THE UNIVERSITY OF WINNIPEG

ACS-2821-001

Information Security in Business

Equifax Data Breach Post Mortem

DISCOVER • ACHIEVE • BELONG

Equifax Data Breach Post Mortem

- U.S. Government Accountability Office released a report on the Equifax breach titled "Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,"
- Detailing how the breach occurred in that **76 day** slowly exfiltrated data from **51 databases**
- All of which Equifax could have prevented or move rapidly to mitigate it
- It center on failing detect, segmentation and data governance
- The five key factors that contributed to the breach:
  - Identification
  - Detection
  - Segmentation
  - Data governance
  - Failure to rate-limit database requests

Problem 1: Ineffective Identification

- U.S. Computer Emergency Readiness Team in March 2017 issued an alert that all Apache Struts implementations should be immediately patched
- Equifax circulated this notice to its systems administrators, but the recipient list for the notice was out of date
- So not all individuals receiving the notice would have been responsible for installing the necessary patch
- In additional, routine scan conducted a week later, that looks for known vulnerabilities inside its network failed to flag the flaw in the Struts implementation that ran its online dispute portal

Problem 2: Poor Detection

- A security device that inspect network traffic, was not working because a digital certificate it required had expired 10 months before the breach occurred
- Encrypted traffic was not inspected throughout the breach had occurred
- Resulting the attacker was able to run commands and remove stolen data over an encrypted connection without being detected

Problem 3: No Segmentation

- Failed to isolate its databases on different network segments
- This lack of segmentation allowed attackers to gain access to additional databases that contain Personal Identifiable Information
- Together with the security device with the expired certificate, it allowed the attackers to successfully remove large amounts of PII without triggering an alarm

Equifax Data Breach Post Mortem

Problem 4: Poor Data Governance

- Equifax stored administrators’ access credentials in an unencrypted format
- The attackers gained access to a database that contained unencrypted credentials for access to additional databases with usernames and passwords
- This enabling the intruders to run queries on client databases
- With proper practice these credentials should only be stored in a secure form and with access restricted using multifactor authentication

Problem 5: No Query Limits

- There were no restrictions in place on database queries.
- The attacker was able to execute approximately 9,000 such queries - many more than would be needed for normal operations
- These queries result contain PII and was exfiltrated without detection

