DATA BREACH ANALYSIS CASE STUDY PAPER

Vanessa Kibaja

CY5010

Prof. Sierra

April 20th 2021

Table of Contents

Abstract

The purpose of this paper is to provide a clear and elaborate analysis of the 2018 data breach at Marriott International Inc. and how it was performed, detected, and responded to. One of Marriott's reservation systems, the Starwood reservation system, had been compromised since 2014 when the company had not acquired Starwood Hotels. The federal investigators traced this data breach to Chinese state hackers. The Chinese spy agency might have planned to track the movements of U.S. government employees around the world using the stolen personal data. The breach was detected on 7th September 2018, after an IBM Guardium database alert tool identified an attempt to access Marriott's legacy Starwood guest reservation database as suspicious. The time between the initial exploit and detection was at least 4 years. The hackers stole the personal data/information (such as passport numbers, addresses, credit cards, and individuals' names) of hundreds of millions of guests. These attackers followed the tactics and utilized some techniques under MITRE ATT&CK Framework. The company responded to the data breach by undertaking considerable containment measures and infrastructure changes. Authorities responded to this breach by opening investigations. The industry peers responded by tightening up the data security of their systems. The company delayed in notifying users about the data breach. It notified authorities on October 29, 2018. The breach brought about calls for harsher legislation to protect the data privacy of the consumers. Among the things that I would have done if I were handling post-breach procedures include investigating it thoroughly and safeguarding physical areas associated with the hacking. This data breach continues to be among the most damaging and biggest data breaches in American history.

Introduction

Data breaches have been a common occurrence, particularly in the twenty-first century. Millions of individuals across the world have had their personal/confidential information exposed. As per a report by Identity Theft Resource Center (ITRC), between January 2005 and March 2018, the number of data breaches in the United States alone amounted to 8,741 and the number of exposed records amounted to 1,069,914,088.[1] Of late, a wave of data breaches has continued to crash down on corporations, and among these corporations is the Marriott Hotel Group.

Description of the 2018 Data Breach at Marriott International Inc.

Source and Motivation of the Attack leading to the Breach

Marriott announced in late 2018 that one of its reservation systems (Starwood reservation system) had been compromised, with the attackers having exfiltrated hundreds of millions of the records of its customers. The company joined the league of the world's largest corporations whose systems had been breached and the information of millions of customers compromised by the attackers.

Regarding the source of the attack resulting in this data breach, the United States Government investigators traced the data breach to Chinese state hackers. The investigators believed that these Chinese attackers were working for China's spy agency (the nation's Ministry of State Security).[2] They also believed that the motivation for the attack leading to the breach was part of a wider effort of the Chinese government to have access to enormous amounts of data on the employees of the federal government as well as intelligence officers. Notably,

---

[1] Liu, Liyuan, Meng Han, Yan Wang, and Yiyun Zhou. "Understanding data breach: A visualization aspect." In *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 883-892. Springer, Cham, 2018, 883.

[2] Rahman, Khaleda. "US Investigators Point to China in Massive Hack of Marriott System." Mail Online. Last modified December 12, 2018. https://www.dailymail.co.uk/news/article-6486803/US-investigators-point-China-massive-hack-Marriott-system.html.

Marriott was a suitable target because it is a leading provider of hotel services not only for the United States government but also for the U.S. military.

It is vital to emphasize that the Chinese spy agency might have planned to track the movements of U.S. government employees around the world using the stolen personal data, particularly passport numbers. Notably, the Chinese attackers had already breached the systems of Starwood when China's Anbang Insurance Group Co abandoned its bid to purchase Starwood Hotels in 2016. Consequently, this might have been a plan by China's spy agency.

How the Breach was Detected

The breach was primarily detected after an internal security tool (IBM Guardium database alert tool) identified an attempt to access Marriott's legacy Starwood guest reservation database as suspicious on September 7, 2018. In particular, the data breach was discovered by the IBM Guardium database alert tool on September 7, 2018, and Marriott International Inc.'s third-party IT contractor, Accenture, which the company had assigned the responsibility of managing the legacy Starwood guest reservation database, notified its IT department on September 8, 2018. As a result, the company tasked CrowdStrike. Inc. and other third-party investigators with the responsibility of carrying out a review of the hacked systems.[3] However, Marriott waited for two months to disclose the breach to the public. Notably, the hackers had installed VPN tools, webshells, and malware (including Remote Access Trojan ("RAT") variants) on the systems of Starwood.[4]

Amount of Time between Initial Exploit and Detection and Methods used for Exploitation

Marriott learned that the breach had started at least in July 2014, a period when this company had not acquired Starwood Hotels. As explained above, the breach was detected on

[3] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 18.

[4] ibid.

