Marriott Data Breach Case Study

In 2018, multinational hospitality company Marriott International, Inc. announced it had discovered a data breach affecting 500 million in a cyberattack. This number was later revised to less than 383 million. The actual hack, however, occurred in 2014, and was not discovered until four years later. Furthermore, the source of the breach did not lie with Marriott itself but with Marriott's Starwood chain, which was acquired in 2016 and was still using the original Starwood IT infrastructure in 2018. It was discovered that an attacker had placed a remote access trojan (RAT) on Starwood's server with a tool called MimiKatz which could access usernames and passwords stored in memory. As a result, massive amounts of sensitive customer data had been siphoned from Marriott on a regular basis since 2016. A post-mortem investigation later linked the attack to Chinese intelligence looking to gather personal information on millions of Americans, particularly federal employees.

In the aftermath of the announcement of the attack, Marriott came under fire for the breach. Under pressure from the US government, Marriott said it would pay for the passport replacements of those customers affected by the breach. Months later, it announced that over 25 million passport numbers had been compromised, with 5.25 million of those being unencrypted. Later in 2019, Marriott also faced a $123 million GDPR fine from a British regulator. There were also ongoing class action lawsuits filed against Marriott in various jurisdictions for not doing enough to protect customer data [1-5].

Background

Marriott International, Inc. is an American multinational hospitality company that manages and franchises hotels and lodging facilities. Marriott International is the third largest hotel chain in the world. On November 16, 2015, Marriott announced the acquisition of Starwood Hotels and Resorts Worldwide for $13 billion (USD). The Starwood acquisition gave Marriott a larger presence outside of the United States. Approximately 75% of Starwood's revenues were from non-US markets [1-3].

Organizational Policies

While the suspected attacker was a state actor, this suggests that this attack should prompt a policy change at the transnational level. However, policies should be immediately addressed at the organizational level. To start with, Marriott should have thoroughly audited and integrated Starwood's IT infrastructure, at which point they could have discovered the breach. Nevertheless, there are several organizational policies changes a hospitality company like Marriott or Starwood could use to minimize the risk of future attacks. Regular risk assessments and security audits needs to be performed on Marriott's IT infrastructure. This would include tracking how and where customer data is stored, how it is accessed and by whom, what weaknesses and points of attack may be present, and knowing the risks of a potential data breach.

As will be discussed later in the Diamond Model analysis, the initial breach on Starwood's server is suspected to have been due to a phishing attack or database misconfiguration. Organizations can implement policies such as training staff to identify potentially malicious emails, whitelisting websites to avoid employees accidentally accessing malicious websites, and implementing strict application control

to prevent systems from running malware. As Marriott and Starwood have to deal with millions of guests' sensitive data, implementing a zero trust framework for their IT infrastructure would also significantly reduce their vulnerability to an attack. As opposed to the traditional approach of trusting anyone inside the company network and nobody outside the network, a zero trust framework does not trust anyone even inside the company until verified [6].

Marriott should have a clear policy on how it deals with data breaches and inform the public accordingly. In the case of this data breach, public pressure came before Marriott offered to pay to replace the passports of the victims. Furthermore, multinational organizations need to consider the laws and regulations in each jurisdiction, especially now that Marriott faces multiple class action lawsuits.

The Diamond Model

The following section will use the Diamond Model to analyze the data breach. (Fig. 1 Marriott data breach diamond model).

Its main axiom by definition: Axiom 1, for every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over an infrastructure and against a victim to produce a result. An event defines time-bound activity restricted to a specific phase where an adversary, requiring external resources, uses a capability and methodology over some infrastructure against a victim with a given result. The core features of an event are: adversary, capability, infrastructure, and victim. [7]. This report will use the Diamond Model for the Marriott breach analysis beginning with the core features.

1. Adversary

According to an investigation of the data breach, Chinese intelligence agencies working on behalf of China's Ministry of State Security were responsible for the attack, and would therefore be the adversary operators in this analysis. The Chinese government, the adversary customer, would benefit in a myriad of ways. First of all, it was revealed that this attack was part of a larger intelligence/counterintelligence operation to gain access to information on US government employees. Since the data breach included passport data, Chinese intelligence could use it to cross-reference a database of known US federal employees and track when and where they cross borders. They could also use it to identify Chinese nationals who had stayed at the same hotels at the same time as those Americans, which would be useful for counterintelligence. Lastly, by collecting such large amounts of data on American nationals, they could use it for future cyberattacks or intelligence operations on specific targets.

