The September 2018 Marriot Data Breach

Marriot Data Breach – 2018

Company Description

Attack Category & Description

Timeline

Vulnerabilities

Costs

Prevention

Company Description

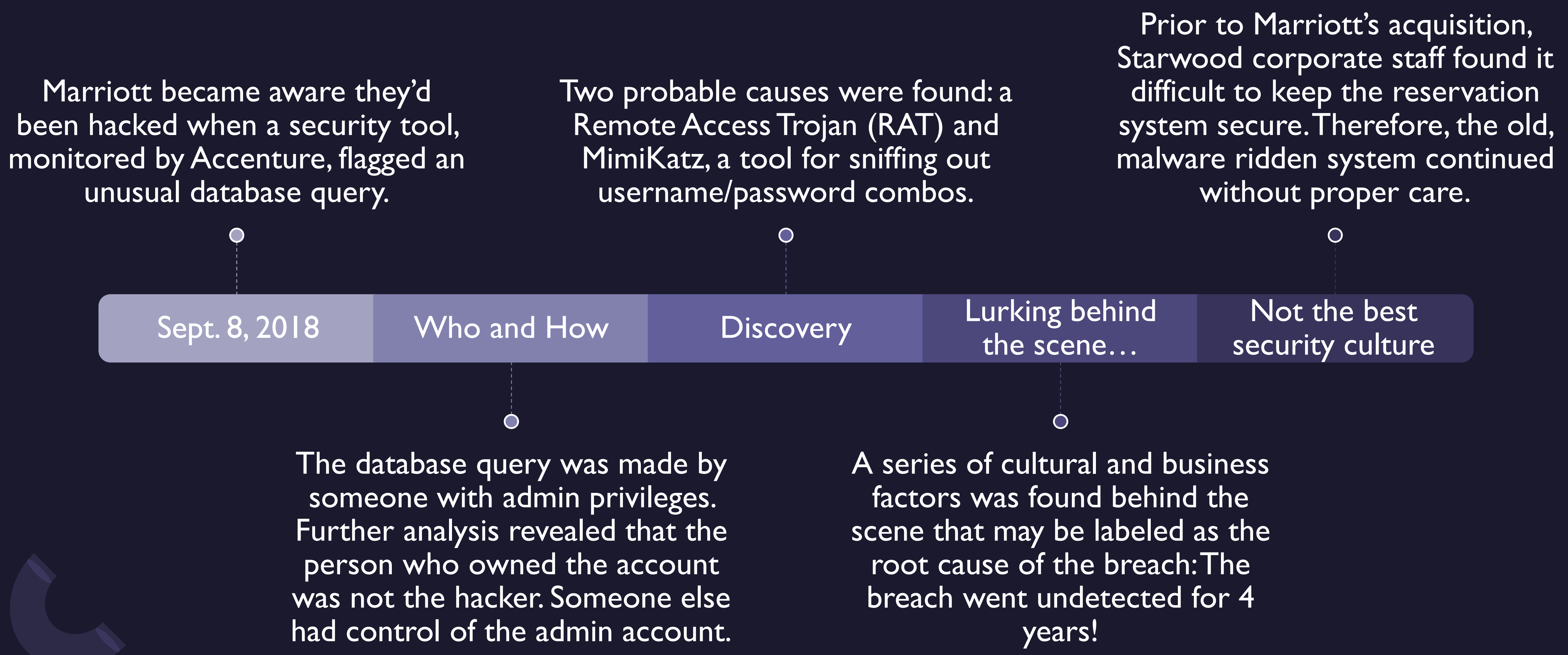
- Marriot International has over 8000 properties across 139 countries and territories giving people more ways to travel, experience, and expand their world. It was founded in 1927 and are guided by their strong principles to this day. Taking care of people's well being is their most precious asset. (marriot.com)