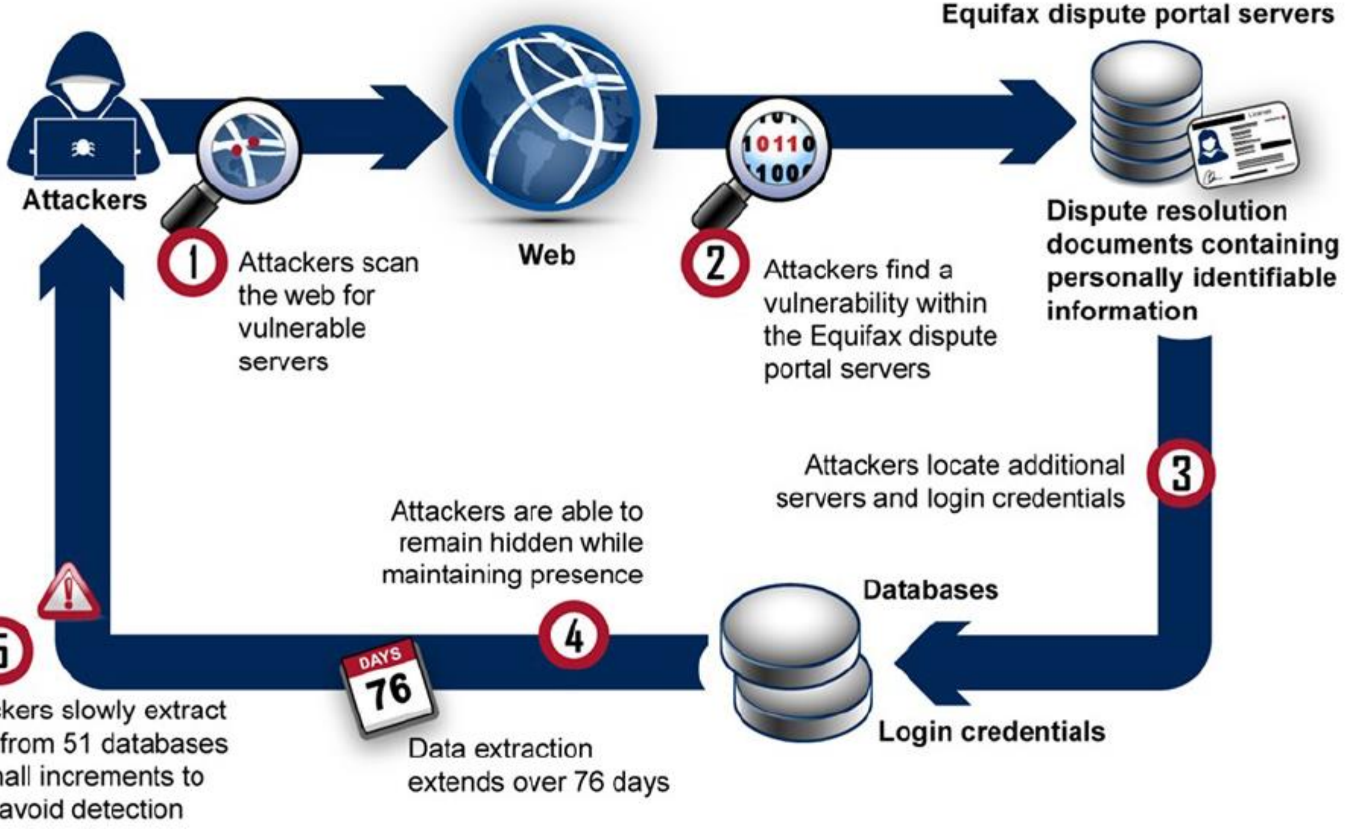
Equifax Data Breach Post Mortem

Bonus Problem: Apache Struts

- Many security experts contributed the breach to Equifax's decision to use Apache Struts
- The open source Apache Struts 2 project released an update that included a patch for a critical vulnerability that attackers could remotely exploit and take full control of the application
- Due to the vulnerability many information security experts repeated ongoing calls for organizations to stop using Apache Struts

Equifax Data Breach Post Mortem

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information


Equifax dispute portal servers
Attackers
Web
Dispute resolution documents containing personally identifiable information
Databases
Login credentials
DAYS
76

1 Attackers scan the web for vulnerable servers

2 Attackers find a vulnerability within the Equifax dispute portal servers

3 Attackers locate additional servers and login credentials

4 Attackers are able to remain hidden while maintaining presence

Data extraction extends over 76 days

5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

United States Government Accountability Office

Equifax Data Breach Post Mortem

Equifax Timeline: Breach and Response

- May 2016
  - Digital certificate for network scanning tool expired, leaving it unable to inspect encrypted traffic for signs of malicious activity
- March 8, 2017
  - US-CERT issues alert about Apache Struts 2, advising all organizations to install a patch
  - The vulnerability allow attacker to remotely execute commands and take control of the web application framework
  - Apache releases the patch on the same day
- March 10
  - An unidentified individuals scanned the company's systems
  - The unidentified individuals discovered the vulnerability on a server hosting the online dispute portal
  - The unidentified individuals subsequently gained unauthorized access to the portal and confirmed that they could run commands, but no data was stolen

Equifax Timeline: Breach and Response (cont.)

- May 13
  - Starting that day and lasting until July 30 - a nearly 80-day period - attackers queried 51 Equifax databases
  - Extracting records containing the PII of at least 145.5 million consumers in the U.S. and nearly 1 million consumers outside of the U.S.
  - The attacker extract the data in small increments to help avoid detection and encrypted their communications to disguise the activities
- July 29
  - A *new digital certificate* was obtained for a tool that scans encrypted network traffic for signs of malicious activity
  - The security team detects unusual activity and blocks it
- July 30
  - The security team detects further unusual activity and takes the Apache Struts portal offline

Equifax Timeline: Breach and Response (cont.)

- Aug. 2
  - Equifax hires cybersecurity firm Mandiant to investigate the breach and alerts the FBI
- Aug. 7
  - Equifax issues first public data breach notification
- Sept. 7
  - The company launches "www.equifaxsecurity2017.com" website to handle consumers' queries
  - The website was not hosted on the official equifax.com domain and people mistaken as a phishing site by some security firms
  - Equifax says it believes 143 million U.S. consumers' PII was stolen, including dispute documents for 209,000 consumers, which contained PII for approximately 182,000 consumers
  - PII for U.K. and Canadian consumers was also exposed
- Sept. 15
  - Equifax's CIO and CSO "retire."

Equifax Data Breach Post Mortem

Equifax Timeline: Breach and Response (cont.)

- Sept. 26
  - Richard Smith, Equifax's CEO, likewise "retires." Smith later appears on Capitol Hill to answer extensive questions from lawmakers about the breach.
- Sept. 28
  - Equifax interim CEO Paulino do Rego authors an op-ed in the Wall Street Journal apologizing for the breach and promising stronger consumer protection services
- Oct. 2
  - Equifax wraps up its initial investigation.
  - Investigators had found the attackers also accessed PII for 2.5 million more U.S. consumers, and revising U.S. breach victim count from 143 million to at least 145.5 million.
- Feb. 12, 2018
  - Equifax announces the hiring of a new CISO: Jamil Farshchi, who comes from Home Depot.

Equifax Data Breach Post Mortem

Equifax Timeline: Breach and Response (cont.)

- Feb. 12, 2018
  - Equifax announces the hiring of a new CISO: Jamil Farshchi, who comes from Home Depot.
- March 1
  - Equifax identifies about 2.4 million U.S. consumers whose names and partial driver's license information were stolen. It says some of these individuals were already included in the count of 145.5 million breach victims, but as of August 2018, it had yet to determine a final count.

ACS-2821-001 – Questions?