Analysis of Marriott Data Breach

This document is a deep dive into the theoretical aspects of the massive Marriott Data Breach.

> Author → Tanishq Rupaal

Marriott and Starwood

Marriott International Inc. is an American multinational hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities.[1]

Current Executive Chairman of Marriott International Inc. is Bill Marriott and the Chief Executive Officer is Arne Sorenson. Pre-2016, Marriott was the third largest hotel chain in the world. However, in September 2016, Marriott closed its merger with Starwood (another large company that operated and franchised hotels, resorts and spas), the result of which was the creation of the world's largest hotel company.

Issue → The Breach

Marriott disclosed the information about a data breach on November 30th 2018. In the disclosure, Marriott informs that an investigation on November 19th 2018 revealed unauthorized access to a database which was associated with the storage of information related to guest reservations at Starwood properties on or before September 10th 2018.[2] Marriott also informs of an alert that was triggered on one of the internal security tools regarding access on the Starwood guest reservation database on September 8th 2018. Following this, Marriott held an investigation through its security team, which revealed that there had been unauthorized access to the database since 2014. Marriott realized that the information from the database had been copied by the unauthorized party, who even tried removing the data, but in the end, encrypted it. On November 19th 2018, Marriott was able to decrypt this information and confirm that it belonged to the Starwood guest reservations database.

As of November 30th 2018, Marriott had not finished removing the duplicate entries from the decrypted entries. However, it released the information on the losses, which were as follows - the database contained information from approximately 500 million guests. Approximately 327 million of them had reservation details along with address, phone numbers, emails, passport numbers and Starwood Guest Preference (SGP) numbers. Some of them also contained credit card numbers which were encrypted with AES-128 (128 bits key). The remainder of the 500 million had just names and sometimes addresses and emails.

Marriott continued to work with its internal and external forensics and analytics investigation teams for a few months and updated the figures for the data breach on January 4th 2019. The updated figures were as follows - total number of unique guests with information in the database were approximately 383 million.[3] 5.25 million unencrypted passport numbers were a part of this, along with 20.3 million encrypted passport numbers. Marriott also informs of the possibility of the master key to these encrypted passport numbers being stolen. 8.6 million encrypted payment cards were stolen with 354,000 of them unexpired as of September 2018. Once again, a possibility of the master key being stolen was indicated.

The Diamond Model

This is a model designed for efficient and detailed intrusion analysis. Its main axiom is as follows →

> For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.[4]

The above statement mainly highlights the 4 core features of an event, which are → the adversary, capabilities, infrastructure and the victim. The sections ahead will use the Diamond Model to fit the intrusion analysis for the issue as described in the earlier sections.

Fitting Marriott Data Breach to Diamond Model

This section will elucidate how the Marriott breach fits into the Diamond Model analysis. All the core features will be detailed upon, along with required meta features. The analysis begins with the core feature of Victim and ends with that of the Adversary.

The Victim

The combined set of the 383 million affected guests as well as Marriott must be considered as the victim persona in this incident. The information of the people is being threatened by directing the capabilities of the adversary towards the assets owned by Marriott. Therefore, the victim asset is the Starwood guest reservation database, which happens to contain the passport numbers and payment card information in it.

How the capabilities of the adversary were delivered is still unknown but speculation reveals that the victim susceptibility includes successful phishing and database misconfiguration. The vulnerability associated with the victim asset must be human error or misjudgment to allow a successful phishing campaign and the absence of tokenization or a differential privacy construct to remove PII (personally identifiable information) from the database.[5] How this was exploited will be detailed in the capabilities subsection.

The Infrastructure

Following the speculation of the capability being delivered in the form of a phishing email, it is clear that the infrastructure includes email addresses from a domain visually similar to that used by Marriott or Starwood. Additionally, the IP addresses used for the domain, and the ones from where the emails may have been sent, may be those spoofed to look from around a particular Starwood or Marriott hotel or central branch. The adversary is suspected to be Chinese hackers (detailed under the adversary section ahead), which also points to the possibility of the C2 (command and control) server being situated in China itself.

Since we are dealing with the process of delivering emails, the infrastructure could fall under any one of the 2 categories i.e., Type 1 Infrastructure (controlled by the adversaries internationally) or Type 2 Infrastructure (sent or delivered through a witting or unwitting intermediary). Hacks from wifi within a hotel is believed to be easier as well, which would be a Type 2 infrastructure controlled by Marriott.[7]

Capabilities

The Capability Capacity includes the attributes of the credit card data leak that occurred on Starwood in 2015. Hold security founder, Alex Holden informed about the offers which were being made on the dark web to make use of an SQL injection vulnerability.[6] This too could have been part of an arguably bi-phasic attack on Marriott.

