Marriott Data Breach 2018

Writing Investigation & Research Report

By - Jasraj

About Marriott International

Hospitality company

Marriott International, Inc. is an American multinational company that operates, franchises, and licenses lodging including hotel, residential and timeshare properties. It is headquartered in Bethesda, Maryland. The company was founded by J. Willard Marriott and his wife Alice Marriott. (Wikipedia Contributors, 2023)

Headquarters: Bethesda, Maryland, United States

Subsidiaries: Ritz-Carlton Hotel Company

CEO: Anthony Capuano (Feb 23, 2021–)

Founders: J. Willard Marriott, Alice Marriott

Founded: May 1927, Washington, D.C., United States

- Global hotel giant Marriott International generated approximately 20.77 billion U.S. dollars in revenue in 2022, up from 13.86 billion the previous year.
- 31 brands and 8,500+ properties across 138 countries and territories

The Breach

- Marriott said the breach involved unauthorized access to a database containing guest information tied to reservations made at Starwood properties on or before Sept. 10, 2018, and that its ongoing investigation suggests the perpetrators had been inside the company's networks since 2014. (Marriott: Data on 500 Million Guests Stolen in 4-Year Breach – Krebs on Security, 2018)
- In 2014, Starwood's guest reservation database had a security vulnerability that allowed unrestricted access

- In 2015, Starwood suffered a credit card breach form malware on their POS systems (InterContinental Confirms Breach at 12 Hotels – Krebs on Security, 2017)
- 2016, Marriot acquired Starwood for $13.6 billion, creating the world's largest hotel chain
- 2018, Vulnerability in Starwood database discovered through security system alert

Technology used in Starwood at the time?

Reports on the Marriott guest data breach have suggested the most probable cause was a result of the technology platform deployed by Starwood under the name "Valhalla."

Some facts are in order:

- Following standard architectures, the Starwood system would consist of multiple databases and sub-systems. The most relevant to the discussion are the SPG System with its SPG members database, the actual reservation system where active bookings are kept, and a Data Warehouse used for analytical and marketing purposes.
- It is known that soon after Marriott took control of Starwood, they began to migrate the Starwood Data Warehouse to Marriott. From a purely business perspective this makes sense, since one of the most valuable and rapidly actionable Starwood assets would have been its historical booking records. Marriott would surely have wanted access to the wealth of Starwood guest data as soon as possible for its own marketing purposes.

As for what we publicly know, the Marriott announcement alleges the following:

- That the data security incident involved the Starwood guest reservation database. Marriott believes information regarding approximately 500 million guests who had ever made a reservation at a Starwood property had been stolen.
- That Marriott's discovery of the breach was triggered on September 8, 2018, when Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott further announced that they learned during the investigation that there had been unauthorized access to the Starwood network since 2014.
- That some information included encrypted payment card numbers and payment card expiration dates. There are two components needed to decrypt the payment card numbers, and that at this point, Marriott has not been able to rule out the possibility that both were stolen. (Israel & Israel, 2018)

- It is possible that the Starwood system was in fact breached. Marriott had laid off most of the Starwood technology staff at the end of 2017, and whatever operational or migration issues this might have caused should be evaluated.

Timeline

- Nov 2014: Chinese State Sponsored Attacker installs malware to steal card data and PII at PoS cash registers of Starwood Hotels.
- Nov 2015: Starwood Hotels reports the breach, impacting 50+ hotels.
- Sep 2016: Marriott International acquires Starwood Hotels for $13 billion, maintaining the same IT system, but laying off responsible staff.
- Sep 2018: Internal security tool flags suspicious attempt to access guest reservation database; Marriott launches internal investigation.
- Nov 2018: Marriott reports breach, losing 500 million guest records including phone numbers, Credit Card data, names, etc.
- Jul 2019: Marriott fined $123 million GDPR fine, with potential for more to be paid.
- Feb 2020: Marriott reports another breach in two of its hotels, potentially caused by phishing schemes.

November 30, 2018 - Marriott has taken measures to investigate and address a data security incident involving the Starwood guest reservation database.

On November 19, 2018, the investigation determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties* on or before September 10, 2018.

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (“SPG”) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and

payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information. (Washington, 2018)

What did Marriot do?

Marriott took several steps to help its customers following the data breach:

1. Notification and Monitoring: Marriott sent out notification emails to affected customers and advised them to monitor their accounts and bank statements for suspicious activity.
2. Phishing Awareness: Customers were warned about the risk of phishing attacks and provided guidance on identifying fraudulent attempts.
3. Password Recommendations: Customers were urged to change passwords for other services if they used the same password for their Marriott accounts.
4. WebWatcher Service: Marriott offered free access to WebWatcher for one year, helping customers monitor their personal information online and providing potential compensation for U.S. users who suffered financial loss.
5. Support for Claims: Marriott provided guidance on potential compensation and actions for customers based on their rights and jurisdiction. U.S. customers were advised to contact the FTC and their state's Attorney General, while E.U. citizens were directed to their country's data regulator.
6. Multilingual Call Center: Marriott established a call center to assist customers in multiple languages, addressing any queries or concerns related to the breach.