September 7, 2018. Consequently, the time between the initial exploit and detection was at least 4 years. The security monitoring tools aimed at identifying possibly malicious activity in real-time that were deployed by CrowdStrike on September 12, 2018, to thousands of devices, which were initially on the Starwood network, revealed that the hackers installed VPN tools, webshells, and malware (such as RAT variants and Mimikatz) on the systems of Starwood.[5]

As described in the Payment Card Industry Forensic Investigator (PFI) report commissioned by Marriott, the attackers took advantage of the known software vulnerabilities to remotely access a server in the Starwood cardholder data environment (CDE) before installing malware on that server and others.[6] As a result, they captured the passwords and usernames for certain administrator and user accounts in the Starwood CDE. Afterwards, the attackers moved through the Starwood cardholder data environment using the credentials from the administrator and user accounts to install additional malware and compile confidential personal information.[7] They then staged or compiled that confidential personal information/data on an additional server. Later, they transferred that information to a server with internet connectivity prior to sending it to a computer outside the cardholder data environment of Starwood.[8]

Type of Data Breached and the Number of Records

Hotel group Marriott revealed that hackers had stolen the personal data/information of up to 500 million guests.[9] This data included passport numbers, addresses, credit cards, individuals' names, gender, dates of birth, reservation information, email addresses, and phone numbers.

---

[5] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 105.

[6] Ibid, 140.

[7] Ibid.

[8] Ibid.

[9] Perlroth, Nicole, Amie Tsang, and Adam Satariano. "Marriott Hacking Exposes Data of Up to 500 Million Guests." *The New York Times*, November 30, 2018. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

MITRE ATT&CK Mapping

It is important to emphasize that the strategic goal of the attackers who perpetrated the 2018 Mariotte data breach was to steal information. In carrying out their attack, these attackers followed the tactics and utilized some techniques described in the MITRE ATT&CK Framework.

Specifically, their attack started with an attempt to gain Initial Access (TA0001) into Starwood reservation systems. As mentioned above, these attackers remotely accessed a server in the Starwood cardholder data environment by taking advantage of the known software vulnerabilities. Under the Execution (TA0002) tactic, these attackers installed malware on the server and other servers that they accessed. The attackers might have maintained their foothold (Persistence (TA0003) tactic) within the systems of Starwood by taking advantage of Starwood's constant non-compliance as well as deviations from baseline configuration standards.[10] Regarding the Privilege Escalation (TA0004) tactic, these attackers gained higher-level permissions on the systems of Starwood by taking advantage of the vulnerabilities, misconfigurations, and weaknesses of this system. For instance, CWs affirmed that Starwood was neither monitoring its security nor privilege access logs.[11] Consequently, the attackers exploited this weakness to gain higher-level permissions on the systems of Starwood.

As regards Defense Evasion (TA0005) tactic, the attackers tried to avoid detection by taking advantage of the Starwood reservation system susceptibility to bypass security features. For example, they took advantage of Starwood's lack of point-to-point encryption and tokenization across its point-of-sale systems.[12] They also tried to avoid detection by deleting the

---

[10] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 92.

[11] ibid., 290.

[12] Ibid., 123.

encrypted and compressed files that were left behind by their intrusion activity. For instance, the investigators of Marriott International Inc. discovered evidence that two encrypted and compressed files containing personal information had been erased from a device they examined on November 13, 2018, and the company finally started preparations to inform affected agents.[13] Additionally, these attackers tried to avoid detection by obtaining and abusing credentials from the administrator and user accounts.

With reference to Credential Access (TA0006) tactic, the attackers moved through the Starwood cardholder data environment using the accessed credentials from the administrator and user accounts to install additional malware and amass confidential personal information, as mentioned above. Regarding Discovery (TA0007) tactic, these attackers tried to figure out the Starwood cardholder data environment by performing searches for, as well as accessing files, in this environment that contained the terms, for example, "script," "password" or "user" in the file name.[14] In regard to Lateral Movement (TA0008) tactic, the attackers moved laterally through the Starwood cardholder data environment (systems) by leveraging the information they had obtained.[15] They also did this to install as well as execute different variants and types of malware on those systems. As regards the Collection (TA0009) tactic, the attackers gathered data/information by leveraging two compromised user accounts.[16]

With regard to the Exfiltration (TA0010) tactic, the attackers exfiltrated data/information by also leveraging the two compromised user accounts. Additionally, as mentioned earlier, these hackers exfiltrated data/information by transferring it to a server with internet connectivity prior

[13] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 106.

[14] ibid., 150.

[15] ibid., 144.

[16] ibid., 150.

to sending it to a computer outside the cardholder data environment of Starwood. Regarding Command and Control (TA0011) tactic, the Remote Access Trojan provided these hackers with command-and-control functionality that allowed them to make use of remote command capabilities, carry out file management, and establish a network connection.[17] Lastly, as regards Impact (TA0040), the attackers deleted data to hide their activities. For instance, Verizon recovered proof of deleted file records, which comprised guest reservation database table exports on Computer 10.[18]

Response, Recovery Actions, and Impact of the Data Breach

Response and Recovery Actions that were taken by Marriott

Marriott International Inc. responded to the data breach by undertaking considerable containment measures as well as infrastructure changes. For instance, regarding containment measures, the company disabled known compromised network/system accounts and database accounts and reset passwords on all accounts, which accessed the environment in a specified timeframe.[19] Additionally, Marriott leveraged Darknet research and threat intelligence in its effort to identify more potential IOCs associated with the event.

