, due to violations of privacy regulations like GDPR (Federal Trade Commision, 2024). In terms of financial consequences, Marriottt faced lawsuits from affected customers and regulatory fines. The company later set aside funds for settlement costs and to cover security upgrades. It has been reported that Marriott has agreed to **pay $52 million to make changes to bolster its data security** to resolve state and federal claims related to major data breaches that affected more than 300 million of its customers worldwide (VeigaAlex, 2024).

RECOMMENDED MITIGATION TECHNIQUES

Given the scope of the breach and the extended time period that the attackers had access to Marriott's systems, MITRE ATT&CK framework have been referenced to determine the most relevant mitigation techniques that would address the vulnerabilities that existed that allowed for the exploitation of such vulnerabilities. The MITRE ATT&CK framework is a knowledge base of adversary tactics, techniques, and procedures based on real-world observations, which provides organizations a grounded understanding how cyber attackers operate. It provides a comprehensive map of potential attack stages, from initial access to exfiltration, allowing defenders to better detect, respond to, and mitigate cyber threats. As such, it has been used to identify the most beneficial mitigation techniques according to the Marriott's data breach.

Following the outline of the specified MITRE ATT&CK mitigation techniques, a more general table of best practices recommended to consider in normal operations will be provided as well.

MITRE ATT&CK MITIGATION TECHNIQUES

Technique	Mitigation	Rationale

Update Software (M1051)	Regular patching of systems and perform regular software updates, particularly for known vulnerabilities, would help prevent attackers from exploiting them to gain unauthorized access (MITRE ATT&CK, 2020).	The breach was likely facilitated by unpatched vulnerabilities in the Starwood reservation system, which Marriottt acquired. Attackers had exploited these vulnerabilities to gain access.
Data Loss Prevention (DLP) (M1057)	Implement DLP solutions to monitor and block unauthorized access to sensitive data and to prevent the unauthorized transmission of data, particularly over unapproved channels (MITRE ATT&CK, 2021).	Sensitive customer data was exfiltrated during the breach. DLP tools could have detected unauthorized access and movement of data within the organization and appropriate actions could have been taken in a timely manner before it had become as large in scale as it did.
Filter Network Traffic (M1037)	Deploy network traffic analysis tools to detect and alert on suspicious activity, such as large volumes of data being transmitted out of the network or anomalous outbound connections to external IPs (MITRE ATT&CK, 2024).	Attackers likely exfiltrated data over the network. Continuous monitoring of network traffic could have detected unusual patterns indicative of data being siphoned off.
Privileged Account Management (M1026)	Enforce least privilege access policies, ensuring that users and systems only have the minimum permissions required to perform their tasks. This would have limited the attackers' ability to access or exfiltrate large amounts of sensitive data (MITRE ATT&CK, 2024).	If attackers had limited access within the Marriottt network, their ability to move laterally and exfiltrate data would have been constrained. In the case of Marriottt, it appears attackers had broad access to critical systems.
Encrypt Sensitive Information – M1041	Encrypting sensitive data in databases, file systems, or backups, so that even if attackers gain unauthorized access to these data stores, the data remains protected and unreadable without the proper decryption keys (MITRE ATT&CK, 2019).	In the Marriottt breach, attackers gained access to sensitive guest information, including personal details and payment data. If this data had been properly encrypted, even if the attackers were able to access the database or storage systems, they would have found the data unreadable without the decryption keys. This would have limited the potential damage of the breach.

GENERAL BEST PRACTICES

Technique	Rationale
Accurate Incident Reporting	Ensuring that public statements and legal disclosures accurately reflect the security measures in place is crucial for maintaining consumer trust and

	compliance. Misleading claims, even if unintentional, can exacerbate legal and reputational damage.
Due Diligence in Mergers and Acquisitions	Companies must conduct thorough cybersecurity due diligence when acquiring other businesses. Understanding the security posture and vulnerabilities of acquired systems can prevent inherited risks and subsequent attacks.
Regular Security Audits	Continuous and rigorous security audits of all systems, especially those involving sensitive customer data, are essential. Identifying and addressing vulnerabilities proactively can mitigate potential breaches and, as a result, the associated costs and consequences.
Advanced Encryption Practices	Utilizing up-to-date and robust encryption methods, rather than outdated hashing algorithms like SHA-1, is critical for protecting sensitive data. Regularly updating encryption standards ensures that data remains secure against ever-evolving threats.
Incident Response Preparedness	Developing and maintaining an effective incident response plan that takes in account the modern threat landscape as well as an organization's previous incidents enables organizations to swiftly and effectively address breaches. This would also include clear communication protocols to inform affected parties and regulatory bodies.

RECOMMENDED SECURITY CONTROLS

In response to the 2018 Marriottt data breach, several NIST (National Institute of Standards and Technology) security controls would be relevant to mitigating the risks and improving the cybersecurity posture of an organization like Marriottt. These controls are part of the **NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)** and **NIST Cybersecurity Framework**. Below are some key NIST controls and frameworks that may be beneficial controls for preliminary preventative measures.

1. ACCESS CONTROL (AC)

- **AC-2: Account Management**
    - Proper management of user accounts, including implementing strict controls for creating, modifying, and deleting accounts. Marriottt's systems could use these access controls to prevent unauthorized users from accessing sensitive data (Special

Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.19).

- **AC-3: Access Enforcement**
    - Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.23). This would prevent unauthorized access to sensitive systems.
- **AC-17: Remote Access**
    - Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing such connections (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.48).

2. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

- **SC-13: Cryptographic Key Establishment and Management**
    - Sensitive data, such as payment card details and passport numbers, should be encrypted with up-to-date industry standards with proper key management practices being followed (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.308,309).

3. CONFIGURATION MANAGEMENT (CM)

- **CM-2: Baseline Configuration**

- Maintained secure and consistent baseline configurations for systems, especially in cases of business acquisitions as entirely foreign systems will need to be integrated and configured appropriately to ensure uniform data security (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.97).

4. INCIDENT RESPONSE (IR)

- **IR-4: Incident Handling**
  - Develop and implement a formalized and practiced incident response process to ensure that Marriottt is able to quickly identify, contain, and mitigate a data breach after detection. This incident response plan should coordinate incident handling activities with contingency planning activities as well as incorporate lessons learned from previous incidence handling (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.152,153).
- **IR-6: Incident Reporting**
  - Ensure that data breaches are reported in a timely manner to stakeholders and relevant authorities (e.g., regulatory bodies, customers, and partners) as it will help reduce the impact on victims and assist in containing the breach (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.157).

5. SECURITY ASSESSMENT AND AUTHORIZATION (CA)

- **CA-7: Continuous Monitoring**
  - Implement continuous monitoring policies to detect anomalous activities in real time. Proactive monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management

decisions (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.90,91).

6. RISK ASSESSMENT (RA)

- **RA-3: Risk Assessment**
  - Ensure regular risk assessments are conducted to evaluate the security posture of systems aid in identifying potential vulnerabilities or threats, enabling Marriottt to take appropriate preventative and mitigating action (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.240).
- **RA-5: Vulnerability Scanning**
  - Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for
    - Enumerating platforms, software flaws, and improper configurations;
    - Formatting checklists and test procedures; and
    - Measuring vulnerability impact (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg. 242)

7. SECURITY TRAINING AND AWARENESS (AT)

- **AT-2: Literary Training and Awareness**
  - Provide regular security awareness training to educate employees about common cyber-attack techniques so they may more easily recognize phishing attempts, social engineering tactics, and other methods attackers could use to infiltrate the systems

(Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg. 60.

- **AT-3: Role-Based Security Training**
    - Ensure that employees responsible for sensitive data (like hotel reservations or customer service personnel) receive specialized training on how to handle and protect personal data securely according to their role's access to establish a layered defense of sensitive data (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012), pg.62,63)

8. CONTINGENCY PLANNING (CP)

- **CP-2: Contingency Plan**
    - Ensure that Marriottt has a comprehensive contingency plan in place for recovering from data breaches, including backup strategies and disaster recovery in order to minimize the impact of the breach on their business operations (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg. 116)
- **CP-9: Information System Backup**
    - Ensure regular backups of critical data and systems are done so as to restore normal operations in the event of a breach without further exposing sensitive information (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.125,126).

9. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

- **SC-12: Cryptographic Key Establishment and Management**

- Ensure proper encryption and management of cryptographic keys for sensitive customer data is essential in preventing data exfiltration or misuse (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.307,308).

- **SC-13: Cryptographic Protection**
  - The use of encryption to protect sensitive data both in transit and at rest, especially for payment card details and personal information, would be especially critical to Marriott in reducing the exposure of that data in the event of a breach (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012)pg.308,309).

REFERENCES

Federal Trade Commision. (2024, October 9). *FTC Takes Action Against Marriottt and Starwood Over Multiple Data Breaches*. Retrieved from Federal Trade Commision: https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-Marriottt-starwood-over-multiple-data-breaches

Marriott International. (2024, April 17). *Marriottt Provides Update on Starwood Database Security Incident*. Retrieved from Marriott International: https://news.Marriottt.com/news/2019/01/04/Marriottt-provides-update-on-starwood-database-security-incident

MITRE ATT&CK. (2019, June 11). *Encrypt Sensitive Information* . Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1041/

MITRE ATT&CK. (2020, July 7). *Update Software* . Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1051/

MITRE ATT&CK. (2021, August 30). *Data Loss Prevention*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1057/

MITRE ATT&CK. (2024, October 17). *Filter Network Traffic* . Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1037/

MITRE ATT&CK. (2024, October 17). *Privileged Account Management* . Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1026/

Newsome, T. (2019, October 31). *The Marriottt/Starwood Data Breach: Why Third-Party Risk Management is Critical During M&A* . Retrieved from Prevalent: https://www.prevalent.net/blog/the-Marriottt-starwood-data-breach-why-third-party-risk-management-is-critical-during-m-a/

Rowan Kelleher, S. (2024, October 10). *Marriottt Gets $52 Million Slap On Wrist For Massive Security Breaches Due To 'Lax Security'*. Retrieved from Forbes: https://www.forbes.com/sites/suzannerowankelleher/2024/10/10/Marriottt-52-million-slap-wrist-cybersecurity-breaches-lax-security/

Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018, December 11). *Marriottt Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*. Retrieved from New York Times: https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Security Team. (2024, July 25). *Marriottt Data Breach.* Retrieved from Cyber SRC: https://cybersrcc.com/2024/07/25/Marriottt-data-breach/

Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. (2012, January 31). Retrieved from NIST: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter3.html

Starwood Captial Group. (2022). *Investments*. Retrieved from Starwood Capital Group: https://www.starwoodcapital.com/investments/

Veiga, A. (2024, October 9). *Marriottt agrees to pay $52 million, beef up data security to resolve probes over data breaches*. Retrieved from AP News: https://apnews.com/article/Marriottt-data-breach-settlement-97534838b650bfc7a9e73a5336b2988e