Case Study
Marriott Data Breach

Denise Devine, Dylan Webb, Gary Sheppard, Taylor Moorman

Marriott Data Breach Introduction

- Marriott - Marriott is a global hospitality corporation that manages over 6500 hotels and lodging facilities. They operate in 127 countries and boasted a revenue of over $22 billion in 2017
- Starwood - Starwood is a subsidiary of Marriott, with over 1200 properties and a revenue surpassing $6 billion in 2013. Acquired by Marriott in 2016 for $13.6 billion creating the world's largest hotel chain
- Attackers - The identity of the attackers is unconfirmed, though speculation from investigators is they were hackers associated with the Chinese Ministry of State Security

Marriott Data Breach Introduction

- Marriott International released a statement that there was unauthorized access to the Starwood guest reservation database
- It is estimated 500 million people had their information leaked from this security breach, 327 million of which had their passport number exposed along with their personal information
- Encrypted payment information has additionally been leaked for some guests, and the keys needed to decrypt it could also have been taken by the attackers

Marriott Data Breach Introduction

- Marriott released details on the attack in late 2018, disclosing the potential impact and addressing next steps for those affected
- Internal investigations revealed the infiltration had been instigated as early as 2014, remaining unresolved for four years
- Data breach was found in guest reservation database of Starwood, Marriott's subsidiary
- Likely a relational database containing customer data in structured format, with potential that access was through a commandeered service account that leaked information undetected

Marriott Data Breach Introduction

- The attackers stand to gain in multiple ways from stealing information on Marriott's customers; they are likely able to commit identity theft if they managed to decrypt payment card data
- Stolen credentials and personal data can be sold illegally to scammers and phishers
- Speculation that China was behind attacks could lead to conclusion that a profile is being built on important Americans that stayed with Starwood including military personnel, politicians, and executives

Timeline

- Starwood's malware credit card breach started as early as November 2014 in some locations, ending sometime in April or May for all affected hotels.
- Starwood's security experts missed the subsequently discovered separate hack from September 2014.
- Starwood had a separate malware-driven credit card data breach that it announced in October 2015, it claimed at the time that it checked and found that hackers hadn't compromised its core guest reservation systems.
- November 2015 – Marriott announces plan to acquire Starwood Hotels and Resorts
- September 2016 – Marriott acquisition of Starwood Hotels & Resorts was finalized

Timeline

- September 8, 2018
  Marriott receives an alert that a hacker attempted to break into the Starwood guest reservation database
- September 10, 2018
  Data from customers who booked stays at Starwood hotels on or before this date was stolen
- November 19, 2018
  Marriott confirms that a data breach had taken place
- November 30, 2018
  Marriott informs customers around the world of the breach

Speculation of how

- How this data breach could occur and be undetected for 4 years is an interesting question.
- Specific facts have not been released so we can only speculate as to how the hacker was able to extract the customer data.

Speculation Scenario

- For large Hospitality entities, it's typical for POS data and the Customer's stay data to be kept locally.
- Typically a nightly process ETL process is used to send various data points to centralized corporate servers.
- The subsequent data mining exploit discovered in November 2018 would seem to indicate that that the core Reservation system was most likely compromised in the prior malware attach in 2014.

Scenario con't.

- The data breach was only discovered when Marriott was trying to integrate the rewards program from Starwood with Marriotts reward program. This would indicate that they were working on a RDBMS platform.
- For enterprises as large as the Marriott and Starwood this would point to either Oracle or SQL as their Database system.
- For the purpose of this Scenario, Microsoft's SQL will be the RDBMS used.

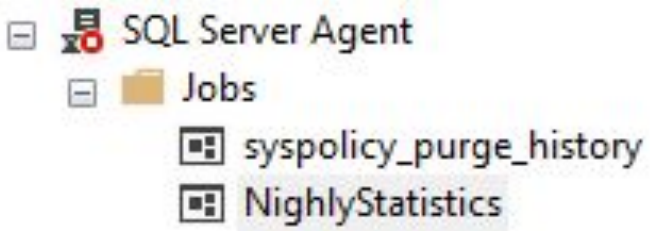
Scenario Con't.

- SQL uses default port number 1433 and uses 1434 for the SQL Monitor.
- Using a port scan against the port number would provide the servername and IP Address.
- Using wireshark and TDS.Query, the hacker could find a simple query and utilizing a tool like **Ettercap** to capture the query and modify it.
- Query captured: **Use mydatabase; Select * from mydatabase.dbo.mymoneytable;**
- Query changed: `CREATE LOGIN myhackeruser WITH PASSWORD='YouGotHacked1#';`
- Submit the query back into the wireshark stream for port 1433
- This has now created a SQL Login called "myhackeruser".
- Using the same process I can then go and change the security for "myhackeruser" to the same as "SA"
- The query to give higher authority is: `ALTER SERVER ROLE sysadmin ADD MEMBER myhackeruser;`
- We now have an authorized user with credentials

Scenario Con't.

