A Cyber Security Data -Breach: The Marriott International Hotel Incidence

Lawal Olumide Olayinka
Department of Cybersecurity and Digital Forensics
University of East London
drolumidelawal@gmail.com:
+2348168480721

ABSTRACT

This paper takes a deep dive into the data breach of March 2020, interestingly 2 years earlier there had been a breach which must have warned Marriott international about the importance of managing the security of their digital assets and also positioning the security operations center in a defensive operational position so as to limit data exposure of the organizations and their very many clients. The breach ultimately was the result of a security logon password compromised by two employees through what would later be seen to be targeted social engineering attacks at one of the franchise locations of the Marriot international. This led to threat actors gaining entry to details and information of over 5.2 million guests an equivalence of almost 20 gigabytes of data being downloaded from the Airport BWI Airport Marriott Maryland allegedly including credit card details and other forms of proprietary information, and personally identifiable information (PII) on flight crews booked to stay at the property (*Latest Marriott Data Breach Not as Serious as Others | Computer Weekly*, n.d.). Looking back, there has been several instances of cybersecurity breach linked to this business enterprise and so much can be learnt from examining the circumstances around this most recent event (The Marriott's data breach 2020). The actions, inactions, countermeasures the organization must have taken to avoid this unfortunate incidence would be discussed also technical circumstances surrounding the attack. Threat actors and the indication of compromise on the information security system detailing the level of compromise and exposure of customer confidential information and what the organization did to prevent the spread on the dark web.

Keywords: Breaches, data, Privacy, Cyber Crime, Cyber Security, Marriot, Incidence

CISDI Journal Reference Format
Lawal Olumide Olayinka (2024): A Cyber Security Data -Breach: The Marriott International Hotel Incidence. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 15 No 4, Pp 25-28.
Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V15N1P4

1. BACKGROUND TO THE STUDY

According to investigations conducted by the company, the compromised data included contact details such as Contact details, loyalty account information, additional personal details (e.g., company, gender, birthday day and month), partnerships and affiliations (e.g., linked airline loyalty programs and numbers) and stay and language preferences of some 5.2 million guests have been compromised (Zorz, 2020) As a containment and security management measure Marriott's has placed all its international customers on a phishing alert (warning them not to fall for any further request of information from any individuals of persons who might need to obtain more information

to be able to make use of the vital information that probably has been gathered from the initial data heist) and strict warning to change their Marriott Bonvoy (loyalty program) account password, and has warned them about the possibility that the compromised information may be used by criminals to "phish" additional sensitive information from them.

This insight was shared and raised as threat warnings from security experts monitoring the situation. While this particular attack was not considered as particularly rewarding for threat actor as were attacks from previous years' warnings and advisories campaigns on the need to actively sensitize victims on possible aftermaths of this initial attack as travel patterns, preferences as to choice of accommodation, travel itinerary and some other peculiar information might be dangerous intelligence readily available to potential adversaries. The Marriott's data breach of 2020 would most likely affect the business space, as much of the stolen data is expected to be recirculated, making possible more criminal activity against other businesses in form of credit card fraud, identity theft, and so many other possible data breaches. Importantly the cyber community must step up security awareness against exposed data employed to sponsor successful attack in the future

2. INCIDENT ANALYSIS

According to information from tech blog wired more than 5.2 members of the bon Marriott Bonvoy loyalty program may have had their personal information stolen. According to Marriott announced that it had once again been hit, with up to 5.2 million guests at risk. Considering the last breach, the organization might as well be relieved on the level of exposure of few clients as opposed to the mega millions, they experienced two years ago. As reported(Arghire, 2022) Marriott International reported a case of social engineering attack used to exploit the vulnerability(a staff of the organization) through which access to organization non-sensitive internal business files. These files it was revealed are related to the day- to-day operation of the property organization.

The attack was primarily a social engineering attack (this is a type of attack which targets individual with valuable credentials useful to access restricted resources based on authentication or encryption). Social engineering has proven to be a potent tool for cybercriminals, they understand that an organization's people are its mot exploitable vulnerability which is why they would most likely exploit this technique over and over again. Phishing a type of social engineering attack was confirmed as the social engineering tool used to obtain the logon information from the employees of Marriot international after which they went ahead to steal download 20 gigabyte of data which is estimated at the information of 5.2 million clients of a package Marriot international its clients (Marriott Bonvoy loyalty program).

The severity of this attack I must admit was not a successful theft of data downloaded from the database in this organization but the use to which the attackers might possibly put the data. According to cybersecurity experts these attackers, a group of hackers active for roughly five years, claim to have stolen 20 gigabytes of files from a server belonging to Marriott international. Arguments and technical analysis according to (Editor et al., 2022) the attack on this particular organization is not as disturbing as the knowledge of the vulnerability status of the organization, its common knowledge, that victims of previous cyberattacks are more likely to be targeted in the future. Also 5 years' operational credit to this group of attackers suggest we might be dealing with experienced professionals most likely interested in financial reward therefore an extended exploit is high possibility.

