REVIEW AND ANALYSIS OF THE EQUIFAX DATA LEAK AND KEY TAKEAWAYS

An Overview of the Case:

Equifax announced that a data breach at the US credit bureau between May and July 2017 compromised the private information of 147.9 million Americans, as well as 15.2 million British citizens and approximately 19,000 Canadian citizens. As a result of this breach, the United States claimed in 2020 that four members of the Chinese People's Liberation Army were involved in the hacking. However, since then, there has been no additional evidence of China's involvement in the breach.

The data breach compromised sensitive data such as names, Social Security numbers, dates of birth, addresses, and credit card information. The breach began with system failures, such as weak security measures and the failure to perform critical updates, as outlined in Equifax's internal audit report, and was then carried out by infiltrating Equifax's internal network. The breach was discovered in July 2017 and publicly disclosed in September 2017. This led to a series of legal investigations and compensation claims against Equifax.

Background to the Incident:

Equifax identified major vulnerabilities in its internal audits in 2015. The company identified issues such as non-compliance with timelines, incomplete asset inventory, and lack of updates to critical systems. Many of the recommended fixes had not been completed at the time of the breach.

An important security patch for Apache Struts was released in March 2017, but Equifax did not update. Attackers exploited this vulnerability to access internal servers, compromise employee credentials, and scan databases. The attack, which continued for 76 days, was discovered on 29 July 2017 and closed on 30 July.

Breach analysis revealed other flaws in Equifax's systems, including a lack of network design, inadequate encryption of personal credentials, and a lack of effective breach detection mechanisms.

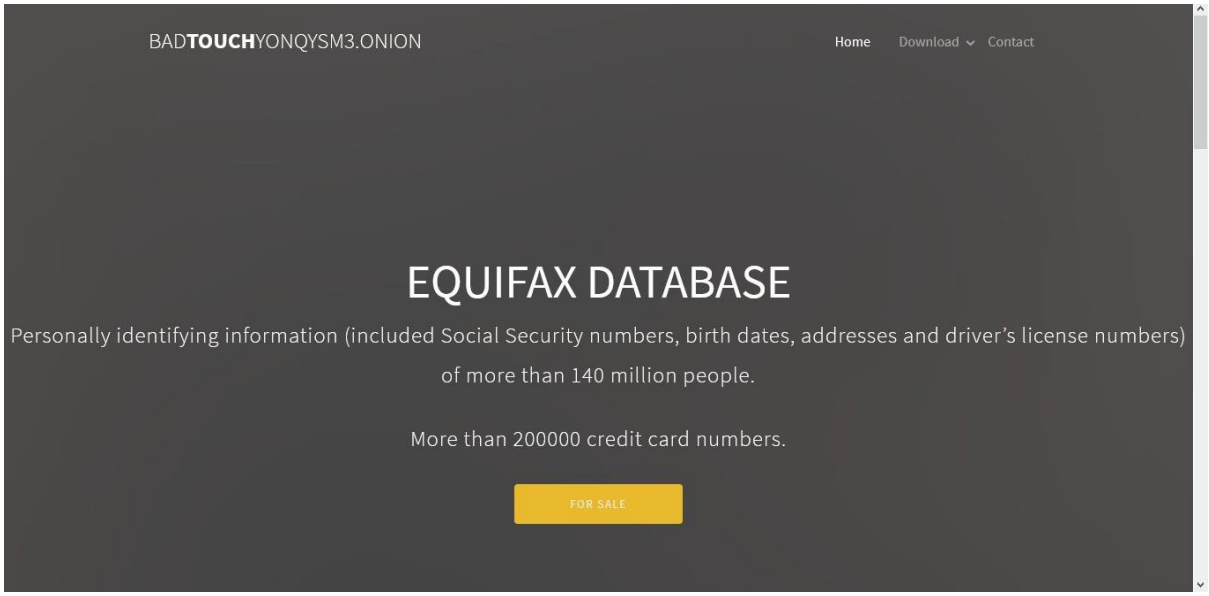
Attackers Exploring System:

Here is a chronological summary of the Equifax data breach:

1. **Breach Initiation (May 12, 2017):** The infiltration process began. Attackers gained access to Equifax's internal servers using a vulnerability in Apache Struts.
2. **Breach Process (May 12, 2017 - July 29, 2017**): Attackers gained unauthorised access to internal databases. They started stealing information pretending to be Equifax employees. This process continued for 76 days.
3. **Detection of the Breach (July 29, 2017):** Equifax's internal IT team updated the SSL certificate of an application used to monitor network traffic. The new SSL certificate enabled them to detect suspicious network activity and the breach was discovered.

