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](https://www.csoonline.com/article/3334396/what-is-digital-forensics-and-how-to-land-a-job-in-this-hot-field.html) 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.

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](http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_First-Response.pdf), 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](https://www.hsgac.senate.gov/imo/media/doc/Soresnson%20Testimony.pdf) 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)](https://www.csoonline.com/article/3086965/remote-access-threats.html) along with [MimiKatz](https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html), 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](https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how-this-tricky-malware-works.html) are often downloaded from [phishing](https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html) emails, and it's [reasonable to guess that might've been the case here](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/).

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](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/), 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](https://hbr.org/2019/03/the-marriott-breach-shows-just-how-inadequate-cyber-risk-disclosures-are). 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](https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html), breached by hackers, and without much by way of continuity of care, for another two years before the breach was finally discovered.