Inherited Responsibility

Marriott/Starwood Data Breach Analysis

May 27, 2020

Tyler McAfee, Vince Plaza, David Primrose,
Beth Rettig, Matthew Sutherland

- For 92 years, Marriot has been in the business of serving people. They started as a small family business in Washington DC serving burgers and sodas and have grown to a global hospitality company. They have operations in all 50 states and 130 countries.

- Founded in 1969, Starwood Hotels was one of the largest companies that owned, operated, franchised and managed hotels, resorts, and vacation ownership properties. In 2016, Starwood was acquired by Marriot International.
- Starwood Guest Reservation Database was used to conduct business operations for 1,297 properties which included 370,000 hotel rooms in approximately 100 countries.

Background – Marriott International

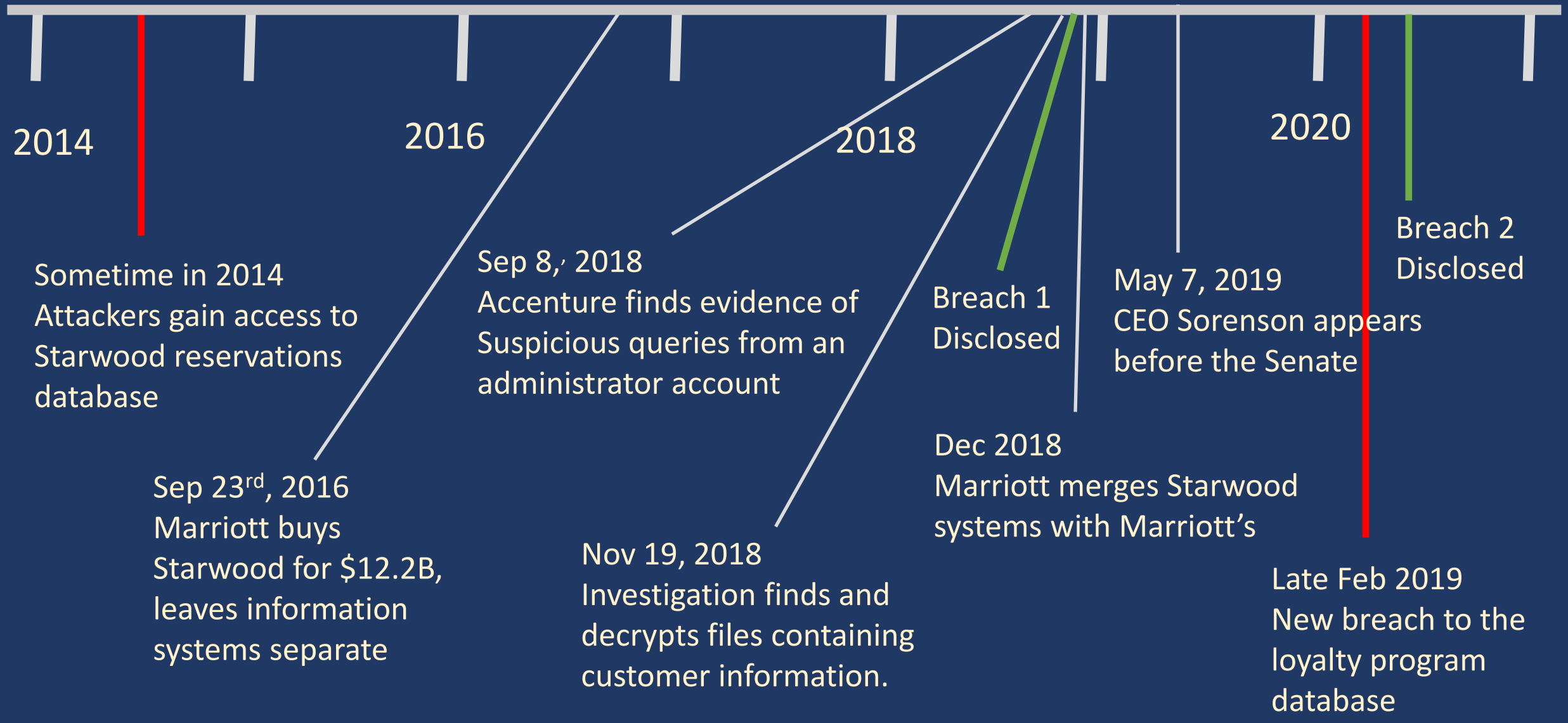
- Before Starwood's acquisition, Marriot had maintained good security of their customer's data. Marriot’s databases were comprised of information including payment data (encrypted with AES-128), names, mailing addresses, phone numbers, email addresses and passport numbers.
  - Once Starwood had merged with Marriot, Marriot obtained all of Starwood’s network and technology information. It was decided that Marriot’s database system would be used as the central system for the combined group of hotels – Starwood’s system would be retired in due time.

