FEATURE

Marriott data breach FAQ: How did it happen and what was the impact?

Many of the details remain undisclosed, but this cyberattack is a cautionary tale about IT security, mergers and acquisitions, and Chinese espionage.

By Josh Fruhlinger

CSO |

FEB 12, 2020 5:13 AM PST

In late 2018, the Marriott hotel chain announced that one of its reservation systems had been compromised, with hundreds of millions of customer records, including credit card and passport numbers, being exfiltrated by the attackers. While Marriott has not disclosed the full timeline or technical details of the assault, what we do know tells us quite a bit about the current threat landscape — and offers lessons for other enterprises on how to protect themselves.

We answer 10 frequently asked questions.

When was the Marriott breach?

On September 8, 2018, an internal security tool flagged as suspicious an attempt to access the internal guest reservation database for Marriott's Starwood brands, which include the Westin, Sheraton, St. Regis, and W hotels. This prompted an internal investigation that determined, through a forensics process that Marriott has not discussed in detail, that the Starwood network had been compromised sometime in 2014 — back when Starwood had been a separate company. Marriott purchased Starwood in 2016, but

nearly two years later, the former Starwood hotels hadn't been migrated to Marriott's own reservation system and were still using IT infrastructure inherited from Starwood, an important factor that we'll revisit in more detail later.

[How much does a data breach cost? Here's where the money goes. | Get the latest from CSO by signing up for our newsletters.]

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.

What caused the Marriott data breach?

Marriott has not made many of the details of the attack public, so we can't say for certain what vulnerability or mistake was the direct cause of the breach. Marriott CEO Arne Sorenson appeared before the U.S. Senate to talk about the attack, and the transcript of his testimony provides a window into what we do know.

As we noted, Marriott first became aware that they'd been hacked when a security tool flagged an unusual database query. (The 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.

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 Trojans are often downloaded from phishing emails, and it's reasonable to guess that might've been the case here.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

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.

What was the impact of the Marriott breach?

At one level, the Marriott breach was potentially catastrophic: hundreds of millions of people had their passport and credit card numbers stolen, which could have disastrous personal impacts. 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.

But the breach in fact does not seem to have had the damaging impact on Starwood customers that it could have. That may seem strange, and to understand the reason for it, we need to answer a couple more questions: who breached Marriott, and why.

Who hacked Marriott and why?

Mass theft of consumer data is often associated with cybercriminals aiming to perform identity theft or make use of stolen credit card numbers. But 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 stolen passport numbers in particular could be used to track movements around the world. The breach of the Office of Personnel Management's systems, which similarly resulted in millions of individuals having their data stolen but none of that data ending up on the dark web or being used for fraud, was probably part of the same campaign. The larger goal is to create a data lake of information on American government employees and agents that big data techniques can be used to analyze.

Somewhat suspiciously in retrospect, Marriott had to fight off a bid from Anbang, a Chinese company, when it acquired Starwood. However, when all that played out in 2016, the Chinese hackers had already breached Starwood's systems, so it may have been a coincidence.

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 Marriott respond to the breach?

Perhaps because there seems to be no immediate threat of the stolen data being used for conventional fraud, Marriott has not gone out of its way to compensate any of its customers whose data was stolen. The *New York Times* quotes a Marriott spokesperson as saying the company would pay the replacement cost for a passport with a new number or cover credit card expenses "if fraud has taken place." While the potential damage from personal data now stored with Chinese intelligence is in theory profound, it's difficult to quantify, especially for individuals.

Is there a Marriott data breach class action lawsuit?

Of course, that's all cold comfort if you're one of the individuals affected, and in fact Marriott and Starwood customers aren't taking the matter lying down. Multiple class action lawsuits have already been filed, and the failure of Marriott to perform due diligence on Starwood's information security (or lack thereof) has been specifically singled out in the court documents from the plaintiffs. Accenture, the consulting company to whom Starwood (and subsequently Marriott) had outsourced much of its day-to-day IT operations, is also being sued as part of the same lawsuit.

Still, don't count on a **Marriott data breach settlement** delivering a big payday. *Consumer Reports* has some details on which customers will automatically be rolled into the class action and how you can opt out; they predict that any compensation to individuals will be modest.

What did the Marriott data breach cost?

That doesn't mean the company's getting away scot free, however. As of March 2019, the company had incurred $28 million in expenses related to breach — and yet that only lowered the company's bottom line by $3 million. By May, the company had cut its losses to a mere $1 million. How? Cyberinsurance, which covered much of the initial costs associated with the crisis. Insurance against cyberattacks is a relatively new offering, but it seems to have paid off for Marriott.

But those initial costs are just that — the beginning. ZDNet estimated that between direct costs and indirect losses caused by customers shying away from the company in the future, Marriott could ultimately see billions of dollars in lost revenue as a result of the breach.

Has Marriott been fined for the data breach?

And indeed, in July of 2019 a much harsher blow landed on the company. The UK's Information Commissioner's Office (ICO) levied a fine of £99 million — more than $120 million — for violating British citizens' privacy rights under the GDPR. (The GDPR is an EU law, but still applies to Britain as Brexit has yet to go through.) Again, the ICO specifically cited Marriott's failure to do due diligence on Starwood's IT infrastructure as an explanation as to why Marriott was being punished for Starwood's mistakes. The massive fine may only be the beginning, as other jurisdictions could also look to punish the company for its lapses.

Marriott data breach case study: What can you learn from Marriott's mistakes?

We may never know all the details behind this breach, but just from what we've discussed here, a lot of important things should have come into focus for you:

- Starwood and Marriott were guilty of basic security failings: Lack of defense in depth that allowed attackers to stay in the system for years after breaching it, for instance, and failure to keep encrypted data and the keys used to encrypt it separate. Marriott failed to follow the most important cybersecurity rule: assume you are compromised and act accordingly.
- The bumpy transition associated with the Marriott-Starwood merger — the firing of Starwood's IT staff, and the long period during which Starwood's legacy systems were maintained in limbo — exacerbated the problem. The big UK fine is a hint that regulators will be holding post-merger corporations liable for these kinds of issues.
- Travel data is rich in information that can offer key insights into the lifestyles, tastes, and relationships of individuals, but the travel industry is far behind sectors like banking when it comes to cybersecurity and needs to catch up now.
- Finally, the hack showed that even private individuals can become collateral damage in the spy vs. spy world of government espionage.

What is the Marriott data breach scam?

One last note on this subject: a common scam in the aftermath of big breaches like this comes in the form of phishing emails claiming to be from the affected company, asking you to reset your password (and in the process tricking you into handing over your login credentials). Be extra vigilant and on the lookout for scams like these. Marriott didn't help things by their decision to put material related to the breach on websites with a bewildering variety of URLs.

More on hacks and breaches:

- **The 16 biggest data breaches of the 21st century**
- **The Target data breach settlement sets a low bar for industry security standards**
- **Two years after the OPM data breach: What government agencies must do now**
- **Anthem: How does a breach like this happen?**
- **Lessons from the Heartland Payment Systems data breach, redux**

Next read this

- *The 10 most powerful cybersecurity companies*
- *12 cheap or free cybersecurity training resources*
- *5 risk management mistakes CISOs still make*
- *6 security metrics that matter – and 4 that don't*
- *8 video chat apps compared: Which is best for security?*
- *How to rob a bank: A social engineering walkthrough*
- *10 ways to get more from your security budget*
- *Cybercrime in a recession: 10 things every CISO needs to know*
- *The CISO's guide to securely handling layoffs*

Josh Fruhlinger is a writer and editor who lives in Los Angeles.

Follow

The 10 most powerful cybersecurity companies