Discovery and Status of Leaked Data:

Equifax announced the breach on 7 September 2017. Following the breach, Equifax dismissed its CIO and CSO and hired cybersecurity firm Mandiant to investigate the incident. During the investigations, it was claimed that the data was offered for sale on some dark web sites, but the data offered for sale could not be verified.



Equifax dataları sattığını iddia eden bir darkweb sitesi. (source: **Robert Hansen**)

There is no clear evidence that the leaked data has been put up for sale. Although security experts have speculated that this data could be sold on the black market or the dark web, there are no reports or evidence of the sale of this information. Therefore, there is no certainty about the ultimate use or fate of the leaked data.

Key Takeaways:

1. **Timely Updating and Patching Matters:** The Equifax incident highlights the critical importance of timely implementation of security patches and updates. The company did not take the necessary steps to close the vulnerabilities in a timely manner, thus providing an opportunity for attackers.
2. **Strengthening Security Teams:** The company announced that it strengthened its security teams by hiring 1000 full-time IT and security professionals following the incident. Equifax acted late to strengthen its team. In addition, investments in security teams should not be limited to increasing the number of personnel; it is also important to improve the capacity and capabilities of the teams.
3. **Fast and Effective Breach Responses:** Equifax was slow to act quickly after the breach was detected. In similar situations, organisations should be prepared and have the right protocols in place to ensure a quick and effective response.
4. **Transparency and Communication:** The company's disclosure of the breach and subsequent communication has been criticised for transparency and accuracy. When a breach occurs, it is vital for companies to communicate clear and accurate information in order to maintain trust.

5. **Comprehensive Internal Audits:** The Equifax incident shows that organisations should conduct comprehensive internal audits. Internal audits are an important tool for identifying and correcting vulnerabilities and should be conducted regularly.

Conclusion:

The Equifax data breach demonstrates the importance of organisational security measures and the serious consequences that a lack of these measures can have for companies. Companies need to continuously review and update their security policies to correct security weaknesses and manage them effectively in crisis situations.

REFERENCES

Wikipedia. (n.d.). 2017 Equifax data breach. Retrieved from [https://en.wikipedia.org/wiki/2017_Equifax_data_breach]

Weisman, R. (2024, Feb 8). Lessons from the Equifax Data Breach. LinkedIn. Retrieved from [https://www.linkedin.com/pulse/lessons-from-equifax-data-breach-digicert-inc--3sogc/?trk=public_post_main-feed-card_feed-article-content]

Liles, J. (2022, Jan. 31). Is the Equifax Data Breach Settlement Email Legit? Retrieved from [https://www.snopes.com/fact-check/equifax-data-breach-settlement-email/]

Fazzini, K. (2019, Feb 13). The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme. CNBC. Retrieved from [https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html]

Dellinger, A. (2017, Sep 8). Is Equifax Data On The Dark Web? Not Yet, But It Will Be. International Business Times. Retrieved from [https://www.ibtimes.com/equifax-data-dark-web-not-yet-it-will-be-2587884]

Bule, G. (2017, Sep 8). How Equifax, Fire Eye & The Darknet Threw Oil On The Breach Fire. Medium. Retrieved from [https://medium.com/secjuice/a-series-of-unfortunate-events-or-how-equifax-fire-eye-threw-oil-on-the-fire-c19285f866ed]

Flashpoint Intel Team. (2017, September 26). Everything You Need to Know About the Equifax Breach: Timeline, Overview, Impact. Flashpoint. Retrieved from [https://flashpoint.io/blog/everything-you-need-to-know-about-equifax-breach-timeline-overview-impact/]