Background – Starwood Hotels and Resorts

- Starwood didn't have the same track record as Marriot. Just days after the company announced its acquisition by Marriot International, they disclosed some credit card breach investigations.
  - Impacting roughly 50 hotel properties, cyber thieves had installed malware on point-of-sale cash registers to steal credit card information.
  - These point-of-sale data breaches lasted for about 6 months - from Nov 2014 until May 2015. Starwood's President at the time, Sergio Rivera announced to customers " We have no indication at this time that our guest reservation or Starwood Preferred Guest membership systems were impacted."

- When Marriot bought Starwood, they intended to migrate all of Starwood's systems to Marriot's central system early on.
- To avoid any disruption to the ongoing reservation process for customers, migration of the company systems would take time (roughly 2 years),
- Important to invest in the people interacting with the systems: “You can have the best security tools money can buy, but if you don’t invest equally in the people interacting with the technology, then you’re making a costly mistake.” (Tom Callahan, Director of MDR Services, ControlScan)

Timeline – Marriott Breaches and Responses



Breach One – Three Steps

1. **Remote Access Trojan (RAT)**
   Allows an intruder to take control of a system for other malicious activity

2. **mimikatz**
   A tool for discovering usernames and passwords in computer memory

3. **Customer Data Theft**
   Credentials stolen in step 2 used to access company databases

Step One – Remote Access Trojan (RAT)

What is a RAT?

- A malicious program that remotely accesses infected resources
- According to Kaspersky Lab, a RAT is the most dangerous type of trojan
- Requires a host program for installation

