2019 Capital One Data Breach

By Jared Anderson, Pranav Dhakal, Matthew Hunderup, Arman Parastaran and Luis Pol

Capital One

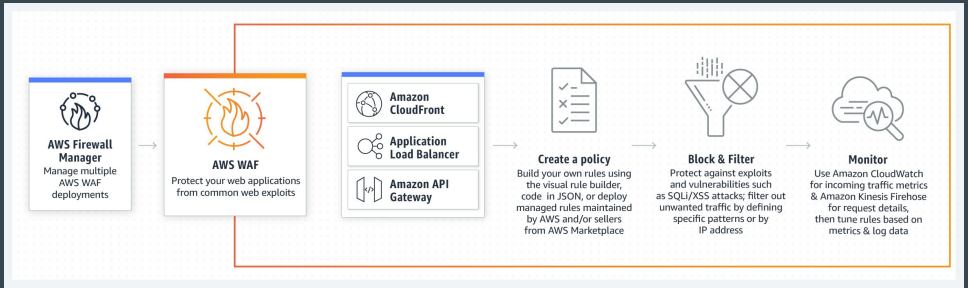
- Largest online bank in the world
- Second largest auto finance company in the U.S
- 50,000 employees
  - 12,000 technology employees
- Shifting from a bank to a technology company
  - New technologies such as Eno Web Assistant and Virtual Credit Card Numbers extension
- $28 billion in revenue in 2019

Data Breach

- On March 22nd and 23rd, 2019 an outside hacker, Paige Thompson, gained access to credit card applications filled through Capital One from 2005 to 2019
- Through an internal security review Capital One discovered the breach on July 19th
- 100 million total people affected
- 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers and 80,000 bank account numbers were stolen
- Names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income were also stolen
- Thompson was caught soon after the breach, as she was bragging about it on her personal GitHub, Slack and other social media
- According to FBI none of this data has been used for fraud yet, and Thompson has been apprehended

How it Happened

- Former employee at Amazon Web Services gained access to a server holding customer information for Capital One
- Server access via a Firewall “misconfiguration” on webApp
- Other tools used:
  - TOR browser, GitHub, IPredator(VPN)



Aftermath

- 106M Personal Data, 140K Social Security Numbers, 800 Bank Account Numbers
- Office of the Comptroller of the Currency - Verdict
  - Capital one “failed to effectively assess risks in advance of its migration of information technology operations to the cloud.”
- Capital One reaches an $80M dollar settlement
  - Did not admit or deny allegations
  - Indicated that they fixed the vulnerability
- Paige Thompson indicted for wire fraud and computer fraud/abuse
  - Could face up to 25 years in federal prison
  - Pleading not guilty
  - Currently staying in halfway house while awaiting trial

2017 Equifax Breach

- Apache Software foundation announced a vulnerability and released a patch
- Equifax did not update their systems
- Hackers were able to gain access in weeks
- Used encrypted channels to stay hidden
- 145 million Social Security numbers stored in plaintext SQL tables
- Failed to use safe modern practices

Discussion

Should large companies be allowed to store such valuable customer data?

Should there be stricter regulations on these companies with how they store data?

How should we prevent these type of attack in the future?

Bibliography

https://www.capitalone.com/facts2019/

https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

https://www.americanbanker.com/news/capital-one-to-pay-80m-in-connection-with-massive-data-breach

https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

https://krebsonsecurity.com/tag/capital-one-breach/

https://www.bankinfosecurity.com/alleged-capital-one-hacker-released-from-prison-a-13364#:~:text=Thompson%20has%20been%20released%20from,2020%2C%20according%20to%20court%20documents.&text=If%20convicted%20on%20both%20counts,25%20years%20in%20federal%20prison.

https://www.washingtonpost.com/context/capital-one-breach-u-s-v-paige-thompson-aka-erratic/2361bb41-302d-43a1-a96f-9eeefcc24c70/