The Marriott Data Breach

A Case Study Unveiling a Major Hospitality Security Lapse

By Chua Lai Chwang

of NTU CE7

on 21 Jun 2024

What Happened?

- Breach occurred in 2014, affecting Starwood guests
- The guest reservation database was compromised
- Personal information of 500 million guests were exposed – such as names, addresses, birth dates, gender, passport numbers, credit cards info including that of Starwood Preferred Guests
- Not discovered until 2018 by an internal security tool - likely a network monitoring tool (ran by Accenture) on suspicious activities. Marriott first became aware that they'd been hacked when this tool flagged an unusual database query.

Impact of the Breach

Financial

- Financial costs estimated at around US$28 million for investigation and remediation in 2018 alone – cyberinsurance helped Marriot to cover much of the initial costs associated with the crisis.
- On the day of the data breach announcement, Marriot stock plummeted from $122.8 to $114 a loss of about 7%[1].

Legal and Regulatory

- Legal repercussions of class-action lawsuits and financial penalties from regulatory bodies - e.g., GDPR fines of more than US$120 million.
- Up to 500 million guest records compromised - one of the largest data breaches ever. In particular, the compromise of guests' credit card numbers and passport numbers has more "disastrous personal impacts".
- Potential for identity theft and financial fraud
- Class-action lawsuits from affected customers

Reputational

- Loss of customer trust and brand reputation – Even the Marriott CEO Arne Sorenson had to appear before the U.S. Senate to talk about the attack.

[1] *https://enrico-frumento.medium.com/what-are-the-consequences-of-marriott-and-dell-data-breaches-on-stock-prices-and-intangible-assets-d8052a19a338*

How Did It Happen?

- The attackers used and leveraged a Remote Access Trojan (RAT) and Mimikatz to gain and maintain remote access hacked systems, move laterally within the network, and to escalate privileges on compromised systems.[2]
  - It is also suspected that rogue state hackers employed by Chinese intelligence services are involved.[1]
- Legacy systems from Starwood lacked proper security measures.
  - Failure to keep encrypted data and encryption keys in separate servers
- Delayed detection due to inadequate monitoring
  - Lack of effort to secure systems resulted in attackers staying in systems years after breaching it.

This incident also showed the importance of proper, full due diligence during mergers and acquisitions.

[1] https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
[2] https://www.prevalent.net/blog/the-marriott-starwood-data-breach-why-third-party-risk-management-is-critical-during-m-a/

Resolving the Problem

- Public disclosure of the breach in November 2018
- Investigation by forensic specialists and law enforcement
- Offering credit monitoring and fraud protection services to affected guests
- Implementing stronger security measures - system upgrades, data encryption

Preventing Similar Breaches

- Regularly update and patch systems
- Implement robust security protocols - e.g., multi-factor authentication
- Educate employees on cybersecurity best practices (e.g. strong password hygiene, phishing awareness)
- Continuous monitoring of systems for suspicious activity and vulnerability management
- Have a data breach response plan in place
- Performing daily backups helps prevent malware from demanding money in exchange for restoring lost data

But did all these prevented further breaches?

NO!

There were further breaches impacting customers data!

2020

Property system of another franchisee was hacked by **stealing two employees' login information**, which the bad actors then used to gain access system access

Impact: Personal information from 5.2 million guests was stolen,

2022

Unnamed hacking group used **social engineering to steal passwords**, to access Marriott's internal system.

The hacking group used their access as leverage in an attempt to extort money from Marriott, which the company did not pay.

Impact: Hackers made out with 20 gigabytes of sensitive customer data, including personal information and credit card numbers.

Key learning point: Organisations must remain vigilant and proactive as cyber attackers continually adapt, refine and test their methods to exploit vulnerabilities in the system.

Source: https://www.threater.com/blog/lessons-learned-from-the-marriott-hack-of-2022/#:~:text=Before%20the%20hotel%20chain%20noticed,long%20as%20the%20encryption%20holds.