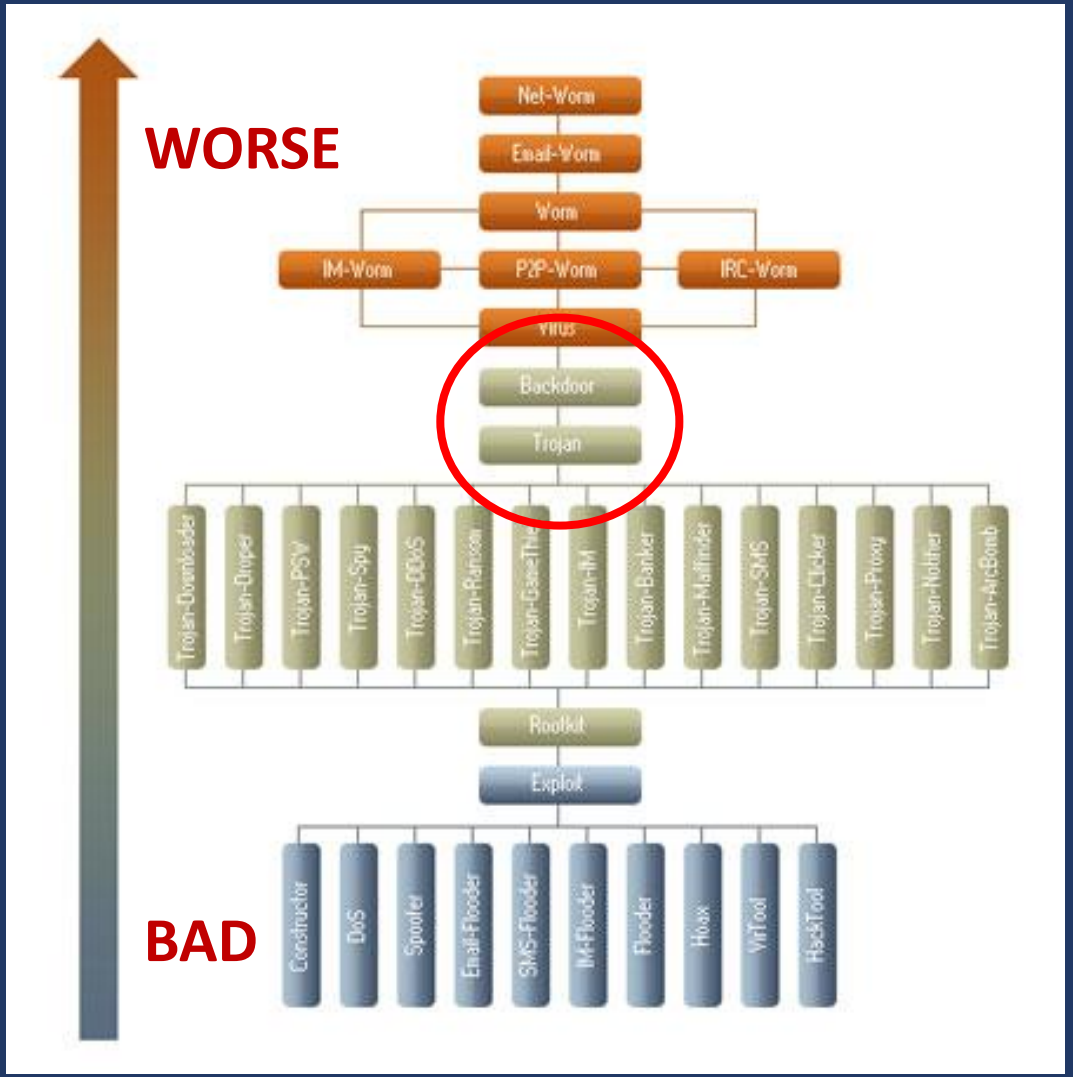


Image Source: Kaspersky Lab

Step One – Remote Access Trojan (RAT)

How do trojans get installed?

- Attached to benign programs and files
- Users introduce the trojan by
  - clicking on email links
  - inserting portable storage media
  - installing host software from an untrustworthy source
- Once installed, hard to find and remove

Step Two – mimikatz

What is mimikatz?

- “Mimikatz is a credential dumping open source program used to obtain account login and password information, normally in the form of a hash or a clear text password, from an operating system or software." Source: Double Octopus Wiki

mimikatz author, Benjamin Delpy

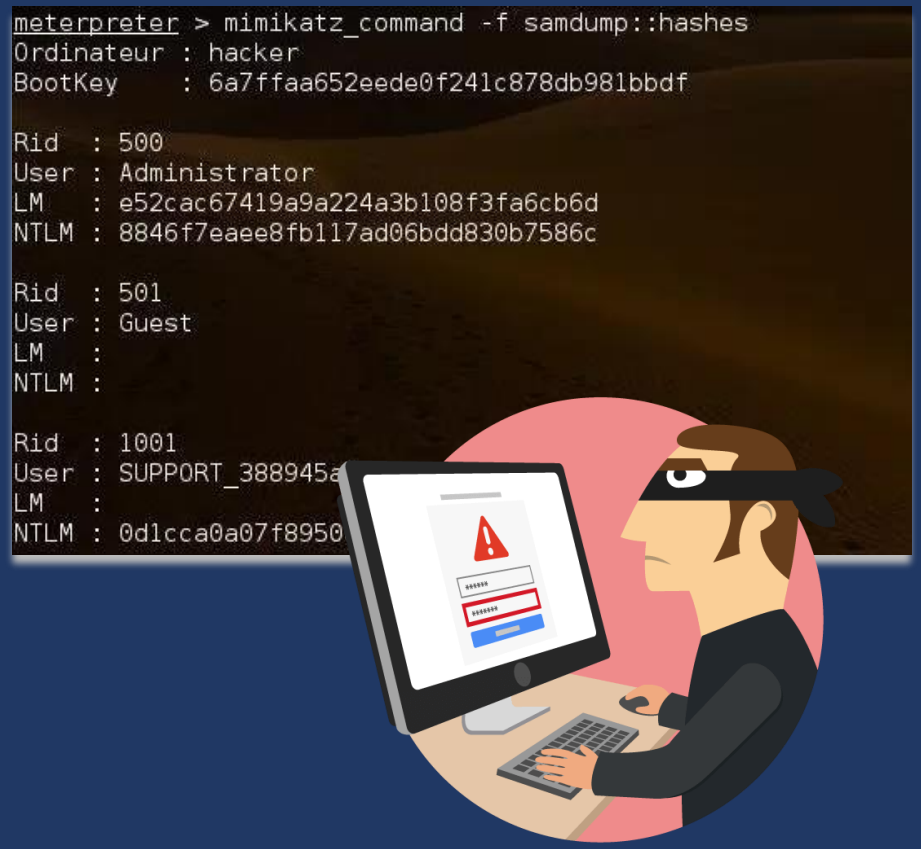
```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Apr 26 2014 00:25:11)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  14 modules * * */
```

