In 2017, Equifax, a major credit reporting agency in the United States, encountered a gigantic data breach, ranking among the most substantial in history, affecting approximately 147 million people. Those who were affected by the breach had a number of valuable personally identifiable information leaked out into the internet, things such as Social Security numbers, birth dates, addresses, and even driver's license numbers. The incredibly widescale nature of the attack raised many questions about the state of data security at Equifax and in general. How did this happen? Who could have done this? Why didn't Equifax see this sooner? Why was personal information so vulnerable? This paper seeks to answer some of these questions and to look into the intricacies of the data breach, as well as the ramifications that followed after the attack. We'll start off with the group allegedly responsible for the breach and their motivations.

During the time of writing, June 4th, 2023, cybersecurity researchers believe that the hacker group known as "Advanced Persistent Threat 41", otherwise known as "APT 41", is responsible for the attack. The group is said to be, according to the Council on Foreign Relations, "backed by the Chinese government" and is known for successfully "targeting the health-care and high-tech sectors and conducting espionage against political dissidents" as well as conducting attacks for their own personal profit, meaning this attack was not their first. Right now, it is not completely certain what their motive was, but with what we know about them, it is likely they carried out this attack for the sake of stealing identities, financial fraud, and espionage against the United States. Due to the low profile the group keeps, it is unknown how APT 41 originated.

Before we can talk about when the attack started, we must mention a crucial moment that would eventually lead to the breach. According to CSOOnline, in March 2017, Apache Struts, an open-source Java enterprise application development framework used by Equifax, was found to have a vulnerability (Fruhlinger, 2020). This would not have been very problematic had Equifax effectively fixed the vulnerability using a patch given by the developers of the framework. However, Equifax IT was unable to successfully flag the issue, leaving the company open to attack.

The hacker group, for reasons unknown, waited two months before launching their attack on May 13, 2017. The criminals were able to steal information for around two months before they were noticed by Equifax admins. Just about a month later, the company let the public know about the breach. Shortly after this, many of Equifax's higher-ups, including the Chief Executive

Officer, Richard Smith, would step down while the company was hit by a barrage of lawsuits and investigations. It would take until 2019 until Equifax could reach a settlement with both the Federal Trade Commission and the Consumer Financial Protection Bureau. They have agreed to pay an astounding $700 million in consumer restitution and fines for their many errors and general negligence.

As mentioned before, an incredible amount of personally identifiable information was leaked and was the intended usage domain of the attack. The group started to sell this information through underground markets on the dark web, and valuable data fell into the hands of malicious actors. With this data, other cyber criminals were able to open fraudulent accounts, apply for loans in another person's name, and more effectively launch social engineering attacks using the credentials of trusted people, among other nefarious actions.

Currently, there have not been any reported active descendants of the Equifax data breach. That is, there have not been any other cyber attacks that were directly linked to the original. It is not impossible that such an attack has gone unnoticed or is happening as you are reading this, but it is fairly unlikely. What is more likely is that some of the data is still floating around on the dark web. The only way this information could be useful six years later is if the person to whom the data belongs failed to either update their security (think two-factor authentication and what-not) or change their passwords to something different and stronger than what they were previously using.

Being one of the biggest cyber-attacks to ever happen, the Equifax data breach has a number of characteristics that gave it such a status. A common theme was delays. Delays in correctly flagging the vulnerability in the framework, delays in noticing the breach, and delays in public disclosure. The sheer amount of time it took Equifax admins to realize they had been compromised is one of the key reasons the attack was as awful as it was. The attack can also be blamed on Equifax's choice to not renew a digital certificate for a long period of time, which meant that "encrypted traffic was not being inspected throughout that period" (Noche, 2018). These blunders made by Equifax are the reason why 147 million individuals had their information leaked.

Due to both the magnitude of the attack and the losses suffered by the company, cybersecurity specialists at Equifax made it their goal to find solutions to help mitigate the risk of having something as catastrophic as this ever happen again. They realized that the time they took

to spot the breach was unacceptable, so they improved their vulnerability management by conducting consistent vulnerability assessments and implementing other processes that help find suspicious activity faster. They also noticed that, once the hackers were able to get into their systems, it was far too easy to steal data. With this in mind, specialists started to utilize more effective encryption measures in the hopes that data will be far more secure than it was in 2017. Lastly, better and more clear policies along with proper training for employees were put into place so that the company can reduce the time it takes to tackle another attack in the future.

After the attack had been publicized, Equifax started to face an abundance of legal backlash and other consequences. We've already talked about how the Federal Trade Commission made Equifax pay millions of dollars in both fines and consumer restitutions, but the FTC also launched several investigations into the company. This would lead to harsher policies being imposed to ensure that data was more secure in the future. Along with the money paid due to lawsuits, Equifax lost a total of $1.4 billion, likely due to the reputational damage they incurred as a result of the attack. The company lost many business partnerships and customers began to look for alternate data providers. Equifax also changed its leadership once the CEO stepped down. This leadership would prioritize and enhance cybersecurity and data protection. They would also invest in infrastructure and technology that would improve the state of data security at the company.

Their attackers, however, faced fairly little punishment due to the fact that they were essentially working for the Chinese government. It would've been against China's best interests to give up the hacker group that has given them so much valuable information about citizens of the United States. The group is still wanted by the FBI to this day.

To conclude, the Equifax data breach serves as a good reminder of the calamitous consequences of cybersecurity failures in large-scale companies. The breach really put a spotlight on the need for increased cyber-security measures and employee protocols that help catch these types of attacks far faster. Heavier regulations were implemented by the government and other related regulatory groups that would ensure that mistakes like the ones made by Equifax would never be able to happen again. As a result of the investigations by Federal organizations after the breach, the confidentiality and security of data have never been better, and this is more than likely why a descendant attack has not yet occurred. While the attack was

extremely damaging to Equifax and its customers, it will always be an example of what can happen when an organization neglects to keep its security systems up to date.

References

Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2020, February 10). Equifax Says Cyberattack May Have Affected 143 Million in the U.S. *The New York Times*. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

Connect the Dots on State-Sponsored Cyber Incidents - APT 41. (n.d.). Council on Foreign Relations. https://www.cfr.org/cyber-operations/apt-41

Barrett, B. (2020, February 10). How 4 Chinese Hackers Allegedly Took Down Equifax. *WIRED*. https://www.wired.com/story/equifax-hack-china/#:~:text=The%20Apache%20Struts%20vulnerability%20had,how%20many%20records%20it%20contained

Nohe, P. (2020, August 26). *The Equifax Data Breach went undetected for 76 days because of an expired certificate*. Hashed Out by the SSL Store™. https://www.thesslstore.com/blog/the-equifax-data-breach-went-undetected-for-76-days-because-of-an-expired-certificate/

Chinese Hackers Charged in Equifax Breach. (2020, September 29). Federal Bureau of Investigation. https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020