The knowledge that Starwood maintains a central server for storing information on guests (either uncovered during the 2015 hack or via a preparatory phishing campaign) also is a part of the capacity. The details given by the investigators of the Marriott data breach also indicate that the adversaries planned to remove the data from the database, however, ended up encrypting it to avoid being detected by data loss prevention measures. This hints to the fact that the adversaries may have had knowledge of the information security systems maintained by Starwood/Marriott IT team, which would be a part of the capacity.

The investigation launched by Marriott on September 10th 2018 with the help of third party security services firms revealed that a RAT (Remote Access Trojan) had made its way into the systems. They also uncovered activities of MimiKatz (a popular tool for man in the middle and credential snooping attacks).[8] These tools together potentially gave the adversaries control of an administrator account. RATs are generally delivered through phishing emails, which is the reasoning behind the hypothesis of the attack initiating as a phishing attack. Therefore, these tools along with the phishing emails make up the Adversary Arsenal.

With the given set of information, it is hypothesized that the adversaries had the C2 (command and control) server setup either inside a branch office/hotel as a Type 2 infrastructure or in an external facility (possibly international).

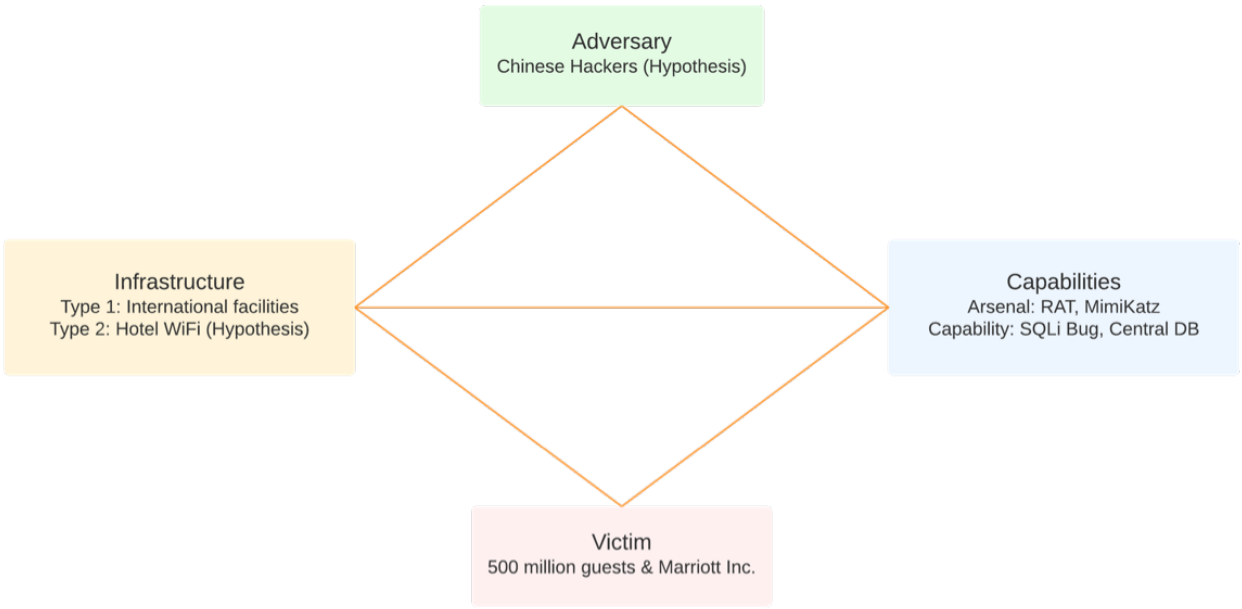
Adversary

Thomas Rid, a political science professor at Johns Hopkins, who specializes in cybersecurity issues, said that hospitality businesses are attractive targets for nation states due to vast databases and proprietary WiFi, etc.[7] A former British Intelligence officer and a cybersecurity expert Matt Tait suspected the attack to be one executed by a nation-state since the access lasted for 4 years without triggering suspicion.[7] Few more experts bolstered the belief that the attack could have been framed by a nation-state. A senior cybersecurity fellow at UT Austin however, believes that nation-states would prefer to silently observe the attacks framed by criminals and take advantage of them without direct involvement with them.[7]

The investigators of the Marriott data breach linked this attack to a Chinese intelligence gathering effort, which is also supposed to be the reason behind hacked health insurers of millions of Americans, and thus accused the Ministry of State Control (a communist controlled Chinese civilian spy agency) to be behind the Marriott breach.[9]

Therefore, the Adversary Operator could be either Chinese intelligence agencies or generic cyber criminals. The Adversary Customers would definitely include the Chinese intelligence agencies as they would benefit from any kind of information like passport numbers, etc. If they were not involved with the attack, then the cyber criminals would also be the adversary customer as they would benefit from selling the information on the dark web or by using the stolen payment records for their own advantage.

