Writing Investigation & Research Report

Marriott International Data Breach 2018

March 29, 2024

By Heather Fincati

Justin Sullivan via Getty Images

Glossary

General Terms

Attacker: A malicious actor who attempts to gain unauthorized access to a computer system or network.
Data Breach: An incident where sensitive information is accessed and disclosed without authorization.
Exploit: A piece of code that takes advantage of a software vulnerability.
Mitigation Technique: An action taken to reduce the risk or impact of a security threat.
Patch: An update to software that fixes a security vulnerability.
Penetration Testing: A simulated cyberattack designed to identify vulnerabilities in a system.
Phishing: A social engineering attack that attempts to trick users into revealing sensitive information.
Remote Access Trojan (RAT): A type of malware that allows an attacker to remotely control a victim's computer.
Security Control: A safeguard implemented to protect a system or network from unauthorized access.
Security Posture: The overall state of an organization's security measures.
Vulnerability: A weakness in a system or software that can be exploited by an attacker.

Specific Terms

Dark Web: A hidden part of the internet that is not indexed by search engines and is often used for illegal activity.
GDPR (General Data Protection Regulation): A regulation in EU law on data protection and privacy in the European Union.
IDS (Intrusion Detection System): A system that monitors network traffic for malicious activity.
IPS (Intrusion Prevention System): A system that can detect and block malicious network traffic.
MFA (Multi-Factor Authentication): An authentication method that requires two or more verification factors to access a system.
NIST (National Institute of Standards and Technology): A US government agency that develops standards for information security.
PII (Personally Identifiable Information): Any information that can be used to identify an individual, such as name, address, or Social Security number.
SIEM (Security Information and Event Management): A system that collects and analyzes security data from various sources.

Executive Summary

Marriott International has suffered at least seven data breaches since 2010 (Entrepreneur, 2022). Not all of these breaches were well documented. There was one in particular that stood out due to the sheer volume of people it affected and will be highlighted in this report. The 2018 Marriott International data breach, a cyberattack that compromised the personal information of millions of Starwood-branded hotel guests. Starwood is a division of Marriott International. The initial breach occurred in 2014 on the Starwood guest reservation database (LI, n.d.), Marriott acquired the company in 2016 and the breach was discovered in 2018 they were found liable for all damages. The report details the victims, potential attack methods, targeted systems, and the attackers' motives. It analyzes the attack's outcome and proposes mitigation techniques and security controls to prevent similar incidents in the future.

Introduction

Data breaches are a growing concern in today's digital world. The 2018 Marriott International data breach stands as a significant example, exposing the personal information of a vast number of individuals. It is also one of the largest data breaches ever reported. This report investigates this cyberattack, providing insights for organizations to strengthen their security posture and prevent data breaches like this in the future.

Victims of the Attack

Marriott believed the data stolen contained information of up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, more personal information was obtained, likely including names, addresses, phone numbers, email addresses, passport details, loyalty program information, and potentially payment card details.

Attack Details

Timeline

From July 2014 to September 2018, hackers had access to the guest reservation database of a hotel chain, Starwood Hotels & Resorts Worldwide, that Marriott had purchased mid-breach in September 2016. *(PUBLISHED UNITED STATES COURT OF APPEAL No. 22-1744 CUSTOMER DATA, 2023)*

Methods

The technology used for this breach was Remote Access Trojan (RAT). A RAT is malware that allows a malicious actor to gain remote access to a target's computer. The attackers also used an open-source tool called Mimikatz, which searches a device or system's memory for user credentials (Newsome, n.d.).

Attacker Motivation

At first glance this could definitely be seen as financial gain motivation, selling credit card information and passport numbers etc on the dark web would bring in money for the attackers. However to date none of the information has been sold, strengthening the theory that this attack was done by a government agency and not by cyber criminals.

The New York Times and The Washington Post both reported that this 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 (Hollander, 2023).