With reference to infrastructure changes, the company substituted encryption keys for each of the cardholder data environment record within the in-scope database, leveraged security tools, including EDR and others, to carry out searches for known IOCs, implemented policies to impose multi-factor authentication access to the cardholder data environment, carried out external scanning for known IOCs as well as external susceptibility scans of Starwood cardholder data environment within the in-scope database, decommissioned whole Starwood

[17] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 149.

[18] ibid., 153.

[19] ibid., 161.

cardholder data environment, rebuilt systems for identified compromised systems, and created new user accounts for workers whose accounts had been disabled.[20]

Authorities and Industry Peers

Authorities, including government regulatory agencies led by the FBI, regulatory authorities in several jurisdictions, and certain committees of the United States House of Representatives and Senate, responded to the Marriott data breach by opening investigations. The company cooperated with the investigators. After the announcement of this breach, about 100 lawsuits were filed against the company and its subsidiary, Starwood, from several plaintiffs, including consumers and others in the Canadian Courts, U.S. federal courts, and U.S. state courts.[21] Notably, all except one of the United States cases were combined into a multi-district litigation ("MDL") and transferred to the United States District Court for the District of Maryland, in consonance with orders of the United States Judicial Panel.[22] The company was fined by the United Kingdom's data privacy watchdog 18.4 million Sterling Pounds.[23] The industry peers responded to this data breach by strengthening the data security of their systems.

Notification to Impacted Users and Authorities

Marriott notified users about the data breach on November 30, 2018. Notably, this is when the company made its initial public revelations about the data breach. The company contacted the FBI to inform them of the intrusion timelines, tools that the attackers utilized, and any forensic results the third-party investigators and it had made on October 29, 2018, over one

---

[20] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 162-163.

[21] *2020 Annual Report*. Marriott International Inc., 2021, 67.

[22] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 118.

[23] BBC News. "Marriott Hotels fined £18.4m for data breach that hit millions." Last modified October 30, 2020. https://www.bbc.com/news/technology-54748843

month before it informed the public.[24] It provided data breach notification to the 4 major payment card networks, regulatory authorities in more than 20 overseas territories and nations, the SEC, the FTC, state Attorney Generals, and 3 major credit reporting agencies on November 29, 2018.[25]

Assessment of the Impact of the Breach on Regulated and Industry, Related Breaches

The data breach spurred a push for new privacy law. It quickly resulted in calls for tougher legislation to safeguard the data privacy of the consumers. In essence, draft legislation called the Consumer Data Protection Act (CDPA) was released by Sen. Ron Wyden in 2018. The players in the industry, particularly the hotel industry, responded by tightening up their cybersecurity strategies. There are several other data breaches related to the Marriott data breach. Among these breaches include the 2016 intrusion/hacking at FriendFinder Networks, the 2019 accidental internet/web exposure at Facebook, intrusion/hacking at Yahoo in 2014, and the 2017 accidental internet/web exposure at River City Media. Notably, these are among the largest data breaches in the history of the United States.

What I would have Done Differently if I were Handling Post Breach Procedures

If I were handling post-breach procedures, I would have responded by investigating thoroughly, safeguarding physical areas associated with the breach, notifying the appropriate authorities, making public revelations about the data breach after the investigations, and involving a team of specialists in fixing the vulnerabilities (the problem).

Conclusion

The 2018 Marriot data breach remains among the most damaging and largest data breaches on record. The company would not have experienced this breach if it had heavily

---

[24] *In Re Marriott International, Inc., Customer Data Security Breach Litigation*, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020), 106.

[25] ibid.

invested to protect consumer data, been ahead of the security curve, carried out due diligence during the acquisition of Starwood Hotels, and nurtured a security-centric culture at the upper management level.

Bibliography

2020 Annual Report. Marriott International Inc., 2021.

In Re Marriott International, Inc., Customer Data Security Breach Litigation, MDL No. 8:19-md-2879-PWG (D. Md. Jul. 24, 2020).

Liu, Liyuan, Meng Han, Yan Wang, and Yiyun Zhou. "Understanding data breach: A visualization aspect." In *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 883-892. Springer, Cham, 2018.

Perlroth, Nicole, Amie Tsang, and Adam Satariano. "Marriott Hacking Exposes Data of Up to 500 Million Guests." *The New York Times*, November 30, 2018. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

BBC News. “Marriott Hotels fined £18.4m for data breach that hit millions.” Last modified October 30, 2020. https://www.bbc.com/news/technology-54748843

Rahman, Khaleda. "US Investigators Point to China in Massive Hack of Marriott System." *Mail Online*. Last modified December 12, 2018. https://www.dailymail.co.uk/news/article-6486803/US-investigators-point-China-massive-hack-Marriott-system.html.