The following is a depiction of the analyzed incident as a diamond model figure →



The two Meta-Features associated with the Extended Diamond Model for the event can be elaborated as follows for a better analysis →

Social-Political

As speculated above, the adversaries could be either Chinese intelligence agencies or an external hacker group which may or may not be acting on behalf of the Chinese intelligence agencies (the closest and most believable scenarios that exist for this case).

The intent of the adversary was definitely to gain information to the database of Starwood. The attack seems to be an effort since 4 years, and the result does not make it seem as though the adversary wasn't a persistent one.

Similarly, the victim could also be classified as one of interest if, say the Chinese intelligence agencies were involved in the attack. They could track movements around the globe with the passport numbers, etc. However, it may also seem like the victim was one of opportunity for cyber criminal hacker groups, whose main motive would most probably be earning money through the information gathered or by selling it (this completely ignores the fact that access had been maintained since 4 years).

Technology

This meta-feature briefs on the technologies used. Considering an elaborate phishing plan and persistent remote access malware, the technologies used would be IP, SMTP, TCP for reverse access shells and DNS if DNS poisoning or web hijacking is involved.

Policy Assessment

Given the details about the type of adversaries faced by Marriott and the array of people affected (whose data was stolen), it is quite clear that the problem exists on a global scale. Thus, the problem is best addressed at the transnational level.

Before looking at how the transnational level best addresses this incident, one must gather the details on how the incident is being handled currently. Since the disclosure of the breach, multiple class action lawsuits have been filed against Marriott while emphasizing its failure to maintain required information security practices with regard to Starwood hotels. In addition to that, even Accenture, to which the IT work had been outsourced, was being sued. By March 2019, Marriott incurred a loss of $28 million regarding the breach. However, Marriott was able to cut down its losses to just $1 million because of the cyber-insurance it had. In July 2019, the UK's ICO levied a fine of $130 million for violating British citizens' privacy rights under the GDPR. Other jurisdictions may look to further fine Marriott by blaming its inability to maintain security measures on Starwood's IT infrastructure.[8]

This clearly shows how various governments have their own way of dealing with global businesses on the subject of privacy law violation. Needless to point out, there are a number of affected citizens from different nations who still have no form of compensation for their data loss, except a tool by Marriott (is that trustworthy?). Industry laws will definitely help in dealing with incidents such as these but that does not stop national governments and other entities to enforce their own judgments based on their predefined set of laws. Moreover, most of the time businesses will not have a choice, whether to adhere or not, to such laws. Definitely, even specific national laws do not help because →

- they already exist
- they have boundaries (limited to the matters of a particular nation)

Such incidents are also national threats because all competing nations would be able to procure the data from other countries once it has been stolen. These incidents thus question privacy on a global scale and the way national and industrial governance deal with such incidents is completely unbalanced and unorganized. One form of government might fine amount X with action A and the other, amount Y with action B. Both terms would be based on laws which may or may not be able to justify the costs levied, relative to the number of people who are affected.

Thus, herein lies the need to handle global events like these internationally. Specific laws must be designed which detail how the affected global citizens should be addressed as well as levy a suitable fine on the concerned business or global industry giant. The laws must also define a limit on all kinds of cyber-insurance firms regarding the amount of finances that can be compensated by them for such incidents, so as to provide an incentive for businesses to maintain protective security measures at all times. All cyber-insurance firms, no matter global or industrial, must adhere to these laws, which must also override any existing contracts with the concerned industry actor/business with respect to the incident at hand. This would ensure effective handling of such cybersecurity incidents.

References

1. Wikipedia (Marriott International)
2. Marriott breach disclosure

3. Marriott breach update January 2019
4. The Diamond Model of Intrusion Analysis
5. Marriott CEO hearing, Sen. Rosen
6. Marriott Breach exposure
7. Marriott Data Breach, Washington Post
8. FAQ on Marriott Data Breach
9. Marriott Data Breach traced to China