Attack Category and Description

- Marriot purchased the Starwood in 2016 after the Starwood network was compromised in 2014.
- The Starwood hotels had not been migrated to Marriott's own reservation system and were still using an IT infrastructure from Starwood.
- On September 8, 2018, an attempt to access the internal guest reservation database for Marriott's Starwood brands was flagged by an internal security tool as suspicious.
- This prompted an internal forensics investigation which determined that because of the prior 2014 compromise the attackers had been able to encrypt the data, probably through a phishing email, and tried to remove the data from the Marriott/Starwood systems.
- Phishing attacks are usually successful because people aren't as vigilant about ensuring email and webpages are real and links get clicked without knowledge of whether they're real or not.
- The U.S. Intelligence service was involved in the investigation because of the sensitive nature of the attack and the fact that the hackers were employed by Chinese intelligence services.

https://www.csoonline.com

Timeline



Sept. 8, 2018

Marriott became aware they'd been hacked when a security tool, monitored by Accenture, flagged an unusual database query.

Who and How

The database query was made by someone with admin privileges. Further analysis revealed that the person who owned the account was not the hacker. Someone else had control of the admin account.

Discovery

Two probable causes were found: a Remote Access Trojan (RAT) and MimiKatz, a tool for sniffing out username/password combos.

Lurking behind the scene…

A series of cultural and business factors was found behind the scene that may be labeled as the root cause of the breach: The breach went undetected for 4 years!

Not the best security culture

Prior to Marriott's acquisition, Starwood corporate staff found it difficult to keep the reservation system secure. Therefore, the old, malware ridden system continued without proper care.

https://www.csoonline.com

Vulnerabilities

- While it's not clear how the RAT was placed onto the Starwood server in the first place, it's reasonable to assume that do to the lax security culture, it was done via a phishing email.

- Even though the Starwood corporate staff, IT management, and IT security were laid off, Marriott was in no position to install its own reservation system. They continued business as usual for 2 more years with the compromised Starwood systems.

- While most credit card numbers were stored in encrypted form, most of them were saved in clear text on the server.

- The encryption keys for the encrypted credit card numbers were stored on the same server.

- Marriott's integration of Starwood's IT systems was a risk as was its global reservation systems.

https://www.csoonline.com

Costs

- Marriott incurred $28 million in expenses related to the breach as of March 2019.
- Cybersecurity liability insurance covered most of the initial costs associated with the breach, lowering the company's losses to only $1 million.
- Marriott has not compensated any of its customers whose data was stolen because it seems that there was no threat of the stolen data being used for fraud.
- The company did say that it would pay the replacement cost (s) for a passport with a new number and/or cover credit card fraud expenses if these do occur.
- Multiple class action lawsuits have been filed and Marriott's failure to perform due diligence has been specifically singled out in court documents.
- ZDNet said that the direct/indirect costs for Marriott will be caused by customers shying away from the company in the future and they could see billions of dollars in lost revenue as a result of the breach.

https://www.csoonline.com and
https://www.ZDNet.com

Prevention

- Follow the most important cybersecurity rule: assume you ARE compromised and ACT accordingly!
- Keep all data encrypted and keep the encryption keys separate from the data. In this case, the data was encrypted using the AES-128 which is inline with the PCI-DSS and the FIPS-197, but because the encryption key wasn't stored properly or protected correctly, it didn't matter what protection was in place.
- The incoming database(s) should have been vetted and tested prior to the merger.
- Have compliance requirements in place where you must pass a security assessment at least every 3 years through a third-party vendor. Done properly, vulnerabilities would've been uncovered or there would've been indications of a compromise.
- Prevent unmonitored Cloud access by having two-factor authentication in place and monitoring who's logging into the network, from where, and what or how much data is transferred or accessed.

https://www.csoonline.com and https://www.deltarisk.com

Thank You for your time and attention.

Leigh Dudenhoeffer

2021 – 2022 Cybersecurity Student at IBM and IBM’s Security Learning Academy