(Perrigo, 2018)

What technologies and tools were used in the attack? (stolen data, ransom, system damage, etc.)

Based on the statements from cybersecurity experts Rusty Carter (VP, Product Management, Arxan), Ian Eyberg (CEO, NanoVMs), Ruston Miles (Founder and Chief Strategy Officer, Bluefin Payment Systems), and Ray Walsh (privacy expert and cyber security advocate, BestVPN.com), the specific technologies and tools used in the Marriott data breach from 2014 to 2018 were not explicitly mentioned or disclosed. However, they did provide insights into possible factors that might have contributed to

the breach and offered recommendations for preventing such incidents in the future. (Fruhlinger, 2020b)

1. **Employee Education (Potential Phishing Attack):** Ruston Miles, Founder and Chief Strategy Officer, Bluefin Payment Systems, suggested that the employee details might have been obtained via phishing. Phishing attacks involve tricking employees into revealing sensitive information or login credentials, which could have provided the attackers with initial access to the system.
2. **Log Analysis, Detection, and Encryption:** Ruston Miles also mentioned that the attackers encrypted the data in Marriott's servers, making it harder to detect in logs. The encryption could have been used to hide their activities and evade detection for an extended period. Additionally, the breach went undetected for about four years, indicating potential shortcomings in log analysis and detection mechanisms.
3. **Remote Access Trojans (RATs) and Mimikatz:** Marriott International reported that attackers used RAT and Mimikatz to obtain the guest list, travel details, and credit card information. Remote Access Trojans are malicious software that provide unauthorized access to a system, while Mimikatz is a tool often used to extract credentials and perform lateral movement within a network. (J.M. Porup, 2019)
4. **Absence of Defense In-Depth:** Ray Walsh, privacy expert and cyber security advocate, BestVPN.com, mentioned the absence of proper in-depth safety measures, which allowed the attackers to access valuable customer information undetected for many years. This suggests that the attackers exploited weak security measures and lack of layered defenses to maintain their presence in the system.

What was the motivation of the attackers in this case? What did they hope to achieve?

- The motivation behind the Marriott data breach appears to be part of a broader cyber espionage campaign conducted by Chinese intelligence services. The attackers were believed to be state-sponsored Chinese hackers, as indicated by the techniques used, the cloud-hosting space utilized, and the lack of data being offered for sale on the dark web. (“Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing (Published 2018),” 2023)
- The primary goal of this cyberattack was to acquire massive amounts of data on American government employees and intelligence officers. Marriott is a major hotel provider for the U.S. government and military, making it a valuable target for gathering sensitive information. The stolen data, including passport numbers,

could be used to track the movements of government personnel and potentially aid in espionage efforts.

- The breach of Marriott's systems was likely part of a larger campaign that also included the hack of the Office of Personnel Management (OPM) (Fruhlinger, 2020a) in which millions of individuals' data was stolen, but the data did not end up on the dark web or used for fraud. (Guccione, 2021) The U.S. government linked the Marriott, OPM, and Equifax breaches together as part of the same operation, indicating a concerted effort by the attackers to create a data lake of information on American government employees and agents. (“U.S. Charges Chinese Military Officers in 2017 Equifax Hacking (Published 2020),” 2023)
- While it's challenging to pinpoint the exact motive behind cyber espionage campaigns, such attacks are often carried out by nation-states to gather intelligence, gain a competitive advantage, or further their geopolitical interests. The Marriott breach was part of a sophisticated and targeted operation aimed at accessing valuable information about U.S. government personnel, and the attackers' motivations were likely aligned with their state's strategic goals. (Fruhlinger, 2020b)

What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

- 91.1 million unique credit card numbers were stolen.
- 23.75 million unique passport numbers were stolen.
- Guests' personal information, including names and dates of birth, was lost.
- Loss of membership points and benefits for affected customers.
- Marriott International's stock price (NASDAQ: MAR) dropped 5.6% after the breach, reaching a low of $100.62 just before Christmas. (Kilgore, 2018)
- Encryption keys for credit card numbers were stored on the same server and were also compromised.
- Some passport numbers were encrypted, but the majority were saved in clear text.

Despite the significant data stolen, the breach did not seem to have a damaging impact on Starwood customers. This might be due to the fact that the attackers were likely state-sponsored Chinese hackers involved in cyber espionage, rather than cybercriminals aiming to use the stolen data for fraud or selling on the dark web. (Fruhlinger, 2020b)

What mitigation technique would you recommend to prevent these attacks in future?

- Maintain and secure Point of Sale (PoS) cash registers.
- Perform thorough audits of the IT system after acquiring new entities like Starwood.
- Integrate all IT systems, including newly acquired ones, with a centralized security system.
- Implement better log analysis and detection using Artificial Intelligence (AI) automation.
- Conduct regular audits of all systems to comply with industry-specific requirements.
- Enforce the use of multi-factor authentication to access guest data.

