The Marriott Data Breach

A Case Study Unveiling a Major Hospitality Security Lapse

By Chua Lai Chwang
of NTU CE7
on 21 Jun 2024

In late 2018, the hospitality industry was rocked by a massive data breach at Marriott International. This presentation will delve into the details of this cyberattack, exploring how it happened, the impact it had, and the steps we can take to prevent similar incidents in the future.

What Happened?

- Breach occurred in 2014, affecting Starwood guests
- The guest reservation database was compromised
- Personal information of millions 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.

The attack began in 2014, targeting the guest reservation system of Starwood Hotels, which Marriott had acquired earlier in 2016. Hackers infiltrated the system and accessed the personal information of millions of guests. This sensitive data remained exposed for four years until an internal security tool at Marriott finally identified the breach on 8 September 2018 – likely an internal security monitor tool that flagged suspicious access attempts. This tool was actually monitored by Accenture, who had been running IT and infosecurity for Starwood before the merger and continued to do for the legacy network afterwards.) The database query was made by a user with administrator privileges, but analysis quickly revealed that the person to whom that account was assigned was not the one who made the query; someone else had managed to take control of account.
In their investigation, Marriott found data that the attackers had encrypted and attempted (probably successfully) to remove from the Starwood systems. By November, they had managed to decrypt that data and discovered that it included information from up to 500 million guest records, though those undoubtedly include duplicate records or multiple records pertaining to individual guests. Many of the records include extremely sensitive information like credit card and passport numbers. Now aware of the severity of the breach, Marriott released a statement on November 30, 2018, outlining the basics we've described here.

Impact of the Breach

- 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.
- 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
- 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.
- Legal repercussions of class-action lawsuits and financial penalties from regulatory bodies - e.g., GDPR fines of more than US$120 million.

The scale of the Marriott data breach was staggering. Up to 500 million guest records were compromised, making it one of the biggest data breaches ever reported. This exposed a vast amount of personal information, putting millions at risk of identity theft and financial fraud. The breach also significantly damaged Marriott's brand reputation and resulted in hefty fines from regulatory bodies enforcing data protection laws like the GDPR (General Data Protection Regulation).

The credit card number aspects are particularly worrying, and were made possible by yet another security failing on Marriott's part: while the credit card numbers were stored in encrypted form, the encryption keys were stored on the same server, and were also apparently scooped up in the breach. As for the passport numbers, while some were encrypted, the majority were simply saved in the clear.

In December 2018, articles in the *New York Times* and the *Washington Post*, citing unnamed sources in the U.S. government, pointed a finger in an entirely different direction: at hackers employed by Chinese intelligence services. The *Post's* and *Times'*s sources had access to more data about the hack than has been made public, and say that the code and attack patterns used match up with techniques employed by state-sponsored Chinese hackers; the attackers used a cloud-hosting space frequently used by Chinese hackers, for instance. (The involvement of U.S.

intelligence service in the investigation and the sensitive nature of the attack probably explains why not much by way of technical details has been released.)
Another clue that this breach is part of a government attack rather than mere cybercriminals is the fact that none of those millions of valuable records have ended up for sale on the dark web; this wasn't a mere plundering raid.
What would the motivation for the attack be, then? The government sources speculate that it was part of a broader Chinese effort to acquire massive amounts of data on American government employees and intelligence officers; Marriott is the top hotel provider for the U.S. government and military. The larger goal may be to create a data lake of information on American government employees and agents that big data techniques can be used to analyze.
In February of 2020, the United States Department of Justice formally charged four members of the Chinese military with the 2017 attack on Equifax that netted personally identifying information on millions of people; in the announcement of the indictment, the Equifax attack was explicitly linked to the Marriott and OPM breaches as part of the same larger operation. This was an extremely rare move — the U.S. rarely files criminal charges against foreign intelligence officers in order to avoid retaliation against American operatives — that underscored how seriously the U.S. government took the attack.

How Did It Happen?

- Initial attack methods remain unclear - possibly malware or compromised credentials
- Legacy systems from Starwood lacked proper security measures
- Delayed detection due to inadequate monitoring

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

While the exact methods used by the attackers haven't been publicly disclosed, it's believed they could have involved malware or compromised employee credentials. The breach highlights the vulnerabilities of legacy systems. Starwood's guest reservation system, integrated into Marriott's network, may not have had the necessary security measures in place. Additionally, inadequate monitoring allowed the attackers to remain undetected for an extended period.

Investigators began scouring the system for clues, and discovered a Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos in system memory. Together, these two tools could have given the attackers control of the administrator account. It's not clear how the RAT was placed onto the Starwood server, but such Trojansare often downloaded from phishing emails, and it's reasonable to guess that might've been the case here.

But lurking behind these specific attack vectors lay a series of cultural and business factors that we might label the root cause of the breach. What stands out here is not the attack's success in breaching Starwood's systems — most security experts today believe it's almost impossible to keep all attackers at bay all the time — but rather that the attack went undetected for four years. Starwood did not have the best security culture before its acquisition by Marriott; the *Wall Street Journal* reported

that Starwood employees perennially found the reservation system difficult to secure, and in fact a *different* attacker breached the system in 2015 and wasn't detected for eight months. Then, after Marriott acquired Starwood in September 2016, most of Starwood's corporate staff, including those managing information technology and security, were laid off. That sort of payroll cutting is exactly what produces the "synergies" and higher profits that drive these sorts of mergers in the first place, of course, but Marriott was nowhere close to ready to book guests at its thousands of newly acquired hotels with its own in-house reservation system, and so Starwood's old system limped on, zombie-like, infected with malware, breached by hackers, and without much by way of continuity of care, for another two years before the breach was finally discovered.

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

Marriott publicly disclosed the data breach in November 2018. They launched an investigation alongside law enforcement and forensic specialists. To mitigate the impact on guests, Marriott offered credit monitoring and fraud protection services. The company also focused on strengthening its security posture by upgrading systems, implementing data encryption, and likely improving internal security protocols.

Preventing Similar Breaches

- Regularly update and patch systems
- Implement robust security protocols - e.g., multi-factor authentication
- Educate employees on cybersecurity best practices
- Continuous monitoring of systems for suspicious activity and vulnerability management
- Have a data breach response plan in place

Several steps can be taken to prevent similar cyberattacks. Regularly updating and patching systems addresses potential vulnerabilities exploited by hackers. Implementing strong security protocols like multi-factor authentication adds an extra layer of protection. Educating staff on cybersecurity best practices, such as password hygiene and phishing awareness, can significantly reduce the risk of human error. Continuous monitoring of systems for suspicious activity and having a well-defined data breach response plan in place allows for faster detection and mitigation of security incidents