Step Two – mimikatz

- mimikatz (cute cats) was written by Benjamin Delpy in 2007 as a way to practice C programming

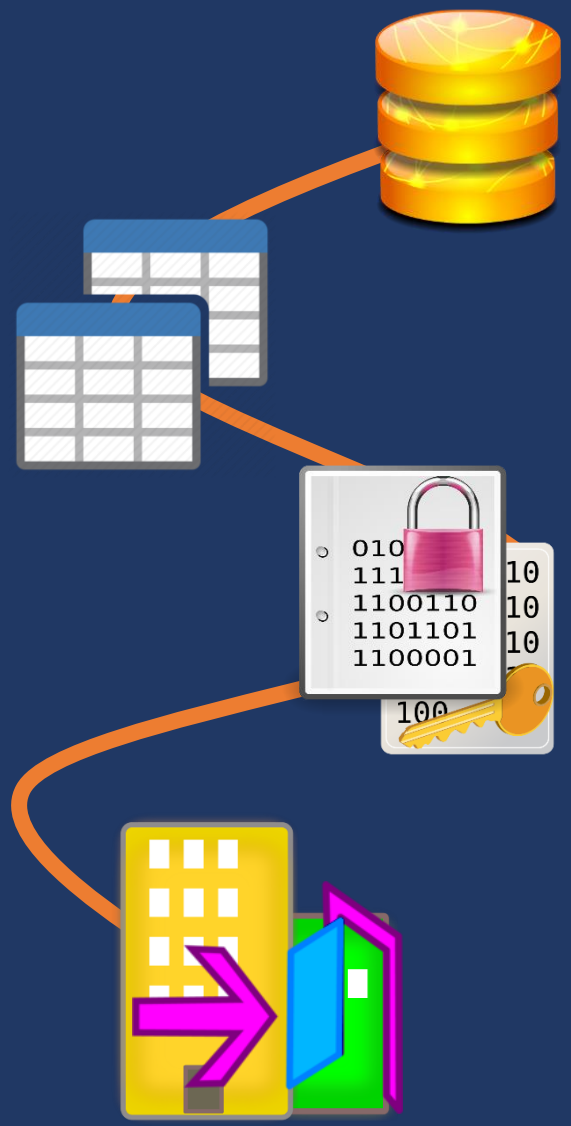
- It is available to download from GitHub AND
- It is widely used as a part of an attack
  - BadRabbit (Ukraine)
  - Russian Hack of German Parliament
  - Angela hacking E Corp on Mr. Robot

- https://github.com/gentilkiwi/mimikatz



Step Three – Data Theft!