Social-Political

The intent of the adversary was undoubtedly to gain information from the Starwood database. As the attack continued over a period of some years it is evident that the adversary was persistent in his efforts.

With the information, the adversary had at least 2 possible ways to use the stolen data. Interest in the victims could be maintained. For example, their movements could be tracked around the globe by their passport numbers. Yet, it seems more likely that the adversary saw their victims as an opportunity in that they could sell their information to others.

Technology

If it was an elaborate phishing scheme and remote access that was used, the technologies used were likely IP, SMTP, TCP for remote access shells, and DNS if web hijacking was involved.

2. Capabilities

Capability capacity includes the attributes of the data breach. Starwood maintained a central server for storing information on guests and this formed a part of the capacity. The investigation revealed that the adversaries planned to remove the data from the database but ended up encrypting it to avoid being detected by any loss prevention measures. They also had the capacity to plant malware, in this case a trojan, undetected in order to to gain remote access to the server. The adversaries may have also had insider knowledge of the security systems used by Starwood and if so, this would also form part of the capacity.

3. The Victim

The victims were the hundreds of millions of affected guests of the Starwood hotel chain, although the primary target is suspected to be US government employees. The adversary directed efforts to breach the network of the hotel chain and threatened the personal data of the guests. The victim asset is the reservation database which contained passport numbers and payment information, and the suspected goal of the attack was to specifically build a database of American government targets.

It is not fully understood how the capabilities of the adversary were delivered. Victim susceptibility has been considered as a potential method. It is suspected that the adversaries used phishing and database misconfiguration.

4. The Infrastructure

Continuing the possibility of phishing as the method used, the infrastructure included email addresses that were similar to those used by Marriott or Starwood. Alternatively, IP addresses may have been spoofed to appear as coming from a Marriott or Starwood hotel.

Infrastructure could be placed under two categories: Type 1 Infrastructure was controlled by the adversaries. Type 2 Infrastructure was sent or delivered through an intermediary.

An investigation revealed that a RAT (Remote Access Trojan) was present on Marriott's systems. MimiKatz (a tool for man-in-the-middle attacks) had also been used at some point. These tools could

have given the adversaries control of an administrator account. These tools and any phishing emails comprise the Adversary Arsenal [8-11].

It is believed that the adversaries had the C2 (command and control) server set up as a Type 2 infrastructure in a hotel or at an external location.

Policy Assessment

It is obvious from the investigation of the adversary in the Marriott data breach that the issue is global in scope. First, the alleged adversary in this attack was one or more people from a foreign country who were perhaps working on behalf of their government. Second, with the internet, "borders" of countries are more easily crossed and these kinds of incidents are not limited by borders.

The issue can be addressed, to some extent, at the transnational level. At the present time, various governments have their own way of dealing with data breaches. Some have extensive laws in his regard, while others have little legislation addressing these situations and offer little to no compensation for those affected by data theft. Specific international laws could address how events like these are handled and how victims are compensated. This could help in handling cybersecurity incidents if the participating nations are on the same page with regard to cybersecurity.

Yet, for laws to be effective, they must be enforceable. This requires all participating parties to agree on laws and enforce specific punishments on transgressors and provide just compensation to victims. Since there are obvious conflicts of interest that exist between nations and countries, it is not realistic to fully implement such an arrangement. This situation is further complicated by the fact that, at least in this specific incident, the suspected adversary was working, at least in part, on behalf of a government. Can governments participate in cybersecurity breaches and at the same time police such activities?

Many would say that security issues should be handled at an organizational level. This confronts the problem at the basic level and encourages companies and organizations to employ best practices regarding security. Companies or organizations entrusted with personal data are viewed by the public as being responsible for the protection of that data. National or international laws can provide a framework for compliance and enforcement but individuals and companies must take the initiative to implement frameworks and practices conducive to effective cybersecurity.

Companies must employ a solid cybersecurity defense: They must regularly monitor their networks and systems for any potential breaches and take corrective action. Prior to this they need to maintain an up-to-date secure environment which fosters safe and secure data storage and transmission. Also, they must accept responsibility for the data security in any mergers and acquisitions they may make. Finally, they can assume that their systems could be compromised at any time and act accordingly.