Describe security controls that would help mitigate these risks.

To mitigate the risks associated with data breaches and cyberattacks, implementing robust security controls is essential. Here are some security controls that would help in preventing and mitigating such risks: (Cyber Security Experts Weigh in on Marriott/Starwood Data Breach, 2021)

1. Access Controls:

Enforce strong access controls with multi-factor authentication (MFA) for all users, especially for accessing sensitive data and critical systems.

2. Data Protection:
    1. Encrypt all sensitive data, including credit card numbers and passport information, both at rest and in transit.
    2. Utilize tokenization to replace sensitive data with non-sensitive tokens to minimize the exposure of critical information.
3. Network Security:
    1. Implement network segmentation to isolate critical systems and limit lateral movement for attackers within the network.
    2. Deploy Intrusion Detection and Prevention Systems (IDPS) to monitor network traffic and identify potential cyber threats in real-time.
4. Logging and Monitoring:
    1. Establish comprehensive logging mechanisms to capture and store logs from critical systems and network devices.
    2. Employ Security Information and Event Management (SIEM) tools for analyzing and correlating logs to detect suspicious activities.
5. Vulnerability Management:

    1. Conduct regular vulnerability assessments to identify and remediate security weaknesses in systems and applications.
    2. Perform periodic penetration testing to simulate real-world attacks and discover potential entry points for attackers.
6. Employee Training and Awareness:
    1. Provide regular cybersecurity training to employees to recognize phishing attempts and other social engineering techniques.
    2. Foster a culture of security awareness to ensure all employees understand their role in maintaining a secure environment.
7. Incident Response Plan:
    1. Develop a well-defined incident response plan that outlines specific steps to be taken in case of a data breach or cyber incident.
    2. Test and update the incident response plan regularly to ensure its effectiveness in handling emerging threats.
8. Continuous Security Monitoring:

Implement continuous security monitoring to detect and respond to threats in real-time, reducing the time between detection and response.

9. Security Audits and Compliance:
    1. Conduct regular security audits to assess the effectiveness of implemented security controls and identify areas for improvement.
    2. Ensure compliance with relevant industry standards and regulations to meet security requirements.

(Cyber Security Experts Weigh in on Marriott/Starwood Data Breach, 2021)

References

Cyber Security Experts Weigh In on Marriott/Starwood Data Breach. (2021, December 17). Hospitality Technology. https://hospitalitytech.com/cyber-security-experts-weigh-marriottstarwood-data-breach

Fruhlinger, J. (2020a, February 12). *Marriott data breach FAQ: How did it happen and what was the impact?* CSO Online; CSO Online. https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-

and-what-was-the-impact.html#:~:text=In%20late%202018%2C%20the%20Marriott,being%20exfiltrated%20by%20the%20attackers.

Fruhlinger, J. (2020b, February 12). *The OPM hack explained: Bad security practices meet China's Captain America*. CSO Online; CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Guccione, D. (2021, July). *What is the dark web? How to access it and what you'll find*. CSO Online; CSO Online. https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

InterContinental Confirms Breach at 12 Hotels – Krebs on Security. (2017, February 6). Krebsonsecurity.com. https://krebsonsecurity.com/2017/02/intercontinental-confirms-breach-at-12-hotels/

Israel, & Israel. (2018, December 10). *Marriott data breach ex Starwood perspective*. Phocuswire.com; PhocusWire. https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective

J.M. Porup. (2019, March 5). *What is Mimikatz? And how to defend against this password stealing tool*. CSO Online; CSO Online. https://www.csoonline.com/article/566987/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html

Kilgore, T. (2018, November 30). *Marriott's stock sinks after disclosing data breach affecting up to 500 million guests*. MarketWatch; MarketWatch. https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing (Published 2018). (2023). *The New York Times*. https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Marriott: Data on 500 Million Guests Stolen in 4-Year Breach – Krebs on Security. (2018, December 11). Krebsonsecurity.com. https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/

Perrigo, B. (2018, November 30). *Stayed at a Marriott Recently? Here's What To Do About That Massive Data Breach*. Time; Time. https://time.com/5467781/marriott-data-breach-information/

U.S. Charges Chinese Military Officers in 2017 Equifax Hacking (Published 2020). (2023). *The New York Times*. https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html

Washington, D. (2018). *UNITED STATES SECURITIES AND EXCHANGE COMMISSION FORM 8-K CURRENT REPORT Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 Date of Report (Date of earliest event reported): Delaware 1-13881 52-2055918 (State or other jurisdiction of incorporation) (Commission File Number)*. https://marriott.gcs-web.com/static-files/733886b2-f409-478a-9986-16044b6fcf58

Wikipedia Contributors. (2023, July 11). *Marriott International*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Marriott_International