- Tables were copied from the reservations database
- The copies were converted to encrypted files
- The encrypted files were exported off-site and then removed from the system… except for the two files that were found during the investigation
- The data theft could not have occurred but for the success of the first two steps in the attack



Breach Two – Franchise Property Data Theft

- Attackers gained access to a franchise property system that was used to provide guest services
- Credential of two employees were used in the breach
- The attack was recent, so many details are unavailable
- At the center of both breaches was theft of passwords

How was the data breach detected?

- September 8, 2018
  - An internal security tool flagged suspicious attempt to access the internal guest registration database.

  - Unusual database query identified
    - Accenture's security monitoring tool
    - Human operator makes specific type of database query by hand.
      - Such queries are considered dangerous and unusual.

Accenture

- Database Monitoring Tool
  - IBM Guardium

- Guardium Alert
  - Triggered by a query from an administrators account to return the count of rows from a table in the database.

  - Remote Access Trojan (RAT) found on September 10th

Events trigger critical security alerts

- Events -> Security Alert
  - Alert prompts an internal investigation

  - Investigation finds that hackers successfully encrypted data and removed it from Starwood systems

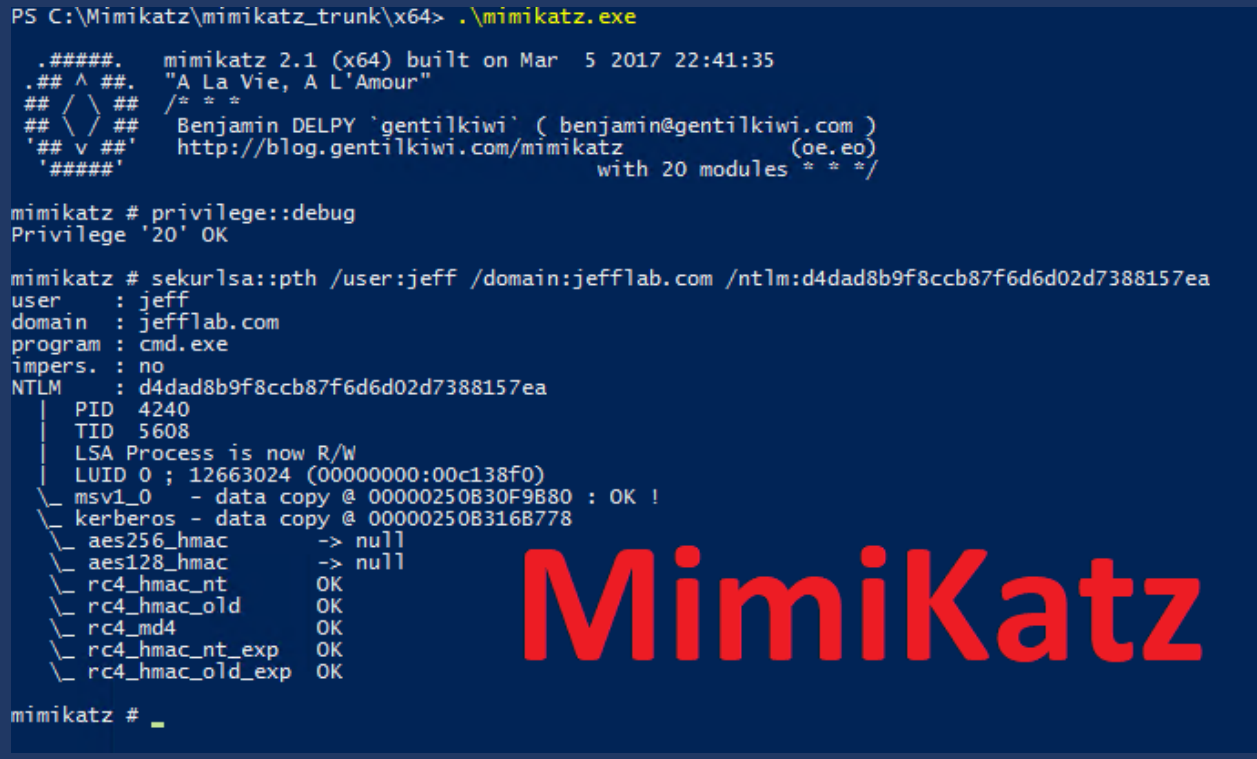
    - Database query was made by someone with admin privileges
      - Admin account is determined to be assigned incorrectly / unassigned and unknown

Traced to Ministry of State Security*

- Often described as a cross between the CIA and FBI
- Responsibilities
  - Counter-Intelligence
  - Foreign Intelligence
  - Domestic Surveillance
  - National Security Intelligence

But wait…there's more.