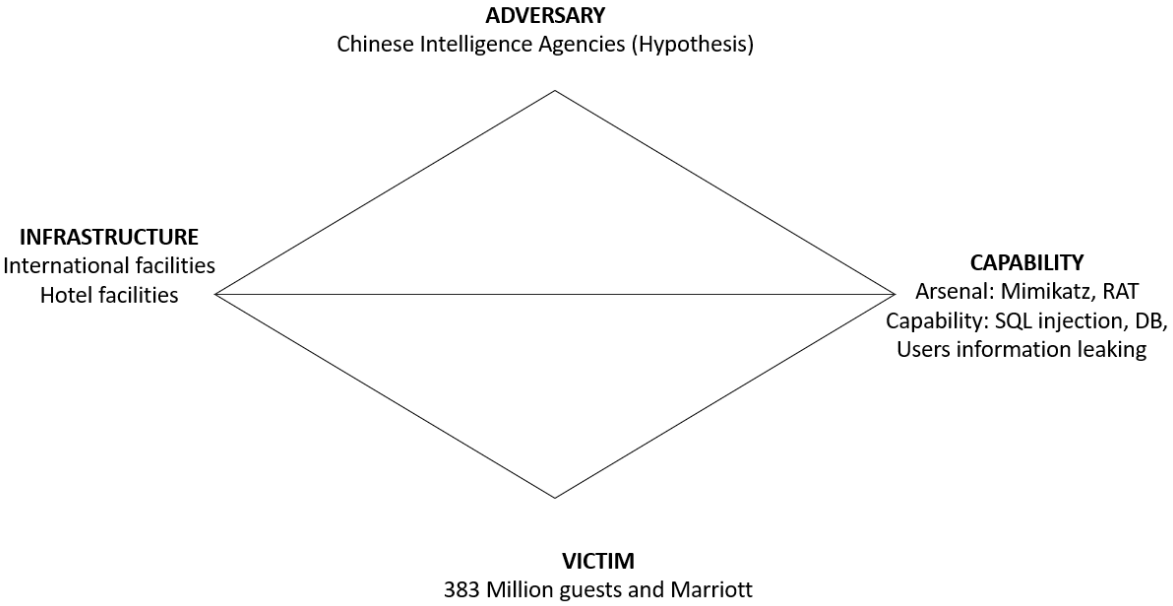

Fig. 1 Marriott data breach diamond model

References:

[1] Sperance, C., Sperance, C., Schaal, D., & Skift. (2019, December 23). What Have Hotels Done on Cybersecurity Since the Marriott Hack? Retrieved from https://webcache.googleusercontent.com/search?q=cache:J7joLXAdy8oJ:https://skift.com/2019/12/24/what-have-hotels-done-on-cybersecurity-since-the-marriott-hack/+&cd=1&hl=en&ct=clnk&gl=ca

[2] Cybersecurity Threats in the Hotel and Hospitality Industry: ThreatModeler. (2020, February 6). Retrieved from https://threatmodeler.com/cybersecurity-threats-in-hotel-and-hospitality-industry/

[3] Social Tables. (2020, March 11). Hotel Data: 5 Strategies to Safeguard Customer Data. Retrieved from https://www.socialtables.com/blog/hospitality-technology/hotel-data/

[4]Brewster, T. (2018, December 3). Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches. Retrieved from https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#49cf6194546f

[5]Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018, December 11). Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. Retrieved from https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

[6] Pratt, M. K. (2018, January 16). What is Zero Trust? A model for more effective security. Retrieved from https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

[7] Caltagirone, S., & Pendergast, A. (n.d.). The Diamond Model of Intrusion Analysis. Retrieved from https://apps.dtic.mil/docs/citations/ADA586960

[8]Mest, E. (2019, January 4). Marriott revises number of impacted guests in Starwood hack. Retrieved from https://www.hotelmanagement.net/operate/marriott-revises-number-impacted-guests-starwood-hack

[9] O'Flaherty, K. (2019, July 10). Marriott Faces $123 Million Fine For 2018 Mega-Breach. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#3a50f55d4525

[10] Pratt, M. K. (2018, January 16). What is Zero Trust? A model for more effective security. Retrieved from https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

[11] Steven Cohen February 25. (2020, February 25). Marriott Data Breach Class Action Allowed To Proceed. Retrieved from https://topclassactions.com/lawsuit-settlements/data-breach/marriott-data-breach-class-action-allowed-to-proceed/