3. DISCUSSION OF FINDINGS

Approaching severity from the business angle, clients most especially people of class and stature profiled to majorly be customers of this luxury lodging enterprise could be said to be discreet and extremely cautious with their confidential information, while some don't even want to be seen as customers of the hospitality origination based on "clandestine" and adventurous escapades, it is very likely such persons look for a more data secured hotel rather than fall victim of blackmail and extortion leading to be boycott of the services of the lodging company by trusted clients leading to reduced revenue and also shareholders and investors would be cautious with investments. This leads to more business decline which is totally unacceptable to business growth. The details of this latest hack seem to be not quite as devastating as the last one, too, given that sensitive information like passport numbers doesn't seem to be affected. Still, that a major company could get hit twice in such a relatively short time frame underscores how at-risk your data is and how not enough is being done to protect it.

- The threat actors were a group of unknown cyber security enthusiast's according to them they had stayed away from public eye and had no business with government, they contacted management of Marriott international notifying them on a successful intrusion of database holding sensitive customer information like names, driver's license, credit card information and preferences form the loyalty program of the hotel. They requested ransomware which the organization was unable to meet the financial demand of the group which made them download about 20 gig data. Intentions and action path after the download of this data wasn't
  known, but experts think this might be connected to a plan for further attack on the business or an attempt for the hackers to target individuals whose information they have in their possession.
- An indicator of compromise is digital evidence that an attack has already occurred. In the case of Marriott's International, it was largely reported management of the hotel put out a statement confirming the attack with promises to reach out to affected users and setting up support channels for enquiries and technical Information also digital evidence confirming attack has occurred was the purported shutting down of accounts through which the intrusion was made possible was said to have been immediately disabled according (Lyngaas, 2020). A further reveled Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers," were some of the information not affected during the data breach
- The element of security that was compromised in the Marriot International Data breach of 2020 was confidentiality. The breach started out from the disclosure of very confidential information which was vital to the security of information systems of the hotel this was the vulnerability that was exploited and data of 5.2 million users downloaded from the information system.
- The vulnerability exploited was human resources the two employees of the organization has shared hey privileged logon unknowingly with threat actors unknowingly who went ahead to download customer information from the information system of the hotel.
- Action taken by the hotel administration was to immediately shit down the accounts through which posed vulnerability to the hotels network hereby making sure to contain further exploits.

4. LESSONS LEARNED

There were different versions of the Marriot attack of 2020. Most information research and analysis most times confused the attacks of 2018 with that 2020 while all these attacks looked quite similar and threat actor had similar operations pattern notable lessons are as follows

1. Marriott international did little to Invest in information security awareness education for their staff, this led to a data breach as a result of social engineering
2. Marriott's international had no concrete security programs for its operations, they relied on security programs existing on the various merger companies they acquired which in itself had vulnerabilities. There a need to hire security professionals to Develop a security plan and integrate all operations. There's need to understand the business flow and develop a
3. Marriott's international had little proactive plans for potential breaches hence had little or no response for breaches to such something catastrophic happens.
4. Marriott's international did not prioritize security investments and they probably put a cap on budget, not knowing they stood good chances of looing much more on fines and litigation in the face of an imminent attack.

5. CONCLUSION

Looking back at the series of attack Marriott International have experiences dating back to 2014 and the attack patterns, information security processes and procedures might be aid not to have been improved upon although the Marriott attack of 2020 shows limited exposure, information security guidelines does not entertain any form of breach or loss figure as potential improvement index of performance (*Marriott Hotel Data Breach Affects 5.2 Million People*, 2020). Which made the Britain information commissioner's office issue a 91-page penalty notice comprised of some of the following

- Insufficient monitoring of privileged accounts and Insufficient monitoring of databases.
- Poor controls for critical systems and Insufficient encryption.
- Reliance on software security protocols rather than personalized management of private data.

REFERENCES

1. Arghire, I. (2022, July 7). *Marriott Confirms Small-Scale Data Breach*. SecurityWeek. https://www.securityweek.com/marriott-confirms-small-scale-data- breach/
2. Editor, B. B., July 06, D. R., & 2022. (2022, July 6). *Marriott Data Breach Exposes PII, Credit Cards*. Dark Reading. https://www.darkreading.com/attacks- breaches/marriott-data-breach-pii-credit-cards
3. *Marriott Hotel Data Breach Affects 5.2 Million People*. (2020, November 11). IDStrong. https://www.idstrong.com/sentinel/marriott-hotel-data-breaches-and-the- aftermath/
4. Zorz, Z. (2020, April 1). Marriott International 2020 data breach: 5.2 million customers affected. *Help Net Security*. https://www.helpnetsecurity.com/2020/04/01/marriott-data-breach-2020///thepointsguy.com/news/marriott-data-breach-march-2020/
5. https://dataprivacymanager.net/new-marriott-breach-2020-what-is-going-on/
6. https://en.wikipedia.org/wiki/Marriott_International
7. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html