Impact of the Attack

The attack resulted in a massive data breach, leading to:

Reputational damage for Marriott International, multiple class-action lawsuits, financial losses in the millions; from fines, paying for customers' passport replacements and loss of revenue because two of three Americans don't trust the brand. Separately, the United Kingdom's Information Commissioner's Office (ICO), a consumer rights watchdog, fined Marriott $23.8 million (down from the original penalty of $123 million) for failing to meet security standards required by GDPR. The ICO argues that Marriott failed to "put appropriate technical or organizational measures in place" when processing data, though it also acknowledged that Marriott has since taken the proper measures to improve security. Notably, the original fine of $123 million would have been one of the largest penalties issued under GDPR, representing around 3% of Marriott's total revenue (Hollander, 2023).

9.1 million unique credit card numbers and 23.7 million unique passport numbers were stolen. Along with guests personal data, such as; names, birth dates, mailing addresses, phone numbers, email addresses, genders, etc. Leaving guests vulnerable to identity theft or fraud (LI, n.d.).

Mitigation Techniques

By following industry standards and best practices outlined by NIST (International Institute of Standards and Technology) (*NIST*, 2020), Marriott International could implement several mitigation techniques to prevent similar attacks:

1. Regular system and software patching to address vulnerabilities

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware (*NIST*, 2013).

- **Importance:** Unpatched vulnerabilities are like open doors for attackers. Regularly patching operating systems, applications, and firmware on all devices (servers, desktops, laptops) significantly reduces the attack surface and makes it harder for attackers to gain a foothold.

- **Benefits in the Marriott case:** Patching vulnerabilities in the Starwood reservation system could have potentially prevented attackers from exploiting weaknesses to gain unauthorized access.

2. Strong access controls including multi-factor authentication (MFA)

Access controls are digital gatekeepers that determine who can access specific systems and data. MFA (*NIST*, 2019) adds an extra layer of security on top of traditional passwords.

- **Multi-factor authentication (MFA):** MFA requires a second factor beyond a password, such as a code sent to your phone or a fingerprint scan. This significantly increases the difficulty for unauthorized users to gain access, even if they have stolen a password.

- **Benefits in the Marriott case:** Implementing strong access controls with MFA on the Starwood reservation system could have prevented attackers from using compromised credentials to access guest data.

3. Network segmentation to limit attacker movement

Network segmentation restricts the movement of attackers within the network. Even if an attacker breaches one zone, they face additional hurdles to reach sensitive data in other zones (*NIST*, 2020).

- **Concept:** Networks can be segmented by department, function, or security level. Firewalls and access control lists further restrict traffic flow between different zones.

- **Benefits in the Marriott case:** Network segmentation could have limited an attacker's ability to move laterally within the Marriott network after compromising the Starwood reservation system. This could have prevented them from accessing other sensitive systems or data.

4. Network traffic monitoring for suspicious activity

Continuously monitoring your network traffic is like having security cameras watching for suspicious activity.

- **Tools:** Security tools like IDS/IPS (mentioned earlier) can continuously analyze network traffic for anomalies and suspicious patterns. These could indicate malware communication, unauthorized access attempts, or data exfiltration.

- **Benefits in the Marriott case**: Monitoring network traffic for suspicious activity could have helped detect unusual data transfer patterns from the Starwood reservation system, potentially alerting security teams to a potential attack.

5. Sensitive data encryption (at rest and in transit)

Encryption scrambles data using a secret key, making it unreadable without the key. This adds a significant layer of protection to sensitive data (Smid & Foti, 2021).

- **Encryption at rest:** This encrypts data when it's stored on servers or storage devices. Even if attackers breach a system, they cannot access the data without the decryption key.

- **Encryption in transit:** This encrypts data while it's being transmitted across the network. This protects sensitive data from being intercepted during transmission between systems.

- **Benefits in the Marriott case:** Encrypting guest data at rest and in transit could have significantly reduced the impact of the breach. Even if attackers stole the data, it would have been useless without the decryption key.

6. Employee cybersecurity training including phishing awareness

Employees are often the first line of defense against cyberattacks. Phishing emails are a common tactic where attackers trick employees into clicking malicious links or revealing sensitive information.

- **Training:** Regularly training employees on cybersecurity best practices, including phishing awareness, can significantly reduce the risk of successful social engineering attacks.

- **Benefits in the Marriott case:** Training employees to identify phishing attempts and raising awareness about data security could have prevented attackers from potentially tricking employees into revealing access credentials to the Starwood reservation system.

By implementing these essential security practices, organizations can significantly reduce the risk of data breaches and protect sensitive information.

Security Controls

Implementing the following Industry standard as outlined in the NIST framework (NIST, 2020) security controls can further mitigate risks:

1. Security Information and Event Management (SIEM) systems

SIEM systems act as the central nervous system for security operations. They collect log data from various security tools and IT infrastructure components, including firewalls, intrusion detection systems, servers, and applications. SIEMs then analyze this vast amount of data to identify potential security incidents.

- **Log aggregation and correlation:** SIEM can ingest logs from various sources related to the Starwood reservation system, user activity, and network traffic. By correlating these logs, SIEM can identify suspicious patterns, such as unusual login attempts, unauthorized data access, or high volumes of data exfiltration attempts.

- **Alert generation:** Based on pre-defined rules or anomaly detection algorithms, SIEM can trigger alerts for suspicious activity. In the Marriott case, SIEM could have alerted security teams to unauthorized access attempts to the Starwood database or unusual data transfer patterns.

- **Incident investigation and forensics:** SIEM provides a centralized platform for security analysts to investigate potential incidents. They can use log data and timelines to understand the attack scope, identify affected systems, and reconstruct the attacker's actions.

2. Intrusion Detection/Prevention Systems (IDS/IPS)

IDS and IPS systems work together to monitor network traffic for malicious activity.

- **Intrusion Detection System (IDS):** IDS acts as a security guard, continuously monitoring network traffic for signatures of known attacks or suspicious patterns. When an IDS detects suspicious activity, it generates alerts for further investigation. In the Marriott breach, an IDS could have detected attempts to exploit vulnerabilities in the Starwood network or identify malware communication attempts.

- **Intrusion Prevention System (IPS):** IPS goes beyond detection and takes preventive actions. It can automatically block malicious traffic or suspicious connections, potentially stopping an attack in its tracks. In the Marriott scenario, an IPS could have blocked attempts to access unauthorized resources or prevented data exfiltration attempts.

3. Data Loss Prevention (DLP) systems

DLP systems focus on protecting sensitive data from unauthorized disclosure. They can monitor data movement across the network and endpoints, identifying and preventing attempts to exfiltrate sensitive information.

- **Data identification and classification:** DLP systems can identify and classify sensitive data based on predefined policies. This could include personally identifiable information (PII) like names, passport details, or credit card numbers in the Marriott case.

- **Data monitoring and control:** DLP monitors data movement and applies pre-defined controls. It could prevent unauthorized users from copying or transferring sensitive data to external devices or cloud storage. For example, DLP could block attempts to email guest passport details or credit card numbers.

4. Regular security assessments and penetration testing

These proactive measures are crucial for identifying vulnerabilities before attackers exploit them.

- **Security assessments**: Regular security assessments involve a systematic evaluation of an organization's security posture. This can include reviewing security policies, configurations, and procedures to identify weaknesses. In the Marriott case, a security assessment might have identified vulnerabilities in the Starwood reservation system that attackers exploited.

- **Penetration testing**: Penetration testing simulates real-world attacks by ethical hackers who attempt to gain unauthorized access to systems. This helps identify exploitable vulnerabilities that attackers might use. Penetration testing of the Starwood system could have revealed weaknesses that allowed attackers to breach the database.

By implementing these security controls in a layered defense approach, organizations can significantly improve their security posture and detect or prevent attacks like the one experienced by Marriott International.