- RATs + Mimikatz Detected
- Mimikatz
  - A tool used for sniffing out username/password combos
- Used together, Mimikatz and a RAT can give a hacker access to an admin account.

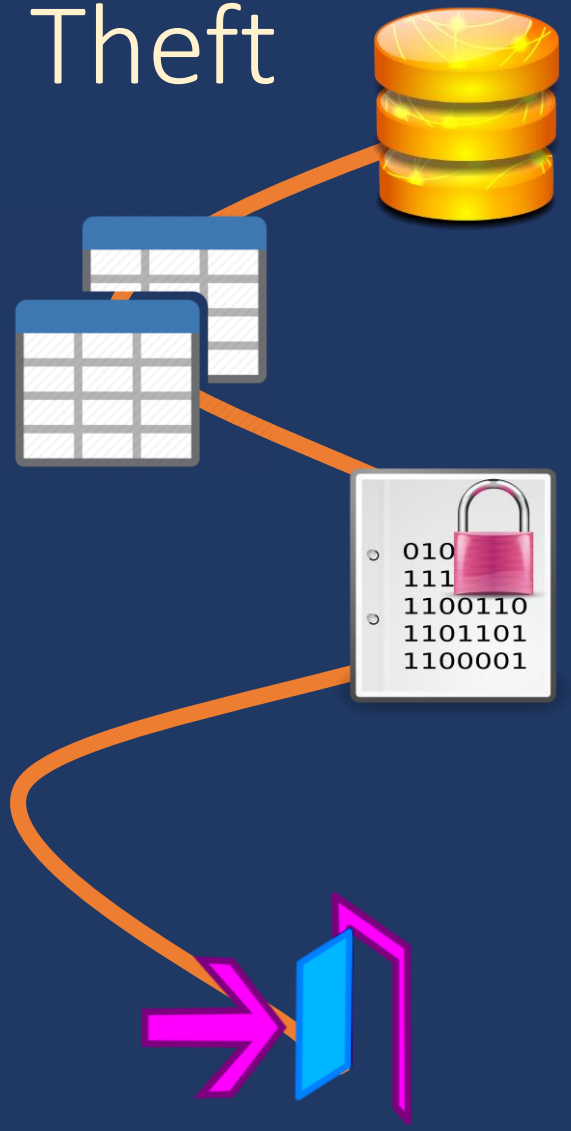


Another data breach?

- When: Disclosed by Marriott International on March 31
- Occurred: Starting mid-January 2020
- Discovered: Late February

- What happened:
  - Login credentials of 2 Marriott employees identified as having accessed guest details