- To continue the data exploit from the database, the hacker now has a login to the RDBMS and can go in and create a Job.
- This Job would run a query that could extract the data and put in a location for the hacker to pick up.
- The following image shows how easily this can be done.

Scenario Con't.



- If someone was looking for malicious code - all they would see is a Job named "NightlyStatistics".
- Inside this job a query has been created that selects data from a selected table. This data could be inserted into a file, another table or some other form.
- A company that employs several DBA's would not think to look at new Jobs, especially if this was a Data Warehouse where there could be hundreds of ETL processes.

Scenario Con't.

- A hacker could have gotten a service account, a local SQL account, a network login account.
- This type of low level data mining could easily be overlooked due to the size of the corporation.
- When you have a large environment, you don't typically have separate server accounts, every server used the same basic logins.

Potential Ramifications

- Actions Taken by Marriott
  - Informational website set up
  - 12 months free cyber security monitoring services
  - Offered compensation for passport replacement
- Current Lawsuits
  - Two different class-action lawsuits have been filed, covering hundreds of guests
- GDPR Concerns
  - First data breach of this magnitude to happen under new GDPR legislation in EU
  - Sanctions could be up to $915 million (4% of annual revenue)
- SEC Prosecution
  - If Marriott is found to have known about breach, U.S. Government could seek prosecution

Lessons learned

- Routine compliance testing was not done or too narrow in scope
  - supposed to happen every three years
- Cyber security auditing should be a part of every M&A
- Lack of effective Cloud monitoring tools
  - being able to monitor traffic in and out and actions of users
- Improper Storage of Encryption Keys
  - stored in easily accessed area

"Your cyber team needs to be successful 100% of the time. A hacker only needs to be successful once."

References

- Cook, J. (2018, November 30). Private data of 500 million Marriott guests exposed in massive breach. Retrieved February 19, 2019, from https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/
- Krebs, B. (2018, November 20). Marriott: Data on 500 Million Guests Stolen in 4-Year Breach. Retrieved February 19, 2019, from https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/
- Marriott International. (2019, February 15). Starwood Guest Reservation Database Security Incident. Retrieved February 19, 2019, from https://answers.kroll.com/
- Nakashima, E., & Timberg, C. (2018, December 12). No hacked Marriott data has posted on 'dark web' — one clue China may have been behind breach, experts say. Retrieved February 19, 2019, from https://www.chicagotribune.com/business/ct-biz-marriott-china-starwood-data-breach-20181212-story.html

References

- Cameron, D. (2019, January 12). Marriott Faces Massive Class-Action Lawsuit Over Hotel Data Breach. Retrieved February 21, 2019, from https://gizmodo.com/marriott-faces-massive-class-action-lawsuit-over-hotel-1831686560
- Melancon, K. (2018, December 12). 4 Big Security Lessons from the Marriott Starwood Data Breach. Retrieved February 21, 2019, from https://deltarisk.com/blog/4-big-security-lessons-from-the-marriott-starwood-data-breach/
- Mouratidis, Y. (2019, January 13). GDPR May Add Up To $915M Marriott's Data Breach Expenses. Retrieved February 21, 2019, from https://www.forbes.com/sites/yiannismouratidis/2019/01/09/gdpr-may-add-up-to-8-8b-marriotts-data-breach-expenses/#4486e94f62e1
- Whitmore, G. (2018, December 19). Steps To Take If The Marriott Data Breach Affected You. Retrieved February 21, 2019, from https://www.forbes.com/sites/geoffwhitmore/2018/12/19/steps-to-take-if-the-marriott-data-breach-affected-you/#6b461aa92c58
- Wyman, O. (n.d.). The Marriott Data Breach. Retrieved February 20, 2019, from https://www.oliverwyman.com/our-expertise/insights/2018/dec/the-marriott-data-breach.html

References

- Osgood, Rick Hacking Microsoft SQL Server Without a Password Retrieved 2/25/2019 https://www.anitian.com/hacking-microsoft-sql-server-without-a-password
- Marriott Announces Starwood Guest Reservation Database Security Incident. (2018, November 30). Retrieved February 15, 2019, from http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
- Gressin, S. (2018, December 4). The Marriott data breach. Retrieved February 19, 2019, from https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach