Alexander Semaan
IA 5010

Marriott Data Breach Analysis

1. Source, Detection and Background

On November 30 2018, Marriott International declared to the public that a data breach had occurred, affecting no less than 500 million of their guests, which constitutes most if not all of their guests.

Effectively, it was on September 8 of 2018 that Marriott received an alert from its internal security countermeasures. Incidence Response and Network Forensics were able to conclude on September 10 that there was an attempt to gain unauthorized access to Starwood's guest reservation database.

After realizing the magnitude of the situation, Marriott rapidly acquired the help of leading security experts in the hopes of accurately determining what occurred. After deep log analysis, it was apparent that the Starwood network, that is now part of Marriott's operations, was infected with malware. It was only then that the malware started copying and successfully encrypted some of its database.

No earlier than November 19, Marriott's Incidence Response team and security experts were able to decrypt the data, and realized that it was Starwood guests' data and sensitive account information, which were located in Starwood's guest reservation database.

To get some additional background information, this breach is linked back to November 2015, when Marriott International declared a bid for Starwood Hotels and Resorts Worldwide at 12.2 billion U.S. dollars. Nevertheless, on March 3 of 2016, a consortium led by Chinese corporation Anbang Insurance Group, weighed in on the deal and offered Starwood 14 billion U.S dollars. As it should, this shifted Starwood's focus towards a deal with the Chinese group, up until Marriott raised its bid on March 21.

Later that year, in September of 2016, the deal was sealed after a long battle with Anbang Insurance Group for a whopping 13.6 billion U.S dollars, and the merging process accelerated efficiently. Their mission with this merger was to grow the company in order to compete with Google, Amazon and other web companies, that use their consumer preference knowledge to facilitate primacy with their clients. Unfortunately, Starwood's systems were infected by malware since July 2014, which set the company back a couple of blocks.

It was only in November of 2015, right after the talks of Marriott purchasing Starwood, that the Committee Chairman came forth with the news revealing that malware was found in Starwood's systems.

2. Quantity and Type of Data Breached

The hotel brands and properties owned by Starwood that were equally affected, being a part of the Starwood Alliance are The Westin, Sheraton, Le Méridien, W Hotels, St. Regis, Four Points, Aloft, Tribute, Design Hotels, Element and The Luxury Collection. After the merger, Marriott operated over 30 hotel brands internationally.

Allegedly, when the malware was first discovered in November 2015, its sole purpose was to exfiltrate credit card information, and was not used to steal any of Starwood guests' personal and identity information. The threat was believed to be dealt with, and wiped off the Starwood network by their Incidence Response team.

However, it is now clear that the malware persisted through the sweep and the countermeasures, and came right back around to bite out a large chunk of Marriott's guests' personal information. The stolen information of 383 million unique guests includes names,

phone numbers, addresses, email addresses, passport numbers, Starwood Preferred Guest account information (Loyalty Program), dates of birth, gender, arrival and departure information.

For some guests, their credit card information was also stolen; although encrypted by AES-128, Incidence Response and security consultants were not able to determine whether the keys needed to decrypt them were stolen as well. However, it is certain that 5.2 million unencrypted passport numbers were snarfed by the hackers.

In addition to that, many clients and loyalty program members complained that they were not able to use their rewards and loyalty program benefits, because they could not access them, or because they were not available. Today, this became clear that the attackers were able to steal these clients' credentials and use their loyalty points and rewards at their expense.

Regarding the remaining 120 million guests, their related stolen data is limited to only names, and in some instances address and email address, "or other information", as stated by Marriott's President and CEO Arne Sorenson; that is definitely not a great sign.

3. Response, Recovery and Notification

After all, the data breach had been ongoing for over 4 years before getting detected, which demonstrates the lack of care and seriousness that Marriott's security experts and their management attribute to the safety of their clients' data. Marriott's board should have definitely payed more attention to their network's security and perhaps allocated a larger budget to Security Risk Management. That would have allowed their security team or

security consultants to provide Marriott's systems with better controls, better log management and more accurate malware detection sensors, or IPSs.