Conclusion

The 2018 Marriott International data breach stands as a cautionary tale for organizations of all sizes. It highlights the critical need for robust cybersecurity practices to safeguard sensitive customer information. By implementing the mitigation techniques and security controls outlined in this report, organizations can significantly reduce the risk of data breaches and regain the trust of their customers.

Furthermore, the regulatory landscape for data breaches is constantly evolving, with stricter regulations emerging worldwide. The General Data Protection Regulation (GDPR) in Europe (*The General Data Protection Regulation - Consilium*, n.d.), for example, imposes significant fines for data breaches. Staying informed about these regulations and ensuring compliance is crucial to avoid hefty penalties and reputational damage.

Finally, even the most comprehensive security controls can be undermined by human error. Ongoing security awareness programs for employees are essential. Regular training can equip employees to identify phishing attempts, avoid social engineering tactics, and handle sensitive data securely. This reduces the risk of unintentional security breaches caused by human actions.

By prioritizing cybersecurity, implementing strong security measures, and fostering a culture of security awareness within the organization, businesses can significantly reduce the risk of data breaches and protect their valuable customer information.

References

1. Garfinkle, M. (2022, July 7). *Marriott's Been Hacked 7 Times - See Data Breach Details*. Entrepreneur. Retrieved March 28, 2024, from: https://www.entrepreneur.com/business-news/marriotts-been-hacked-7-times-see-data-breach-details/430988#:~:text=Since%202010%2C%20Marriott%20has%20suffered,U.K.'s%20Information%20Commissioner's%20Office.

2. *LI, A. (n.d.). Marriott Data Breach.pdf*. Retrieved March 28, 2024, from https://www3.cs.stonybrook.edu/~ise331/Slides/Marriott%20Data%20Breach.pdf

3. Newsome, T. (n.d.). *The Marriott/Starwood Data Breach & Third-Party Risk*. Prevalent. Retrieved March 28, 2024, from https://www.prevalent.net/blog/the-marriott-starwood-data-breach-why-third-party-risk-management-is-critical-during-m-a/

4. *PUBLISHED UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT No. 22-1744 In re: MARRIOTT INTERNATIONAL, INC., CUSTOMER DATA*. (2023, August 18). Fourth Circuit Court of Appeals. Retrieved March 28, 2024, from https://www.ca4.uscourts.gov/opinions/221744.P.pdf

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

6. Timberg, C., & Nakashima, E. (2018, December 11). *U.S. investigators point to China in Marriott hack affecting 500 million guests*. The Washington Post. Retrieved March 28, 2024, from https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/

7. Hollander, J. (2023, February 16). *Marriott Data Breach FAQ: What Really Happened?* Hotel Tech Report, from https://hoteltechreport.com/news/marriott-data-breach

8. *NIST Privacy Framework: An Overview*. (2020, June 25). NIST. https://www.nist.gov/publications/nist-privacy-framework-overview

9. *SP 800-40 Rev 3 Guide to Enterprise Patch Management Technologies*. (2013, July 22). NIST. https://www.nist.gov/publications/guide-enterprise-patch-management-technologies

10. *SP 1800-17 Multifactor Authentication for E-Commerce*. (2019, July 30). NIST. https://www.nist.gov/publications/multifactor-authentication-e-commerce

11. Smid, M. E., & Foti, J. (2021, August 16). *Journal of Research (NIST JRES) Volume 126,Development of the Advanced Encryption Standard*. NIST. https://www.nist.gov/publications/development-advanced-encryption-standard

12. *The general data protection regulation - Consilium*. (n.d.). Consilium.europa.eu. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

13. NIST Special Publication 800-53 Revision 5, Section 5.3.1 - Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53) https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

14. *NIST Special Publication (SP) 800-53 Rev. 5, Section AC-12.1 - Access Enforcement*. (n.d.). NIST Computer Security Resource Center. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

15. *NIST Special Publication (SP) 800-53 Rev. 5 Section SC-4 - System and Communications Protection - Security and Privacy Controls for Information Systems and Organizations*. (2020). NIST Computer Security Resource Center. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final