Fallout From Data Breach One- Data Theft

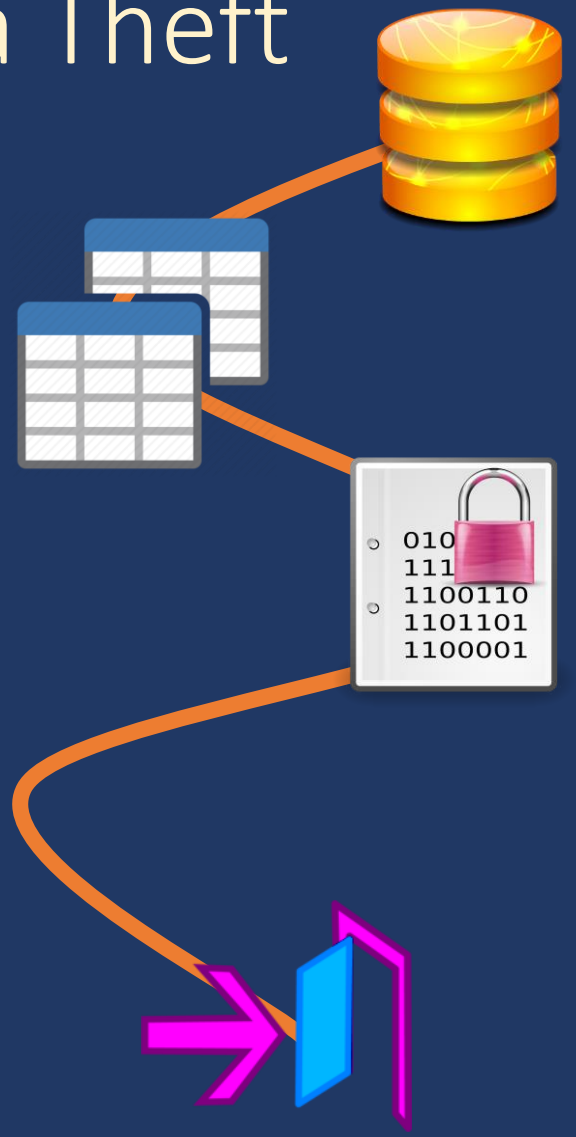


- Upwards of 383 million consumers impacted
- Marriott was hit with a $123 million fine in the EU as a result of the 2018 data breach (0.5% of company's annual revenue).
  *Penalty amount could have been as high as 4.0% of global revenue per EU's rule
- Began the conversation as to what point should merger and acquisition due diligence extend into cybersecurity audit periods

Fallout From Data Breach One- Data Theft

- Millions of ongoing phishing attacks continue to strike unsuspecting customers as a result

- February 2020: Legal proceedings/Class Action Lawsuits approved to move through U.S Federal Court
  - “In total, Marriott allegedly disclosed that the breach impacted at least 383 million guest records, including nearly 24 million passport numbers and more than 9 million credit and debit cards,” the judge’s opinion notes.
  - Marriott did agree to pay for passport replacement.



Financial Fallout From Data Breach One- Data Theft

- First Data Breach had little financial impact on Marriott as a whole
  - May 2019: Breach cost approximately 72 Million
    - 71 Million was collected from insurance to assist with covering costs
  - Company's operating profit down only 1% from year prior
  - 5% increase in earnings per share for stock re-purchase options
  - Revenue was consistent with prior years at 5 Billion

Fallout From Data Breach Two- Franchise Property Data Theft

- *Investigation Ongoing*

- *May* have impacted upwards of 5.2 million customers
  - Breach included names, addresses, birthdays, loyalty information and airline/room preferences
  - Is not believed to include credit card information, passport numbers or drivers license information

- Offered impacted guests free enrollment in personal information monitoring services

Financial Fallout From Data Breach Two- Franchise Property Data Theft

- UK's Information Commissioners Office (ICO) is reassessing Mariotts systems and weighing the possibility of administering additional fines

- Q1 stocks down over 5% (coupled with covid 19 implications)

- Customer loyalty and trust might be shaken

as compared to a relative non-impact after Breach One

Lessons Learned Breach #1

IMPACT: $72,000,000 US (of which $71M covered by insurance), $123,000,000 by UK

Guest payment card information: 9.1 million encrypted payment card numbers and expiration dates

- 385,000 of the cards were valid at time of breach
- Potentially “several thousand” unencrypted card numbers were breached

Guest records: Records of 383 million accounts with Starwood (owned by Marriott) that include:

- Full names
- Drivers License
- Mailing addresses
- Phone numbers
- Email addresses
- Gender
- Rewards information
- Arrival/departure/preferences for rooms & airlines

Passport numbers: 18.5 million encrypted and 5.25 million unencrypted passport numbers of guests

Lessons Learned Breach #1

Security Culture – 50% increase in investment; ecosystem awareness
Consistent Security Policy – + PCI DSS certification respect
Data: - a revenue asset, not just an expense

- ❑ Data Collection – what, when, where, why?
- ❑ Data Protection – how (encryption, tokenization, digitization)
- ❑ Data Retention – storage policy, time-based expiration
- ❑ Data Response – faster and with customer focus and notification

