# Incident Response Report: Analysis of the 2018 Marriott Data Breach

## 1. Incident Overview

Incident Type: Unauthorized Access and Data Breach

Date of Detection: September 8, 2018

Affected Systems: Starwood guest reservation database

Impact Level: High (compromised personal information of up to 500 million guests)

## 2. Forensic Analysis and Log Investigation

### 2.1 Detection and Initial Response

On September 8, 2018, Marriott's internal security tool flagged suspicious activity involving an attempt to access the Starwood guest reservation database. An internal investigation revealed that unauthorized access had been ongoing since 2014, predating Marriott's acquisition of Starwood in 2016.

### 2.2 Nature of the Breach

Attackers had copied and encrypted information from the database and attempted to remove it from the system. The compromised data included:

• Names  
• Mailing addresses  
• Phone numbers  
• Email addresses  
• Passport numbers  
• Starwood Preferred Guest (SPG) account information  
• Dates of birth  
• Gender  
• Arrival and departure information  
• Reservation dates  
• Communication preferences

For some guests, encrypted payment card numbers and expiration dates were also compromised. However, Marriott stated that there was no evidence that the encryption keys were accessed.

### 2.3 Log Analysis

Detailed log analysis indicated that the attackers had maintained persistent access to the network for an extended period. The breach was facilitated by:

• Lack of Network Segmentation: The attackers moved laterally within the network without significant obstacles.  
• Insufficient Monitoring: The prolonged unauthorized access went undetected due to inadequate monitoring of network activities.

## 3. Incident Mitigation Steps Taken

### 3.1 Containment Measures

• Disabled compromised accounts and increased monitoring of privileged accounts.  
• Implemented additional security measures to strengthen network defenses.

### 3.2 Notification and Communication

• Notified law enforcement and regulatory authorities promptly.  
• Informed affected customers and provided resources for credit monitoring and guidance on protecting personal information.

## 4. Recommendations to Prevent Future Incidents

### 4.1 Enhance Network Security

• Implement Network Segmentation: Isolate critical systems to limit lateral movement within the network.  
• Continuous Monitoring: Deploy advanced intrusion detection systems to monitor network traffic and identify anomalies in real-time.

### 4.2 Strengthen Access Controls

• Multi-Factor Authentication (MFA): Enforce MFA for all users, especially those with privileged access, to add an extra layer of security.  
• Regular Access Reviews: Conduct periodic reviews of user access rights to ensure they align with current job responsibilities.

### 4.3 Conduct Regular Security Assessments

• Vulnerability Assessments and Penetration Testing: Regularly test the network and systems for vulnerabilities and address identified issues promptly.  
• Third-Party Security Evaluations: Assess the security posture of third-party vendors and partners to ensure they meet security standards.

### 4.4 Enhance Employee Training and Awareness

• Security Awareness Programs: Educate employees about security policies, phishing attacks, and social engineering tactics to foster a security-conscious culture.

## 5. Conclusion

The 2018 Marriott data breach underscores the critical importance of robust cybersecurity measures, including network segmentation, continuous monitoring, and stringent access controls. Implementing the recommended actions can significantly enhance an organization's security posture and reduce the risk of similar incidents in the future.