[Crowdstrike](https://www.crowdstrike.com/) cybersecurity expert Ryan Cornateanu [told Hotel Tech Report](https://hoteltechreport.com/news/marriott-hacked), “The attack on Marriott was hapless and a popular entry point for adversaries is through email spoofing. This tactic is used in phishing in order to get malware onto a target network to then move laterally across all systems.  From there hackers can leverage account numbers, driver's license numbers and other sensitive information from loyalty programs and reservations systems.  The general data protection regulation has gone a long way to protect consumers but there's only so much that can be done when a hacker is able to secure login credentials or access servers directly.”

Starwood was notorious for having an [insecure reservation system](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/); a separate attack in 2015 compromised data and wasn’t detected for [eight months](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html). Marriott then compounded the issue by laying off Starwoods IT staff during the acquisition in 2016. The lack of personnel prevented Marriott from quickly integrating newly added hotel properties into its own in-house reservation system. Starwood’s already-insecure guest reservation system, therefore, “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,” reports [CSO Online](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html).

As to the question of who hacked Marriott, that answer is even more complicated. Both the [New York Times](https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html) and the [Washington Post](https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/) reported that the attack was part of a state-sponsored intelligence-gathering effort on behalf of the Chinese government. Patterns in the code as well as the method of the attack echo techniques previously employed by Chinese hackers, and none of the guest records ended up for sale on the dark web – a clue that this wasn’t a hack for profit.