M&A Security Due Diligence – this was a missed signal
Security Audits – avoids having to go back through 4 years of trail
Insurance – saved Marriott – try to keep it- super expensive now!
Security Inventory – learned from Equifax – find it, know it, have it handy
Best Practice Review – signals from multiple parties (Financial Services)
Focused Enhanced Security Measures

- ❑ Defense in Depth – multiple tools at each level; IP whitelisting
- ❑ Encryption – verify it work; keep Keys separate
- ❑ Network Segmentation
- ❑ Tokenization
- ❑ Less centralization – smaller target; encrypted at each location
- ❑ Endpoint security – applied to 270,000 devices

References

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

Marriott CEO Testimony Before Congress, March 7, 2020
https://www.hsgac.senate.gov/templates/watch.cfm?id=ED7AA8F1-5056-A066-6067-80CD2EC5A6C3
https://www.hsgac.senate.gov/imo/media/doc/Soresnson%20Testimony.pdf

Forbes
https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#2621a0cc155c

InfoSec Institute:
https://resources.infosecinstitute.com/lessons-learned-the-marriott-breach/#gref

Marriott:
https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

ZDNet
https://www.zdnet.com/article/marriott-discloses-new-data-breach-impacting-5-2-million-hotel-guests/

References

"Mimikatz," Offensive Security. Accessed May 1, 2020. https://www.offensive-security.com/metasploit-unleashed/Mimikatz/

Gressin, Seena, "The Marriott data breach," Federal Trade Commission, Dec 4, 2018. https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

Zorz, Selijka, "Marriott CEO reveals more details about the massive data breach," Help Net Security, Mar 12, 2019. https://www.helpnetsecurity.com/2019/03/12/marriott-data-breach-details/

"How does a computer get infected with a virus or spyware," ComputerHope, accessed May 9, 2020. https://www.computerhope.com/issues/ch001045.htm

"Types of Malware," Kaspersky Lab, accessed May 9, 2020. https://usa.kaspersky.com/resource-center/threats/types-of-malware

"Remote Access Trojan," Kaspersky Lab, accessed May 9, 2020. https://encyclopedia.kaspersky.com/glossary/remote-access-trojan-rat/

"Marriot Suffers New Data Breach," Security Magazine, Apr 1, 2020. https://www.securitymagazine.com/articles/92030-marriott-suffers-new-data-breach

"Metasploit's mimikatz Module," **Hackers Arise**, accessed May 10, 2020. https://www.hackers-arise.com/mimikatz

References

"Marriott buys Starwood, becoming world's largest hotel chain", CNBC.com, Sep 23, 2016. https://www.cnbc.com/2016/09/23/marriott-buys-starwood-becoming-worlds-largest-hotel-chain.html

Tunggal, Abi Tyas, "22 Types of Malware and How to Recognize Them", UpGuard, Oct 3, 2019. https://www.upguard.com/blog/types-of-malware

"Marriott International Notifies Guests of Property System Incident," Marriott International, Mar 31, 2020. https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident/

Delpy, Benjamin,"mimikatz," GitHub, accessed May 10, 2020. https://github.com/gentilkiwi/mimikatz

"Mr. Robot Hacks: How Angela Stole Her Boss' Password Using mimikatz," Hackers Arise, Oct 1, 2016. https://www.hackers-arise.com/post/2016/09/13/mr-robot-hacks-how-angela-stole-her-bosss-password-using-mimikatz

Greenberg, Andy, "New Ransomware Linked to NotPetya Sweeps Russia and Ukraine," Wired, Oct 24, 2017. https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/

Greenberg, Andy, "He Perfected a Password-Hacking Tool – Then the Russians Came Calling," Wired, Nov 9, 2017. https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

Poston, Howard, “Top 5 Remote Access Trojans,” Infosec Institute, accessed May 26, 2020. https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/post-exploitation-techniques/

Thank You!

Tyler McAfee, Vince Plaza, David Primrose,
Beth Rettig, Matthew Sutherland