The age of the malware and the initial exploitation dates back to July 2014. The network was vaccinated, and the malware completely bleached on November 19 2018, marking 52 months of undetected malicious activity in the Starwood network. Marriott immediately involved Law Enforcement, when they detected the breach in September.

The recovery process started right when the malware was detected, on September 8 2018. Incidence Response and Network Forensics were able to conclude on September 10 that there was an attempt to gain unauthorized access to Starwood's guest reservation database. On November 30 of 2018, Marriott International's CEO and President, Arne Sorenson declared the breach to the public, and sent out an email to all of Marriott's client base, discussing details of the incident, and apologizing for the incident. The president's response to the breach also specified what recovery measures were put in place, to remediate from this breach. The president also explained how Marriott's team is cooperating with Law Enforcement to improve security, secure the data and potentially track down the hackers.

Marriott put up dedicated call centers and guest support to deal with any issues related to the breach, and any problems Starwood Loyalty Members were facing.

4. Privacy and Legal Impacts

Though the legal impact that Marriott has suffered due to the breach may not be as immense as one would think; this only seems to be the case in the United States. Marriott does business internationally and its acquisition of Starwood increased its international exposure

since 75% of Starwood's revenue is internationally acquired. The GDPR regulation that was implemented in Europe implicates a massive legal disruption to Marriott on that side of the globe. This impacts Marriott through several angles:

- The fees and impacts of the law itself in Europe
- Negative publicity worldwide (greater in Europe)
- Potential for the federal U.S government to mimic the GDPR regulations and potentially relay those back to the Marriott case

The U.S has already seen some forms of legal mimicking and a push toward stricter regulations across the cyber security world. In California, the Consumer Privacy Act was passed resulting in data breach fees ranging from $2,500-$7,500 per violation.

5. Related Incidents and Breach Consequences

Marriott International's reputation was tainted in result of this data breach scandal. Its stock prices dipped from $120/share on November 30, when the breach was declared, to $100/share on December 24. However, since January its stock recovered and is currently back up to $135/share.

Up till March 1st, Marriott has had to pay 28 million U.S dollars' worth of damages to clients, 25 million of which were paid off by their insurance. However, many lawsuits are still ongoing and could potentially make Marriott pay a hefty price. It is still unclear when these lawsuits will start settling.

Relationship with the Chinese was affected as the breach was traced back to the Chinese government. The evidence behind it is not definitive and perhaps not clear enough, however the US government is justifying the Chinese's involvement because of the bidding

war between Anbang Insurance Group and Marriott International over Starwood's acquisition.

6. Proposed Guidance

Regarding Incidence Response and Forensics, I believe their methodology was effective, as they have prioritized stopping the breach and the exfiltration of data, against attempting to track down the perpetrators.

I would suggest increasing marketing campaigns to restore consumer confidence in Marriott and its hotel brands. I would also add benefits and attempt to restore previous loyalty point balances, for those who claim their points were stolen.

7. Preventative Controls

For Marriott to have prevented a breach like this, they should have implemented more sophisticated IPSs, to start with. They should have powerful and regular database and network scans for malware, viruses and potential threats. They should have a larger budget allocated to Risk Analysis and countermeasures. Although, from the looks of it Marriott is not doing bad so far. It is still too early to tell what the damages might total to, since many lawsuits are still ongoing.

References

https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

https://www.databreaches.net/marriott-ceo-apologizes-for-data-breach-unsure-if-china-responsible/

https://www.databreaches.net/marriott-breach-has-already-cost-tens-of-million/

https://www.databreaches.net/marriott-says-less-than-383-million-guests-impacted-by-breach-not-500-million/

https://www.forbes.com/sites/geoffwhitmore/2018/04/18/details-surrounding-the-marriott-starwood-merger/#718ce0895c07

https://www.nytimes.com/2015/11/17/business/marriott-to-buy-starwood-hotels.html

https://www.insurancejournal.com/news/national/2018/12/03/510811.htm

https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers

https://blog.domaintools.com/2018/12/the-monday-media-wrap-up-marriott-breach-crowdstrike-report-and-android-malware/

https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

https://www.synack.com/blog/the-marriott-breach-implications-consequences-accountability/